

Epicode Unit 1, Week 3, Day 4

Traccia:

Nell'esercizio di oggi pomeriggio vedremo da vicino nmap e i suoi comandi.

Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- Host discovery (sulla propria rete LAN)
- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

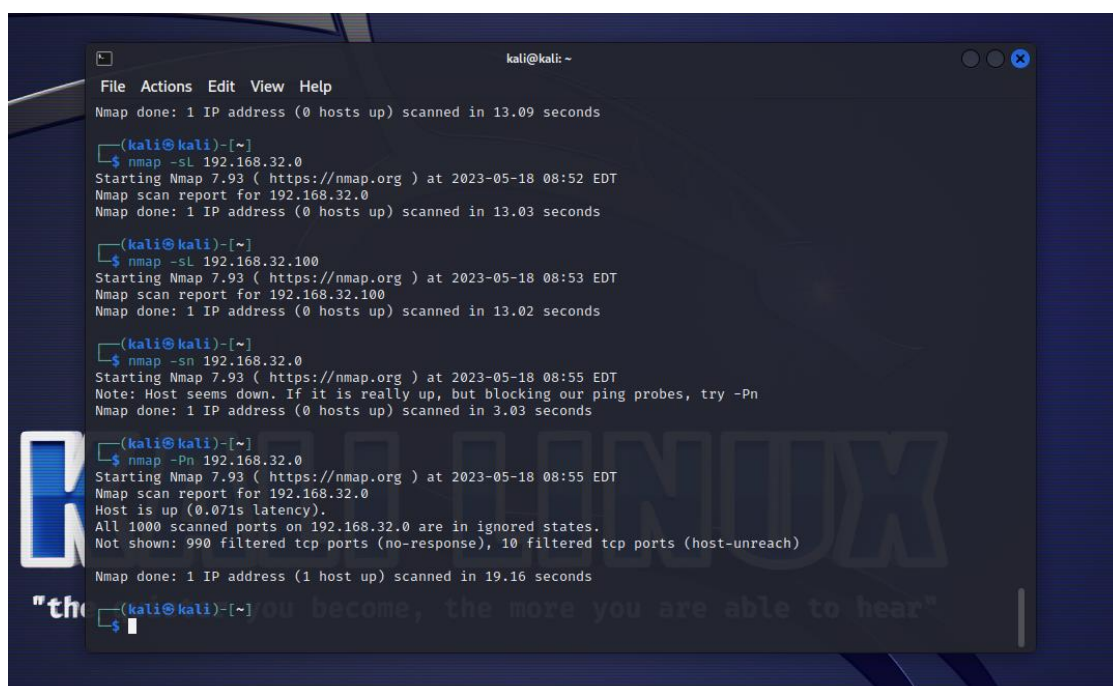
Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente (Kali) con Wireshark.

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine. E' molto importante in questa fase essere organizzati e strutturati. Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro (tabella su word ad esempio) che riporti in maniera chiara:

- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

Per lo svolgimento della traccia odierna, mi assicuro anzitutto che la macchina Metasploitable sia correttamente configurata sulla rete di Kali (192.168.32.100), andando quindi ad assegnarle l'IP 192.168.32.105.

Apro dunque nMap, iniziando con le procedure di Host discovery sulla rete interna alla quale sono collegate le macchine, al fine di individuare gli host attivi.



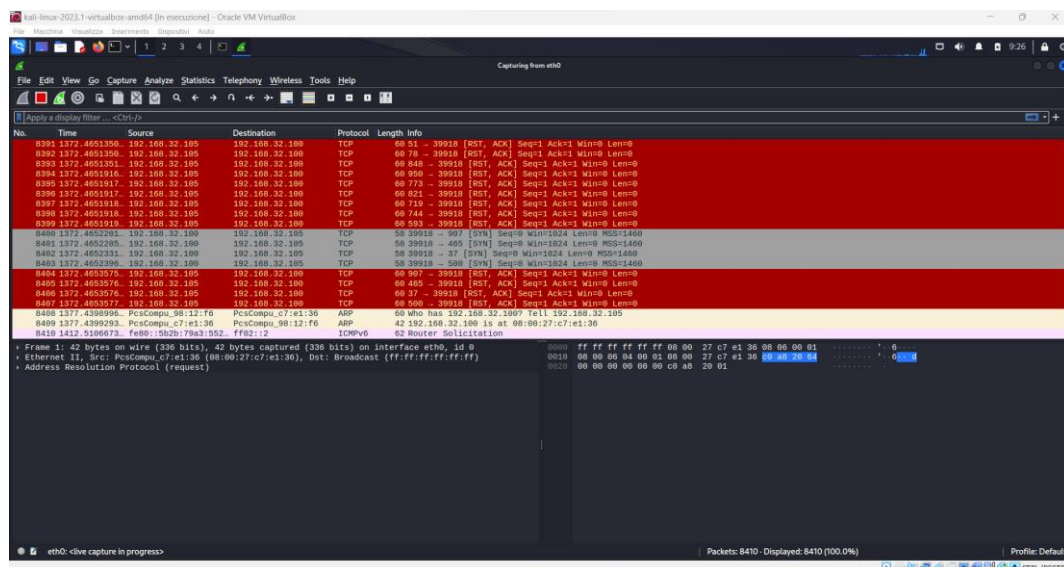
```
kali@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (0 hosts up) scanned in 13.09 seconds  
  
(kali@kali)-[~]  
$ nmap -sL 192.168.32.0  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:52 EDT  
Nmap scan report for 192.168.32.0  
Nmap done: 1 IP address (0 hosts up) scanned in 13.03 seconds  
  
(kali@kali)-[~]  
$ nmap -sL 192.168.32.100  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:53 EDT  
Nmap scan report for 192.168.32.100  
Nmap done: 1 IP address (0 hosts up) scanned in 13.02 seconds  
  
(kali@kali)-[~]  
$ nmap -sn 192.168.32.0  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:55 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds  
  
(kali@kali)-[~]  
$ nmap -Pn 192.168.32.0  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:55 EDT  
Nmap scan report for 192.168.32.0  
Host is up (0.071s latency).  
All 1000 scanned ports on 192.168.32.0 are in ignored states.  
Not shown: 990 filtered tcp ports (no-response), 10 filtered tcp ports (host-unreach)  
Nmap done: 1 IP address (1 host up) scanned in 19.16 seconds  
  
(kali@kali)-[~]  
$
```

Proseguo ora con la scansione delle porte con il Comando `-sS`, che dovrebbe interrompere il three-way-handshake e permettermi una scansione della macchina target, in questo caso Metasploitable (192.168.32.105).

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sS -p0-1023 192.168.32.105  
You requested a scan type which requires root privileges.  
QUITTING!  
(kali@kali)-[~]  
$ sudo nmap -sS -p0-1023 192.168.32.105  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:24 EDT  
Nmap scan report for 192.168.32.105  
Host is up (0.00012s latency).  
Not shown: 1012 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
MAC Address: 08:00:27:98:12:F6 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds  
(kali@kali)-[~]  
$
```

In pochi secondi, nMap restituisce, grazie all'apposito comando, una lista di porte aperte sulla macchina target, insieme anche al tipo di protocollo utilizzato e il servizio collegato alla porta.

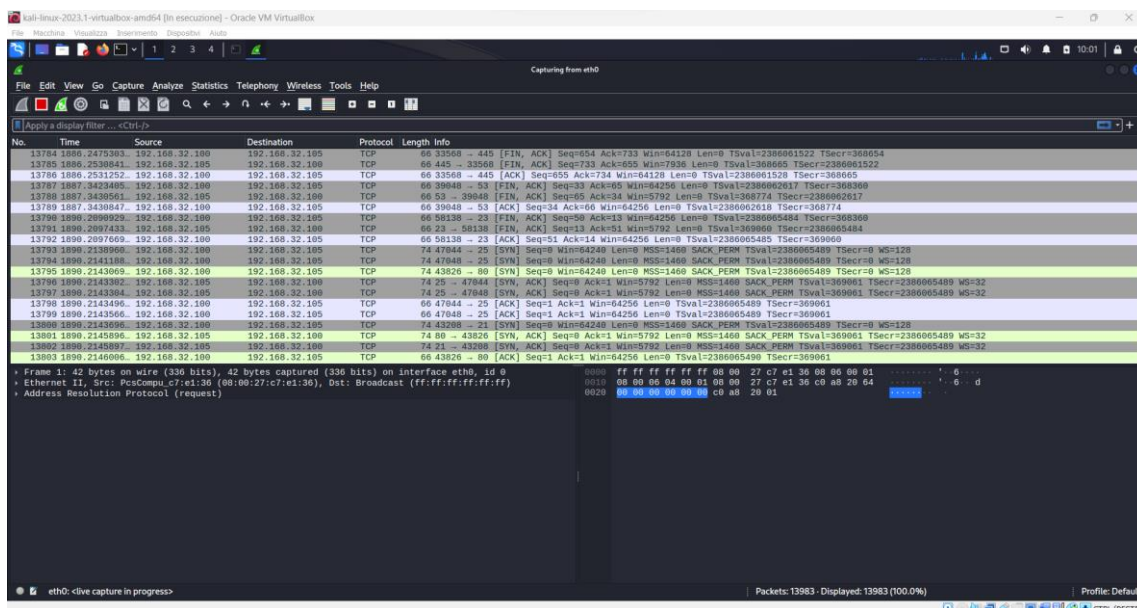
Utilizzando Wireshark, inoltre, si può notare come con il comando `-sS`, nMap non chiuda il protocollo TCP, evitando, di fatto, un congestionamento della rete.



Analizzo ora i dati estrapolati con il comando `-sT` e il comando `-A`, notando anzitutto quanto più traffico generino all'interno della rete. Con il comando `-sT`, il risultato che appare sul terminale di nMap non cambia molto, il software restituirà comunque un elenco di porte.

```
kali@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds  
  
(kali@kali)-[~]  
$ nmap -sT -p0-1023  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:19 EDT  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds  
  
(kali@kali)-[~]  
$ nmap -sT -p0-1023 192.168.32.105  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:20 EDT  
Nmap scan report for 192.168.32.105  
Host is up (0.00013s latency).  
Not shown: 1012 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
  
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds  
  
(kali@kali)-[~]  
$
```

La differenza sostanziale, in questo caso, sarà su Wireshark, in quanto, questa volta, il comando utilizzato fa completare a Nmap il three-way-handshake, stabilendo di fatto una connessione rilevabile.



Infine, con il comando **-A**, nMap esegue una scansione completa di tutte le porte e i servizi aperti sulla macchina, fornendo quindi una vasta scelta di opzioni per un eventuale attacco. Tale comando, però, risulta essere molto invasivo, permettendo di fatto a chi è in ascolto sulla rete di individuare l'azione di port-scanning che si sta eseguendo.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ nmap -A -p0-1023 192.168.32.105  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:31 EDT  
Nmap scan report for 192.168.32.105  
Host is up (0.00014s latency).  
Not shown: 1012 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_ftp-syst:  
|_STAT:  
|_FTP server status:  
|_Connected to 192.168.32.100  
|_Logged in as ftp  
|_TYPE: ASCII  
|_No session bandwidth limit  
|_Session timeout in seconds is 300  
|_Control connection is plain text  
|_Data connections will be plain text  
|_vsFTPd 2.3.4 - secure, fast, stable  
|_End of status  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
|_ssh-hostkey:  
|_1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)  
|_2048 5656240f211ddea72bae61b1243de8f3 (RSA)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
|_smtp-command: metaspoitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCO  
DES, 8BITIME, DSN  
|_sslv2:  
|_SSLv2 supported  
|_ciphers:
```

```
kali@kali: ~  
File Actions Edit View Help  
|_SSLv2 supported  
|_ciphers:  
|_SSL2_RC2_128_CBC_WITH_MD5  
|_SSL2_DES_64_CBC_WITH_MD5  
|_SSL2_RC4_128_WITH_MD5  
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5  
|_SSL2_DES_192_EDE3_CBC_WITH_MD5  
|_SSL2_RC4_128_EXPORT40_WITH_MD5  
53/tcp    open  domain       ISC BIND 9.4.2  
|_dns-nsid:  
|_bind.version: 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
|_http-title: Metasploitable2 - Linux  
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  
111/tcp    open  rpcbind      2 (RPC #100000)  
|_rpcinfo:  
|_program version port/proto service  
|_100000 2 111/tcp rpcbind  
|_100000 2 111/udp rpcbind  
|_100003 2,3,4 2049/tcp nfs  
|_100003 2,3,4 2049/udp nfs  
|_100005 1,2,3 34177/tcp mountd  
|_100005 1,2,3 38661/udp mountd  
|_100021 1,3,4 49113/tcp nlockmgr  
|_100021 1,3,4 55222/udp nlockmgr  
|_100024 1 34638/udp status  
|_100024 1 39020/tcp status  
139/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp    open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)  
512/tcp    open  exec         netkit-rsh rshd  
513/tcp    open  login?       netkit-rsh rexecd  
514/tcp    open  shell        Netkit rshd
```



```

kali@kali: ~
File Actions Edit View Help
| 100021 1,3,4 55222/udp nlockmgr
| 100024 1 34638/udp status
| 100024 1 39020/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 2h00m05s, deviation: 2h49m52s, median: -1s
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-05-18T09:32:46-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.14 seconds

kali@kali:~$

```

13831 1890.2283256.. 192.168.32.105	192.168.32.100	HTTP	1152 HTTP/1.1 200 OK (text/html)
13832 1890.2283257.. 192.168.32.105	192.168.32.100	TCP	66 80 - 43826 [FIN, ACK] Seq=1087 Ack=19 Win=5792 Len=0 TSval=369062 TSecr=2386065492
13833 1890.2283431.. 192.168.32.100	192.168.32.105	TCP	66 43826 - 80 [ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=2386065593 TSecr=369062
13834 1890.2690404.. 192.168.32.100	192.168.32.105	Portmap	110 V46632025 proc=0 Call (Reply In 13845)
13835 1890.2690904.. 192.168.32.100	192.168.32.105	RSTAT	110 V123324797 proc=0 Call (Reply In 13846)
13836 1890.2691334.. 192.168.32.100	192.168.32.105	FTP	70 Request: AUTH TLS
13837 1890.2691446.. 192.168.32.100	192.168.32.105	RPC	110 Continuation
13838 1890.2691549.. 192.168.32.100	192.168.32.105	NFS	110 V114534903 proc=0 Call (Reply In 13848)
13839 1890.2692692.. 192.168.32.100	192.168.32.105	TCP	66 43826 - 80 [ACK] Seq=19 Ack=1088 Win=64128 Len=0 TSval=2386065544 TSecr=369062
13840 1890.2697904.. 192.168.32.105	192.168.32.100	TCP	66 111 - 33510 [ACK] Seq=1 Ack=45 Win=5792 Len=0 TSval=369066 TSecr=2386065544

Segue una tabella riassuntiva di tutti i dati raccolti

Kali (192.168.32.100)	-sS scan	-sT scan	-A Scan
Metasploitable (192.168.32.105)	12 porte aperte, 12 servizi	12 porte aperte, 12 servizi, SYN/ACK completato	12 porte aperte, con analisi specifiche di esse e dei servizi ad esse collegate.