Network Scanning con Nmap

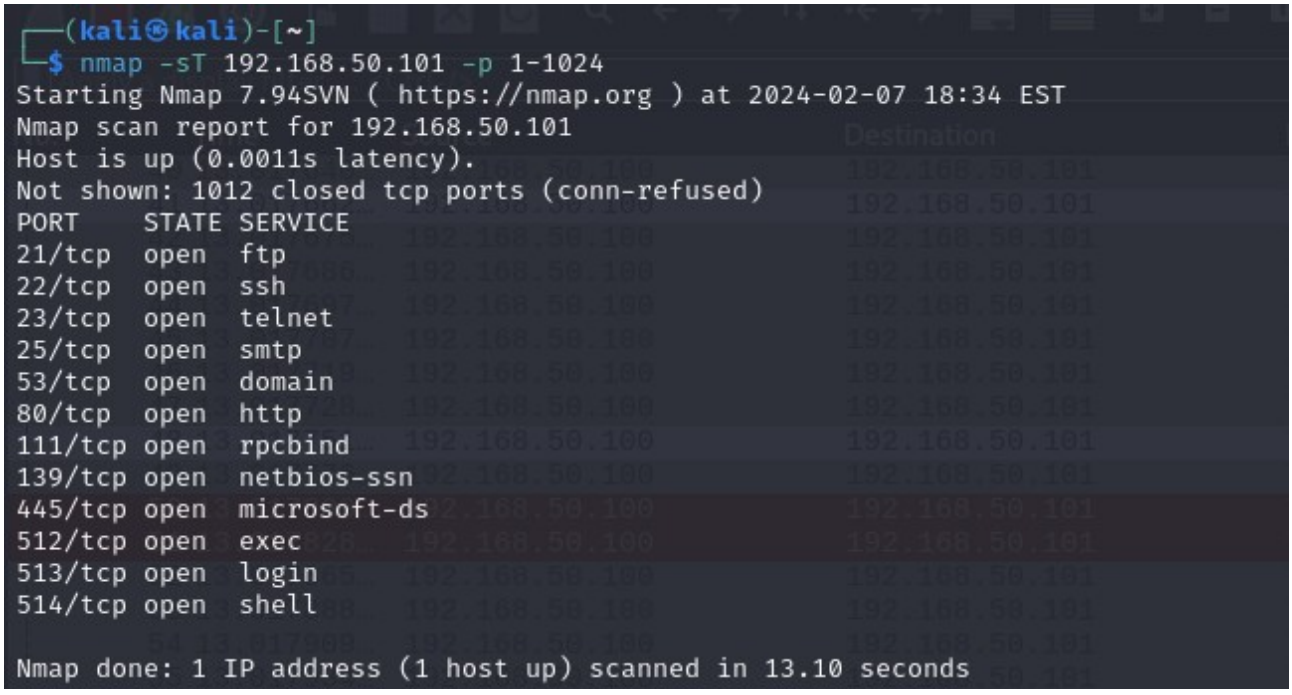
Nmap e un port scanner , o vero e un Tool che mette a disposizione Kali Linux in grado di detterminare quali porte sono in ascolto /aperte su una determinata macchina bersaglio.

Vedremo ora in dettaglio due tipi di scansione che utilizzano la trasmissione di pacchetti TCP .

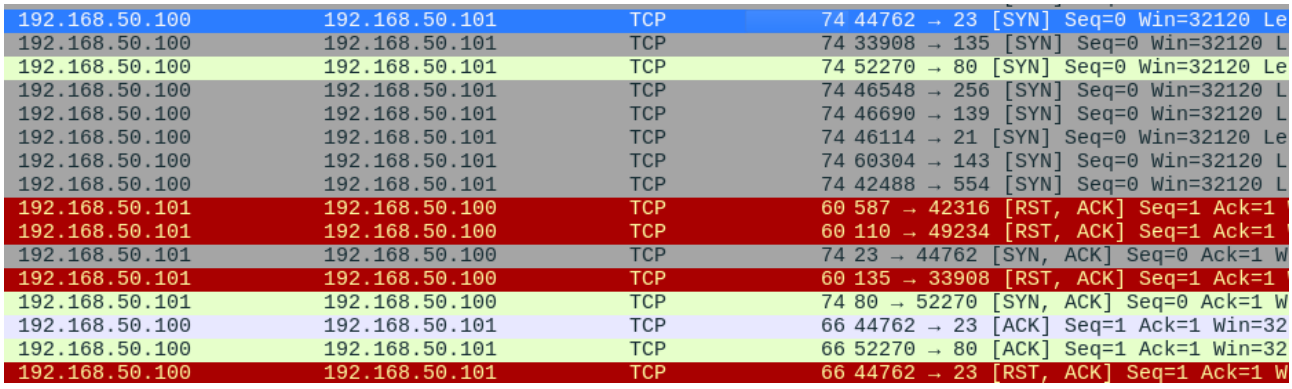
La prima scansione che andremmo ad effettuare e la scansione tramite il comando(nmap -sT IP Target -p 1-1024). Il comando -sT e una scansione piu invasiva in quanto sfrutta la 3 way handshake o vero il client inviera un pacchetto SYN verso il target su una porta compresa nel range, se la porta e aperta ricevera in risposta un SYN/ACK, la se sequenza continuera con la creazione di un canale di comunicazone.

Dimostrazione:

Vediamo come dopo la scansione output che esce ci mostra le porte con i relativi servizi attivi:



Analizziamo ora il traffico di rete durante la scansione porte



Prendiamo in esame la porte 23, notiamo subito come il client sonda la porta del target inviandole un SYN e come la porta a dimostrazione che e aperta risponde al messaggio con un SYN ,ACK e il client instaura il canale di comunicazione (che poco dopo

verra interrotto) inviando al target un ACK . Questa scansione e facilmente rilevabile proprio a causa del 3 way handshak che anche se per un breve periodo va ad utilizzare la porta libera che sta scansionando.

Per la seconda scansione utilizzeremo il comando (nmap -sS IP Target -p 1-1024) dove -sS indica la scansione SYN

La seconda scansione e molto piu leggera , in quanto il processo si limita a contattare la porta del target inviandole un SYN e non appena riceve un SYN/ACK la trasmissione viene immediatamente interrotta (l interuzione avviene tramite l invio di un RST dal client verso la porta del target)

Dimostrazione:

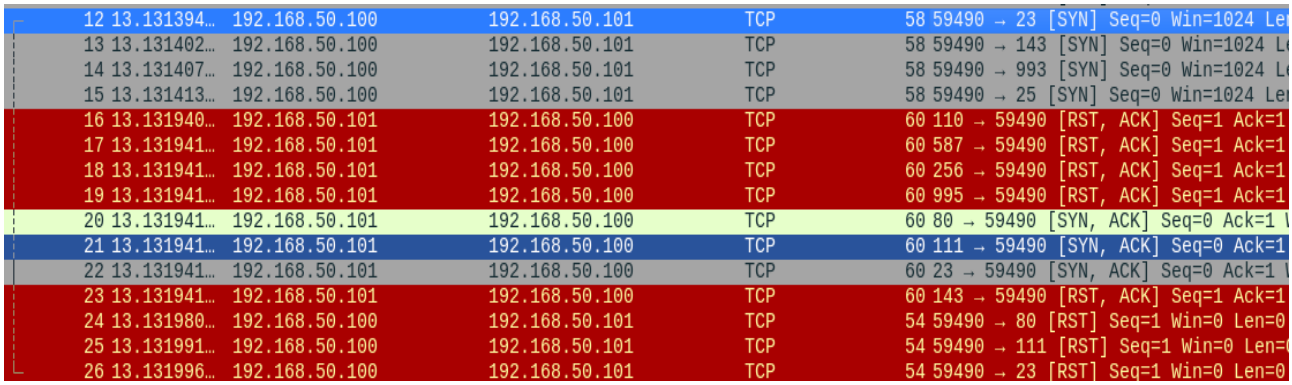
osserviamo attentamente l output che esce in risposta al comando

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 19:08 EST
Nmap scan report for 192.168.50.101
Host is up (0.00018s 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: 08:00:27:48:A0:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

La scansione crea meno latenza a dimostrazione del fatto che e piu “leggera” rispetto la precedente

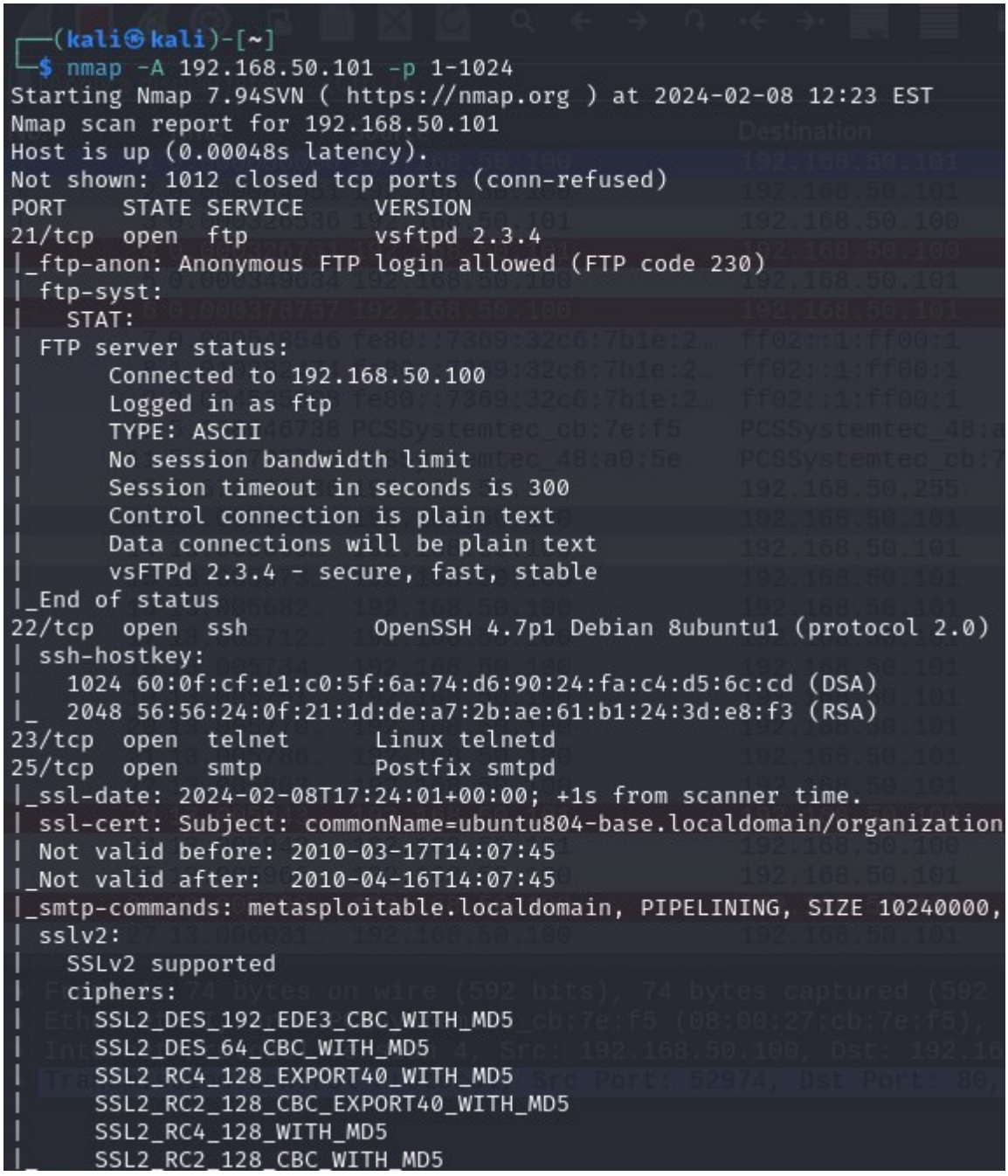
Vediamo da vicino il traffico dati che si crea durante la scansione:



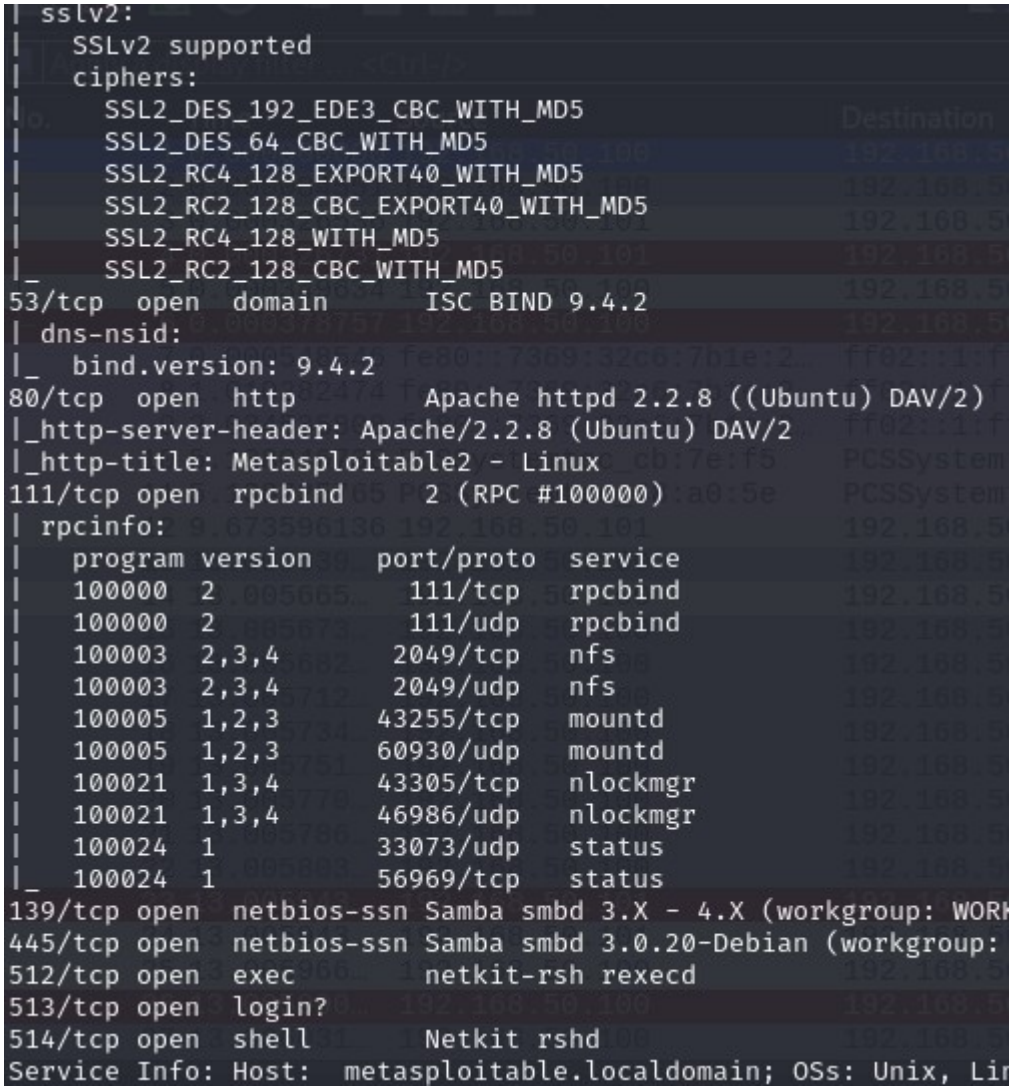
Prendiamo in esame sempre la porta 23 . Possiamo notare come i primi due passaggi SYN , SYN/ACK siano esattamente identici . A cambiare infatti e il 3

passaggio , dove non troviamo piu come risposta ACK con la creazione di conseguenza di un “anche se breve” canale di comunicazione , ma ben si un pacchetto RST . Il pacchetto RST che invia il client verso il target e un messaggio di stop (abbiamo capito che la porta e aperta) evitando cosi il 3 way handshake citato prima.

Osserviamo in fine l ultima scansione che prevede il comando (nmap -A IP Target -p 1-1024). La variante -A ci restituira oltre alle porte aperte del range e i relativi servizi , informazioni dettagliate riguardo il sistema operativo del target. Questo tipo di scansione risulta piu pesante (basta guardere il suo tempo di latenza …nettamente superiore rispetto alle scansioni precedenti) e percio facilmente individuabbile.



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 12:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.00048s 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 192.168.50.100
|      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      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_ssl-date: 2024-02-08T17:24:01+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organization
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000,
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
```



```
|  sslv2:
|    SSLv2 supported
|    ciphers:
|      SSL2_DES_192_EDE3_CBC_WITH_MD5
|      SSL2_DES_64_CBC_WITH_MD5
|      SSL2_RC4_128_EXPORT40_WITH_MD5
|      SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|      SSL2_RC4_128_WITH_MD5
|_     SSL2_RC2_128_CBC_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-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
|    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      43255/tcp   mountd
|    100005  1,2,3      60930/udp   mountd
|    100021  1,3,4      43305/tcp   nlockmgr
|    100021  1,3,4      46986/udp   nlockmgr
|    100024  1          33073/udp   status
|_   100024  1          56969/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORK
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (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, Lin
```

Fonte	Target	Tipo Scan.	Porta	Servizio	Stato
192.168.50.100	192.169.50.101	TCP	21	ftp	Open
192.168.50.100	192.168.50.101	TCP	22	ssh	Open
192.168.50.100	192.168.50.101	TCP	23	telnet	Open
192.168.50.100	192.168.50.101	TCP	25	smtp	Open
192.168.50.100	192.168.50.101	TCP	53	domain	Open
192.168.50.100	192.168.50.101	TCP	80	http	Open
192.168.50.100	192.168.50.101	TCP	111	rpcbind	Open
192.168.50.100	192.168.50.101	TCP	139	Netbios-ssn	Open
192.168.50.100	192.168.50.101	TCP	445	Microsoft-ds	Open
192.168.50.100	192.168.50.101	TCP	512	exec	Open
192.168.50.100	192.168.50.101	TCP	513	Login	Open
192.168.50.100	192.168.50.101	TCP	514	shell	Open

Scansione -sT

Fonte	Target	Tipo Scan.	Porta	Servizio	Stato
192.168.50.100	192.169.50.101	TCP	21	ftp	Open
192.168.50.100	192.168.50.101	TCP	22	ssh	Open
192.168.50.100	192.168.50.101	TCP	23	telnet	Open
192.168.50.100	192.168.50.101	TCP	25	smtp	Open
192.168.50.100	192.168.50.101	TCP	53	domain	Open
192.168.50.100	192.168.50.101	TCP	80	http	Open
192.168.50.100	192.168.50.101	TCP	111	rpcbind	Open
192.168.50.100	192.168.50.101	TCP	139	Netbios-ssn	Open
192.168.50.100	192.168.50.101	TCP	445	Microsoft-ds	Open
192.168.50.100	192.168.50.101	TCP	512	exec	Open
192.168.50.100	192.168.50.101	TCP	513	Login	Open
192.168.50.100	192.168.50.101	TCP	514	shell	Open

Scansione -sS