Network security – basic attacks

Lab Report 1

Information Systems Security course (01TYM, 02KRQ)

prepared by:
Anuar Elio Magliari (s317033@studenti.polito.it)
George Florin Eftime (s303483@studenti.polito.it)
AleKos Interrante Bonadia (s319849@studenti.polito.it)

Section 1.1 : Network Scanning

How can this be done in practice? Which is the most common method used to determine whether a certain host is reachable?

```
┌──(kali㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether a8:a1:59:1f:d0:1c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.36/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 1769sec preferred_lft 1769sec
    inet6 fe80::b668:c877:8e70:85d9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.1 -c 5
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.36 icmp_seq=1 Destination Host Unreachable
From 192.168.1.36 icmp_seq=2 Destination Host Unreachable
From 192.168.1.36 icmp_seq=3 Destination Host Unreachable
From 192.168.1.36 icmp_seq=4 Destination Host Unreachable
From 192.168.1.36 icmp_seq=5 Destination Host Unreachable

── 192.168.1.1 ping statistics ──
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4096ms
pipe 4

┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.35 -c 5
PING 192.168.1.35 (192.168.1.35) 56(84) bytes of data.
64 bytes from 192.168.1.35: icmp_seq=1 ttl=64 time=0.257 ms
64 bytes from 192.168.1.35: icmp_seq=2 ttl=64 time=0.228 ms
64 bytes from 192.168.1.35: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 192.168.1.35: icmp_seq=4 ttl=64 time=0.222 ms
64 bytes from 192.168.1.35: icmp_seq=5 ttl=64 time=0.256 ms

── 192.168.1.35 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.220/0.236/0.257/0.016 ms
```

- The most common method used to verify if a certain host is reachable is using PING which use ICMP protocol. In other words, it communicates with the destination (the address ip destination must be specified) sending ICMP packets where him can reply to them.

Why (in general) it is not recommended to perform network scanning inside a monitored network?

- In general, performing network scanning inside a monitored network is not recommended because you can be revealed from the detecter.

Exercise 1

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p 80 -O -v 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 15:21 UTC
Initiating ARP Ping Scan at 15:21
Scanning 192.168.1.35 [1 port]
Completed ARP Ping Scan at 15:21, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:21
Completed Parallel DNS resolution of 1 host. at 15:21, 0.00s elapsed
Initiating Connect Scan at 15:21
Scanning 192.168.1.35 [1 port]
Completed Connect Scan at 15:21, 0.00s elapsed (1 total ports)
Initiating OS detection (try #1) against 192.168.1.35
Retrying OS detection (try #2) against 192.168.1.35
Nmap scan report for 192.168.1.35
Host is up (0.00026s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: A8:A1:59:1F:CF:43 (ASRock Incorporation)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 1.61 seconds
           Raw packets sent: 13 (1.696KB) | Rcvd: 13 (1.632KB)
```

Exercise 2

Do you manage to discover which services have been activated by the victim (Alice)?

- Yes, we are able to discover which services have been activated.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -Pn -p 1-1024 -v 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 15:25 UTC
Initiating Parallel DNS resolution of 1 host. at 15:25
Completed Parallel DNS resolution of 1 host. at 15:25, 0.00s elapsed
Initiating Connect Scan at 15:25
Scanning 192.168.1.35 [1024 ports]
Discovered open port 21/tcp on 192.168.1.35
Discovered open port 80/tcp on 192.168.1.35
Completed Connect Scan at 15:25, 0.05s elapsed (1024 total ports)
Nmap scan report for 192.168.1.35
Host is up (0.00019s latency).
Not shown: 1022 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

Why is it useful to avoid pinging the host (the option -Pn)?

- It is useful to avoid using ping during a port scanning of a host because this can trigger suspicious activity by the host, thus risking being blocked.

Exercise 3

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -Pn -p 21 -v 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 16:36 UTC
Initiating Parallel DNS resolution of 1 host. at 16:36
Completed Parallel DNS resolution of 1 host. at 16:36, 0.00s elapsed
Initiating Connect Scan at 16:36
Scanning 192.168.1.35 [1 port]
Completed Connect Scan at 16:36, 0.00s elapsed (1 total ports)
Nmap scan report for 192.168.1.35
Host is up (0.00023s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -Pn -p 201 -v 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 16:36 UTC
Initiating Parallel DNS resolution of 1 host. at 16:36
Completed Parallel DNS resolution of 1 host. at 16:36, 0.00s elapsed
Initiating Connect Scan at 16:36
Scanning 192.168.1.35 [1 port]
Discovered open port 201/tcp on 192.168.1.35
Completed Connect Scan at 16:36, 0.00s elapsed (1 total ports)
Nmap scan report for 192.168.1.35
Host is up (0.00024s latency).

PORT    STATE SERVICE
201/tcp open  at-rtmp

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Have you encountered problems? How do you think they can be solved?

- No, we haven’t! In this case we see two different available service opened each other in the relative port.

Exercise 4

Why is it recommended to use the flag -sV rather than the option -A ?

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -Pn -p 1-2020 -v 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 16:46 UTC
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 16:46
Scanning 192.168.1.35 [1 port]
Completed ARP Ping Scan at 16:46, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:46
Completed Parallel DNS resolution of 1 host. at 16:46, 0.00s elapsed
Initiating SYN Stealth Scan at 16:46
Scanning 192.168.1.35 [2020 ports]
Discovered open port 80/tcp on 192.168.1.35
Discovered open port 2000/tcp on 192.168.1.35
Completed SYN Stealth Scan at 16:46, 0.06s elapsed (2020 total ports)
Initiating Service scan at 16:46
Scanning 2 services on 192.168.1.35
Completed Service scan at 16:46, 6.05s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.1.35.
Initiating NSE at 16:46
Completed NSE at 16:46, 0.01s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.01s elapsed
Nmap scan report for 192.168.1.35
Host is up (0.00013s latency).
Not shown: 2018 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.57 ((Debian))
2000/tcp open  ftp     vsftpd 3.0.3
MAC Address: A8:A1:59:1F:CF:43 (ASRock Incorporation)
Service Info: OS: Unix

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.46 seconds
           Raw packets sent: 2021 (88.908KB) | Rcvd: 2021 (80.836KB)
```

In your opinion, which techniques and security tools can be used to defend against the security attacks presented above?

Exercise 5

Before the attack

Role	IP Address	MAC Address
Alice	192.168.1.58/24	a8:a1:59:1f:12:cb
Bob	192.168.1.60/24	a8:a1:59:1f:cf:f7
Chunk	192.168.1.59/24	a8:a1:59:1f:12:df

After the attack

Role	IP Address	MAC Address
Alice	192.168.1.58/24	a8:a1:59:1f:12:cb
Bob	192.168.1.60/24	a8:a1:59:1f:12:df
Chunk	192.168.1.59/24	a8:a1:59:1f:12:df

What kind of network traffic was able to capture Chuck before the attack?

- Before the attack, Chunk was only able to capture the broadcast messages but not the direct comunication.

What type of network traffic is able to sniff Chuck after the attack?

- After the attack, due to the table modified he was able to sniff all messages between Alice and Bob.

Can you figure out from the captured network traffic how the attack works?

- Simply put, when Chuck sends the Ettercap command, it modifies the ARP table of Alice and Bob so that each of their IP addresses corresponds to Chuck's MAC address. Consequently, every message between Alice and Bob passes through Chuck, and he acts as a router forwarding the messages.

What happened to the ARP tables of Alice, Bob and Chuck? Check out.

- The ARP tables of Alice and Bob are modified with the correct IP addresses, but the MAC address corresponds to Chuck's MAC address. Meanwhile, Chuck's ARP table remains unchanged.

Take a look at the Figure ?? and try to respond to this question (where ? can be a hub, a switch, a router or even Internet): when is it possible to make a man-in-the-middle attack with ARP poisoning and which are its effects?

- The man-in-the-middle attack with ARP poisoning is only possible on a LAN due to the nature of ARP. However, its effects can compromise the security of the network. For example, an attacker within the network can carry out attacks such as DoS, MITM, sniffing, reply attacks, and others, thereby undermining repudiation, integrity, confidentiality, and availability.

Optionally, try to identify a possible countermeasure to this security attack

- One possible countermeasure can be the use of an authentication/non-repudiation method involving RSA keys between the two parties, encrypting all messages with their respective private keys. This will ensure that the message was indeed sent by the legitimate sender.

What happened?

- Bob will send the messages to the real MAC address of Alice.

What Chuck did at point 1?

- Chuck modifies the ARP poisoning delay; consequently, Chuck will re-modify the victims' ARP tables every 1000 seconds, making the attacks more effective

What is the meaning of the variable arp poison delay? Prove again the exercise by setting the variable to 1 or to the default value, 10

- For instance, if it is set to 1, the attacker will not be stealthy enough to avoid detection by potential detectors within the network.

Exercise 8

How can Chuck intercept all the web traffic of Alice?

- By using the Ettercap tool, we can poison the ARP tables of both Bob and Alice, allowing us to carry out a man-in-the-middle attack. This means that all traffic from Bob will pass through Chuck and then be forwarded to Alice.

How can you defend against these types of sniffing attacks

- To enhance the security of our messages, we can employ encryption using the RSA algorithm. In this method, Bob encrypts their messages with their private key to ensure confidentiality between Alice and Bob. When Alice receives the messages, she can decrypt them using Bob's public key.

Try to execute a login by using SSH protocol and to capture the username and password. Are you able to do so (why)?

- The attacker encounters more difficulty with SSH because it encrypts all messages from Bob to Alice and vice versa.

Exercise 9

You should see information provided by DNS.

- Trying "polito.it"

  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34818

  ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

  ;; QUESTION SECTION:

  ;polito.it. IN A

  ;; ANSWER SECTION:

polito.it. 86400 IN A 192.168.59.6

polito.it. 86400 IN A 192.168.40.1

Received 59 bytes from 130.192.3.21#53 in 12 ms

Trying "polito.it"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55137

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

;polito.it. IN AAAA

;; AUTHORITY SECTION:

polito.it. 86400 IN SOA leonardo.polito.it. root.leonardo.polito.it. 2023101203 10800 1800 1209600 86400

Received 77 bytes from 130.192.3.21#53 in 0 ms

Trying "polito.it"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19893

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:

;polito.it. IN MX

;; ANSWER SECTION:

polito.it. 3600 IN MX 10 exchedge.polito.it.

;; ADDITIONAL SECTION:

exchedge.polito.it. 86400 IN A 130.192.67.194

exchedge.polito.it. 86400 IN A 130.192.67.195

Received 84 bytes from 130.192.3.21#53 in 0 ms

What does Bob see in his web browser?

- Bob sees the page associated with the IP address manipulated by Alice.

What could have happened if the attack didn’t work? Make your assumptions and confront them with what we have indicated in the initial note.

- In our case, the attack has been successfully conducted.

What does Alice see in the ettercap window?

- Alice sees all the HTTP requests made by Bob when he tries to reach www.polito.it.

How can an attacker obtain similar results (as the ones described in this section), even though the attacker is not close to the victim?

- The attack can be conducted in various ways. We can consider having access to a VPN, thereby simulating access to the LAN even if it's not physically located in the same place. Alternatively, a phishing attack can be employed, where the victim is induced to visit the desired website or to exploit potential vulnerabilities in the network that allow the attacker to gain access.