Report sulle Scansioni di Rete Utilizzando Nmap

In questa analisi, ho eseguito una serie di scansioni su Metasploitable all'indirizzo IP 192.168.100.101 utilizzando Nmap. Le scansioni effettuate includono:

1. Scansione TCP (-sT)
2. Scansione SYN (-sS)
3. Scansione Completa con Nmap -A

Per esportare i risultati delle scansioni, ho utilizzato lo switch `-oX` per salvare l'analisi in file XML, facilitandone la consultazione come report. Durante le scansioni, ho utilizzato un programma di sniffing, WiredShark, per monitorare i pacchetti scambiati tra Nmap (eseguito su 192.168.50.100,ossia Kali) e Metasploitable. È importante notare che le due macchine si trovavano su reti diverse, configurate tramite PfSense.

Configurazione della Rete:

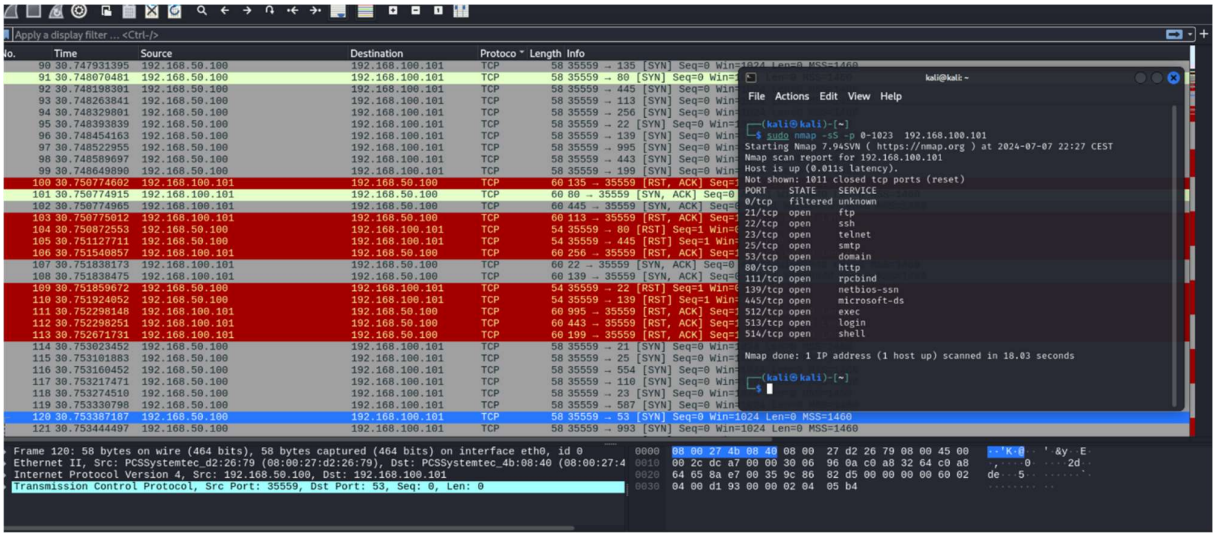
Per collegare le due macchine su reti diverse, ho utilizzato l'impostazione di due gateway su PfSense. I gateway sono stati impostati come segue:

- Gateway per Kali Linux: 192.168.50.100
- Gateway per Metasploitable: 192.168.100.101

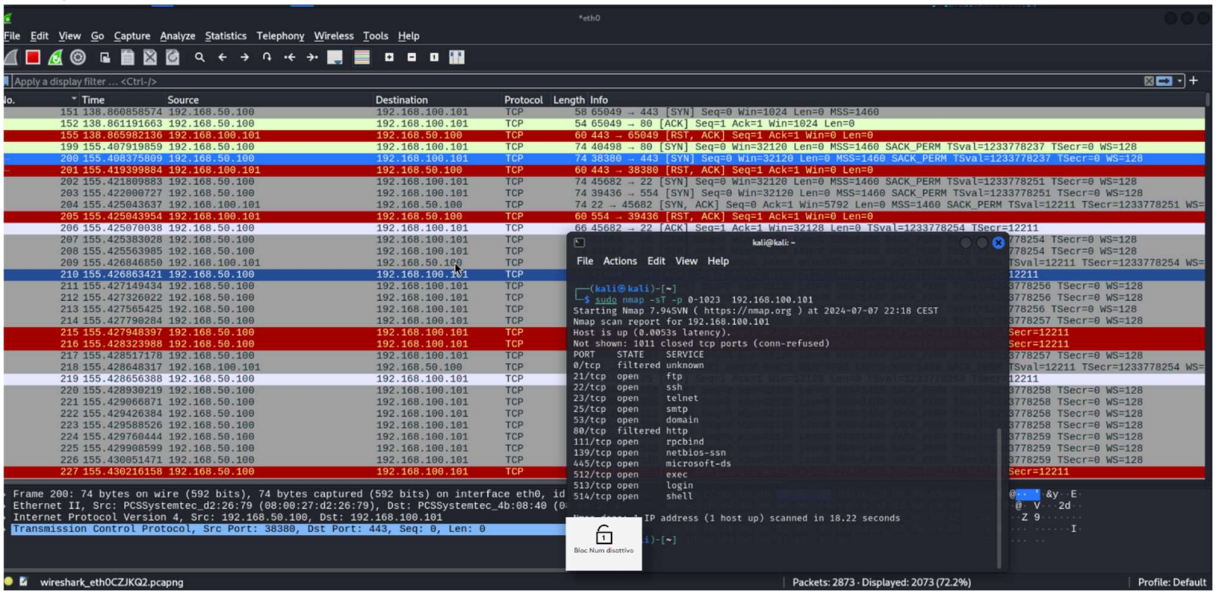
Per filtrare la porta, ho configurato un firewall su PfSense che bloccasse l'IP di Kali (192.168.50.100) dalla comunicazione HTTP verso l'IP di Metasploitable (192.168.100.101).

Metodi di Scansione Dettagliati:

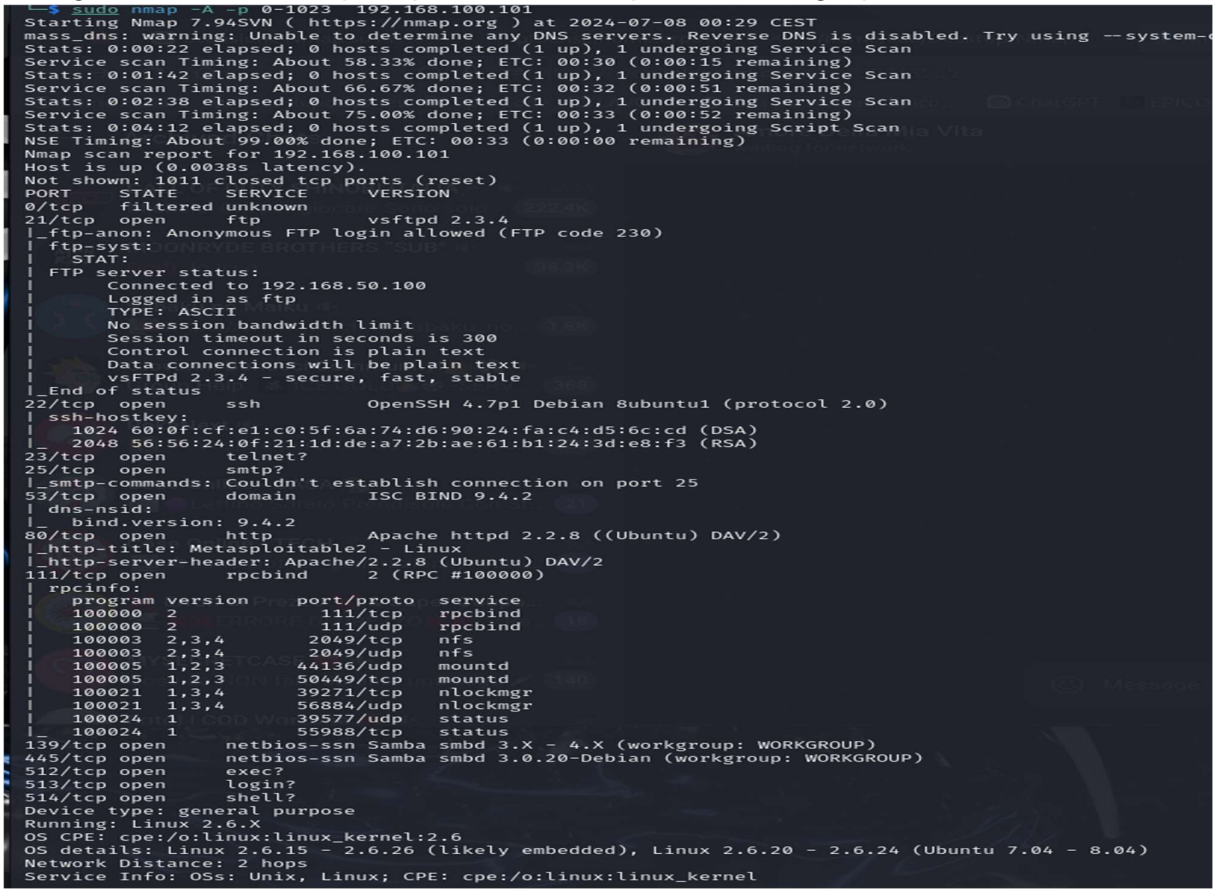
- Scansione SYN (-sS): Durante una scansione SYN, come osservato in Wireshark, viene inviata una richiesta per avviare la sessione TCP (Three-Way Handshake). Se la macchina TARGET risponde al SYN, indicando che la porta è aperta, Nmap invia un flag RST per interrompere la connessione, rendendo questo metodo più furtivo e veloce.



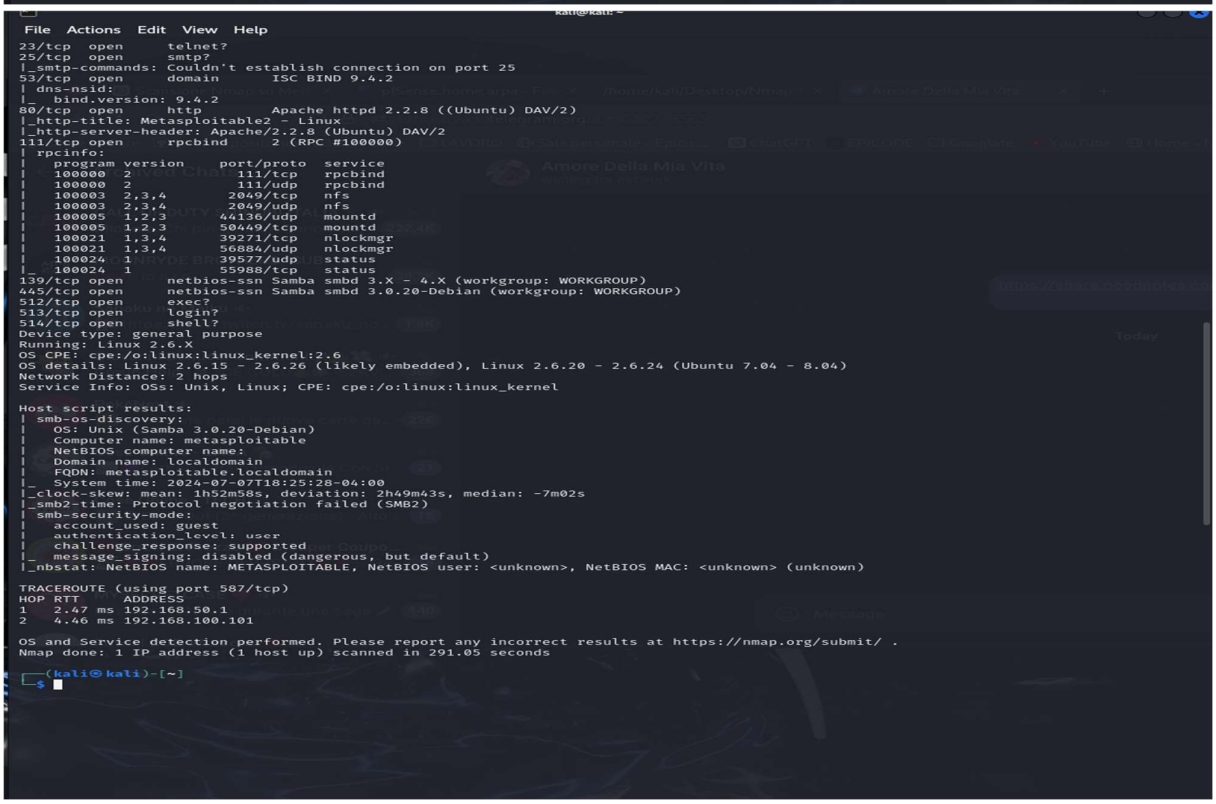
- Scansione TCP Connect (-sT): Questa scansione è analoga alla scansione SYN, ma in questo caso il Three-Way Handshake viene completato, rendendola meno furtiva ma più completa.



- Scansione Aggressiva (-A): Questa scansione fornisce un'analisi più approfondita, dettagliando anche nel report quale software è presente su ogni porta e la sua versione.



```
└─$ sudo nmap -A -p 0-1023  192.168.100.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 00:29 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.33% done; ETC: 00:30 (0:00:15 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 00:32 (0:00:51 remaining)
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 00:33 (0:00:52 remaining)
Stats: 0:04:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.00% done; ETC: 00:33 (0:00:00 remaining)
Nmap scan report for 192.168.100.101
Host is up (0.00038s latency).
Not shown: 1011 closed tcp ports (reset)
PORT    STATE    SERVICE     VERSION
0/tcp   filtered unknown
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 192.168.50.100
|      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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open     telnet?
25/tcp  open     smtp?
|_smtp-commands: Couldn't establish connection on port 25
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      44136/udp   mountd
|   100005  1,2,3      50449/tcp   mountd
|   100021  1,3,4      39271/tcp   nlockmgr
|   100021  1,3,4      56884/udp   nlockmgr
|   100024  1          39577/udp   status
|_  100024  1          55988/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?
513/tcp open     login?
514/tcp open     shell?
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



```
File  Actions  Edit  View  Help
23/tcp  open     telnet?
25/tcp  open     smtp?
|_smtp-commands: Couldn't establish connection on port 25
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      44136/udp   mountd
|   100005  1,2,3      50449/tcp   mountd
|   100021  1,3,4      39271/tcp   nlockmgr
|   100021  1,3,4      56884/udp   nlockmgr
|   100024  1          39577/udp   status
|_  100024  1          55988/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?
513/tcp open     login?
514/tcp open     shell?
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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: 2024-07-07T18:25:28-04:00
|_clock-skew: mean: 1h52m58s, deviation: 2h49m43s, median: -7m02s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE (using port 587/tcp)
HOP RTT     ADDRESS
1   2.47 ms 192.168.50.1
2   4.46 ms 192.168.100.101

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 291.05 seconds

┌──(kali㉿kali)-[~]
└─$
```

Esecuzione delle Scansioni:

I comandi utilizzati per eseguire le scansioni sono stati:

sudo nmap -sT (variato con -sS o -A per le diverse scansioni) -p 0-1025 (range porte conosciute)-oX file.xml <IP macchina target>

Modifiche alla Configurazione del Firewall:

Ho anche testato variazioni nella configurazione del firewall sulla rete di Metasploitable 2. In particolare, ho configurato il firewall per filtrare la porta 80. Ho quindi eseguito due scansioni: una con la porta 80 aperta e un'altra con la porta 80 filtrata dal firewall. I risultati sono stati salvati in due file XML separati, che ho poi confrontato utilizzando il comando:

ndiff ss.xml ss2.xml > confronto.xml

Questo comando evidenzia e filtra i cambiamenti nello stato delle porte, fornendo una chiara visione della variazione di stato delle porte della macchina Target.

Report e File XML

Questo report in formato PDF includerà immagini per mostrare l'uso di Wireshark, lo sniffer utilizzato durante le scansioni con le opzioni `-sS` e `-sT`. Oltre al PDF, i file XML contenenti i vari report delle scansioni saranno caricati su una repository, permettendo una consultazione dettagliata e approfondita dei risultati delle scansioni.