## **Nmap Scan**

Nmap (port scanner) è un tool essenziale per gli ethical hacker. Viene usato per scoprire I "host" e "services" sul computer network, inviando I pacchetti e analizzando le risposte. Nmap ha tante opzioni che possiamo controllare inviando al terminal "nmap" o "nmap –help" per I dettagli profonditi possiamo leggere anche il manual del nmap scrivendo "man nmap".

## Obbiettivo di oggi:

- 1. Scansione TCP sulle porte well-known
- 2. Scansione SYN sulle porte well-known
- 3. Scansione Aggressiva sulle porte well-known

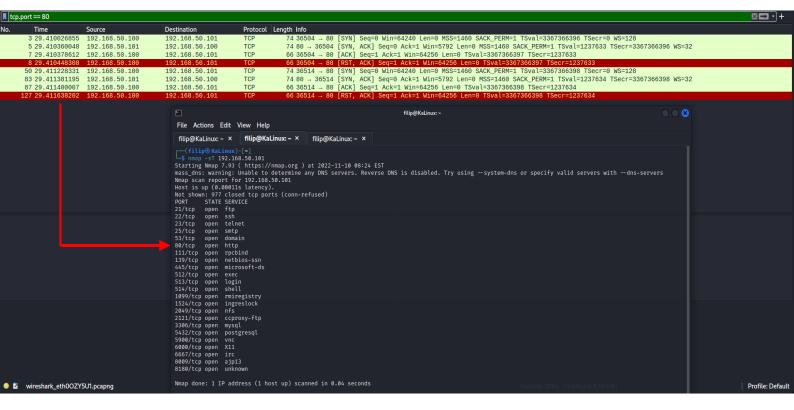
Tools: VM Kali Linux (Wireshark Nmap), Metasploitable

Apriamo le 2 Virtual machines, kali e metasploitable, sul Kali apriamo il terminal e scriviamo "wireshark" per aprire il Wireshark e iniziamo a catturare i pacchetti. Apriamo il nuovo terminal e scriviamo "nmap -sT 192.168.50.101" (-sT = TCP connect scan) per scansionare in default le 1000 port più usate.

Per analizzare meglio il risultato applicheremo il filtro sul Wireshark "tcp.port == 80"

## Il risultato:

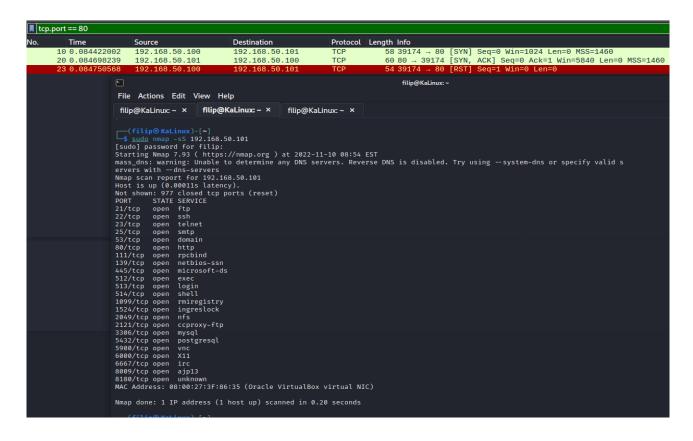
Si può vedere il three-way handshake tra kali e meta, con la finale del reset [RST], quindi questa port è aperta.



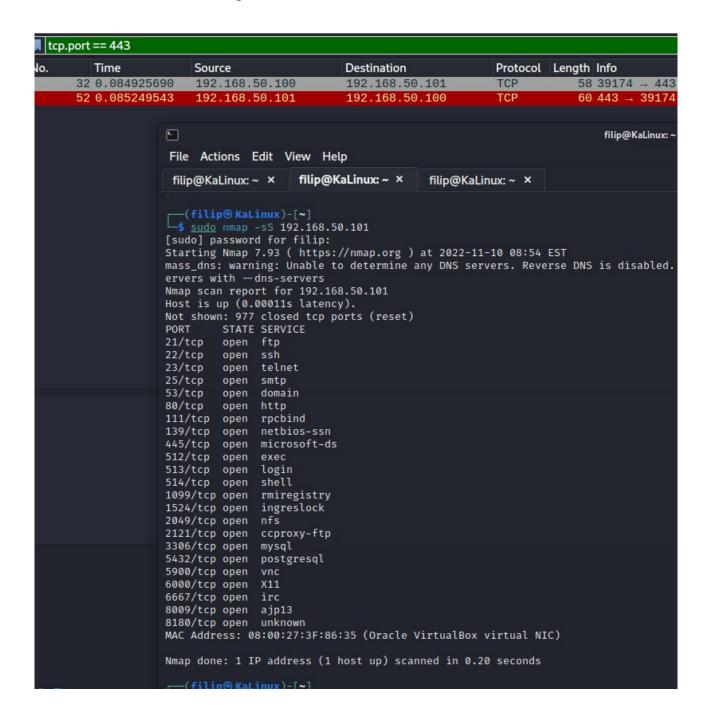
Se invece filtriamo il port 443, possiamo vedere che la Three-way handshake non cè perche la Metasploitable ha inviato subito [RST], infatti sul terminal la port 443 non è presente.

tcp.	port == 443							
No.	Time	Source	Destination		Length Info			
	4 29.410056410	192.168.50.100	192.168.50.101	TCP				4240 Len=0 MSS=146
		192.168.50.101	192.168.50.100	TCP				Ack=1 Win=0 Len=0
		192.168.50.100	192.168.50.101	TCP				4240 Len=0 MSS=146
	20 29.410914659		192.168.50.100	ТСР		File Action filip@KaLin Not shown PORT 21/tcp 22/tcp 23/tcp 25/tcp	seq=1 // ss Edit sux: ~ × 1: 977 STATE open open open open	View Help  filip@KaLinux: ~ ×  closed tcp ports SERVICE ftp ssh telnet
						53/tcp 80/tcp 111/tcp 139/tcp 445/tcp 512/tcp 513/tcp 514/tcp 1099/tcp 1524/tcp 2049/tcp 2121/tcp	open open open open open open open open	http rpcbind netbios-ssn microsoft-ds exec login shell rmiregistry ingreslock nfs ccproxy-ftp
						3306/tcp 5432/tcp 5900/tcp 6000/tcp 6667/tcp 8009/tcp 8180/tcp	open open open open open open	mysql postgresql vnc X11 irc ajp13 unknown

Il prossimo scan da fare è il SYN scan, con il comando "sudo nmap -sS 192.168.50.101". A differenza di prima possiamo vedere che Kali inizia la TCP three-way handshake, visto che la port è aperta, Metasploitable risponde con SYN-ACK, però questa volta Kali non risponde con ACK perché sa già che la port è aperta visto che ha avuto la risposta SYN-ACK e quindi risponde con RST per non creare la connessione.



Se filtriamo di nuovo la port 443, possiamo vedere ancora una volta che Metasploitable ha chiuso subito la connessione con la flag [RST]



Ultimo scan che faremmo è Aggressive scan, ovvero lo scan che ci fa ottenere piu informazioni quindi il comando che useremo sarà "sudo nmap -A 192.168.50.101"

Qui a differenza di prima possiamo vedere anche la versione del SERVICE

```
filip@KaLinux: ~
File Actions Edit View Help
 filip@KaLinux: ~ ×
                  filip@KaLinux: ~ ×
                                     filip@KaLinux: ~ ×
  —(filip⊛KaLinux)-[~]
 -$ nmap -A 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 09:14 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is d
Nmap scan report for 192.168.50.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2
                           vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
  ftp-syst:
   STAT:
  FTP server status:
       Connected to 192.168.50.100
       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-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000,
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
 _http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
 rpcinfo:
   program version port/proto service
                                  rpcbind
    100000 2 111/tcp
100000 2 111/udp
                                   rpcbind
    100003 2,3,4
                        2049/tcp
    100003 2,3,4
                        2049/udp
```

anche il Sistema Operativo

```
Host script results:
| smb-os-discovery:
   OS: Unix (Samba 3.0.20-Debian)
   Computer name: metasploitable
   NetBIOS computer name:
   Domain name: localdomain
   FQDN: metasploitable.localdomain
  System time: 2022-11-10T09:15:00-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 0000000000000 (Xerox)
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
| smb-security-mode:
   account_used: guest
   authentication_level: user
   challenge_response: supported
| message_signing: disabled (dangerous, but default)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.25 seconds
```

No.	▼ Time	Source	Destination	Protocol L	enath Info					
	2156 4.064013535	192.168.50.101	192.168.50.100	TCP	74 [TCP Retransmission] 80 - 44486 [SYN, ACK] Seg=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM=1 TSval=1537839 TSecr=3370365685 WS=5					
	2157 4.064028982	192.168.50.100	192.168.50.101	TCP	66 TCP Dup ACK 2081#1 44486 - 80 ACK Seq=1 Ack=1 Win=64256 Len=0 TSval=3370369679 TSecr=1537439					
	2158 4.084547846	PcsCompu_3f:86:35	Broadcast	ARP	60 Who has 192.168.50.1? Tell 192.168.50.101					
	2159 5.085354106	PcsCompu_3f:86:35	Broadcast	ARP	60 Who has 192.168.50.1? Tell 192.168.50.101					
	2160 6.080103926	192.168.50.100	192.168.50.101	SMTP	72 C: EHLO					
		192.168.50.100	192.168.50.101	TELNET	70 Telnet Data					
	2162 6.080145626	192.168.50.100	192.168.50.101	DNS	98 Standard query 0x0006 TXT version.bind					
	2163 6.080151532	192.168.50.100	192.168.50.101	HTTP	84 GET / HTTP/1.0					
		192.168.50.100	192.168.50.101	Portmap	110 V104316 proc-0 Call (Reply In 2192)					
	2165 6.080167994	192.168.50.100	192.168.50.101	SMB	234 Negotiate Protocol Request					
	2166 6.080175267	192.168.50.100	192.168.50.101	NBSS	84 NBSS Continuation Message					
1	2167 6.080181677	192.168.50.100	192.168.50.101	EXEC	98 Client -> Server data					
		192.168.50.100	192.168.50.101	Rlogin	98 Start Handshake					
		192.168.50.100	192.168.50.101	RSH	84 Client -> Server data					
		192.168.50.100	192.168.50.101	RMI	73 JRMI, Version: 2, StreamProtocol					
		192.168.50.100	192.168.50.101	Portmap	110 V104316 proc-0 Call (Reply In 2201)					
		192.168.50.100	192.168.50.101	TCP	70 51104 - 2121 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4 TSval=3370371695 TSecr=1537439					
		192.168.50.100	192.168.50.101	TCP	70 44466 - 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4 TSval=3370371695 TSecr=1537439 [TCP segment of a reassembled PDU]					
	2174 6.080239105	192.168.50.100	192.168.50.101	TCP	70 33560 → 5432 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4 TSval=3370371695 TSecr=1537439 [TCP segment of a reassembled PDU]					
	2175 6.080262031		192.168.50.101	TCP	88 51002 - 6000 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=22 TSval=3370371695 TSecr=1537439 [TCP segment of a reassembled PDU]					
	2176 6.080272644	192.168.50.100	192.168.50.101	TCP	84 48058 - 8009 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=18 TSval=3370371695 TSecr=1537440 [TCP segment of a reassembled PDU]					
	0477 6 000004400	400 400 F0 400	400 400 50 404	TAB	70 MCCO 0400 [DOM ACC] 00-04 Asked Microsoft Land TOWN 2007007400F TOWN 4507440					
	Source Port: 5485									
	Destination Port:									
	[Stream index: 10		TTU DATA (04)3							
		pleteness: Complete, V	NITH_DATA (31)]							
	[TCP Segment Len:									
	Sequence Number: 1 (relative sequence number)									
	Sequence Number (raw): 181702157									
	[Next Sequence Number: 5 (relative sequence number)]									
	Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 219724086									
		mber (raw): 219/24086 r Longth: 22 hytoc (9)								
		35 08 00 27 c0 5a c9		'.ZE						
	9919 99 38 4c 89 49 90 49 96 98 1d c0 a8 32 64 c0 a8 -81 -81 -81 -91 2d									
	9020 32 65 d6 4a 90 17 9a d4 8e 9d 9d 18 b9 36 80 18 2e 3 · · · · · · 6 · ·									
		00 01 01 08 0a c8 e3								
	0 75 9f 0d 0a 0d	0a								

					1				
Fonte dello	Targe	Tipo	Port	Port	Numero di	Numero di	Versione	Numero di	Tempo per finire
scan	t	di	apert	chius	versioni di	versioni di	del	pacchetti catturati	lo scan in secondi
	dello	scan	e	e	servizi	servizi non	sistema	con Wireshark	
	scan				identificati	identificati	operativo		
Kali	Meta	-sT	23	977	22	1	No	~2054	0.04
Kali	Meta	-sS	23	977	22	1	No	~2025	0.20
Kali	Meta	-A	23	977	23	/	Si	~4488	126.25