2021

Fachhochschule Dortmund
University of Applied Sciences and Arts

PROJETARBEIT

Untersuchungen zur Netzwerksicherheit

Autor:
Ano Jean-Michel Ekra

Betreuer:
Prof. Dr.-Ing Niemeyer

Eine Projektarbeit, erstellt im Rahmen der Vorbereitung

zur Bachelor -These des Studienganges

Digitale Technologien (B.Sc.)

30 April. 2021

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

Das Computernetzwerk ist zu einem besonders wichtigen Element in der Informationstechnologie (IT) geworden. Aufgrund des großen Erfolgs des Internets und der damit verbundenen Kommunikationsprotokolle führen Unternehmen eine große Anzahl von IT-Prozessen über internetbasierte Netzwerke durch: Einige werden nur innerhalb des Standorts ausgeführt, andere können jedoch auch miteinander verbunden werden und sogar mit Kunden und Geschäftspartnern kommunizieren. Infolgedessen wird das Netzwerk zunehmend Teil der kritischen Infrastruktur. Ein Versagen oder Verlust der Vertraulichkeit, Integrität oder Authentizität der internen Kommunikation kann der entsprechenden Organisation großen Schaden zufügen.

Deshalb beschäftigen Netzwerkadministratoren unter anderem Fragen wie: ”Wie können unberechtigte Zugriffe von außen auf das Netzwerk verhindert werden?“ oder ”Ist die Kopplung der Netzwerke zwischen unseren Standorten wirklich sicher vor Angreifern, die Kommunikationsdaten abhören oder manipulieren wollen?“. Die Verwendung und Auswahl geeigneter Sicherheitsausrüstung hängt von vielen Faktoren ab, sodass sie vollständig beurteilt werden kann, um die Sicherheit des Computernetzwerks zu prüfen.
Die Sicherheit ist komplex und vielfältig. Neben der Bestimmung dem Zunehmen der der Nachfrage, dem Spezialisieren nach individuellem Schutz ist es daher wichtig, das notwendige Hintergrundwissen zu haben und von der Auswahl der Sicherheitsmechanismen zu profitieren. Mehrere Optionen zum Schutz der Netzwerksicherheit stellen Netzwerkadministratoren und Endbenutzer vor das Problem, die sinnvollste Kombination zu finden, um Sicherheitstechnologien, die für ihre jeweiligen Zwecke verwendet werden, möglichst effizient zu nutzen (1).
Auf der anderen Seite ist wichtig zu erwähnen, dass häufig Präventivmaßnahmen durch Produkte von Drittherstellern realisiert werden (Anti Viren-Programme, Desktopfirewalls, weitere Produkte zur Erhöhung der Netzwerksicherheit, etc.), um

Gefahren zu begegnen. Dabei stellt sich die Frage, wie die Entwicklung von Anwendungssoftware Einfluss auf die Sicherheit nehmen kann, damit ein gewisser Schutz auch ohne diese Produkte gewährleistet ist.

1.2 Ziel der Arbeit

Kernziel dieser Projektarbeit ist die Entwicklung einer Umgebung für diverse Sicherheitsuntersuchungen zu schaffen und diese Sicherheitsuntersuchungen durchzuführen: Aus der Kenntnis, der in einem Netzwerk vorkommenden Protokolle und Protokollabläufe sollen Angriffsszenarien und entsprechende Abwehrmechanismen entwickelt und demonstriert werden.
„Um das weite Feld einzugrenzen werde zunächst der Layer-2 in den Fokus der Betrachtung genommen werden, wobei auch Layer-übergreifende Protokolle mit Layer-2-Bezug in Betracht kommen –bspw. DHCP,ARP, das auf Layer-2 angegriffen werden kann, die Auswirkungen des Angriffs aber im Wesentlichen auf anderen Layer zum Tragen kommen(2)“. Parallel dazu wird ein Einblick in existierende, im Rahmen des Praktikums verwendete Netzwerktechnologien gegeben und die Thematik der Netzwerksimulation behandelt. Für die Demonstration von Angriff und Abwehr werden eigene Skripte und Tools entwickelt. Es ist nötig zu erwähnen, dass am häufigsten bereits fertige Tool für diese Demonstration verwenden werden. In dieser Arbeit fokussiere mich anschließend auf die Selbstentwicklung von Python Skript, um die anderweitig verfügbaren Tools zu vergleichen.

1.3 Abgrenzung

In einer komplexen digitalen Welt beobachten wir zunehmende Angriffsszenarien, im Laufe meiner Arbeit werde ich mich auf die Angriffsmöglichkeiten fokussieren, die von praktischer Relevanz sind und diese analysieren. Die digitale Vernetzung ermöglicht eine Vielzahl von Angriffsszenarien. Angriffsszenarien, die über dem Layer 2 Schicht (OSI-Modell) sind, werde nicht im Rahmen meiner Arbeit berücksichtigen. Es wird nur bestimmte Angriffe. Besondere Layer 2 Netzwerkangriffe bspw.-ARP Spoofing, DHCP Spoofing werden analysiert und Sicherheitskritisches Nutzer verhalten behandeln. Weiterhin werden spezielle

Cyberangriffe nicht behandelt, wie zum Beispiel: Brute Force Attacke, DDOS Formatstring-Angriffe oder Cross-Site Scripting.

2 Das Vorgehen

In diesem Kapitel sollen Grundlagen vermittelt werden, die für ein Verständnis des weiteren Vorgehens wichtig sind.
Dazu wird in Abschnitt 2.1 der Begriff „Netzwerksicherheit“ ganz deutlich definiert und ebenso die Frage: „Was ist Netzwerksicherheit?“.
Da in Kapitel 3 die Schwachstellen und Angriffsmöglichkeiten behandelt werden, ist es notwendig, dass zuvor im Abschnitt 2.1.2 die grundsätzlichen Funktionsweisen der Netzwerksicherheit erläutert werden. Dabei wird sich auf die Funktionsweisen beschränkt, die nötig sind, um die Angriffe und die im Kapitel 4 behandelten Gegenmaßnahmen und Argumentationen nachvollziehen zu können.
Zur Erweiterung der Nachvollziehbarkeit wird zusätzlich erklärt, wie man sich gegen bestimmte Angriffe auf Layer 2 z.B. ARP-Spoofing, DHCP-Spoofing Angriffe schützen kann. (Abschnitt 4.3)

2.1 Netzwerksicherheit

Zu dem Bereich Netzwerksicherheit gehört eine Vielzahl von Technologien, Geräten und Prozessen. Dafür gibt es eine einfache Erklärung: Netzwerksicherheit ist eine Reihe von Regeln und Konfigurationen zum Schutz der Integrität, Vertraulichkeit und Zugänglichkeit von Computernetzwerken und Daten. Diese Reihe von Maßnahmen werden von Software- und Hardwaretechnologien unterstützt.
Bei der Frage der Netzwerksicherheit spielt die Größe, die Branche oder die Infrastruktur des Unternehmens überhaupt keine Rolle. Es geht in erster Linie um die Sicherheit des Netzwerks, deshalb werden Netzwerk-Sicherheit Lösungen entwickelt. Unternehmen müssen sich gegen Cyberbedrohungen schützen, um Ihre Geschäftsmodelle, ihre sensiblen Daten oder ihr Wachstum von Angriffen von außen zu sichern.
In der heutigen digitalen Welt beobachten wir eine Komplexität der Netzwerkarchitektur. Diese Situation verändert die Bedrohungssituation und hilf den Angreifern Schwachstellen zu finden und effizient auszunutzen. Für Angreifer ist es

möglich in verschiedenen Bereichen Schwachstellen zu finden, wie z. B. Geräten, Daten, Anwendungen, Benutzern und Standorten. Deshalb nehmen die Verwendungsmöglichkeiten von Tools und Anwendungen für das Management der Netzwerksicherheit immer mehr an Bedeutung zu. Die Verwendung von Tools für die Sicherheitsanalyse bieten den Verbrauchern Schutz gegen einzelne Bedrohungen und Exploit, aber auch mit der Nichteinhaltung von Vorschriften befassen…. Das Thema Schutzmaßnahmen wird für ein Unternehmen unerlässlich und ausgiebig besprochen, sobald es zu nur wenigen Minuten Ausfallzeit kommt, da diese Ausfallzeit führt zu weitreichenden Störungen und massiven Rufschäden und Verlust führt(3).

2.2 Was ist Netzwerksicherheit?

Netzwerksicherheit bezeichnet das Gesamtkonzept der Planung, Ausführung und Überwachung der Sicherheit in Netzwerken zur elektronischen Datenverarbeitung. Es müssen nicht nur technische Sicherungsmaßnahmen bedacht werden, sondern auch organisatorische, betriebliche und juristische Optionen mitberücksichtigt werden. Einige der Maßnahmen können anhand der folgenden Fragen kategorisiert werden(4)*:*

- *Technisch: (Was wird eingesetzt?)*
- *Organisatorisch: (Wer darf was?)*
- *Betrieblich: (Wie wird Sicherheit im Betriebsablauf realisiert?)*
- *Rechtlich: (Was darf eingesetzt werden?)*

2.2.1 Wie funktioniert Netzwerksicherheit?

Das Thema Netzwerksicherheit in einem Unternehmen kann nur durch Zahlreiche unterschiedliche Ebene beachten werden. In jeder Schicht des Schichtenmodells für Netzwerksicherheit können mehrere Vulnerabilitäten gefunden werden. Durch die Nichtbetrachtung könnten Angriffe ermöglicht werden. Anwender müssen auf Ihre Hardware, Software und die Richtlinien für Netzwerksicherheit für jeden Bereich achten. In der Regel besteht die Netzwerksicherheit aus(3):

- Physische Netzwerksicherheit

- Technische Netzwerksicherheit
- Administrative Netzwerksicherheit

3 Schwachstellen und Angriffsmöglichkeit

3.1 Angriffsarten

Die Masse an verschiedenen Angriffsszenarios, kann in drei Kategorien unterteilt werden:

1. Netzwerkangriffe
2. Angriffe auf Anwenderebene
3. Softwareangriffe

Netzwerkangriffe zielen darauf ab, den Zugriff auf einen bestimmten Netzwerkdienst (E-Mail, Internetverbindung oder WLAN) zu stören. Eines der bekanntesten Angriffstechniken auf die Infrastruktur sind zum Beispiel Denial of Service (DOS) Attacken. Das Ziel eines DOS Angriffs kann beispielweise darin bestehen, einen Webserver in einer bestimmten Zeit lang zum Absturz zu bringen. Die Ursache ist meisten ein Verstoß auf Anwenderebene durch den Benutzer absichtlich oder unbewusst. Die unkontrollierbaren Aktionen auf Anwenderebene führen zu einem höhen Sicherheitsrisiko. Im Bezug auf Sicherheit trägt der „Faktor Mensch“ häufig durch die Wahl schwacher, d.h. leicht zu erratender Passwörter dazu bei, dass der Schutz unzureichend wird, solche Angriffe auf den „Faktor Mensch“ nennt man „*Sozial Engineering“*. Des Weiteren ist festzustellen, dass Angreifer in der Letzten Zeit ihre Taktiken massiven verändert haben. Sie profitieren von der Unaufmerksamkeit der Benutzer, um ihrer Zugangskennungen und Passwörter *(Website oder E-Mail)* zu knacken, solche Methoden werden als „*Password Fishing, kurz Pishing“* genannt. Menschliche Faktoren bringen häufig ein sehr hohes Sicherheitsrisiko für die gesamte Netzwerkinfrastruktur, weil Sicherheitsmaßnahmen oft nicht von den Mitarbeitern ernst genommen werden(5). Software ist eine wichtige digitale Komponente, da sie die Grundlage für einen Computer, das Internet und alle Kommunikationsinfrastrukturen ist. Softwareanwendungen werden in rasantem Tempo für Kommunikation, Bildung, Handel, Gesundheitswesen, Cloud und viele andere Bereiche entwickelt. Gleichzeitig kann Software in kürzester Zeit angegriffen

und für völlig andere oder bösartige Zwecke verwendet werden. Derartige Angriffe werden durch Sicherheitslücken in der Software ermöglicht, die auf einem Gerät ausgeführt wird. Eine Sicherheitslücke in einem Computer-programm ist ein Programmierfehler mit Konsequenzen für die Sicherheitsaspekte des Programms((Takamen et al. 2004 S.93) 6). Durch solche Lücken kann die mit dem Programm durchgeführte Kommunikation kompromittiert, sowie Daten ausgelesen, verändert oder vernichtet, aber auch das Gerät selbst außer Betrieb gesetzt werden, was zu enormen wirtschaftlichen Schäden führt.

Es gibt einen Unterschied zwischen den drei Angriffsszenarios und dieser Unterschied könnte besser durch das OSI veranschaulicht werden.

Abbildung 1.1.: Schichtenmodell um Schichten erweitert(7)

Das OSI-Referenzmodell ist am besten als idealisiertes Modell der logischen Verbindungen zu verstehen, die für die Netzwerkkommunikation erforderlich sind. Die meisten in der realen Welt verwendeten Protokollsuiten, wie TCP/IP, DECnet und Systems Network Architekturen (SNA), bilden das OSI-Referenzmodell nur grob ab. Das OSI-Modell ist ein guter Ausgangspunkt, um zu verstehen, wie die verschiedenen Protokolle innerhalb einer Protokollsuite funktionieren und

zusammenwirken. „Das Open System Interconnection-Modell“(OSI) ist ein Sieben-Schichten-Modell, das zur Visualisierung von Computernetzwerken verwendet wird. Das OSI-Modell gehört zur „International Organisation for Standards“ (ISO) und wird durch die Kennung ISO/IEC 7498-1 gepflegt(7).

Des Öfteren wird über die Benutzer-Schicht gesprochen, die befindet sich auf OSI Layer 8.Beim Thema Cybersicherheit stellt man fest, dass der Benutzer auf OSI Layer 8 eine wichtige Rolle spielt. Wie schon erwähnt, werden die meisten Angriffe auf Anwenderebene durchgeführt. Das OSI-Modell dient zum Verständnis, wie Computernetzwerke funktionieren und miteinander kommunizieren. Zusätzlich zeigt uns das OSI-Modell, wo potentielle Angriffspunkte liegen. Dafür ist es möglich das Modell in unterschiedliche Sicherheiten Ebenen aufzuteilen:

- 1-4 Schicht: Netzwerkangriffe
- 5-7 Schicht: Angriffe auf die Software
- 6-7 Schicht: Sicherheit auf Anwendungsebene
- 8 Schicht: Attacken auf Anwenderebene

Darüber hinaus wird die Sicherheit auf Anwendungsebene durch verschiedene Methoden beispielsweise: Verschlüsselungen, Datenverarbeitung, Darstellung garantiert. In dem Bereich, wo der Softwareentwicklung angewendet wird (S.11 (2)).

4 Angriffssimulation

4.1 Bedrohungsanalyse

Gefährliche Entwicklungen von Cyberangriffen und Netzwerkangriffen weltweit macht es notwendig, dass Cybersicherheit experten in der Richtung von mehr Prävention und der Modernisierung von Abwehr-Tools ihren Schwerpunkt setzen. Während dieser Entwicklung, ist es möglich auch festzustellen, dass in der Zukunft mehr in den Bereichen Bedrohungsanalyse investiert wird. *Genauso war es bereits bei den schnell wachsenden Märkten während der Einführung von Systemen_zur Intrusion Detection und Intrusion Prevention, Firewalls oder auch VPNs der Fall(8).*

In der Bedrohungsanalyse sind die potentiellen organisatorischen, technischen und benutzerbedingten Ursachen für Bedrohungen, die Schäden hervorrufen können, systematisch zu ermitteln. Die möglichst vollständige Erfassung der Bedrohungen eines Systems ist eine schwierige Aufgabe, die fundierte Kenntnisse über Sicherheitsprobleme und Schwachstellen existierender Systeme und deren Dienste erfordert.(S.184(6).

Allerdings wird am häufigsten über Hacker und Malware gesprochen. Obwohl es vielfältige Arten von Bedrohungen gibt. Im weiteren Verlauf werden diese Arten ganz konkret definiert.(10)

4.1.1 Natürliche Bedrohungen

Diese können am besten als Bedrohungen der Informationssicherheit betrachtet werden, die von Mutter Natur verursacht werden, hierzu gehören: Naturkatastrophen, Überschwemmungen, Erdbeben, Tornados, Temperaturextreme, Wirbelstürme und Stürme. Die allgemeinen Analyse Faktoren haben uns gezeigt, welche Einfluss diese Faktoren auf das Schutzziel: „Verfügbarkeit“ haben. Dabei ist es noch nicht notwendig, dass das Gebäude des Unternehmens gegen Natur Katastrophe zu schützen. Oft führt die Situation dazu, dass die Energie, Telekommunikation, und Wasserleitungen beschädigt werden. Außerdem könnte massive Gewalt zum Ausfall der Versorgungsinfrastrukturen führen.

Neben dem Staat, der ein Schutzinteresse gegenüber „Kritischen Infrastrukturen“ hat, haben auch Wirtschaftsbetriebe ein Schutzinteresse gegenüber „unternehmenskritischen Infrastrukturen“(10).

4.1.2 Interne oder Insider-Bedrohungen

Insider-Angriffe sind die teuerste Form der Verletzung der Informationssicherheit, da die Kosten pro Insidervorfall bei 250.000 £ liegen, wie ein aktueller Bericht von der INSA aufzeigt. Das liegt daran, dass der Insider-Zugang zu den Vermögenswerten seines Arbeitgebers hat. Dies kommt dadurch zustande, weil eine solche Person das Vertrauen der Organisation genießt, was dazu führt, dass er oder sie einen autorisierten Zugang hat, so dass es möglich ist, alle physischen und elektronischen

Sicherheitsmaßnahmen zu umgehen. Allerdings hat die Zahl der Vorfälle von Insider-Bedrohungen in einem erheblichem Maße zugenommen. In der Tat ergab eine aktuelle Studie des „Ponemon Institute „dass 88 % der IT-Experten glauben, dass das Risiko von Insider-Bedrohungen in den nächsten zwei Jahren gleichbleibt oder in den nächsten zwei Jahren steigen wird. Aber mehr als drei Viertel dieser Vorfälle werden normalerweise nicht gemeldet und intern gehandhabt und nur selten an die Strafverfolgungsbehörden weitergeleitet, sodass meist keine rechtlichen Schritte eingeleitet werden(8). Eine Insider-Bedrohung ist eine bösartige Aktivität gegen eine Organisation, die von Benutzern mit legitimem Zugriff auf das Netzwerk, die Anwendungen oder Datenbanken einer Organisation ausgeht.

Bei diesen Benutzern kann es sich um aktuelle oder ehemalige Mitarbeiter oder um Dritte wie Partner, Auftragnehmer oder Zeitarbeiter mit Zugriff auf die physischen oder digitalen Ressourcen des Unternehmens handeln. Obwohl der Begriff meist zur Beschreibung illegaler oder böswilliger Aktivitäten verwendet wird, kann er sich auch auf Benutzer beziehen, die dem Unternehmen unbeabsichtigt Schaden zufügen.(12) Es gibt mehrere Arten von Insider-Bedrohungen:

. **Malicious Insider:**

ein Mitarbeiter oder Auftragnehmer, der wissentlich versucht, Informationen zu stehlen oder den Betrieb zu stören. Dabei kann es sich um einen Opportunisten handeln, der nach Möglichkeiten sucht, Informationen zu stehlen, die er verkaufen kann oder die ihm bei seiner Karriere helfen können, oder um einen verärgerten Mitarbeiter, der nach Möglichkeiten sucht, einer Organisation zu schaden, seinen Arbeitgeber zu bestrafen oder zu blamieren. Ein Beispiel für einen böswilligen Insider sind die verschiedenen Apple-Ingenieure, die wegen Datendiebstahls angeklagt wurden, weil sie für ein in China ansässiges Unternehmen Geheimnisse über fahrerlose Autos gestohlen haben(13).

. **Negligent Insider:**

ein Mitarbeiter, der nicht die richtigen IT-Verfahren befolgt. Zum Beispiel jemand, der seinen Computer verlässt, ohne sich abzumelden, oder ein Administrator, der ein Standardpasswort nicht geändert oder es versäumt hat, einen Sicherheitspatch

anzuwenden(12). Ein Beispiel für einen fahrlässigen Insider ist der Datenanalyst, der ohne Autorisierung eine Festplatte mit persönlichen Daten von 26,5 Millionen US-Militärveteranen mit nach Hause nahm, die bei einem Hauseinbruch gestohlen wurde(14).

. Kompromisse Insider:

Ein häufiges Beispiel ist ein Mitarbeiter, dessen Computer mit Malware infiziert wurde. Dies geschieht in der Regel über Phishing-Betrügereien oder durch Anklicken von Links, die zu Malware-Downloads führen. Kompromittierte Insider-Rechner können als "Homebase" für Cyberkriminelle genutzt werden, von der aus sie Dateifreigaben scannen, Privilegien erweitern, andere Systeme infizieren und vieles mehr(12). Wie im Fall des jüngsten Twitter-Einbruchs, bei dem Angreifer eine Telefon-Speer-Phishing-Attacke nutzten, um Zugang zu den Anmeldedaten von Mitarbeitern und deren internem Netzwerk zu erhalten. Die Angreifer schafften es, Informationen über die Prozesse von Twitter zu erlangen und Mitarbeiter mit Zugang zu Kontosupport-Tools ins Visier zu nehmen, um hochkarätige Konten zu hacken und einen Kryptowährung-Betrug zu verbreiten, der 120.000 US-Dollar einbrachte(15).

4.1.3 Externe Bedrohungen

Externe Bedrohungen können von Personen oder Organisationen ausgehen, die außerhalb eines Unternehmens tätig sind. Sie haben keinen autorisierten Zugriff auf die Computersysteme oder das Netzwerk(16). Sie haben, die Möglichkeit sich den Zugang auf die interne Netzinfrastruktur eines Unternehmens zu verschaffen. Diese Cyberkriminellen können manchmal monatelang unbemerkt bleiben und Extrahieren Informationen. Die meisten werden nie gefunden oder erst später entdeckt. Besonders berisant ist dabei, dass diese Externe (Cyberkriminelle) sich überall befundenen können, auch im Pyjama in ihrem Bett, während ihre Zero-Day- oder Brute-Force-Passwort-Attacke ständig das System angreift und nach einem Weg hinein sucht; tausendmal pro Sekunde; immer und immer wieder, bis sie Zugang erhalten. Diese Hacker sind nicht nur brillante Programmierer, sondern sie verstehen auch, wie Menschen arbeiten, und sie werden einen Weg finden, das System zu hacken: Wenn man sich nicht genug Mühe gibt, um besser zu schützen(17).

Außerdem lassen sich externe Angreifer lassen sich in der Regel in folgende Kategorien einordnen (10):

- *Hacker*
- *Cracker*
- *Skript-Kiddies*
- *(Wirtschafts-) Spione und Saboteure*
- *Schadsoftware*

4.2 Ziel und Environment

Das Ziel der Simulation (MITM ARP Spoofing) auf OSI Layer 2 ist zu beweisen, dass Verwundbarkeit des ARP Protokolls besteht: Die Ergebnisse vergleichen und das Verhalten der einzelnen Knoten in beiden Fällen analysieren.

Abbildung 1.2: GNS3 Logo(17)

Das Betriebssystem, das wir zum Einrichten unserer Simulation verwendet haben, ist Ubuntu und das von uns verwendete Simulationswerkzeug ist GNS-3.
Auf GNS-3 werden 2 Betriebssysteme (Kali Linux und Windows 10) und Cisco IOS (Router und Switch) installiert. GNS3 ist eine Software, die eine Schnittstelle zu Emulationssoftware wie Dynamips, Virtual Box, QEMU bietet und die Emulation ermöglicht die Konfiguration von Netzwerksystemen mit verschiedenen Geräten (Cisco, Juniper, HP, Arista, Citrix, Blockade Router und Switchen-Geräte) und verschiedenen Betriebssystemen. Ein echtes Cisco IOS kann mit Dynamips ausgeführt werden.

Mit QEMU können das Juniper-Betriebssystem Junos, Cisco ASA und IDS / IPS-Systeme betrieben werden. Auf diese Weise ist es möglich, unterschiedliche physikalische Hardware mit GNS3 zu testen. Mit Virtualbox ist es möglich, dem virtuellen Netzwerksystem Rechner hinzuzufügen, die unterschiedliche Betriebssysteme emulieren. GNS3 kann auf verschiedenen Betriebssystemen installiert werden. Der größte Unterschied der GNS3-Software zur Cisco Packet Tracer-Software besteht darin, dass GNS3 ein Emulator ist und Cisco Packet Tracer ein Simulator(19). GNS3 simuliert die Merkmale und die Funktionalität eines Geräts, z. B. eines Switches. Sie führen keine tatsächlichen Betriebssysteme (wie z. B. Cisco IOS) aus, sondern ein von GNS3 entwickeltes simuliertes Gerät, wie z. B. den eingebauten Layer-2-Switch.

4.2.1 Was ist ein Man-in-The Middle-Angriff?

Heutzutage kann fast jeder Aspekt unseres Lebens mit der Nutzung des Internets oder von Mobilfunknetzen verbunden sein. Zum Beispiel nutzen wir Online-Homebanking, Online-Unterhaltung und -Einkauf, soziale Netzwerke und so weiter. Alle diese Online-Dienste speichern oder übertragen vertrauliche Informationen des Benutzers, die ein Hauptziel für Hacker darstellen. Neben Privatpersonen haben es Hacker auch auf Unternehmen und Organisationen abgesehen, was zu großen wirtschaftlichen Verlusten führt. In dieser neuen Welt, in der Menschen und Dinge durch das Internet immer miteinander verbunden sind, liest man täglich von erfolgreichen Angriffen auf vernetzte Dinge und Online-Dienste. Einer der erfolgreichsten Angriffe ist als Man-In-The-Middle (MITM) bekannt, der dazu führt, dass die Kontrolle über die übertragenen Daten der Endbenutzer erlangt wird.

Der Man-In-The-Middle-Angriff (MITM) ist einer der bekanntesten Angriffe im Bereich der Computersicherheit und stellt eine der größten Sorgen für Sicherheitsexperten dar. MITM zielt auf die eigentlichen Daten, die zwischen den Endpunkten fließen, sowie auf die Vertraulichkeit und Integrität der Daten selbst(20).

4.2.2 ARP Spoofing Scenario with Packet Inspection

ARP ist ein Protokoll, das innerhalb des LANs arbeitet, wenn ein Knoten eine IP-Adresse eines lokalen Ziels hat und die MAC-Adresse dieses Ziels wissen will. Wenn das Ziel außerhalb des LANs liegt, dann gibt es einen Zwischenknoten, der

als Standard-Gateway (Router) bezeichnet wird und die Daten außerhalb des LANs weiterleitet. In diesem Fall wird das ARP verwendet, um die IP-Adresse des Gateways auf seine zugehörige MAC-Adresse abzubilden. Die IP-Adresse des Gateways wird entweder statisch in den Knoten gespeichert oder dynamisch vom DHCP-Server abgeholt. Bei dem MITM-Angriff wird der Angreifer die ARP-Tabellen so, dass er entweder vorgibt, das Gateway oder das Zielgerät zu sein.
Zum Beispiel bei einer Kommunikation zwischen zwei Computern A und C mit den IPs 10.0.1.2 und 10.0.2.2, wie in **Abbildung 1.3** dargestellt. Computer A sendet ein Paket an Computer C, der sich außerhalb des LANs befindet, mit der Quell-IP von A und der Ziel-IP von C. Dann versucht Computer A herauszufinden, ob sich die Ziel-IP im selben Netzwerk oder außerhalb befindet. A wird feststellen, dass 10.0.2.2 außerhalb des Netzwerks liegt.
Daher sollte A das Paket an das Gateway weiterleiten, das Router 1 mit der IP-Adresse 10.0.1.1 ist. Das IP-Paket wird an die untere Schicht des OSI-Modells (Datenverbindungsschicht) gesendet. Die Quell-MAC-Adresse ist auf die MAC-Adresse von Computer A eingestellt, und die Ziel-MAC-Adresse ist diejenige, die zur Schnittstelle von Router 1 mit der IP-Adresse 10.0.1.1 passt. Wenn die ARP-Tabelle von A die MAC-Adresse der Schnittstelle 10.0.1.1 nicht enthält, dann sendet A ein ARP-Anforderungspaket, um die MAC-Adresse des Gateways herauszufinden. Der Angreifer empfängt die gesendete ARP-Anfrage und antwortet mit einem gefälschten ARP-Antwortpaket an den Rechner des Opfers (d. h. an Rechner A). Selbst wenn das Gateway eine legitime ARP-Antwort sendet, kann der Angreifer mehrere gefälschte ARP-Antwortpakete senden, um das legitime ARP-Antwortpaket des Gateways zu überschreiben. Im ARP-Protokoll überschreibt die neueste Antwort die älteste. Daher speichert der ARP-Cache auf dem Opfercomputer die gefälschte IP/MAC-Zuordnung.

Nun wird der gesamte Verkehr, der vom Rechner des Opfers zum Gateway geht, an den Rechner des Angreifers gesendet. Die ARP-Tabelle des Gateways könnte nur manipuliert werden, wenn alle Pakete (Opfer) außerhalb des LAN vom Angreifer empfangen werden. Das oben beschriebene Verfahren wird wiederholt, indem gefälschte ARP-Antwortpakete an das Gateway gesendet werden, um die Verbindung des Opfers zum Gateway aufrechtzuerhalten, so dass der Angriff

unentdeckbar ist, muss der Angreifer den Datenverkehr des Opfers an das Gateway weiterleiten und umgekehrt(21).

Abbildung 1.4 zeigt eine Netzwerktopologie mit einem Angreifer, einem Opferrechner, auf den ein MITM-Angriff angewendet wird, und einem Router, der die Rolle eines Gateways spielt. **Tabelle 1** zeigt den Inhalt der gefälschten ARP-Antwortpakete, die vom Angreifer gesendet werden sollen. Beide Pakete sollten einen geeigneten Opcode enthalten, der sie als ARP-Antwortpakete kennzeichnet. **Tabelle 2** zeigt die IP/MAC-Cache-Einträge des Rechners des Opfers und des Routers; vor und nach dem Angriff(21).

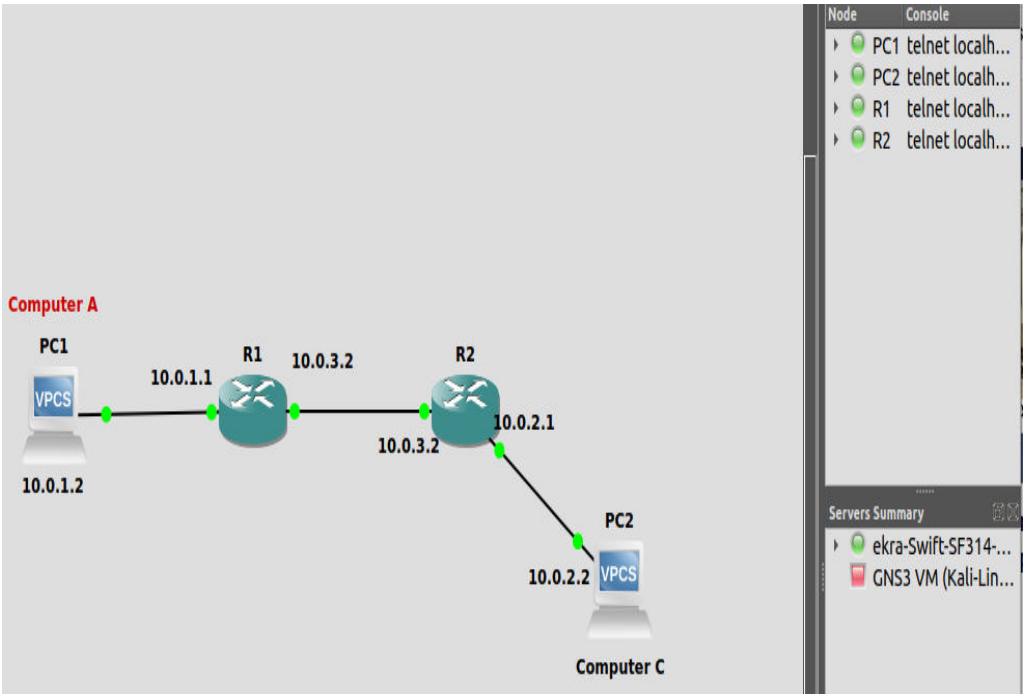

Abbildung 1.3: Beispiel für eine Netzwerktopologie

Tabelle 1: Erforderliche ARP-Nachrichtenfelder zum Senden

ARP-Nachrichtenfelder	Zum Opfer	Zu Router
Sender MAC Adresse	0c-cf-c6-c6-6a-39-00	0c-cf-c6-c2-f0-00
Sender IP-Adresse	192.168.1.1	192.168.1.5
Ziel MAC Adresse	0c-cf-c6-02-16-00	12-34-56-78-9A-BC

Ziel IP-Adresse	192.168.1.5	192.168.1.1

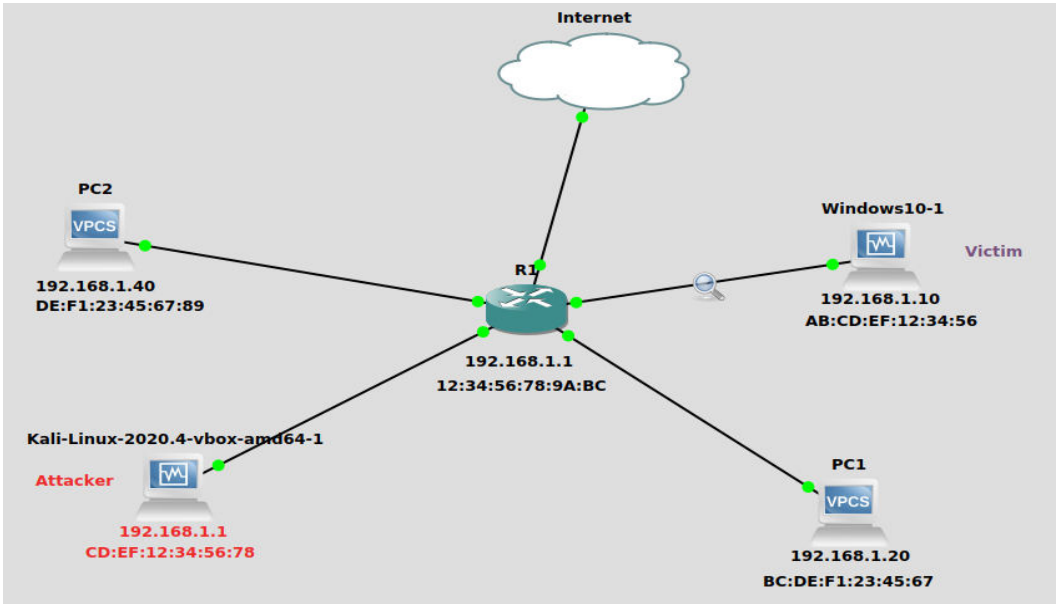

Abbildung 1.4: Beispiel Opfer und Angreifer im LAN

Tabelle 2: ARP-Cache-Einträge vor und nach einem ARP-Spoofing-Angriff.

	Die Maschine des Opfers		**Router**	
	IP	**MAC**	**IP**	**MAC**
Vorher	192.168.1.1	12:34:56:78:9A: BC	192.168.1.10	AB:CD: EF:12:34:56
Später	192.168.1.1	CD: EF:34:56:78	192.168.1.10	CD: EF:12:34:56:78

Anschließend wird der gesamte Datenverkehr vom Opfer zum LAN über den Computer des Angreifers geleitet. Angenommen, das Opfer hat eine Webseite auf dem HTTP-Server mit einer externen IP-Adresse (A.B.C.D) außerhalb des LAN. Das Betriebssystem, das auf dem Computer des Opfers ausgeführt wird, wählt den Router als nächsten Hop aus.

Um das Paket der Netzwerkschicht in einen Datenübertragungsrahmen einzukapseln, sollte das Opfer die MAC-Adresse des Routers kennen.
Es wird zuerst die ARP-Cash-Tabelle überprüfen. Die ARP-Tabelle hat die vergiftete Zuordnung der Router-IP zur MAC-Adresse des Angreifers, die das Ergebnis der ARP-gefälschten Antwortpakete ist. Daher wird dieses Paket an den Rechner des Angreifers statt an den echten HTTP-Server gesendet. Wenn der Angreifer die Pakete verwirft, führt dies zu einem DOS-Angriff, bei dem das Opfer am Surfen im Internet gehindert wird. Leitet der Angreifer den Datenverkehr hingegen an sein eigentliches Ziel weiter, wird der Angriff als MITM-Angriff eingestuft.
Einige Einstellungen sollten auf dem Computer des Angreifers vorgenommen werden, damit er Pakete weiterleiten kann, auch wenn die IP nicht dafür reserviert ist. Dies liegt daran, dass die Netzwerkschicht auf dem angreifenden Computer das Paket verwirft (wenn das Paket nicht für das Paket geeignet ist). Um dies zu ändern, muss eine Funktion namens Weiterleitung im Betriebssystem des angreifenden Computers implementiert sein. Diese Funktion muss aktiviert sein.
Wenn die Weiterleitungsfunktion auf dem Computer aktiviert ist, liest sie die Ziel-IP-Adresse im Datenpaket basierend auf der ARP-Tabelle des Computers (mit rechtlichen Informationen) und leitet sie zusammen mit der mit der IP-Adresse verknüpften MAC-Adresse an den Computer weiter. Die Weiterleitung von Datenpaketen ist in den meisten Betriebssystemen implementiert, einschließlich Microsoft Windows, Linux und Mac OS.
Allerdings ist die Paketweiterleitung standardmäßig deaktiviert. Sie kann jedoch leicht aktiviert werden, wie wir später sehen werden. Wenn die Paketweiterleitung aktiviert ist, funktionieren die Verbindungen des Opfers weiterhin ohne Unterbrechungen. Der Angreifer kann immer noch die Pakete inspizieren und alle gewünschten Informationen extrahieren(21).
Paket Inspektion Prozess: Nachdem der Datenverkehr erfolgreich auf den Computer des Angreifers gelockt wurde, muss der Angreifer ihn filtern und Informationen aus dem Datenpaket extrahieren. Da Millionen von Datenpaketen aus dem Netzwerk kommen oder gehen, ist es unmöglich, jedes einzelne Datenpaket manuell zu überprüfen, um die erforderlichen Informationen zu erhalten. Daher filtert der Angreifer die Pakete, um die interessierenden Pakete zu extrahieren.

Der bequemste Weg, Pakete zu filtern, besteht darin, festzustellen, welche Pakete für einen Angreifer wertvoll sind. Das erste, was mir in den Sinn kommt, sind Informationen, die vertrauliche Informationen wie Passwörter enthalten. Darüber hinaus kann der Angreifer an der vom Opfer besuchten Website interessiert sein. Jede dieser Verpackungsarten weist unterschiedliche Fingerabdrücke auf.
Bei der Paketinspektion wird jedes Paket aufgeschlüsselt und nach Protokollen von Interesse und Fingerabdrücken dieser Pakete gesucht, um die erforderlichen Informationen zu extrahieren.
Abbildung 1.5 zeigt als Beispiel den Datenpaket-Dump. Das Parsen der ersten 14 Bytes ergibt einen Bezug zur Schicht 2, die Informationen, die aus dieser Schicht extrahiert werden können, sind die MAC-Adressen der Quelle und des Ziels. MAC-Adressen sind 48 Bit oder 6 Bytes lang. Die ersten 6 Bytes repräsentieren die Zieladresse (c8:3a: 35:1f:1b:c8), während die zweiten 6 Bytes die Quelladresse darstellen (a4:17:31:0c:9a:65). Die Bytes Offset 14 bis 33 gehören zur Schicht 3, die IP-Adressen und das Netzwerkprotokoll enthält.
Tabelle 3: Zeigt einige dekodierte Teile des Datenpakets und die aus diesen Teilen extrahierten Informationen an. Aus der Tabelle ist klar ersichtlich, dass das Datenpaket eine Standard-IP-Abfrage ist, die vom Computer mit der IP-Adresse 192.168.1.115 an den DNS-Server mit dem Domänennamen www.fh-dortmund.de und der IP-Adresse gesendet wird von 193.25.16.29 (22).

4.3 Abwehr des MITM Angriff

Man-in-the-Middle-Angriffe haben sehr gefährliche Folgen für die Opfer. Sensible Daten können extrahiert werden, ohne das Opfer zu benachrichtigen. Es sollte ein Weg gefunden werden, mit diesem Angriff umzugehen. In der Welt der Cybersicherheit gibt es zwei Arten von Gegenmaßnahmen: Präventionssysteme und Erkennungssysteme. Das Präventionssystem versucht, das Auftreten eines Angriffs zu verhindern, und das Erkennungssystem löst eine Art Alarm aus, wenn ein Angriff erkannt wird. Um die besten Sicherheitsmaßnahmen zu erhalten, sollten sowohl Präventions- als auch Erkennungssysteme im Netzwerk implementiert werden.

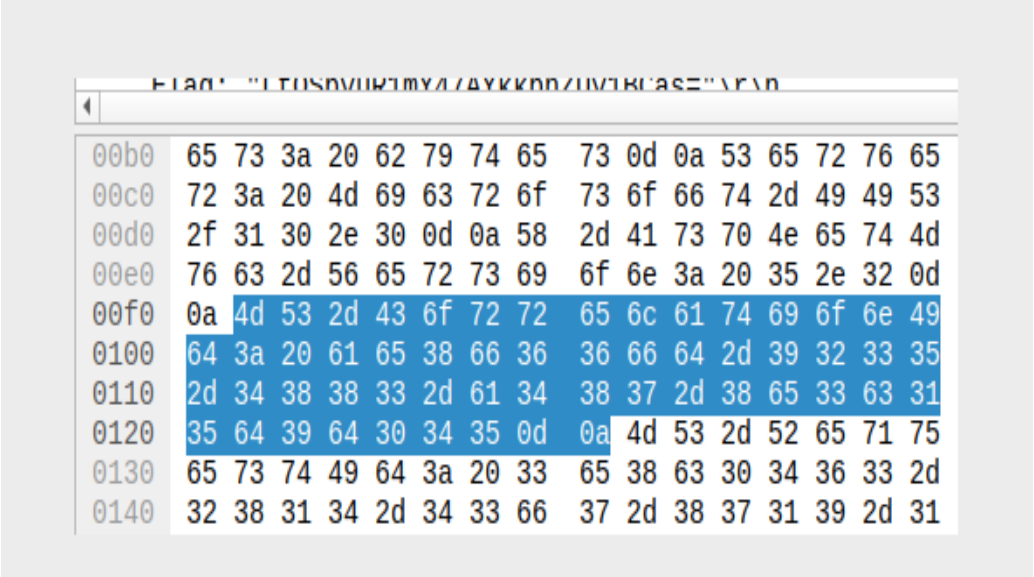

Abbildung 1.5: Ein Beispiel: Erfassung von Paket mit Wireshark

Tabelle 3: Abbildung 1.5 Inspektion des gezeigten Pakets in Hexadezimal.

Byte-Offset	Hex-Daten	Decodierte Daten	Deskription
23. Protokoll	11	17	UDP
26:30 Adresse	A0 A8 0B 75	192.168.1.115	Source IP
31 :33 Adresse	D0 43 DE	193.25.16.29	Destination IP
34 :35 Source Port	DF 81	57217	
36 :37 Port.	15 35	35	Destination
44.45 Parameter	02 20	15 25	DNS

4.3.1 Dynamic ARP inspection (DAI)

Diese Funktion verwendet, die von der DHCP-Snooping-Funktion erstellte, Tabelle, um alle ARP-Antworten zu überprüfen, die an den Switch-Ports eingehen. Unerlaubte ARPs sind ein wesentlicher Bestandteil aller Man-in-the-Middle-Angriffe, die ARP-Cache-Poisoning verwenden. Was DAI tut, ist einfach alle ARP-Antworten zu verwerfen, die keine entsprechenden Einträge in der DHCP-Snooping-Bindungsdatenbank haben. ARP-Antwortpakete, bei denen die MAC-Adresse im Hauptteil des Pakets nicht mit der MAC-Adresse im Ethernet-Header übereinstimmt, werden ebenfalls verworfen. In Nicht-DHCP-Umgebungen kann DAI gegen eine statisch definierte ARP-ACL arbeiten. Ports, die mehrere MAC-Adressen haben, z. B. Uplink zu physischen oder virtuellen Switches, sollten als "vertrauenswürdig" konfiguriert werden, dies umgeht alle DAI-Funktionen(23).

Konfiguration:

Switch(config)# ip arp inspection vlan 1	*Turn on arp inspection for vlan 1*
Switch(config)# int g0/8 *Switch(config-if)# ip arp inspection trust*	*trust int g0/8 to have multiple arp entries - for instance, uplinks to physical or virtual switches, clusters, load balancers in some cases.*

Abbildung 1.6: Ein Beispiel: DAI Switch Konfiguration befehle

4.4 IDS/IPS Intrusion Detection /Intrusion Prevention System

Das Hauptziel von IDS besteht darin, die Integrität, Verfügbarkeit und / oder Vertraulichkeit des Systems sicherzustellen, indem Aktivitäten in Computern und Netzwerken identifiziert, überwacht und analysiert werden und erforderlichenfalls Gegenmaßnahmen gegen illegale Aktivitäten ergriffen werden. IDS sollte Eingriffe von außen und innen in die zu schützenden Ressourcen erkennen. Aus funktionaler Sicht kann IDS mit Nachrichtendiensten verglichen werden. Die Aufgabe der Nachrichtendienste besteht darin, potenzielle interne und externe

Gefahren durch Analyse der gesammelten Informationen zu identifizieren und rechtzeitig Gegenmaßnahmen zu ergreifen, um die Integrität des Systems sicherzustellen.
Ein IDS erfüllt auch einige Nebenziele. Dazu gehört die Sicherung von Beweismaterial über erfolgte Angriffe für juristische Maßnahmen gegen den Angreifer. Weiter können die Erkenntnisse, welche durch Analyse der gesammelten Information gewonnen wurden, bei der Verbesserung des Systems gegen solche Angriffe einfließen(24).
Zusätzlich zu den Funktionen von IDS bietet das Intrusion Prävention System (IPS) folgende Funktionen: IPS kann automatisch auf erkannte Angriffe reagieren. Hierzu wird bei einem
erkannten Angriff zum Beispiel der Datenstrom gekappt oder die Firewall-Regeln werden entsprechend beeinflusst, um einen Abbruch der Verbindung vorzunehmen. Des Weiteren kann das IPS unfragmentierte Datenstreams, TCP-Fehler oder ungewollten Transport von Daten aufdecken und bereinigen. Bekannte Open Source-Implementierungen sind Snort oder Lokkit. Die Verwendung und Überwachung mit IDS oder IPS sollte von Experten durchgeführt werden(4).

“If you know the enemy and know yourself, you need not fear the result of a hundred battles”-Sun Tzu(25)

5 Vergleichbare Tools

5.1 Snort

Kurz gesagt, Snort ist ein Paket-Sniffer/Paket-Logger/Netzwerk-IDS. Snort war ursprünglich als Packet Sniffer gedacht. Im November 1998 schrieb Marty Roesch einen reinen Linux-Packet-Sniffer namens APE geschrieben. Trotz der großartigen Funktionen von APE wollte Roesch jedoch einen Sniffer, der auch die folgenden Aufgaben erfüllt:

- Funktioniert auf mehreren Betriebssystemen
- verwendet einen Hexdump-Payload-Dump (tcpdump hatte später diese Funktionalität.)

- zeigt alle verschiedenen Netzwerkpakete auf die gleiche Weise an (tcpdump hatte diese Funktion nicht)

Roeschs Ziel war es, einen besseren Sniffer für seinen eigenen Gebrauch zu schreiben. Er schrieb Snort als eine Libcap-Anwendung, was Snort Portabilität in Bezug auf Netzwerkfilterung und Sniffing Sichtweise verleiht. Zu dieser Zeit wurde nur tcpdump ebenfalls mit Libcap kompiliert, so dass dies dem Systemadministrator einen weiteren Sniffer, mit dem er arbeiten konnte, zur Verfügung stellte. Snort wurde bei Packet Storm *(www.packetstormsecurity.com)* am 22. Dezember 1998 entwickelt. Zu diesem Zeitpunkt enthielt Snort nur etwa 1.600 Zeilen Code Das war etwa einen Monat nach der ersten Vorstellung von Snort, und Snort wurde zu diesem Zeitpunkt nur für Packet Sniffer verwendet. Roeschs erste Anwendungen von Snort waren die Überwachung seiner Kabelmodemverbindung und das Debuggen von Netzwerkanwendungen, die er programmierte(26).
Snort füllt eine wichtige "ökologische Nische" im Bereich der Netzwerksicherheit: ein plattformübergreifendes, leichtgewichtiges Tool zur Erkennung von Eindringlingen in das Netzwerk, das zur Überwachung kleiner TCP/IP-Netzwerke eingesetzt werden kann und eine Vielzahl von verdächtigem Netzwerkverkehr sowie offener Angriffe erkennt. Es kann Administratoren mit genügend Daten versorgen, um fundierte Entscheidungen über die richtige Vorgehensweise bei verdächtigen Aktivitäten zu treffen. Snort kann auch schnell eingesetzt werden, um potenzielle Lücken in der Sicherheitsabdeckung eines Netzwerks zu schließen, z. B. wenn ein neuer Angriff auftaucht und kommerzielle Sicherheitsanbieter nur langsam neue Signaturen zur Angriffserkennung veröffentlichen. Snort ist ein Werkzeug für kleine, wenig ausgelastete Netzwerke. Snort ist nützlich, wenn es nicht kosteneffizient ist, kommerzielle NIDS-Sensoren einzusetzen. Moderne kommerzielle Intrusion-Detektion-Systeme kosten allgemeine sehr viel Geld.

Zum Schluss steht Snort der GNU (27) zur Verfügung und kann in jeder Umgebung frei verwendet werden, sodass der Einsatz von Snort als Netzwerksicherheitssystem eher eine Frage des Netzwerkmanagements und der Koordination als eine der Erschwinglichkeit ist(28)

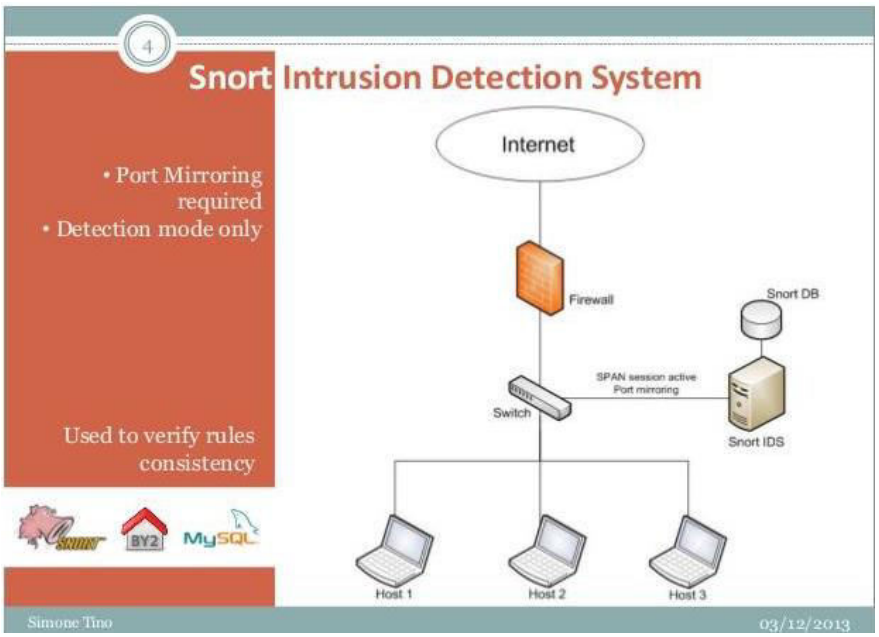

Abbildung 1.7: Snort IDS (Intrusion Detection System (29))

5.1.1 Wireshark

Wireshark ist einer der beliebtesten als Open Source erhältlichen grafischen Sniffer und lässt dank der weitgehenden Aufarbeitung der empfangenen Daten die schnelle Analyse vieler Protokolle zu. Aber das grafische Benutzerinterface muss nicht zwangsläufig zum Einsatz kommen. Auf Computern ohne grafische Bedienmöglichkeit lässt sich das zusammen mit Wireshark entwickelte Programm *Tshark* verwenden, um fast alle Möglichkeiten auch in der Konsole zu nutzen.
Wireshark kann unter *http://www.wireshark.org* für fast alle modernen Betriebssysteme heruntergeladen werden. Weiterhin ist Wireshark ein Netzwerk-Paketanalysator. Ein Netzwerk-Paketanalysator versucht, Netzwerkpakete zu erfassen und versucht, diese Paketdaten so detailliert wie möglich darzustellen. Sie können sich einen Netzwerk-Paketanalysator als ein Messgerät vorstellen, das verwendet wird, um zu untersuchen, was in einem Netzwerkkabel vor sich geht, so wie ein Voltmeter von einem Elektriker verwendet wird, um zu untersuchen, was in einem elektrischen Kabel vor sich geht (aber natürlich auf einer höheren Ebene). In der Vergangenheit waren solche Tools sehr teuer. Doch mit dem Aufkommen von Wireshark hat sich das alles geändert. Wireshark ist vielleicht einer der besten Open-Source-Paketanalysatoren, die heute verfügbar sind(30)

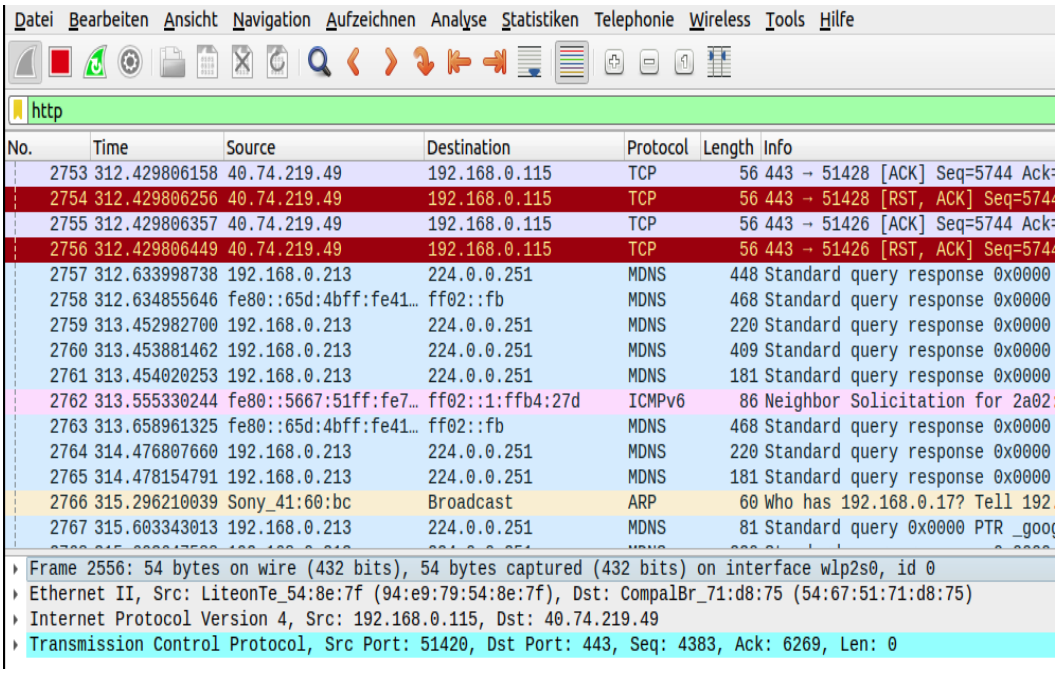

Abbildung 1.8: Wireshark Paket Analyse

6 Entwicklung Tools (Python Skript)

6.1 Sicherheit Tools zur Erkennung von ARP-Spoof Angriffe

In diesem Abschnitt werde ich ein selbstentwickelt Python Skript erstellen. Diese soll, als Schutzmaßnahme gegen ARP-Spoofing dienen. Durch dieser Python Skript werde ich die Möglichkeit haben ARP-Spoofing Angriffe frühzeitig zu erkennen.
Jetzt beobachten wir gemeinsam wie das ARP-Spoofer-Programm funktioniert. Wir werden feststellen, dass ich eine Funktion zum Senden von ARP-Antworten erstellt habe. Diese Funktion zeigt uns, dass die ARP-Tabelle des Opferrechners vergiftet wurde.
Zusätzlich habe ich einige Änderungen an dieser Funktion vorgenommen und sie so bearbeiten, dass das Programm erkennen kann, wenn die Pakete einen Layer mit gefälschtem ARP haben. Dazu habe ich den folgenden Code entwickelt:

```
 2  import scapy.all as scapy
 3  def mac(ipadd):
 4      arp_request = scapy.ARP(pdst=ipadd)
 5      br = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
 6      arp_req_br = br / arp_request
 7      list_1 = scapy.srp(arp_req_br, timeout=5, verbose=False)[0]
 8      return list_1[0][1].hwsrc
 9  def sniff(interface):
10      scapy.sniff(iface=interface, store=False, prn=process_sniffed_packet)
11
12 def process_sniffed_packet(packet):
13      if packet.haslayer(scapy.ARP) and packet[scapy.ARP].op == 2:
14          originalmac = mac(packet[scapy.ARP].psrc)
15          responsemac = packet[scapy.ARP].hwsrc
16
17   if originalmac != responsemac:
18
19      print("[*] ALERT!! You are under attack, the ARP table is being poisoned.!")
20
21 sniff("eth0")
```

Hier finden wir die Funktion zum Abrufen der MAC-Adresse :

```
def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose=False)[0]
    return answered_list[0][1].hwsrc
```

Funktion, um das gesniffte Paket zu verarbeiten und die Werte der alten MAC in der Variable "originalmac" und den Wert der MAC in der Antwort als Variable "responsemac" zu erhalten.

```
def process_sniffed_packet(packet):
    if packet.haslayer(scapy.ARP) and packet[scapy.ARP].op == 2:
        originalmac = mac(packet[scapy.ARP].psrc)
        responsemac = packet[scapy.ARP].hwsrc
```

Nun werden wir beide Werte vergleichen, um zu prüfen, ob sie ähnlich sind oder nicht, wenn nicht, dann ist es offensichtlich, dass die Werte gefälscht wurden.

```
if originalmac != responsemac:
        print("[*] ALERT!! Sie werden angegriffen, die ARP-Tabelle wird vergiftet.!")
sniff("eth0")
```

Fazit

Nach dem allgemeinen Eindruck hat die Aufmerksamkeit für Netzwerk Sicherheitsprobleme bei Computersystemen in den letzten Jahren zugenommen, was aber auch mit der drastisch angestiegenen Zahl der Vorfälle zusammenhängt. Meine Untersuchung basiert auf begrenzter Layer-Ebene.

Deshalb wurden in Kapitel 4 einige wichtige praxisrelevante Angriffsmöglichkeiten vorgestellt und ihre Funktionsfähigkeit durch praktische Beispiele bewiesen. Es konnte festgestellt werden, dass die Sicherheit auf Anwendungsebene von fehlender Konfiguration, Präventionssystemen und Erkennungssystemen negativ beeinflusst werden kann. Die in Kapitel 3 gewonnenen Kenntnisse wurde in Kapitel 4 und 5 genutzt, um praktische und theoretische Vorschläge für Prävention Maßnahmen zu entwickeln. Dabei könnte unter anderem festgestellt werden, dass der Programmiersprache Python eine wichtige Rolle in der Netzwerkssicherheit spielt.

Python gibt an Netzwerkadministrator die Möglichkeit Ihre Netzwerkinfrastruktur zu sichern und Sicherheitsmaßnahmen zu erstellen.

Nach dem Begriff logische Sicherheit, gibt es allgemein keine 100-prozent-Sicherheit-Garantie. Daher werden uns mit dem Thema Netzwerksicherheit lange Zeit beschäftigt.

Darüber hinaus sollte in Zukunft die Zusammenarbeit zwischen IT-Sicherheit Experte und Unternehmen intensivieren. Der Einsatz von Automatisierten Sicherheit Tools oder Betriebssystem (Nmap, Kali Linux…) werde langfristig die Arbeit von Netzwerkadministrator oder IT Expert deutlich verbessert.

Anschließen ist es festzustellen, dass das OSI-Modell Verwundbar ist. Deshalb müssen wir die Untersuchung auf weitere Schicht führen.

7 A. Glossar

7.1 Begriffe

Hacker

Ein Computerhacker ist ein Computerexperte, der sein technisches Wissen einsetzt, um ein Ziel zu erreichen oder ein Hindernis zu überwinden, und zwar innerhalb eines computergestützten Systems mit nicht standardisierten Mitteln.

Cracker

Cracker haben einen mit Hackern vergleichbaren technischen Hintergrund und entsprechende Systemkenntnisse, nutzen diese – in der Regel gegen Bezahlung – zur Informationsgewinnung oder Sabotage zugunsten Dritter(31). Die Auftraggeber sind Marktbegleiter des Angegriffenen und/oder Wissensträger mit besonderer Bedeutung; Aufgrund zunehmender Intensität, Dauer und Zielgenauigkeit der Angriffe wird durch das Bundesamt für Verfassungsschutz zunehmend ein nachrichtendienstlicher Hintergrund bzw. eine nachrichtendienstliche Unterstützung bei Ausspähung und Sabotage vermutet(32).

(Wirtschafts-) Spione und Saboteure

Industriespionageaktivitäten werden vom Staat kontrolliert und von Geheimdiensten unterstützt. Ziel ist es, Unternehmen oder wissenschaftliche Forschungseinrichtungen zu erforschen und ihr Know-how illegal zu erlangen.
Es gibt eine klare Unterscheidung zwischen Industrie- oder Wettbewerbsspionage, die nicht vom Staat kontrolliert wird. Die Digitalisierung eröffnet viele Möglichkeiten für die digitale Spionage von Informationen.

Schadsoftware

Malware oder "Malware" ist der allgemeine Begriff für jedes schädliche Programm oder jeden schädlichen Code, der das System beschädigt. Böswillige, absichtlich böswillige, anstößige Malware versucht, Computer, Computersysteme, Netzwerke, Tablets und mobile Geräte zu infiltrieren, zu beschädigen oder zu deaktivieren. Dies

bedeutet normalerweise, einen Teil der Kontrolle über den Geräteprozess zu übernehmen. Wie die menschliche Grippe beeinträchtigt sie die normalen Funktionen. Bei Malware geht es darum, illegal Geld mit Ihnen zu verdienen. Obwohl Malware die physische Hardware des Systems oder der Netzwerkgeräte nicht beschädigt (mit einer bekannten Ausnahme - siehe Abschnitt Google Android unten), kann sie Ihre Daten stehlen, verschlüsseln oder löschen, die Hauptfunktionen Ihres Computers ändern oder übernehmen, ohne Ihr Wissen oder Wissen über Ihre Spionageerlaubnis(33).

Skript Kiddies

Skript Kiddies ist ein Begriff, der verwendet wird, um typische junge Menschen zu beschreiben, die vorgefertigte Programme oder Software verwenden, um in andere Computer oder Computersysteme einzudringen oder diese zu manipulieren, ohne Computer oder das Internet zu kennen.

Zero-Day- Oder Brute-Force-Password-Attack

Brute-Force-Angriff ist eine Hacking-Methode, bei der mithilfe von Versuch und Irrtum Kennwörter, Anmeldedaten und Verschlüsselungsschlüssel geknackt werden. Dies ist eine einfache und zuverlässige Strategie, um unbefugten Zugriff auf persönliche Konten und Systeme und Netzwerke von Organisationen zu erhalten. Hacker versuchen normalerweise, mehrere Benutzernamen und Passwörter zu verwenden, um verschiedene Kombinationen mithilfe von Computern zu testen, bis sie die richtigen Anmeldeinformationen gefunden haben. Der Name "Brute Force" kommt von der Tatsache, dass der Angreifer übermäßig versucht hat, Zugriff auf das Benutzerkonto zu erhalten. Obwohl dies eine alte Netzwerkangriffsmethode ist, haben sich Brute-Force-Angriffe bewährt und sind immer noch eine beliebte Strategie bei Hackern(34).

Denial of Service (DoS) Angriff

DoS-Angriffe (Denial of Service) können die Funktionalität des Dienstes beeinträchtigen und Nutzern sowie Unternehmen stehen nur eingeschränkt zur

Verfügung. Solche Ausfälle ermöglichen Cyberkriminelle Angriff zu starten: Cyberkriminelle bombardieren beispielsweise einen Dienst oder eine Homepage mit deutlich mehr Anfragen, als das System verarbeiten kann und legen so das Zielobjekt, zumindest für eine bestimmte Zeit, lahm.

Ponemon Institute

Ponemon Institute ist eine Private Forschung Organisation, die unabhängig Forschung in Bereichen Netzwerksicherheit, Datenschutz und Informationssicherheit Strategie durchführt.

DHCP-Snooping

DHCP-Snooping ist eine in das Betriebssystem eines fähigen Netzwerk-Switches integrierte Layer-2-Sicherheitstechnologie, die DHCP-Verkehr, der als inakzeptabel eingestuft wird, unterbindet. Durch DHCP-Snooping wird verhindert, dass nicht autorisierte (rogue) DHCP-Server IP-Adressen an DHCP-Clients anbieten. Die DHCP-Snooping-Funktion führt die folgenden Aktivitäten aus: Validiert DHCP-Nachrichten aus nicht vertrauenswürdigen Quellen und filtert ungültige Nachrichten heraus. Aufbau und Pflege der Binding-Datenbank für DHCP-Snooping, die Informationen über nicht vertrauenswürdige Hosts mit geleasten IP-Adressen enthält. Verwendet die DHCP-Snooping-Binding-Datenbank, um nachfolgende Anfragen von nicht vertrauenswürdigen Hosts zu überprüfen(35).

ARP-Cache-Poisoning

ARP-Cache-Poisoning ist ein typischer Angriff auf Netzwerkebene (Layer 3) zum Einleiten einer sog. Man-In-The-Middle Attacke. Hierbei wird das ARP-Protokoll (Adresse Resolution Protocol) von einem potenziellen Angreifer missbraucht, um einen abzuhörenden PC im Netzwerk mitzuteilen, dass sich die MAC-Adresse des zugeordneten Default-Gateways geändert hat. Danach kann der Angreifer alle Daten (z.B. Passwörter, E-Mails) zwischen dem angegriffenen Computer und dem Gateway mitlesen. Dieser Angriff wird ausschließlich in Netzwerken verwendet, welche über so genannte Switches betrieben werden(36).

Opcode

Opcode ist eine Zahl. Opcode gibt die Anzahl der Maschinenanweisungen für einen bestimmten Prozessortyp an.

Hop (Netzwerktechnologie)

Hop nennt man in Rechnernetzen den Weg von einem Netzsegment bzw. Subnetz zum nächsten. Allgemein wird der Begriff Hop auch Synonym für die Zwischenstation selbst, also den Router bzw. das Gateway verwendet[1]. Der Sender (z.B. ein Computer oder Router) definiert hier den s.g. "next hops" als das Gerät welches den Zugang in das nächste Netzwerksegment/Subnetz gewährt.

Dynamips

Dynamips ist eine Software, um Cisco-Hardware auf einem herkömmlichen PC zu emulieren. Wichtig ist hierbei, dass Dynamips nicht den kompletten Router emuliert, sondern nur die Hardware (analog zu VMware für herkömmliche PCs). Das bedeutet, dass passendes IOS benötigt wird, um Dynamips nutzen zu können.

ARP

Das Address Resolution Protocol (ARP) ermöglicht die Zuordnung von physikalischen Adressen zu IP-Adressen. Dies ist notwendig, da das verwendete Netzwerkmedium nicht mit IP-Adressen arbeitet, sondern in der Regel eigene Adressformate benutzt.

8 B. Quellcode

```
1  import scapy.all as scapy
2  import time
3
4  # arpspoofer
5  def mac(ipadd):
6      arp_request = scapy.ARP(pdst=ipadd)
7      br = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
```

```
    arp_req_br = br / arp_request
    list_1 = scapy.srp(arp_req_br, timeout=5, verbose=False)[0]
    return list_1[0][1].hwsrc
def spoof(targ, spoof):
    packet = scapy.ARP(op=2, pdst=targ, hwdst=mac(targ),
                       psrc=spoof)
    scapy.send(packet, verbose=False)
def reset(dest_ip, src_ip):
    dest_mac = mac(dest_ip)
    source_mac = mac(src_ip)
    packet = scapy.ARP(op=2, pdst=dest_ip, hwdst=dest_mac, psrc=src_ip,
hwsrc=source_mac)
    scapy.send(packet, verbose=False)

target_ip = input("[*] Geben Sie Ihre Ziel-IP ein > ")  # Geben Sie Ihre Ziel-IP ein
gateway_ip = input("[*] Geben Sie Ihre Ziel-IP ein> ")  # Geben Sie Ihre Ziel-IP ein

try:
    countpackets = 0
    while True:
        spoof(target_ip, gateway_ip)
        spoof(gateway_ip, target_ip)
        countpackets = countpackets + 2
        print("\r[*] Packets Sent " + str(countpackets), end="")
        time.sleep(2)  # Nur Zwei Seconden Warten
except KeyboardInterrupt:
    print("\nCtrl + C pressed..... Quitting. ")
    reset(gateway_ip, target_ip)
    reset(target_ip, gateway_ip)
    print("[*] Arp Spoof Gestoppt, IP wiederhergestellt. ")

    def mac(ipadd):
        arp_request = scapy.ARP(pdst=ipadd)
```

```
41        br = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
42        arp_req_br = br / arp_request
43        list_1 = scapy.srp(arp_req_br, timeout=5, verbose=False)[0]
44        return list_1[0][1].hwsrc
45
46 # arpspoof-detector.py
47    def sniff(interface):
48        scapy.sniff(iface=interface, store=False, prn=process_sniffed_packet)
49    def process_sniffed_packet(packet):
50        if packet.haslayer(scapy.ARP) and packet[scapy.ARP].op == 2:
51            originalmac = mac(packet[scapy.ARP].psrc)
52            responsemac = packet[scapy.ARP].hwsrc
53
54            if originalmac != responsemac:
55                print("[*] ALARM!! Sie werden angegriffen, die ARP -
56                Tabelle wird vergiftet.!")
57    sniff("wlan0")
```

Abkürzungsverzeichnis

IPS	Intrusion Prävention System
IDS.	Intrusion Detection System
INSA	The Intelligence and National Security Alliance
GNS3	Graphical Network Simulator-3
GNU	General Public License
QEMU	Quick Emulator
ISO	International Organization for Standards
ARP	Address Resolution Protocol
DDOS	Distributed Denial of Service

Literaturverzeichnis

1. Wendzel S. IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung Springer Vieweg; 2018 [13.04.2020]. Verfügbar unter: https://www.springer.com/de/book/9783658226022

2. ProjektorientiertesArbeiten_Ekra (2).pdf.

3. What is Network Security? Force Point. 2018 [28.03.2021]. Verfügbar unter: https://www.forcepoint.com/de/cyber-edu/network-security

4. Netzwerksicherheit-Prof-Norbert-Pohlmann.pdf [13.04.2020]. Verfügbar unter: https://norbert-pohlmann.com/app/uploads/2015/12/Netzwerksicherheit-Prof-Norbert-Pohlmann.pdf

5. Bless R, Mink S, Blaß E-O, Conrad M, Hof H-J, Kutzner K, u. a. Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen [Internet]. Berlin Heidelberg: Springer-Verlag; 2005 [16.04.2021]. (X. Systems. Press). Verfügbar unter: https://www.springer.com/de/book/9783540278962

6. Takanen et al. - 2004 - Agents of responsibility in software vulnerability.pdf [17.04.2021]. Verfügbar unter: https://link.springer.com/content/pdf/10.1007/s10676-004-1266-3.pdf

7. Prüfer et al. - André Harms Cyberwar Sicherheit auf Anwendungsebe.pdf [1.04.2021] verfügbar unter: https://reposit.haw-hamburg.de/bitstream/20.500.12738/5417/1/Cyberwar_Sicherheit_auf_Anwendungsebene.pdf

8. Threat Intelligente: Bedrohungsanalysen verstehen und richtig einsetzen [Internet]. ComputerWeekly.de. [zitiert 22. März 2021]. Verfügbar unter: https://www.computerweekly.com/de/tipp/Threat-Intelligence-Bedrohungsanalysen-verstehen-und-richtig-einsetzen

9. Eckert C. IT-Sicherheit: Konzepte, Verfahren, Protokolle. 10. Auflage.

München: De Gruyter Oldenburg; 2018. 1004 S. (De Gruyter Studium).

10. Nagenborg B. Bedrohung der Informationssicherheit: Ein Überblick über Gefahrenquellen, Angriffspunkte und Sicherungsmaßnahmen. diplom.de; 2009. 41 S.

11. Elmrabit N, Yang S-H, Yang L. Insider threats in information security categories and approaches. In 2015.

12. What is an Insider Threat? Definition, Detection & Prevention Exabeam. [23.04.2021]. Verfügbar unter: https://www.exabeam.com/ueba/insider-threats/

13. What Is an Insider Threat | Malicious Insider Attack Examples | Imperva Learning Center. [26.04.2021] verfügbar unter: https://www.imperva.com/learn/application-security/insider-threats/

14. ResearchGate Link [Internet]. [zitiert 23. März 2021]. Verfügbar unter: https://www.researchgate.net/publication/283503171_Insider_threats_in_information_security_categories_and_approaches

15. Kienzle J. Was sind Insider-Bedrohungen? [Internet]. Log Point. 2020 [zitiert 26. April 2021]. Verfügbar unter: https://www.logpoint.com/de/blog/insider-threat/

16. ScienceDirect Full Text PDF [24.04.2021]. Verfügbar unter: https://www.sciencedirect.com/science/article/pii/S1877050914006528/pdf?md5=e2c1a62a477f1251106e844735049415&pid=1-s2.0-S1877050914006528-main.pdf&isDTMRedir=Y

17. External vs. Internal Cybersecurity Risks: Know the Difference Cybersecurity and Training. [24.04.2021]. Verfügbar unter: https://ermprotect.com/blog/external-vs-internal-cybersecurity-risks-know-difference/

18. File:GNS3 logo.png - Wikimedia Commons [3.04.2021]. Verfügbar unter: https://commons.wikimedia.org/wiki/File:GNS3_logo.png

19. What is GNS3 [Internet]. Cisco Pods. 2020 [zitiert 3. April 2021]. Verfügbar unter: https://www.ciscopods.com/what-is-gns3/

20. Conti M, Dragoni N, Lesyk V. A Survey of Man In The Middle Attacks. IEEE Communications Surveys Tutorials. third quarter 2016;18(3):2027–51.

21. Al Sukkar et al. - 2016 - Address Resolution Protocol (ARP) Spoofing Attack.pdf [9.04.2021] Verfügbar unter: http://41.89.240.73/bitstream/handle/123456789/856/Address%20Resolution%20Protocol%20%28ARP%29%20Spoofing%20Attack%20and%20Proposed%20Defense.pdf?sequence=1&isAllowed=y

22. Al Sukkar G, Saifan R, Khwaldeh S, Maqableh M, Jafar I. Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defense.2016 [9.04. 2021];08(03):118–30.verfügbar unter: http://www.scirp.org/journal/doi.aspx?DOI=10.4236/cn.2016.83012

23. Layer 2 Network Protections against Man in the Middle Attacks [Internet]. SANS Internet Storm Center. [26.04.2021]. Verfügbar unter: https://isc.sans.edu/forums/diary/7567/

24. Alexander M. Netzwerke und Netzwerksicherheit: das Lehrbuch. 1. Aufl. Heidelberg: Hüthig; 2006. 480 S.

25. Sunzi und Giles - 2008 - Sun Tzu's The art of war.pdf [Internet]. [zitiert 4. April 2021]. Verfügbar unter: https://sgp1.digitaloceanspaces.com/proletarian-library/books/203ea0ae84b21fab951c5a55c5e0749d.pdf

26. Snort IDS and IPS Toolkit.pdf [31.04.2021]. Verfügbar unter: http://index-of.es/Networking/Snort%20IDS%20and%20IPS%20Toolkit.pdf

27. https://www.gnu.org/licenses/gpl-3.0.txt [3.04.2021] verfügbar unter: https://www.gnu.org/licenses/gpl-3.0.txt

28. Roesch M. Snort – Lightweight Intrusion Detection for Networks. 1999;11.

29. Son D. dalton: Suricata & Snort IDS rule and pcap testing system Penetration Testing. 2018 [3.04.2021]. Verfügbar unter: https://securityonline.info/dalton-suricata-snort-ids-rule/

30. Lamping et al. - Wireshark Users Guide - v1.11.4-rc1-54-g9496733 f.pdf

[[zitiert 3.04.2021]. Verfügbar unter: http://download2.upload.de/software/41563/14/user-guide-a4.pdf

31. Information Security Risk Management [Internet]. springerprofessional.de. [25.04.2021]. Verfügbar unter: https://www.springerprofessional.de/information-security-risk-management/4334760

32. 2007 Verfassungsschutzbericht [25.04.2021]. Verfügbar unter: https://bibliothek.hsbund.de/Recherche/Einfache-Suche?&top=y&id=9094004

33. Was ist Schadsoftware? Malwarebytes. [10.04.2021]. Verfügbar unter: https://de.malwarebytes.com/malware/

34. What is a Brute Force Attack? Fortinet. [10.04.2021]. Verfügbar unter: /resources/cyberglossary/brute-force-attack

35. Was ist DHCP-Snooping und wie funktioniert es? Blog. 2021 [18.04.2021]. Verfügbar unter: https://community.fs.com/de/blog/what-is-dhcp-snooping-and-how-it-works.html

36. ARP Cache Poisoning – SecuPedia [13.04.2021]. Verfügbar unter: https://www.secupedia.info/wiki/ARP_Cache_Poisoning

Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe Selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Ort, Datum: _____

Unterschrift: _____