ESERCIZIO W9D1 PARTE 2

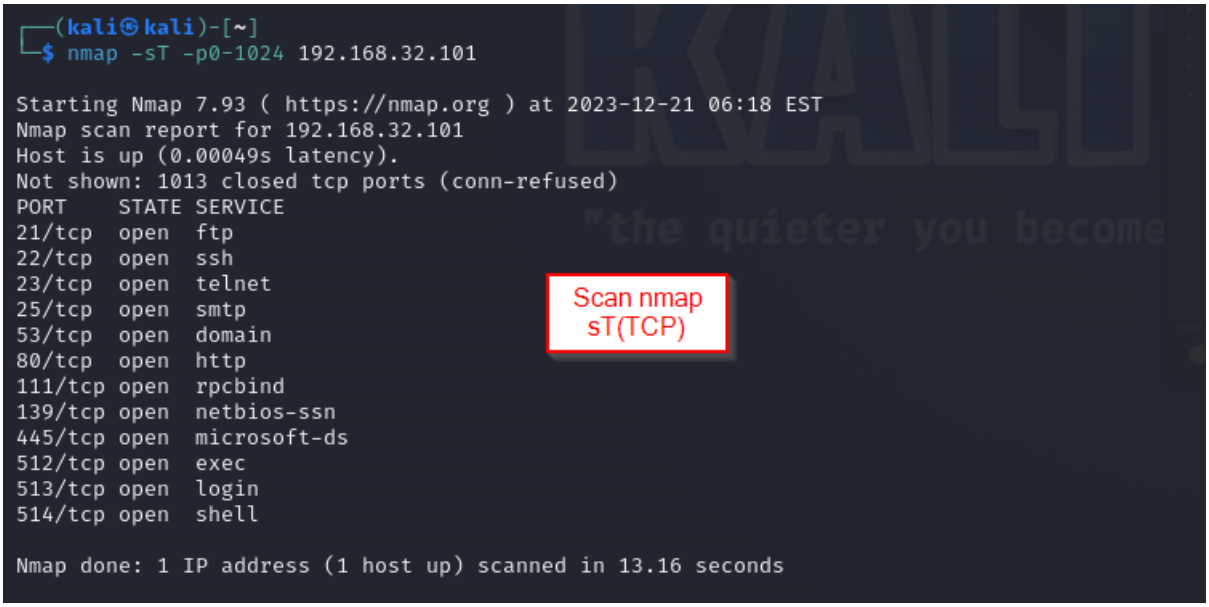
Il prossimo esercizio ci permetterà di esplorare meglio nmap e le sue funzioni. CI vengono proposte diverse traccie da portare a termine, cominciamo con la prima:

Traccia 1

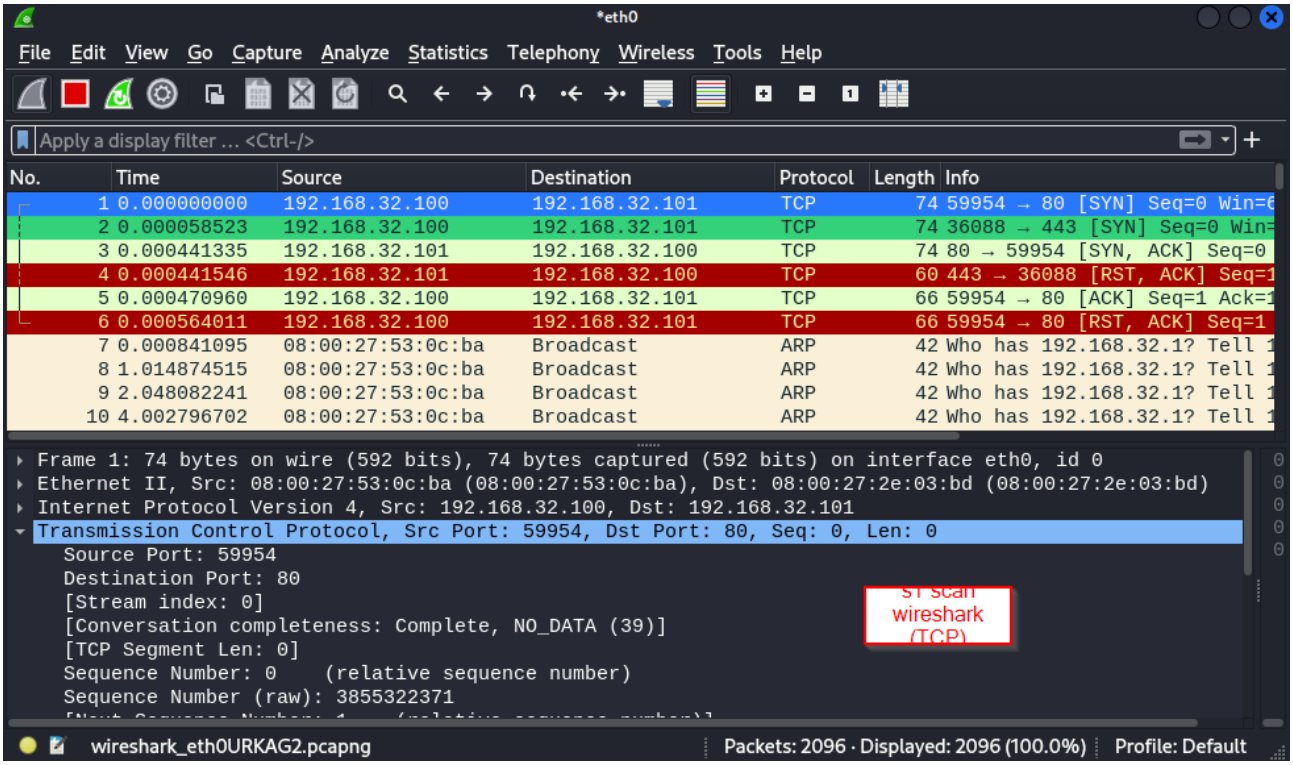
Vedremo da vicino nmap e i suoi comandi. Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulle macchine metasploitable, come di seguito:

- 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 dalle macchine sorgente con Wireshark.

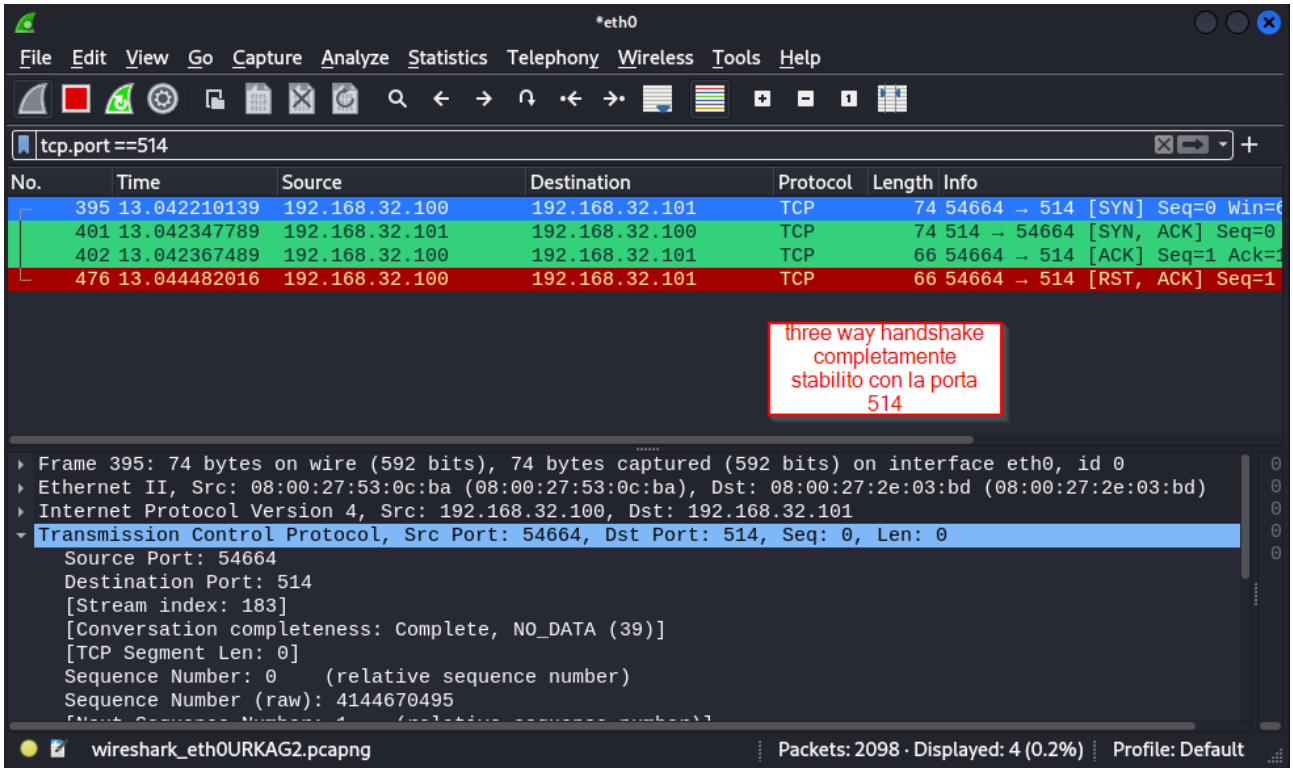
Scansione TCP sulle porte well-known



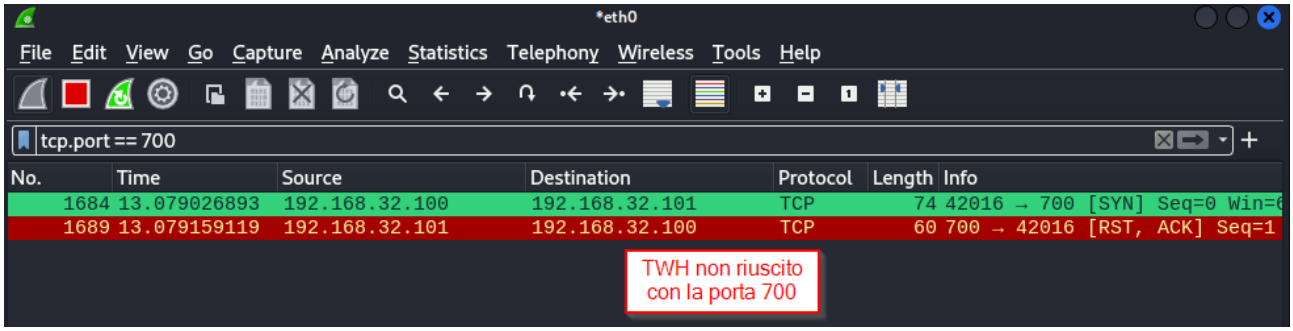
Su Kali Linux inseriamo sul terminale il comando nmap -sT -p0-1024 192.168.32.101. Il termine -sT indica che il client completerà il three way handshake, generando più rumore a livello di rete, p0-1024 definirà il range di porte di cui verificare la disponibilità, mentre l'indirizzo IPV4 (Metaploitable) rappresenterà il target in cui ricercare le porte. Nel frattempo teniamo pronto Wireshark, sulla scheda di rete eth0, per intercettare i pacchetti.



Dopo l'invio del protocollo ARP per individuare l'indirizzo MAC avente 192.168.32.101 all'interno della rete, partiranno le richieste TCP. Aiutandoci con il terminale di Linux, andiamo a scovare una delle porte individuate durante la raccolta. Inseriamo nel filtro tcp.port == 514 per controllare meglio gli scambi tra client e server.



Il nostro client (Kali Linux) genera una porta per creare un collegamento con la porta 514. Il server risponde al protocollo SYN inviato ed il tutto viene poi sincronizzato con l'ultimo ACK del client. Questo significa che la porta è disponibile all'utilizzo.



Questa invece è la situazione che concerne una porta non aperta. Il client invia il protocollo, ma non essendoci disponibilità, il server risponde direttamente con un pacchetto avente il flag reset (RST).

Scansione SYN sulle porte well-known

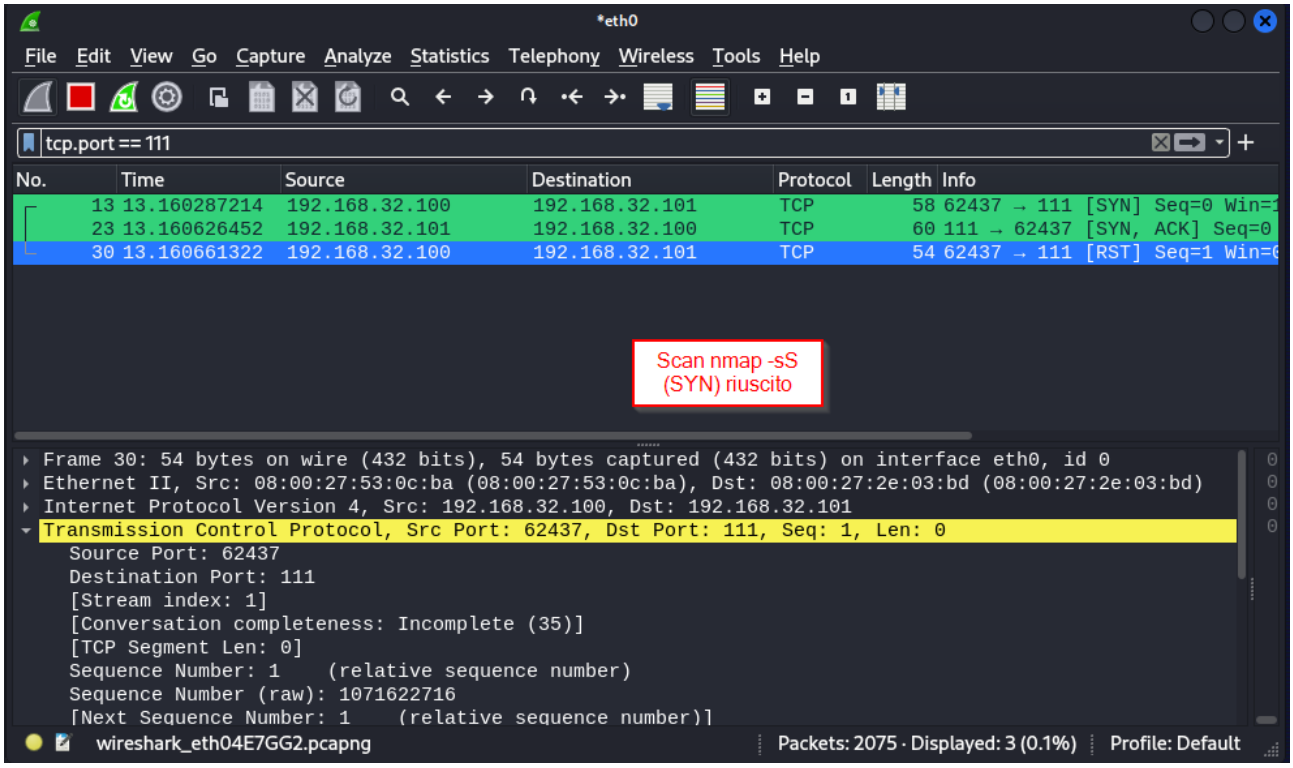
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p0-1024 192.168.32.101

Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-21 09:00 EST
Nmap scan report for 192.168.32.101
Host is up (0.00026s latency).
Not shown: 1013 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: 08:00:27:2E:03:BD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

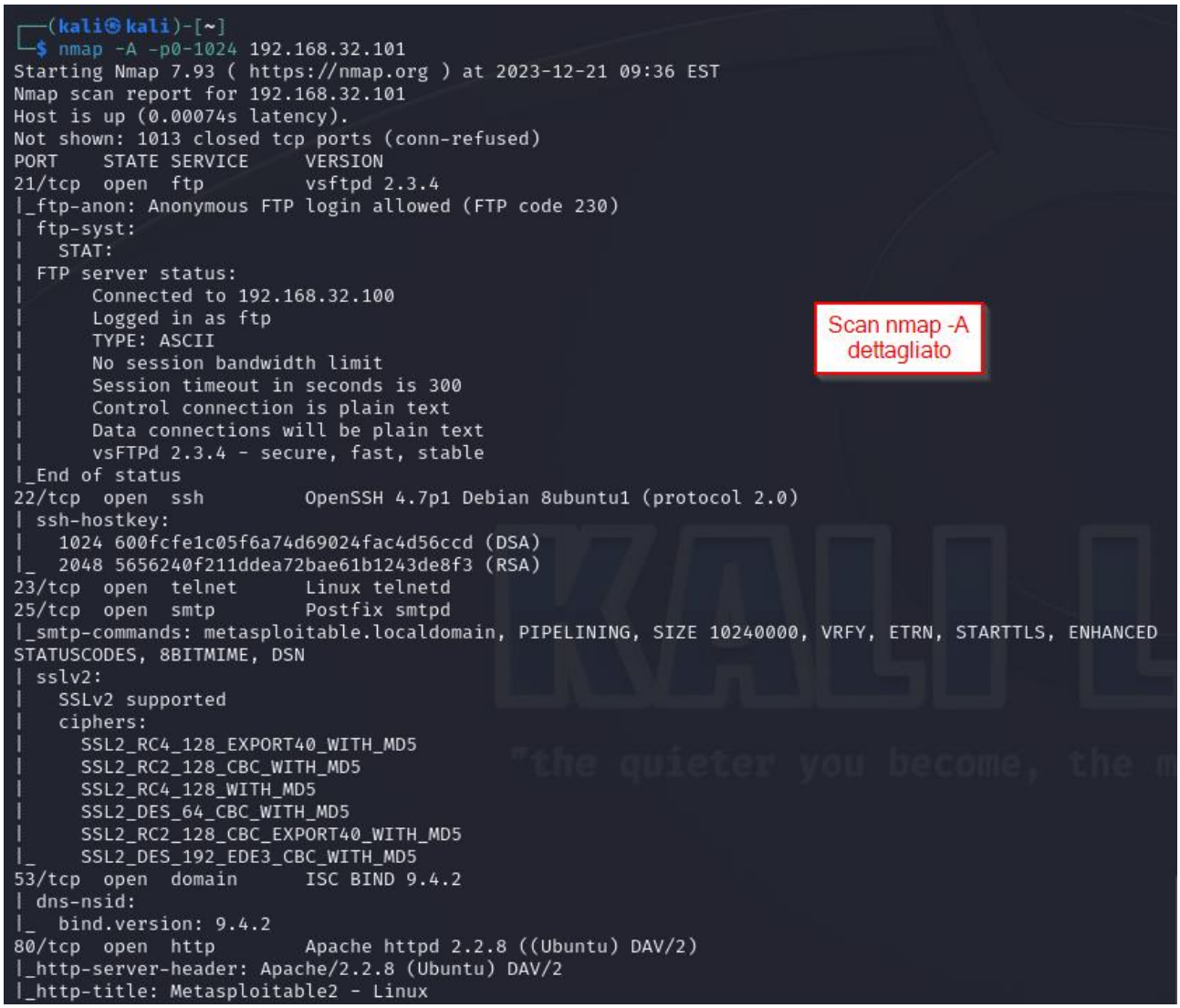
Scan -sS nmap

Per cambiare il tipo di scan ci basterà semplicemente inserire -sS invece che -sT. Lo scan di nmap con -sS è un SYN scan, una tipologia che interrompe la comunicazione del client con il server durante la fase di sincronizzazione, andando a inviare un pacchetto con il protocollo RTS. Osserviamo subito la differenza con Wireshark.

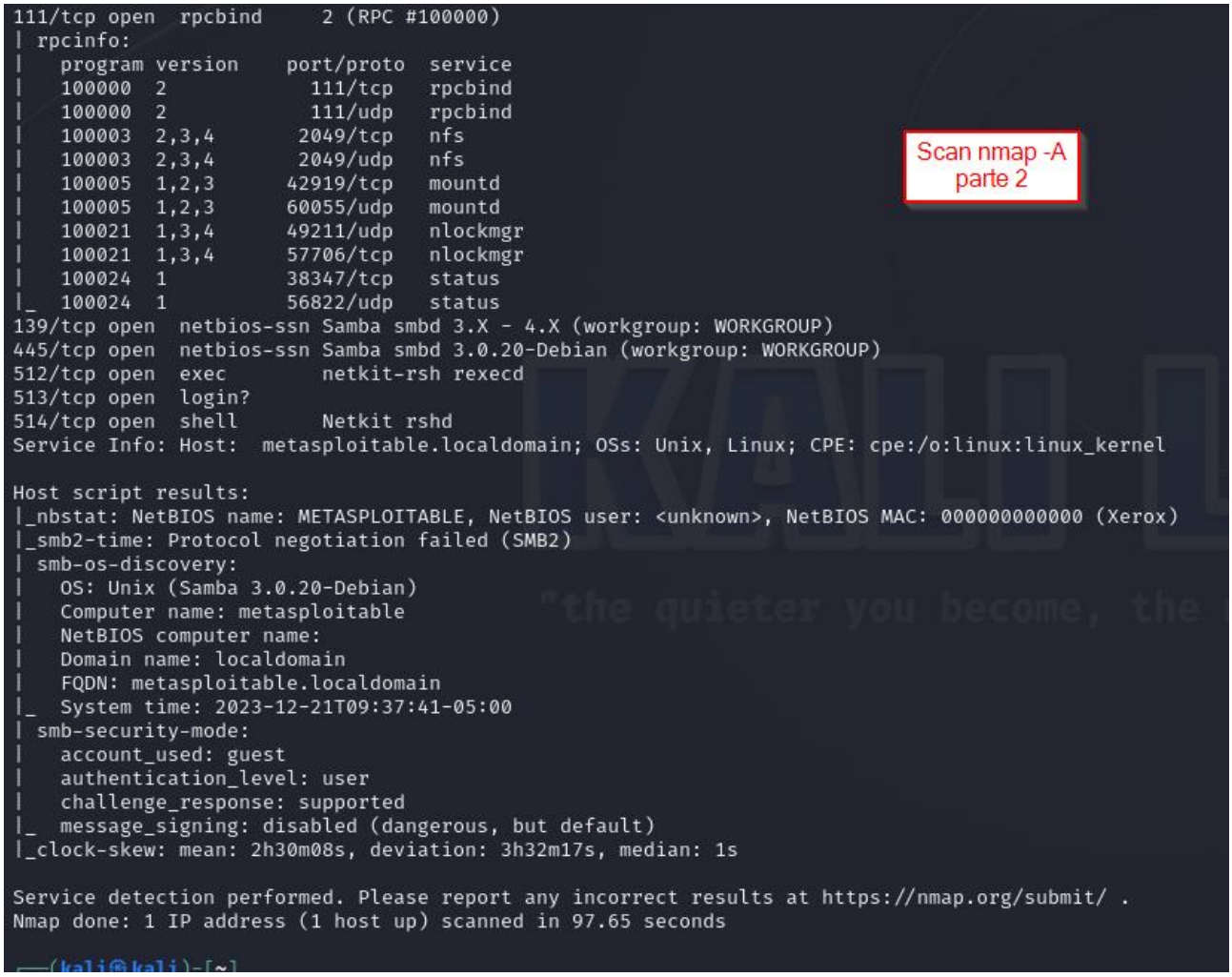


Come si può vedere dall'immagine, la terza fase di sincronizzazione viene saltata con un pacchetto finale RTS da parte del client. A differenza dello scan -st, lo scan -sS non genera il tipico overload causato da un canale di comunicazione ben stabilito.

Scansione con switch «-A» sulle porte well-known




```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p0-1024 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-21 09:36 EST
Nmap scan report for 192.168.32.101
Host is up (0.00074s latency).
Not shown: 1013 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-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCED
STATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_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
```



Lo scan nmap con lo switch -A esegue un'analisi dettagliata del sistema e di tutte le porte attive specificate nel range del comando. Ad esempio, la porta 21 appartiene al servizio FTP, il quale è dotato di uno stato, un tipo, una versione etc. Più in basso invece troviamo il target Host, il nome del computer, il nome di dominio, il livello di autenticazione etc.

Traccia 2

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alle 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).

Scan Source	Scan Target	Scan Type	Result
-OS: Kali GNU/Linux(2023.4) -IPV4: 192.168.32.100 -Tool: nmap	-OS: Unix (Samba 3.0.20-Debian) -IPV4: 192.168.32.101	-Scansione TCP(-sT)	-12 porte trovate attive ed i relativi servizi associati, come FTP, SSH, telnet, SMTP, DNS e HTTP -1 host attivo
-OS: Kali GNU/Linux(2023.4) -IPV4: 192.168.32.100 -Tool: nmap	-OS: Unix(Samba 3.0.20-Debain) -IPV4: 192.168.32.101	-Scansione SYN(-sS)	-12 porte trovate attive ed i relativi servizi associati, come FTP, SSH, telnet, SMTP, DNS e HTTP -1 host attivo -Target MAC address: 08:00:27:2E:03:BD
-OS: Kali GNU/Linux(2023.4) -IPV4: 192.168.32.100 -Tool: nmap	-OS: Unix(Samba 3.0.20-Debain) -IPV4: 192.168.32.101	-Scansione -A(dettagliata)	-12 porte trovate attive ed i relativi servizi associati, come FTP, SSH, telnet, SMTP, DNS e HTTP -1 host attivo