Laboratory III

Reschenhofer Andreas

Course: Internet Infrastructure and Security

Lecturer: FH-Prof. DI Mag. Dr. Dominik Engel

14.12.2016

Table of Contents

List of Abbreviations

ARP	Address Resolution Protocol
MAC	Media Access Control
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
POP3	Post Office Protocol Version 3
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
HTTPS	Hyper Text Transport Protocol Secure

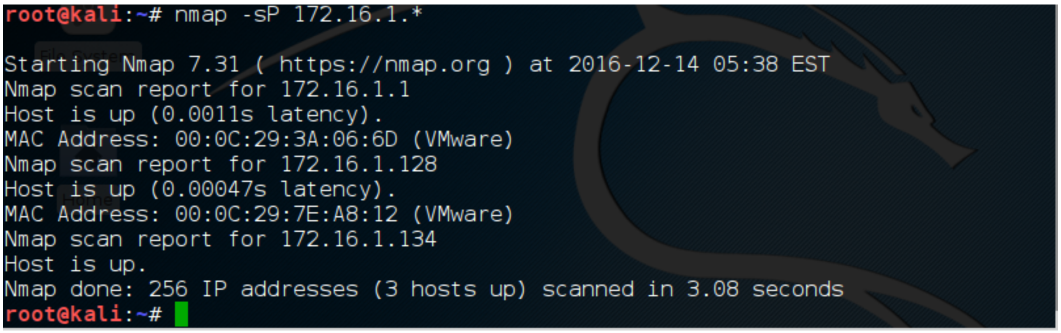
1 Network Reconnaissance

1.1 Network Ping Sweep

In this part information about hosts in a connected network is gathered. With the help of the Kali VM a nmap Ping Sweep command is executed to gather information of the connected devices within the network of the given IP.

```
nmap -sP 172.16.1.*
```

The information gathered are the IP address of the connected device and his MAC address.



```
root@kali:~# nmap -sP 172.16.1.*

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-14 05:38 EST
Nmap scan report for 172.16.1.1
Host is up (0.0011s latency).
MAC Address: 00:0C:29:3A:06:6D (VMware)
Nmap scan report for 172.16.1.128
Host is up (0.00047s latency).
MAC Address: 00:0C:29:7E:A8:12 (VMware)
Nmap scan report for 172.16.1.134
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.08 seconds
root@kali:~#
```

Figure 1.1: Network Ping Sweep with Kali VM

After the switch to the Ubuntu VM we can analyze the Wireshark trace we started in first place. The trace shows that the nmap Ping Sweep command executes an Address Resolution Protocol (ARP)-request on every host on the given IP network range. If a host is available he answers with his MAC address.

Advanced:
If a system detects a certain amount of new ARP-requests on every host system in a network then this could be a sign for an intrution. Since ARP is a stateless protocol, hosts in the network can be compromised by spoofing with falsified IP-MAC pairs.

1.2 OS Detection

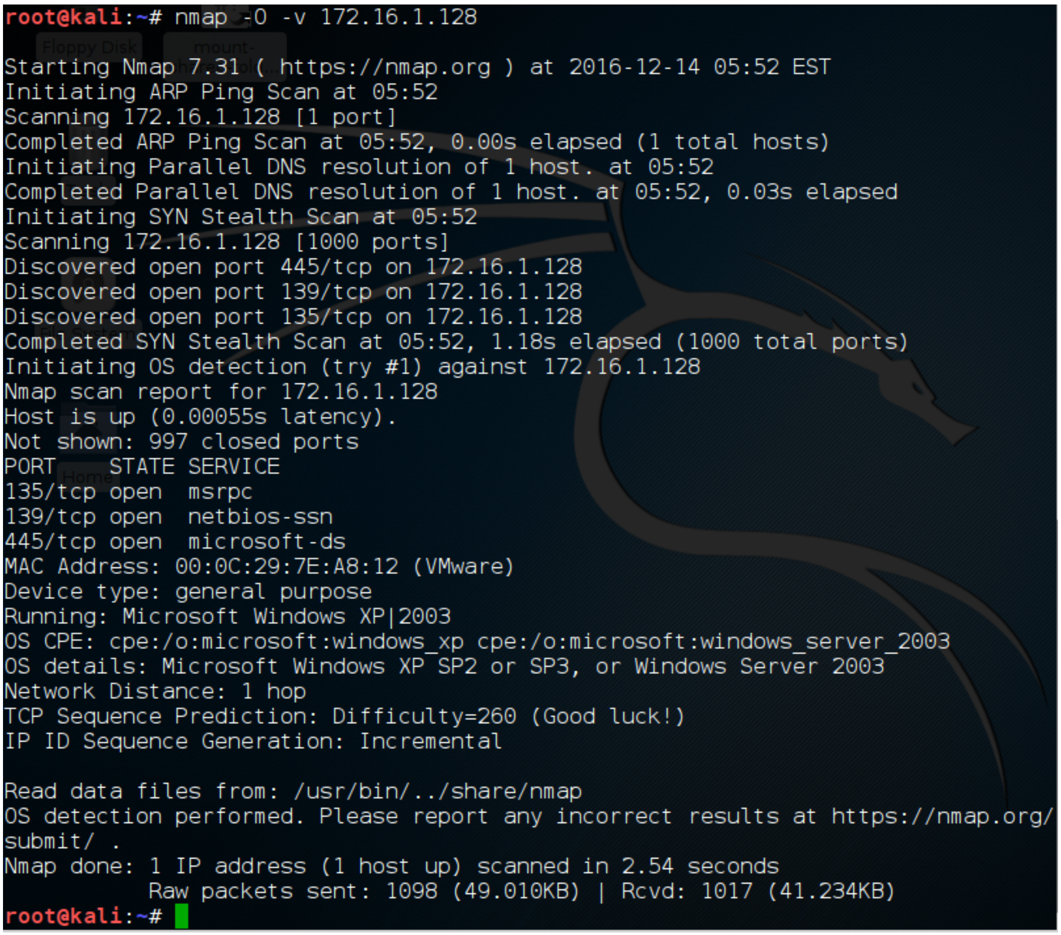
Informations about a specific host in the network are gathered. With the help of the Kali VM an OS detection command is executed.

```
nmap -O -v 172.16.1.X
```

The gathered informations are:

- Open ports
- MAC address
- Device type
- The running operation system
- The network distance to the host (in hops)
- TCP Sequence Prediction

With these information further steps can be planned and executed to compromise this specific host system.



```
root@kali:~# nmap -O -v 172.16.1.128

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-14 05:52 EST
Initiating ARP Ping Scan at 05:52
Scanning 172.16.1.128 [1 port]
Completed ARP Ping Scan at 05:52, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:52
Completed Parallel DNS resolution of 1 host. at 05:52, 0.03s elapsed
Initiating SYN Stealth Scan at 05:52
Scanning 172.16.1.128 [1000 ports]
Discovered open port 445/tcp on 172.16.1.128
Discovered open port 139/tcp on 172.16.1.128
Discovered open port 135/tcp on 172.16.1.128
Completed SYN Stealth Scan at 05:52, 1.18s elapsed (1000 total ports)
Initiating OS detection (try #1) against 172.16.1.128
Nmap scan report for 172.16.1.128
Host is up (0.00055s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:7E:A8:12 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds
           Raw packets sent: 1098 (49.010KB) | Rcvd: 1017 (41.234KB)
root@kali:~#
```

Figure 1.2: OS detection nmap command with Kali VM

1.3 Email Sniffing

In this part Wireshark is used to listen to packets of the Post Office Protocol Version 3 (POP3) protocol. After receiving the authentication packets from the mail server a few POP3 packages can be found. One of the packets contains a character sequence which is base64-encoded (e.g. `"AHJla3RvcgByZWt0b3I"`). This sequence can then be decoded with an external decoder to the username and password of the client which tried to authenticate on the mail server (in this example it is `"rektor rektor"`).

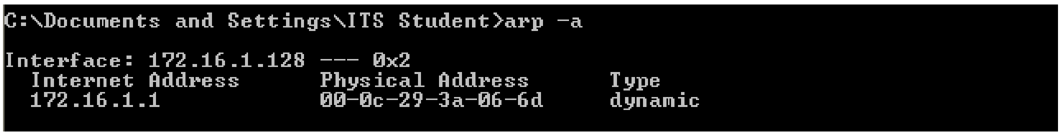
After sending an receiving an email from the mail server an Simple Mail Transfer Protocol (SMTP) packet can be found where the sender, receives, subject and the email text is shown in plaintext. When the attack is performed on the Kali VM it shows the same results (base64-decoded authentication and plaintext SMTP packet).

Advanced:
To let this attack be successful an non secured transport protocol need to be used and the used SMTP needs to be in plain-text. One counter-measure is the use of Secure Socket Layer (SSL) for SMTP connections. This raises another problem. By default, all SMTP servers use port 25. But if you use SSL on port 25, non-SSL will not be able to connect through that port. And if you use a non-standard port number, other servers will not be able to find your server. Another counter-measure is the use of Transport Layer Security (TLS) for an SMTP connection. Each end of the connection can choose to authenticate the other, or the TLS connection can be used purely for privacy. (http://windowsitpro.com/exchange-server/securing-smtp-email-traffic)

2 Active Attacks

2.1 ARP Poisoning

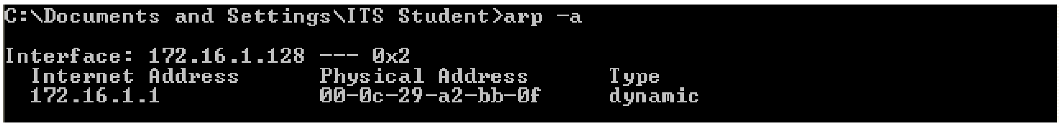
With the ARP poisoning attack a host system should be compromised by sending out a wrong Internet Protocol (IP) and Media Access Control (MAC) address assignment to the host. When the compromised host then wants to authenticate on the mail server he actually sends the username and password of his email account to the wrong IP address.



```
C:\Documents and Settings\ITS Student>arp -a

Interface: 172.16.1.128 --- 0x2
  Internet Address      Physical Address      Type
  172.16.1.1            00-0c-29-3a-06-6d     dynamic
```

Figure 2.1: arp -a before the ARP poisoning



```
C:\Documents and Settings\ITS Student>arp -a

Interface: 172.16.1.128 --- 0x2
  Internet Address      Physical Address      Type
  172.16.1.1            00-0c-29-a2-bb-0f     dynamic
```

Figure 2.2: arp -a after the ARP poisoning

Figure 2.2 shows that a wrong MAC address is now in the ARP table. Before ending the ettercap attack, ettercap sends out a new ARP request with the correct IP and MAC address assignment to the host.

Advanced:
ARP spoofing is a so called Man In the Middle Attack. Mallory is between the communication of host A and B. To keep the attack alive he constantly needs to send wrong ARP requests to both host A and B. If Mallory would not do this a new ARP lookup would happen after a certain amount of time and this would replace the ARP entry of Mallory.

2.2 DHCP Spoofing

During the attack the attacker listens on Dynamic Host Configuration Protocol (DHCP) request. Since the request is a broadcast everyone in the LAN will receive it. Normaly the real DHCP server will reply to the request but since the attacker host, which simulates a DHCP server is closer to the host that sent out the request, the host will receive the wrong DHCP answer earlier. The host then stores the attacker host IP as default-gateway and all the communication passes the attacker.

A possible counter-measure against DHCP spoofing is DHCP snooping. This feature implement2 two different types of ports in a switched environment, trusted and untrusted ports. The first have no restrictions on DHCP messages. If a unstrusted port then receives an incoming DHCP packet it will be blocked.

2.3 SSL Capturing

With the use of ARP poisoning a compromised communication from a host A to any kind of IP address is established. If host A now wants to access a Hyper Text Transport Protocol Secure (HTTPS) website, a certification notification occurs. If host A confirms this untrusted certification then the attacker has the private key which is used to decrypt the encrypt packets from the HTTPS website. He then can find possible passwords. This can be avoided by accepting only trusted certifications.

3 Metasploit

3.1 Brute-Force Attacks

Using the `"mysql_login"` scanner-tool from the metasploit framework executed a brute-force attack onto the host `"10.1.1.10"` which is the metasploitable linux distribution. First the list of all usernames and passwords have to be set wit a few commands. Also the IP of the host has to be set. Afterwards the attack can be started by using the `run` command. The attack showed that the username `root` can be accessed with the password `root`.

3.2 Tomcat

Using the `"tomcat_mgr_login"` scanner-tool from the metasploit framework executed a brute-force attack onto the host `"10.1.1.10"` which is the metasploitable linux distribution. First the list of all usernames and passwords have to be set wit a few commands. Also the IP of the host has to be set. Afterwards the attack can be started by using the `run` command. Running an OS detection scan on the host IP showed an unknown port `8180`. This port was later used to be set in the scanner-tool via `"set RPORT 8180"`. The attack showed that the username `tomcat` can be accessed with the password `tomcat`. Since tomcat uses a web-interface for e.g. managing applications, the web-interface can be accessed with `"10.1.1.10:8180"`. Then the "Tomcat Web Application Manager" can be accessed with username and password.

3.3 Summary

Systems can easily be hacked with brute-force attacks. Since the computing power is rising longer passwords or other security mechanism are needed to be safe. One of those can be a limit of maximum number of tries in a certain amount of time. Another one can be captchas. An administrator of a webserver for example can implement such counter-measures to limit the brute-force attacks although such attacks are difficult to stop completely.

4 Counter Measures

At first the `"auth.log"` displays all the incorrect ssh-login attempts with the IP of the host from which the login happened. After applying the firewall rule `"iptables -A INPUT -s 172.16.1.134 -p tcp -j DROP"` the brute-force output on the Kali VM showed that the connection timed out. When using `fail2ban` the IP address of the host with too many failed login tries will be automatically addded to the iptable.