HE Übungen 1

Juventus Technikerschule HF

Diese Übung ist Teil der Vorlesung Hacking Exposed an der Juventus Technikerschule HF in Zürich.

1 Warm-Up

Aussage	Wahr	Falsch
IT-Security ist kein Zustand der erreicht werden kann, sondern ist als Prozess zu verstehen, an dem man kontinuierlich arbeitet.		
Ein Apache2 Webserver hört auf der IP/Port Kombination 127.0.0.1/80,443. Es kann ohne weiteres eine weitere Apache2 Instanz gestartet werden, die auf der IP/Port Kombination 127.0.0.2/80,443 hört.		
Ein modernes Unternehmensnetzwerk ist wie eine mittelalterliche Burg in mehrere Sicherheitszonen unterteilt.		
Ein NAT-Router ist eine Firewall.		
Ein Reverse Web Proxy, auch WAF genannt, soll primär eigene Server Infrastruktur schützen.		
Eine Server-Applikation kann auf mehreren Ports und IP-Adressen lauschen.		
Die Firewall Aktionen Block, Deny und Reject machen dasselbe, sind einfach andere Bezeichnungen.		
Ein TCP 3-Way Handshake besteht aus den Teilen SYN, SYN/ACK, ACK		
Wenn Nmap nur SYN-Pakete zum scannen verschickt spricht man von einem TCP Connect scan.		
Nmap unterstützt verschiedene Scan-Methoden um herauszufinden, ob ein Port offen ist.		

2 Perimeter Security

1. Auf welcher Schicht des OSI-Referenzmodells arbeitet eine Netzwerk Firewall hauptsächlich und was ist ihre Aufgabe?

2. Beschreiben Sie die Funktion einer DMZ und was sich darin befindet.

3. Nennen Sie Gründe, die für einen Reverse Web Proxy sprechen.

3 Iptables

Sie haben folgendes Iptables Regelset:

```
# iptables -L -n
Chain INPUT (policy DROP)
target     prot opt source               destination
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  0.0.0.0/0            5.6.7.8/0           tcp dpt:25
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:587
DROP       tcp  --  1.2.3.4/0            0.0.0.0/0           tcp dpt:143

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  1.3.5.7/0            8.8.8.8/0
```

1. Vervollständigen Sie das tabellarische Regelset anhand des Iptables-Regelset.

Interface	INPUT / OUTPUT / FORWARD	Source	Destination	Port	Action
	INPUPT	Any	Any	80	
eth0		Any	Any		ALLOW
eth0	INPUT				
eth0	INPUT	Any		587	ACCEPT
eth0	INPUT	1.2.3.4	Any		
		Any	Any	Any	DROP
eth0	OUTPUT			Any	
eth0		Any	Any	Any	ACCEPT

4 Nmap

Nmap unterstützt verschiedene Ausgabedarstellungen (OUTPUT). Verschaffen Sie sich einen Überblick und beschreiben Sie die Eigenschaften und mögliche Verwendungszwecke.

Tipp: Verwenden Sie die Manual Page ($ man nmap).

`-oN`	
`-oX`	
`-oS`	
`-oG`	

4.1 Nmap Scan-Analyse

Gegeben ist folgende Nmap Scan Ausgabe:

```
$ nmap scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-04 13:00 CEST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 17.88 seconds
```

1. Wie viele Ports sind offen? _____
2. Wie viele Ports sind geschlossen? _____
3. Wie viele Ports wurden gescannt? _____
4. Wie viele IPv4 Adressen wurden gescannt? _____
5. Wie viele IPv6 Adressen wurden gescannt? _____

4.2 Wireshark Scan Analyse

Gegeben ist folgende vollständige Wireshark Ausgabe (siehe auch Übung-Wireshark-Scan-Analyse.pcapng):

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.218	37.120.160.86	TCP	74	54484 → 80 [SYN] Seq=0 W
2	0.000012	192.168.100.218	37.120.160.86	TCP	74	52754 → 443 [SYN] Seq=0
3	0.024782	37.120.160.86	192.168.100.218	TCP	74	80 → 54484 [SYN, ACK] Se
4	0.000025	192.168.100.218	37.120.160.86	TCP	66	54484 → 80 [ACK] Seq=1 A
5	0.000008	37.120.160.86	192.168.100.218	TCP	74	443 → 52754 [SYN, ACK] S
6	0.000004	192.168.100.218	37.120.160.86	TCP	66	52754 → 443 [ACK] Seq=1
7	0.000050	192.168.100.218	37.120.160.86	TCP	66	54484 → 80 [RST, ACK] Se
8	0.000016	192.168.100.218	37.120.160.86	TCP	66	52754 → 443 [RST, ACK] S
9	0.001537	192.168.100.218	37.120.160.86	TCP	74	52756 → 443 [SYN] Seq=0
10	0.000022	192.168.100.218	37.120.160.86	TCP	74	37618 → 25 [SYN] Seq=0 W
11	0.000008	192.168.100.218	37.120.160.86	TCP	74	45634 → 22 [SYN] Seq=0 W
12	0.000008	192.168.100.218	37.120.160.86	TCP	74	54494 → 80 [SYN] Seq=0 W
13	0.000007	192.168.100.218	37.120.160.86	TCP	74	35672 → 53 [SYN] Seq=0 W
14	0.024026	37.120.160.86	192.168.100.218	TCP	74	53 → 35672 [SYN, ACK] Se
15	0.000102	192.168.100.218	37.120.160.86	TCP	66	35672 → 53 [ACK] Seq=1 A
16	0.000043	37.120.160.86	192.168.100.218	TCP	74	443 → 52756 [SYN, ACK] S
17	0.000032	192.168.100.218	37.120.160.86	TCP	66	52756 → 443 [ACK] Seq=1
18	0.000022	192.168.100.218	37.120.160.86	TCP	66	35672 → 53 [RST, ACK] Se
19	0.000063	192.168.100.218	37.120.160.86	TCP	66	52756 → 443 [RST, ACK] S
20	0.000058	37.120.160.86	192.168.100.218	TCP	74	80 → 54494 [SYN, ACK] Se
21	0.000053	192.168.100.218	37.120.160.86	TCP	66	54494 → 80 [ACK] Seq=1 A
22	0.000066	192.168.100.218	37.120.160.86	TCP	66	54494 → 80 [RST, ACK] Se
23	1.075843	192.168.100.218	37.120.160.86	TCP	74	45640 → 22 [SYN] Seq=0 W
24	0.000080	192.168.100.218	37.120.160.86	TCP	74	37628 → 25 [SYN] Seq=0 W

1. Welche IP Adresse wurde gescannt? _____

2. Welche Ports wurden gescannt? _____
3. Welche Ports sind offen? _____
4. Welche Ports sind geschlossen? _____
5. Welche Ports sind gefiltert? _____
6. Vermuten Sie, dass eine Firewall im Einsatz ist? Begründen Sie:

7. Wie lautet der mögliche Nmap Befehl um diese Ausgabe zu erhalten?

4.3 Nmap Scan-Methode Analyse

Gegeben ist folgende vollständige Wireshark Ausgabe (siehe auch Übung-Nmap-Scan-Methode-Analyse.pcapng):

No.	Time	Source	Destination	Protocol	Length	Info
9	0.231157	192.168.100.218	37.120.160.86	TCP	58	61114 → 80 [SYN] Seq=0 Win=1024 Len
10	0.000066	192.168.100.218	37.120.160.86	TCP	58	61114 → 10 [SYN] Seq=0 Win=1024 Len
11	0.000017	192.168.100.218	37.120.160.86	TCP	58	61114 → 160 [SYN] Seq=0 Win=1024 Le
12	0.000017	192.168.100.218	37.120.160.86	TCP	58	61114 → 40 [SYN] Seq=0 Win=1024 Len
13	0.000014	192.168.100.218	37.120.160.86	TCP	58	61114 → 20 [SYN] Seq=0 Win=1024 Len
14	0.024131	37.120.160.86	192.168.100.218	TCP	58	80 → 61114 [SYN, ACK] Seq=0 Ack=1 W
15	0.000053	192.168.100.218	37.120.160.86	TCP	54	61114 → 80 [RST] Seq=1 Win=0 Len=0
16	1.101958	192.168.100.218	37.120.160.86	TCP	58	61115 → 20 [SYN] Seq=0 Win=1024 Len
17	0.000021	192.168.100.218	37.120.160.86	TCP	58	61115 → 40 [SYN] Seq=0 Win=1024 Len
18	0.000005	192.168.100.218	37.120.160.86	TCP	58	61115 → 160 [SYN] Seq=0 Win=1024 Le
19	0.000003	192.168.100.218	37.120.160.86	TCP	58	61115 → 10 [SYN] Seq=0 Win=1024 Len

1. Wurde in diesem Scan ein TCP SYN scan oder ein TCP connect scan ausgeführt? Begründen Sie.