



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	1
1 Network Reconnaissance	2
1.1 Network Ping Sweep	2
1.2 OS Detection	2
1.3 Email Sniffing	4

List of Abbreviations

ARP	Address Resolution Protocol
POP3	Post Office Protocol Version 3
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security

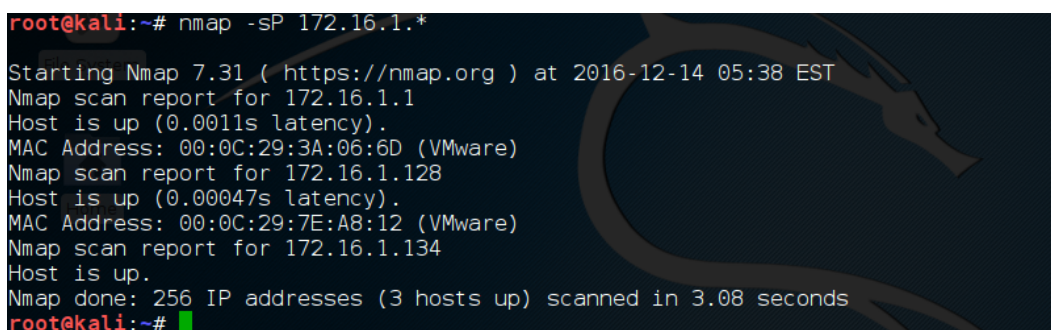
1 Network Reconnaissance

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.

A terminal window screenshot from a Kali Linux VM. The prompt is root@kali:~#. The command nmap -sP 172.16.1.* is entered. The output shows the start of Nmap 7.31 at 2016-12-14 05:38 EST. It reports three hosts up: 172.16.1.1 (MAC 00:0C:29:3A:06:6D), 172.16.1.128 (MAC 00:0C:29:7E:A8:12), and 172.16.1.134. The scan took 3.08 seconds to complete, finding 256 IP addresses with 3 hosts up. The prompt returns to root@kali:~#.

```
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 intrusion. Since ARP is a stateless protocol, hosts in the network can be compromised by spoofing with falsified IP-MAC pairs.

1.2 OS Detection

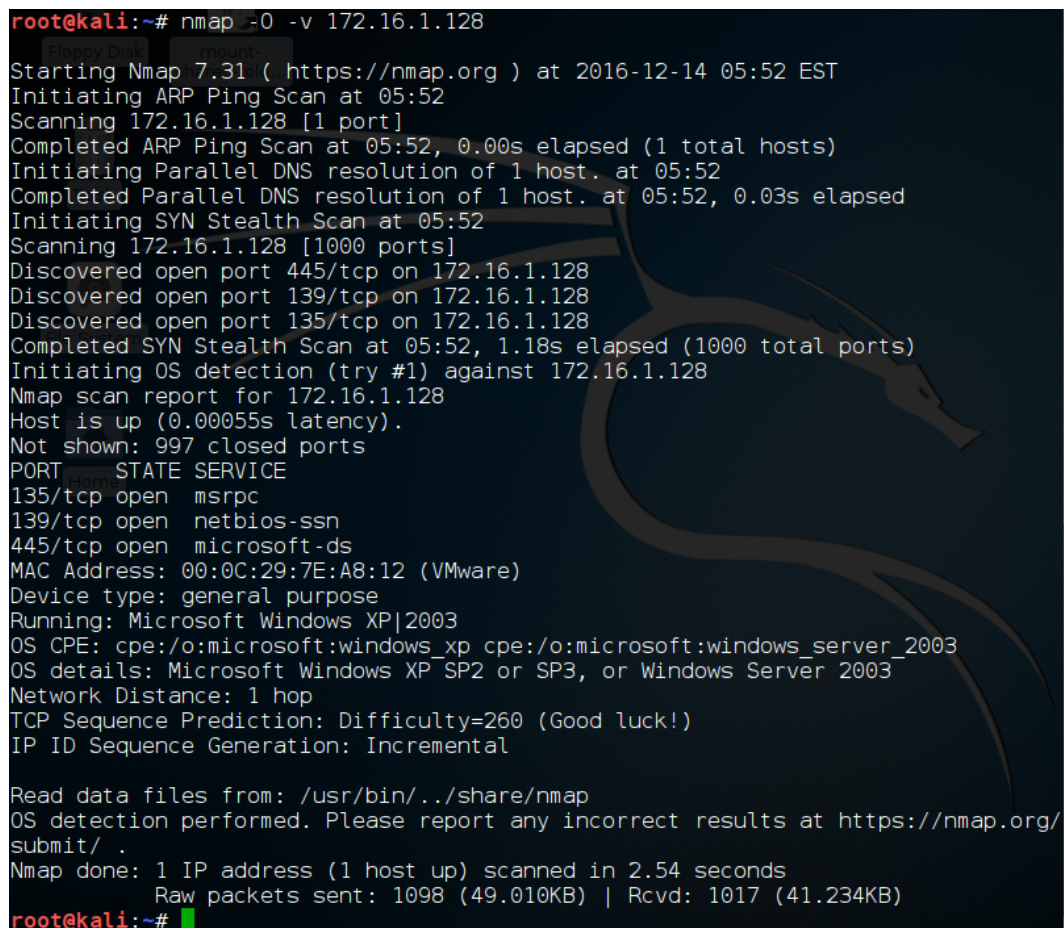
Informations about a specific host in the network are gathered. With the help of the Kali VM an OS detection command is executed.

```
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. "AHJ1a3RvcgByZWt0b3I"). 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 plaintext. 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 nonstandard 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>)