

Final presentation

Steven Lemaire

Idea of the problem

- ▶ Security PROBLEMS in Telecommunication Networks may concern 3 points
 - ▶ Confidentiality : Access to the only people permitted
 - ▶ Integrity : No change of the information
 - ▶ Availability : Data always available when we need

ISECOM

- ▶ To protect your system there are 2 ways, first one is manually
- ▶ The Open Source Security Testing Methodology Manual is a complete methodology for the testing, analysis and measurement of operational security towards building the best possible security defenses. This company makes penetration testing :
 - ▶ Reconnaissance
 - ▶ Scanning and enumeration
 - ▶ Exploitation (gaining access)
 - ▶ Post-exploitation (maintaining access)
 - ▶ Covering tracks

Penetration test

- Discover other users of the network, list them, obtain data from users by observing the exchanges.

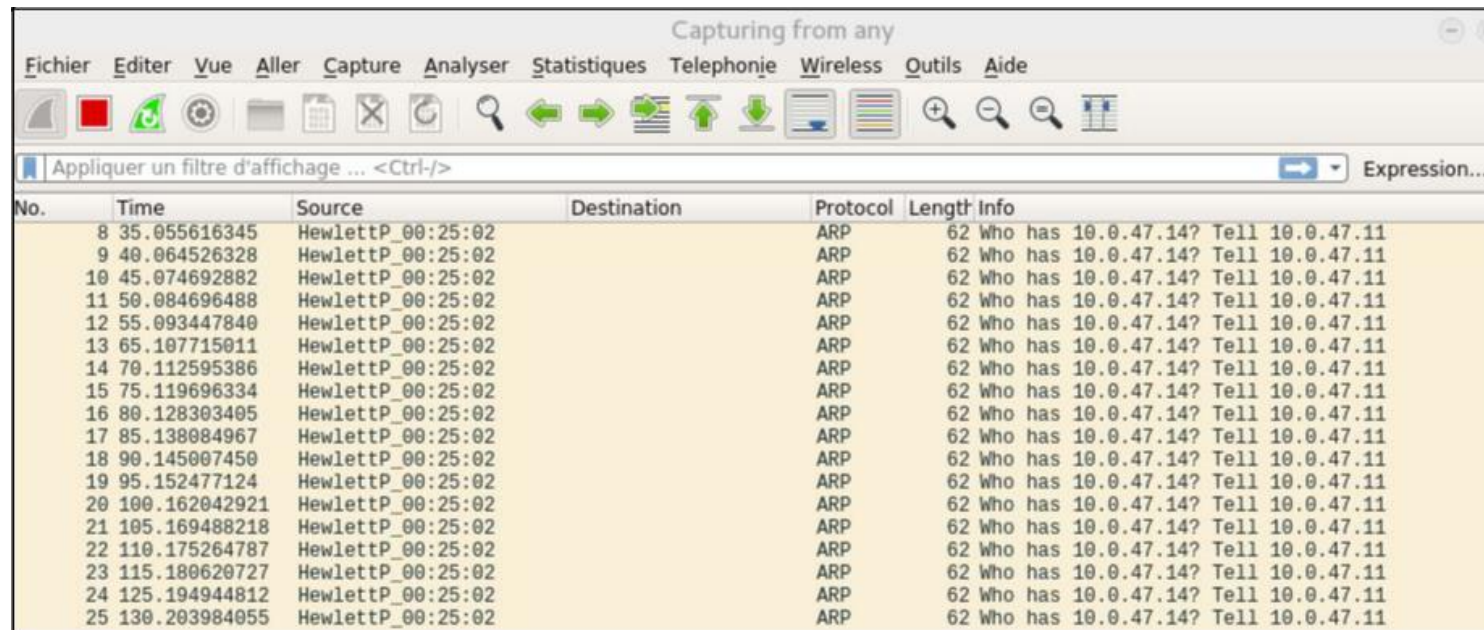
Characteristic	Vulnerability Assessments	Penetration Testing
Goal	Uncover known vulnerabilities across the environment	Uncover and exploit vulnerabilities to show how criminals would use them to move laterally or deeper into the environment
Scope	Wide, broad, scanning the surface	Focused, deep
Performed by	Automated tool(s) (with human oversight)	Experienced hackers
Outcome	List of vulnerabilities	Prioritized list of vulnerabilities, methodologies to exploit them, narrative walkthrough of attack scenario, remediation recommendations
Next step	Prioritize for remediation and apply patches	Apply patches and other fixes that reduce the most risk
Best for	Understanding basic level of security posture	Understanding all facets of security posture

Kali Linux

- ▶ Automatic tool
- ▶ The Kali Linux penetration testing platform contains a vast array of tools and utilities, from information gathering to final reporting, that enable security and IT professionals to assess the security of their systems.
- ▶ It integrates a lot of well-known security software, for example :
 - ▶ Aircrack-ng
 - ▶ Burp suite
 - ▶ Foremost
 - ▶ HT-WPS Breaker
 - ▶ John The Ripper
 - ▶ Kismet
 - ▶ Maltego
 - ▶ Metasploit Framework
 - ▶ Nmap
 - ▶ OWASP ZAP
 - ▶ Volatility
 - ▶ Wireshark

Mapping a network

- ▶ Using a virtual machine with Kali distribution to use the integrated tools
- ▶ The purpose is to identify equipment on the local network
- ▶ First method : Manual passive identification with Wireshark



The image shows a Wireshark window titled "Capturing from any". The menu bar includes Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Telephonie, Wireless, Outils, and Aide. The toolbar contains various icons for file operations, capture control, and analysis. A filter bar at the top shows "Appliquer un filtre d'affichage ... <Ctrl-/>" and an "Expression..." button. The main display area shows a list of 25 network packets, all of which are ARP requests. Each packet has a number, a time, a source MAC address (HewlettP_00:25:02), a destination IP address (10.0.47.14), and a protocol of ARP. The length of each packet is 62 bytes, and the info column shows "Who has 10.0.47.14? Tell 10.0.47.11".

No.	Time	Source	Destination	Protocol	Length	Info
8	35.055616345	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
9	40.064526328	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
10	45.074692882	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
11	50.084696488	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
12	55.093447840	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
13	65.107715011	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
14	70.112595386	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
15	75.119696334	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
16	80.128303405	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
17	85.138084967	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
18	90.145007450	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
19	95.152477124	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
20	100.162042921	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
21	105.169488218	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
22	110.175264787	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
23	115.180620727	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
24	125.194944812	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11
25	130.203984055	HewlettP_00:25:02	10.0.47.14	ARP	62	Who has 10.0.47.14? Tell 10.0.47.11

Mapping a network

- ▶ Second method : Automated passive identification with netdiscover
- ▶ Using the `-netdiscover -p` command, the network is passively scanned.

```
root@kali: ~  
Fichier Édition Affichage Rechercher Terminal Aide  
Currently scanning: (passive) | Screen View: Unique Hosts  
7 Captured ARP Req/Rep packets, from 6 hosts. 44 Total size: 420  
AvlabTec 00:27:93 AvlabTec 00:06:04 0xc042 44 Ethernet II  
-----  
IP At MAC Address Count Len MAC Vendor / Hostname  
-----  
10.0.47.10 27:93 00:10:83:00:25:01 0xc142 60 HEWLETT-PACKARD COMPANY  
10.0.47.11 27:93 00:10:83:00:25:02 0xc142 60 HEWLETT-PACKARD COMPANY  
10.0.47.12 27:93 00:10:83:00:25:03 0xc142 60 HEWLETT-PACKARD COMPANY  
10.0.47.13 27:93 00:10:83:00:25:04 0xc142 60 HEWLETT-PACKARD COMPANY  
10.0.47.14 27:93 00:10:83:00:25:05 0xc142 60 HEWLETT-PACKARD COMPANY  
10.0.47.254 27:93 00:01:42:00:2f:fe 0xc042 120 CISCO SYSTEMS, INC.  
AvlabTec 00:27:93 AvlabTec 00:06:04 0xc042 44 Ethernet II
```

Mapping a network

- ▶ Third method : Automated active identification with arp-scan
- ▶ To get a new IP from the DHCP server, you can release it and get a new one
 - ▶ `sudo dhclient -r`
 - ▶ `sudo dhclient`

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.47.16 netmask 255.255.255.0 broadcast 10.0.47.255
    inet6 fe80::a00:27ff:fe93:c642 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:93:c6:42 txqueuelen 1000 (Ethernet)
    RX packets 183 bytes 16679 (16.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 109070 bytes 6545097 (6.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```


Mapping a network

- ▶ Third method : Automated active identification with arp-scan
- ▶ *arp-scan --interface=eth0 10.0.47.0/24*
 - ▶ arp-scan sends ARP packets to hosts on the local network and displays any responses that are received.

```
root@kali:~# arp-scan --interface=eth0 10.0.47.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
10.0.47.10      00:10:83:00:25:01    HEWLETT-PACKARD COMPANY
10.0.47.11      00:10:83:00:25:02    HEWLETT-PACKARD COMPANY
10.0.47.12      00:10:83:00:25:03    HEWLETT-PACKARD COMPANY
10.0.47.13      00:10:83:00:25:04    HEWLETT-PACKARD COMPANY
10.0.47.14      00:10:83:00:25:05    HEWLETT-PACKARD COMPANY
10.0.47.254     00:01:42:00:2f:fe    CISCO SYSTEMS, INC.

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 1.874 seconds (136.61 hosts/sec). 6 re
sponded
```

Difference between active and passive mode ?

- ▶ Passive mode allows you to remain invisible on the network by listening to requests and responses on the network. We will only see the hosts that generated the broadcast.
- ▶ The active mode will generate successive ARP requests to the network hosts and retrieve the MAC and IP address. The machine identifying the network equipment will be visible to everyone because it will broadcast.

Identification of open ports

- ▶ On the local network with nmap
- ▶ `nmap -sU -p 67 10.0.47.254`
- ▶ This command allows to identify open port via UDP, for example the DHCP port (67)

```
root@kali: ~  
Fichier Édition Affichage Rechercher Terminal Aide  
root@kali:~# nmap -sU -p 67 10.0.47.254  
Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-14 06:42 EDT  
Nmap scan report for 10.0.47.254  
Host is up (0.00078s latency).  
PORT      STATE SERVICE  
67/udp    open|filtered dhcp  
MAC Address: 00:01:42:00:2F:FE (Cisco Systems)  
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Identification of OS

- ▶ `nmap -sU -sV -O -p 67 10.0.47.254`
- ▶ Nmap will try to identify the OS by sending messages and examining the behaviour of the equipment on the network.
- ▶ Nmap sends packets to all ports of the machine, so there is unusual activity coming from our IP address. Therefore Nmap is considered as a passive attack.

```
root@kali:~# nmap -sU -sV -O -p 67 10.0.47.254
Nmap Version 4, Src: 10.0.47.254, Dst: 10.0.47.16
Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-14 07:00 EDT
Nmap scan report for 10.0.47.254
Host is up (0.0021s latency).
PORT      STATE      SERVICE VERSION
67/udp    open|filtered dhcpd
MAC Address: 00:01:42:00:2F:FE (Cisco Systems)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.42 seconds
```

Identification of services on the global network

- ▶ To search for the DNS address, we do a reverse search with the dnsrecon tool
- ▶ We target the 10.0.47.0/16 network and **identify the 10.0.23.7 address as the DNS address.**

```
root@kali:~# dnsrecon -r 10.0.47.0/16
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 10.0.0.0 to 10.0.255.255
[*] PTR intranet.mycompany 10.0.23.7
[*] PTR ns.mycompany 10.0.81.3
[*] 2 Records Found
```

Identification of services on the global network

- Get the available services from the DNS address
 - Open or filtered

Service (port)
DHCP (67)
NTP (123)
TFTP (69)
DNS (53)
FTP (21)
SSH (22)
HTTP (80)

```
root@kali:~# nmap -sV -p 67 10.0.23.7
Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-14 08:17 EDT
Nmap scan report for intranet.mycompany (10.0.23.7)
Host is up (0.00083s latency).
PORT      STATE      SERVICE VERSION
67/tcp    filtered  dhcp
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
root@kali:~# nmap -sV -p 123 10.0.23.7
Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-14 08:18 EDT
Nmap scan report for intranet.mycompany (10.0.23.7)
Host is up (0.00059s latency).
PORT      STATE      SERVICE VERSION
123/tcp   filtered  ntp
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
root@kali:~# nmap -sV -p 69 10.0.23.7
Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-14 08:18 EDT
Nmap scan report for intranet.mycompany (10.0.23.7)
Host is up (0.00066s latency).
PORT      STATE      SERVICE VERSION
69/tcp    filtered  tftp
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
root@kali:~# nmap -sV -p 53 10.0.23.7
Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-14 08:18 EDT
Nmap scan report for intranet.mycompany (10.0.23.7)
Host is up (0.00071s latency).
PORT      STATE      SERVICE VERSION
53/tcp    filtered  domain
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

Protect your network

- ▶ No matter the network scanning method, it is recommended to **set up a firewall** to counter this scanning with ARP or by sending DNS requests to retrieve information. **The activation of logs** can be a first step (in addition to the firewall) to identify requests made on our system, regardless of the software.
- ▶ The dangers with ARP other than network mapping is only one of our equipment, can be usurped (ARP spoofing...). **Indeed, this protocol allows to know the MAC address corresponding to an IP address.** The implementation of static ARP recording can be implemented even if it can be very cumbersome and depends mainly on the number of equipment on the network.

What is ARP spoofing ?

- ▶ “**ARP spoofing** is a type of attack in which a malicious actor sends forged ARP (Address Resolution Protocol) messages over a local network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network”.
By Veracode.com
- ▶ It is therefore recommended to configure the DNS server so that it only resolves the names of the machines of the domain on which it has authority, limits the cache and checks the records and does not rely on domain name authentication systems. You can also use DNSSEC which is a more secure version of DNS.

The background features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

Thank you for your
attention !

Source

- ▶ <https://tools.kali.org/>
- ▶ <https://www.hitachi-systems-security.com/blog/penetration-testing-vs-vulnerability-assessment/>
- ▶ <https://linuxhint.com/configure-snort-ids-create-rules/>
- ▶ https://fr.wikipedia.org/wiki/Kali_Linux
- ▶ <https://linux.die.net/man/1/arp-scan>
- ▶ <https://www.cyberciti.biz/faq/howto-linux-renew-dhcp-client-ip-address/>
- ▶ <https://pentest-tools.com/blog/nmap-port-scanner/>
- ▶ <https://www.veracode.com/security/arp-spoofing>

Appendices

```
steven@steven-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::867f:3a16:fc05:2a1a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:81:57:56 txqueuelen 1000 (Ethernet)
    RX packets 13056 bytes 17748059 (17.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17022 bytes 1327177 (1.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 959 bytes 68943 (68.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 959 bytes 68943 (68.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lxcbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.0.3.1 netmask 255.255.255.0 broadcast 0.0.0.0
    ether 00:16:3e:00:00:00 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
steven@steven-VirtualBox:~$ dnsrecon -r 10.0.2.0/16
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 10.0.0.0 to 10.0.255.255

^Z
[3]+  Arrêté                  dnsrecon -r 10.0.2.0/16
```

```
steven@steven-VirtualBox:~$ sudo nmap -sU -p 67 10.0.2.4

Starting Nmap 7.60 ( https://nmap.org ) at 2019-12-17 11:38 EET
Nmap scan report for 10.0.2.4
Host is up (-0.20s latency).

PORT      STATE      SERVICE
67/udp    open|filtered dhcps
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
steven@steven-VirtualBox:~$ sudo nmap -sU -sV -O -p 67 10.0.2.4

Starting Nmap 7.60 ( https://nmap.org ) at 2019-12-17 11:39 EET
Stats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
```