

Utilizzo di Nmap

Nell'esercizio ho usato nmap per scansionare le intervallo di porte (1-1024) sul machina Metasploitable

La seguente tabella indica i risultati dell'esercizio:

N	Tipo dello scan	La fonte dello scan	Il target dello scan	Risultati ottenuti
1	nmap -sT	Kali Linux IP: 192.168.1.31	Metasploitable IP: 192.168.1.35	Numero della porta, Lo stato, il tipo del servizio
2	nmap -sS	Kali Linux IP: 192.168.1.31	Metasploitable IP: 192.168.1.35	Numero della porta, Lo stato, il tipo del servizio
3	nmap -A	Kali Linux IP: 192.168.1.31	Metasploitable IP: 192.168.1.35	Numero della porta, Lo stato, il tipo del servizio, versione del servizio, maggior informazioni sul servizio e il traceroute

In seguente si trova descrizione profondato dello scan:

1- Scan -sT:

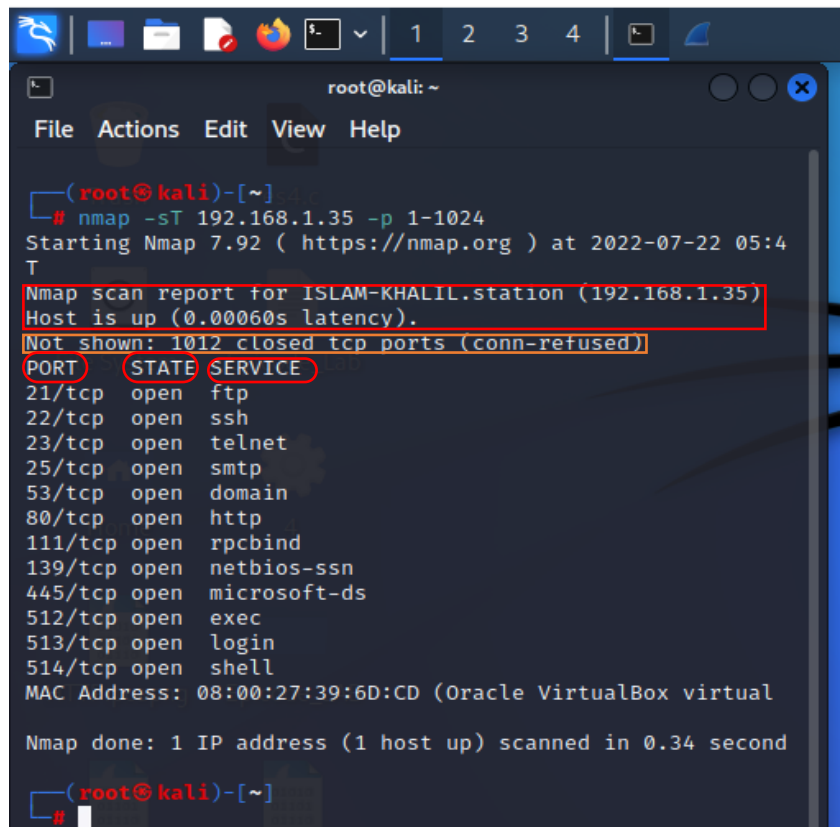
Un metodo di scansione più invasivo per farci sapere se la porta e aperta o meno in questa scansione il nmap completa tutti passaggi del (3 way hand-shake)

Come si vede dall'immagine,

la scansione -sT ci presenta,

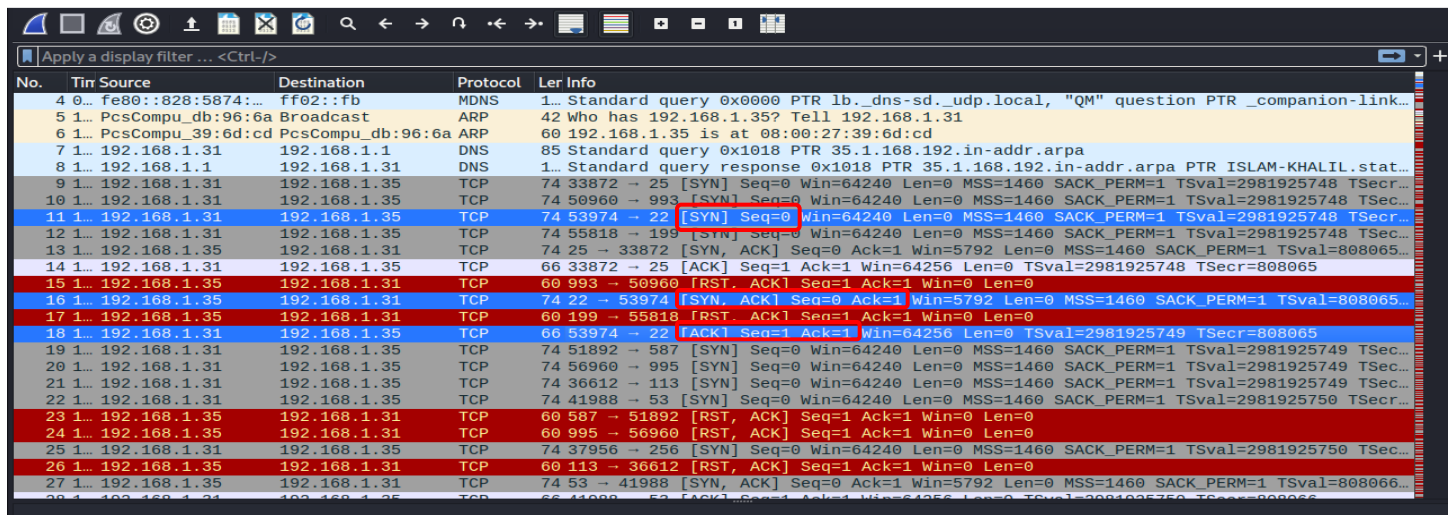
- a- Lo stato della vittima.
 - b- Numero di porte chiuse.
 - c- Le porte aperte nell'intervallo predefinito (1-1024) con il tipo di connessione (UDP/TCP).
 - d- Lo stato della porta (**aperta**/chiusa).
 - e- Il tipo del servizio su ogni porta.
- Es.

-porta: 21-ftp→File Transfer Protocol:
che ci permette di trasferire i file da una sistema ad altra tramite la rete.
-Porta:139-netbios-ssn→
viene utilizzata per la risoluzione dei nomi del sistema NetBIOS
-Porta:25-smtp→ simple mail transfer Protocol: il protocollo usato per trasferimento dell'email da un server all'altro



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap -sT 192.168.1.35 -p 1-1024  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 05:4  
T  
Nmap scan report for ISLAM-KHALIL.stacion (192.168.1.35)  
Host is up (0.00060s 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  
MAC Address: 08:00:27:39:6D:CD (Oracle VirtualBox virtual)  
Nmap done: 1 IP address (1 host up) scanned in 0.34 second  
(root@kali)-[~]  
#
```

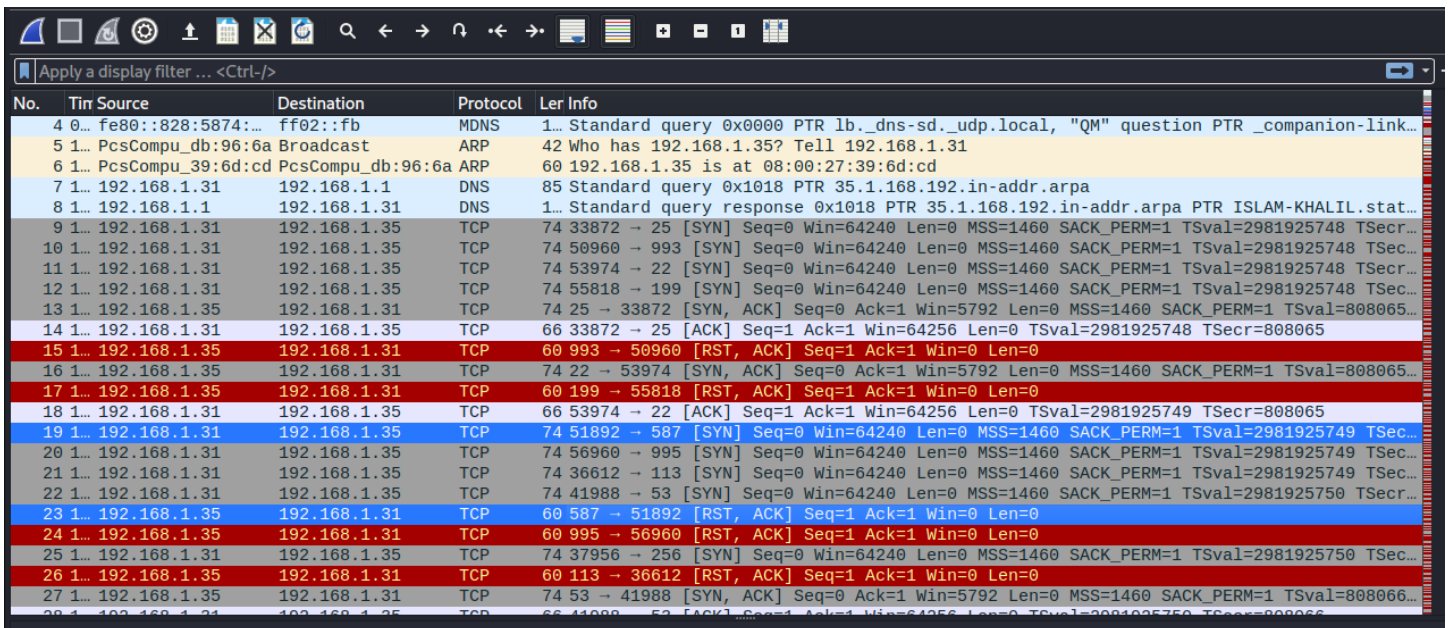
la figura si mostra i pacchetti catturati dal wireshark



No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	fe80::828:5874::...	ff02::fb	MDNS	100	1... Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-link...
5	1.000000	PcsCompu_db:96:6a	Broadcast	ARP	60	42 Who has 192.168.1.35? Tell 192.168.1.31
6	1.000000	PcsCompu_39:6d:cd	PcsCompu_db:96:6a	ARP	60	192.168.1.35 is at 08:00:27:39:6d:cd
7	1.000000	192.168.1.31	192.168.1.1	DNS	85	Standard query 0x1018 PTR 35.1.168.192.in-addr.arpa
8	1.000000	192.168.1.1	192.168.1.31	DNS	100	Standard query response 0x1018 PTR 35.1.168.192.in-addr.arpa PTR ISLAM-KHALIL.stat...
9	1.000000	192.168.1.31	192.168.1.35	TCP	74	33872 -> 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
10	1.000000	192.168.1.31	192.168.1.35	TCP	74	50960 -> 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
11	1.000000	192.168.1.31	192.168.1.35	TCP	74	53974 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
12	1.000000	192.168.1.31	192.168.1.35	TCP	74	55818 -> 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
13	1.000000	192.168.1.35	192.168.1.31	TCP	74	25 -> 33872 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=808065...
14	1.000000	192.168.1.31	192.168.1.35	TCP	66	33872 -> 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2981925748 TSecr=808065
15	1.000000	192.168.1.35	192.168.1.31	TCP	60	993 -> 50960 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	1.000000	192.168.1.35	192.168.1.31	TCP	74	22 -> 53974 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=808065...
17	1.000000	192.168.1.35	192.168.1.31	TCP	60	199 -> 55818 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	1.000000	192.168.1.31	192.168.1.35	TCP	66	53974 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2981925749 TSecr=808065
19	1.000000	192.168.1.31	192.168.1.35	TCP	74	51892 -> 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925749 TSecr...
20	1.000000	192.168.1.31	192.168.1.35	TCP	74	56960 -> 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925749 TSecr...
21	1.000000	192.168.1.31	192.168.1.35	TCP	74	36612 -> 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925749 TSecr...
22	1.000000	192.168.1.31	192.168.1.35	TCP	74	41988 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925750 TSecr...
23	1.000000	192.168.1.35	192.168.1.31	TCP	60	587 -> 51892 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	1.000000	192.168.1.35	192.168.1.31	TCP	60	995 -> 56960 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	1.000000	192.168.1.31	192.168.1.35	TCP	74	37956 -> 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925750 TSecr...
26	1.000000	192.168.1.35	192.168.1.31	TCP	60	113 -> 36612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	1.000000	192.168.1.35	192.168.1.31	TCP	74	53 -> 41988 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=808066...

Si vede un esempio di una porta aperta (porta 22: ssh), [come mostrato nelle righe blu](#), notato che il nmap completa la 3 way hand-shake, [SYN, SYN-ACK, ACK].

Un altro esempio dei dati catturati da wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	fe80::828:5874::...	ff02::fb	MDNS	100	1... Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-link...
5	1.000000	PcsCompu_db:96:6a	Broadcast	ARP	60	42 Who has 192.168.1.35? Tell 192.168.1.31
6	1.000000	PcsCompu_39:6d:cd	PcsCompu_db:96:6a	ARP	60	192.168.1.35 is at 08:00:27:39:6d:cd
7	1.000000	192.168.1.31	192.168.1.1	DNS	85	Standard query 0x1018 PTR 35.1.168.192.in-addr.arpa
8	1.000000	192.168.1.1	192.168.1.31	DNS	100	Standard query response 0x1018 PTR 35.1.168.192.in-addr.arpa PTR ISLAM-KHALIL.stat...
9	1.000000	192.168.1.31	192.168.1.35	TCP	74	33872 -> 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
10	1.000000	192.168.1.31	192.168.1.35	TCP	74	50960 -> 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
11	1.000000	192.168.1.31	192.168.1.35	TCP	74	53974 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
12	1.000000	192.168.1.31	192.168.1.35	TCP	74	55818 -> 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925748 TSecr...
13	1.000000	192.168.1.35	192.168.1.31	TCP	74	25 -> 33872 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=808065...
14	1.000000	192.168.1.31	192.168.1.35	TCP	66	33872 -> 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2981925748 TSecr=808065
15	1.000000	192.168.1.35	192.168.1.31	TCP	60	993 -> 50960 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	1.000000	192.168.1.35	192.168.1.31	TCP	74	22 -> 53974 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=808065...
17	1.000000	192.168.1.35	192.168.1.31	TCP	60	199 -> 55818 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	1.000000	192.168.1.31	192.168.1.35	TCP	66	53974 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2981925749 TSecr=808065
19	1.000000	192.168.1.31	192.168.1.35	TCP	74	51892 -> 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925749 TSecr...
20	1.000000	192.168.1.31	192.168.1.35	TCP	74	56960 -> 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925749 TSecr...
21	1.000000	192.168.1.31	192.168.1.35	TCP	74	36612 -> 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925749 TSecr...
22	1.000000	192.168.1.31	192.168.1.35	TCP	74	41988 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925750 TSecr...
23	1.000000	192.168.1.35	192.168.1.31	TCP	60	587 -> 51892 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	1.000000	192.168.1.35	192.168.1.31	TCP	60	995 -> 56960 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	1.000000	192.168.1.31	192.168.1.35	TCP	74	37956 -> 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2981925750 TSecr...
26	1.000000	192.168.1.35	192.168.1.31	TCP	60	113 -> 36612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	1.000000	192.168.1.35	192.168.1.31	TCP	74	53 -> 41988 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=808066...

Si vede nel esempio una richiesta di connessione a porta 587 che è chiusa, [come mostrato nelle righe blu](#), la richiesta da Kali [SYN], La Metasploitable ha risposto con [RST,ACK] significando che la porta non è in ascolto (chiusa).

2- Scan -sS:

Un metodo di scansione meno invasivo in questo metodo il nmap non conclude il 3 way hand-shake

si vede che nmap mostra le stesse informazioni mostrate da scan -sT

Porta 23/TCP: Telnet

Il telnet è un protocollo usato per fare connessione da remoto a un dispositivo

in seguente farò scansione a questa porta per mostrare i pacchetti su wireshark

```
root@kali: ~  
File Actions Edit View Help  
root@kali)-[~]  
# nmap -sS 192.168.1.35 -p 1-1024  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 07:0  
Nmap scan report for ISLAM-KHALIL.station (192.168.1.35)  
Host is up (0.00066s 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: 08:00:27:39:6D:CD (Oracle VirtualBox virtual  
Nmap done: 1 IP address (1 host up) scanned in 0.39 second  
root@kali)-[~]  
#
```

- Per poter mostrare i pacchetti su wireshark ho fatto scansione a singola porta (23:Telnet)

The image shows a Wireshark packet capture and a terminal window. The Wireshark interface displays a list of network packets. Packet 7 is highlighted in red, showing a TCP RST from 192.168.1.31 to 192.168.1.35 on port 23. The terminal window shows the command `nmap -sS 192.168.1.35 -p 23` and its output, which reports that port 23/tcp is open and running telnet.

No.	Time	Source	Destination	Protocol	Len	Info
1	0.000000000	PcsCompu_db:96:...	Broadcast	ARP	42	Who has 192.168.1.35? Tell 192.168.1.31
2	0.000485976	PcsCompu_39:6d:...	PcsCompu_db:96:6a	ARP	60	192.168.1.35 is at 08:00:27:39:6d:cd
3	0.051632253	192.168.1.31	192.168.1.1	DNS	85	Standard query 0xe06a PTR 35.1.168.192.in-addr.arpa
4	0.062178864	192.168.1.1	192.168.1.31	DNS	1...	Standard query response 0xe06a PTR 35.1.168.192.in-addr.arpa PTR ISLAM-K...
5	0.101394618	192.168.1.31	192.168.1.35	TCP	58	55914 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.102473029	192.168.1.35	192.168.1.31	TCP	60	23 → 55914 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
7	0.102569215	192.168.1.31	192.168.1.35	TCP	54	55914 → 23 [RST] Seq=1 Win=0 Len=0

```
root@kali: ~  
File Actions Edit View Help  
root@kali)-[~]  
# nmap -sS 192.168.1.35 -p 23  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 04:50 EDT  
Nmap scan report for ISLAM-KHALIL.station (192.168.1.35)  
Host is up (0.00061s latency).  
PORT      STATE SERVICE  
23/tcp    open  telnet  
MAC Address: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds  
root@kali)-[~]  
#
```

All'immagine si vede che nmap ha fatto richiesta di connessione [SYN], la vittima (Metasploitable) ha risposto la richiesta con [SYN, ACK] ma poi il nmap ha chiuso l'ascolta alla porta 55914 per non concludere il 3 way hand-shake

3- Scan -A

Un altro metodo da scansione su nmap ma questo metodo scansiona ovvero mostra più informazione di -sT e -sS

Nell'immagine a destra si mostra nmap -A.

- a- Si vede che nmap -A fa scansione alla **Porta**, lo **stato**, **tipo di servizio** è **versione del servizio**
- b- Mostra più informazioni sul Protocollo es.
ftp → mostra il tipo ASCII → per indicare che il tipo di file trasferito e testo normale non è binario.
→ Session time out: 300 sec
→ session bandwidth: illimitato
- 22:ssh → mostra il hostkey
le chiavi pubblici usati in una sessione criptati sia in **DSA** che **RSA**.
- c- Scan -A Mostra anche le porte Chiuse come 24 con il tipo di servizio Private-mail
- d- Si mostra anche il sistema operativo con la versione del sistema
- e- Alla fine, si mostra un traceroute della machina e il numero del hop per raggiungere il machina.

```
File Actions Edit View Help
# nmap -A 192.168.1.35 -p 21-24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 08:10 EDT
Nmap scan report for ISLAM-KHALIL.station (192.168.1.35)
Host is up (0.00082s latency).

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 192.168.1.31
|_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
24/tcp    closed priv-mail
MAC Address: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.82 ms ISLAM-KHALIL.station (192.168.1.35)
```