HE Übungen 2

Juventus Technikerschule HF

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

1 Warm-Up

Aussage	Wahr	Falsch
Jemand überflutet einen Server mit so vielen Anfragen, dass dieser die Last nicht tragen kann und zusammenbricht. Das bedeutet, dass das Schutzziel *Verfügbarkeit* angegriffen wurde.		
Sie machen Ihrer Freundin Alice den Gefallen und transportieren ihren USB-Stick mit Daten für Bob zu diesem. Können Sie das Schutzziel Vertraulichkeit verletzen?		
Host Discovery bezeichnet eine Technik um Herauszufinden ob ein Zielsystem online ist.		
Host Discovery verwendet dieselben Scan-Techniken unabhängig, ob ein Host lokal im Netzwerk oder sich im Internet befinden.		
Nmap macht standardmässig immer einen Port Scan eines Zielsystems auch wenn dieses laut Host Discovery nicht online ist.		
Machine-in-the-Middle und Man-in-the-Middle bezeichnen dasselbe.		
ARP ist ein Protokoll zum Auflösen von DNS-Namen in IP-Adressen.		
MAC-Adressen sind fix in der Hardware hinterlegt und können nicht permanent verändert werden.		
DNSSEC ist kein umfassender Schutz vor DNS-Spoofing-Attacken		

2 Nmap Host Discovery

1. Ist folgender Host online und erreichbar oder nicht? Begründen Sie.

```
1 0.000000000  192.168.105.118  193.99.144.85    ICMP   42 Echo (ping) request  id=0x89fa, seq=0/0, ttl=50
2 0.000026088  192.168.105.118  193.99.144.85    TCP    58 54859 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3 0.000035102  192.168.105.118  193.99.144.85    TCP    54 54859 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4 0.000041955  192.168.105.118  193.99.144.85    ICMP   54 Timestamp request    id=0x752f, seq=0/0, ttl=51
5 0.019827398  193.99.144.85    192.168.105.118  ICMP   42 Echo (ping) reply    id=0x89fa, seq=0/0, ttl=235
6 0.019852886  193.99.144.85    192.168.105.118  TCP    58 443 → 54859 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=
7 0.019868697  192.168.105.118  193.99.144.85    TCP    54 54859 → 443 [RST] Seq=1 Win=0 Len=0
8 0.019898497  193.99.144.85    192.168.105.118  ICMP   70 Destination unreachable (Network administrative
9 0.019903720  193.99.144.85    192.168.105.118  TCP    54 80 → 54859 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

3 ARP-Spoofing

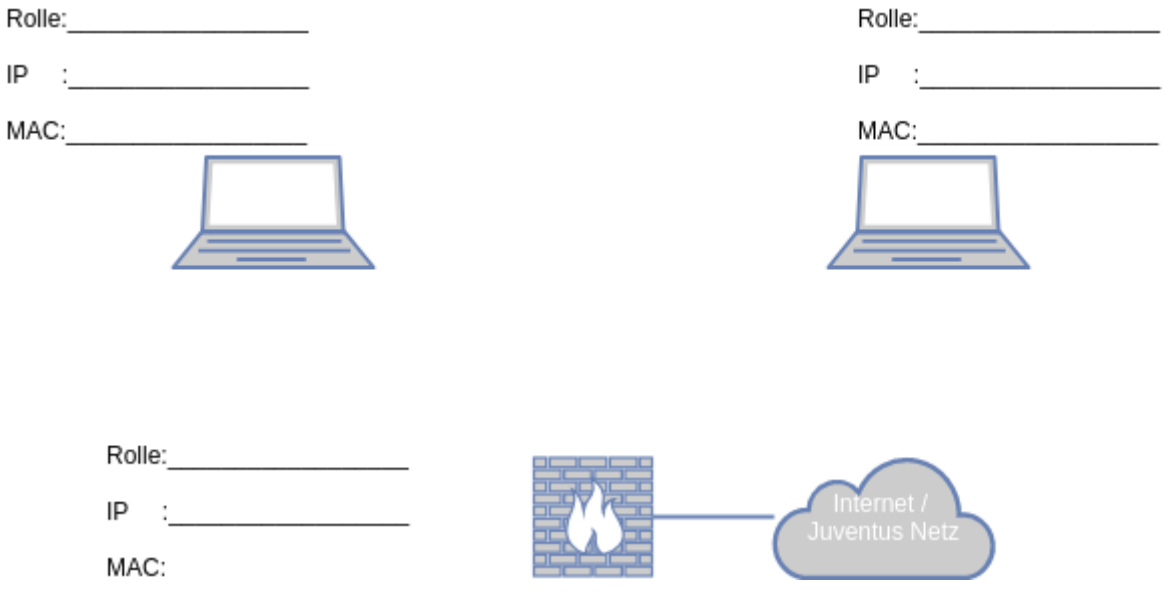
1. Was ist die Idee von ARP-Spoofing?

2. Funktioniert ARP-Spoofing nur über verkabelte Netzwerke oder auch per WLAN?

3. Im Paket Capture «ARP_Spoofing.pcapng» findet offensichtlich ein ARP Spoofing Angriff statt. Analysieren Sie die Aufzeichnung mit Wireshark und beantworten Sie die Fragen.
   a) Welche drei MAC Adressen sind relevant? Notieren Sie nur NIC-Teil. Tipp: Statistics > Endpoints

   b) Mit welcher Paket Nummer startet der ARP Angriff?

   c) Tragen Sie den Datenfluss, die IP- und die MAC-Adressen der Systeme während des Angriffes ein:



4 DNS-Spoofing

1. Was ist die Idee von DNS-Spoofing?

2. Was ist die zwingende Voraussetzung, damit eine DNS Spoofing Attacke funktioniert?

3. Das Opfer hat via DHCP alle Informationen für das lokale Netzwerk bekommen. Jedoch wurde eine DNS-Spoofing-Attacke gegen das Opfer gefahren. Welche IP-Adresse steht beim Opfer in der DNS Netzwerkkonfiguration? Begründen Sie Ihre Antwort:

Die IP des: [ ] Angreifers [ ] Default Gateway [ ] Googles 8.8.8.8 [ ] kann man nicht wissen [ ] die Adresse wurde nicht verändert [ ] Opfer

4. Welche Informationen können bei DNS-Request von einem Angreifer verändert werden?

5. Welche Informationen können bei DNS Response von einem Angreifer verändert werden?