Traccia:

Vedremo da vicino nmap e i suoi comandi. Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla 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 dalla macchine sorgente con Wireshark.

Ambiente:

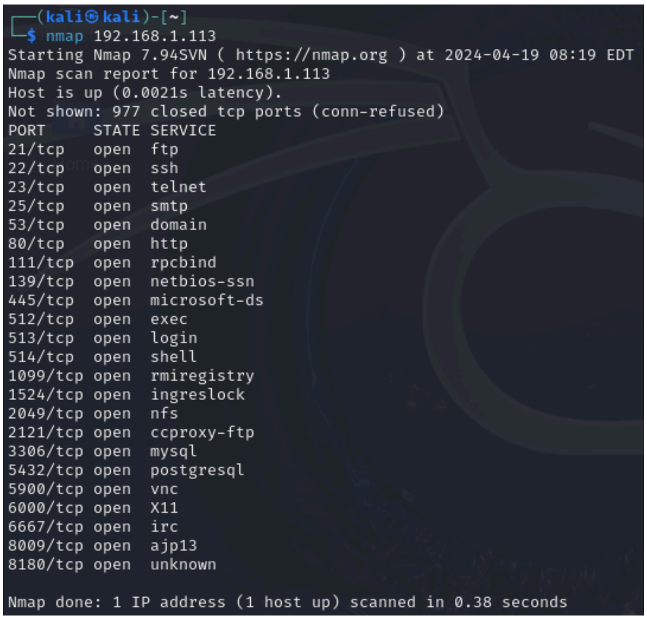
L'esercizio va svolto utilizzando due VM, una kali linux e l'altra metasploitable. Entrambe saranno settate con scheda di rete bridged e ip statico sulla stessa rete (gw 192.168.1.1 nm 255.255.255.0):
-Kali Linux con ip 192.168.1.100/24
-Metasploitable con ip 192.168.1.113/24

Svolgimento:

Andremo ad utilizzare il comando "nmap" per svolgere questo esercizio. La macchina attaccante sarà Kali Linux mentre Metasploitable sarà il bersaglio.

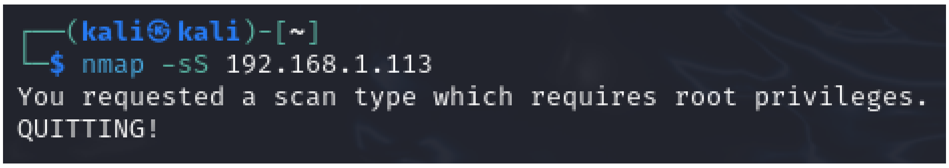
Tipologia	**Comando**	**Fonte**	**Target**	**Risultati**
TCP scan	nmap	192.168.1.100	192.168.1.113	23 risultati attivi
SYN scan	nmap -sS	192.168.1.100	192.168.1.113	accesso negato
UDP scan	nmap -sU	192.168.1.100	192.168.1.113	accesso negato

TCP SCAN RESULTS:



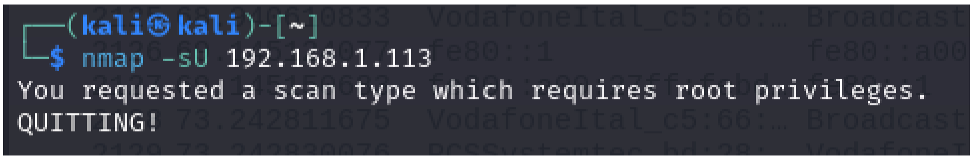
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 08:19 EDT
Nmap scan report for 192.168.1.113
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

SYN CAN RESULTS:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.113
You requested a scan type which requires root privileges.
QUITTING!
```

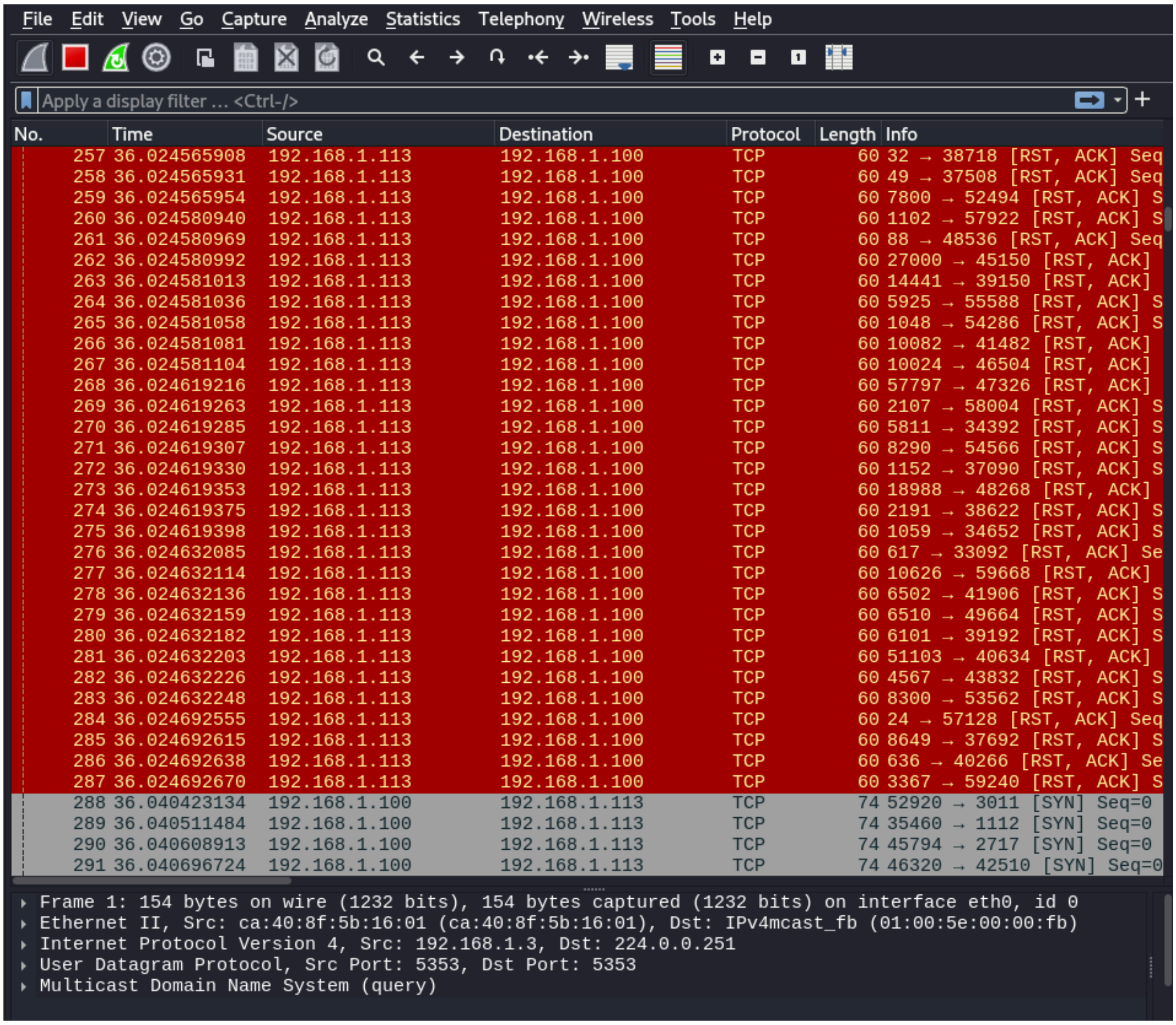
UDP SCAN RESULTS:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sU 192.168.1.113
You requested a scan type which requires root privileges.
QUITTING!
```

WIRESHARK CAPTURE:

TCP REQUEST:

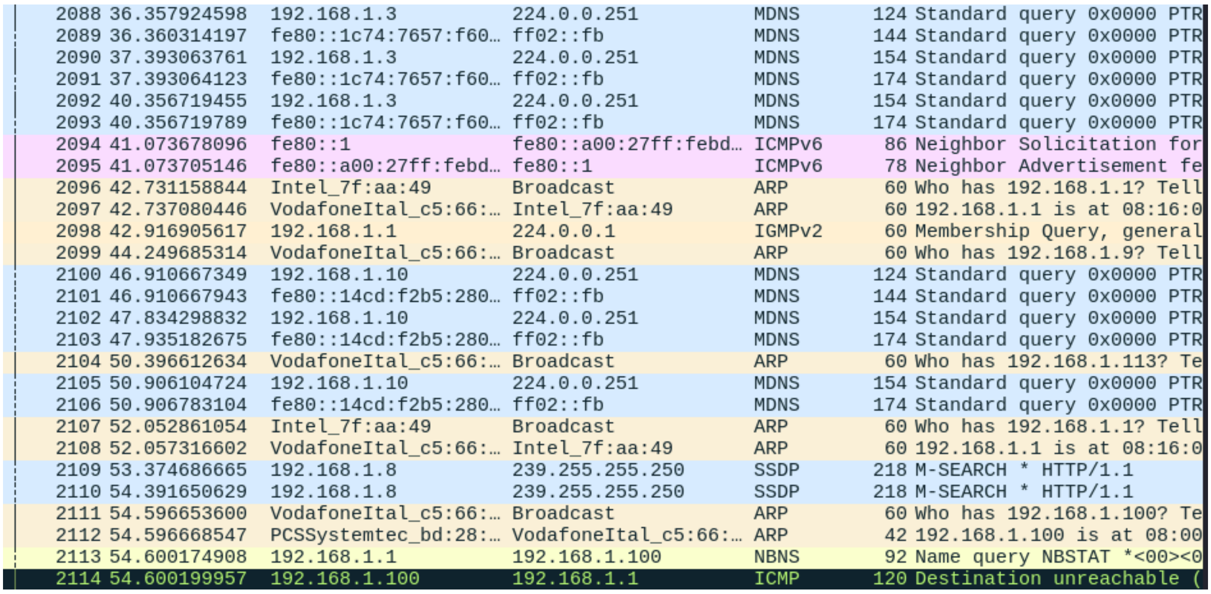


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source          Destination     Protocol  Length Info
  257 36.024565908  192.168.1.113   192.168.1.100   TCP       60 32 → 38718 [RST, ACK] Seq
  258 36.024565931  192.168.1.113   192.168.1.100   TCP       60 49 → 37508 [RST, ACK] Seq
  259 36.024565954  192.168.1.113   192.168.1.100   TCP       60 7800 → 52494 [RST, ACK] S
  260 36.024580940  192.168.1.113   192.168.1.100   TCP       60 1102 → 57922 [RST, ACK] S
  261 36.024580969  192.168.1.113   192.168.1.100   TCP       60 88 → 48536 [RST, ACK] Seq
  262 36.024580992  192.168.1.113   192.168.1.100   TCP       60 27000 → 45150 [RST, ACK]
  263 36.024581013  192.168.1.113   192.168.1.100   TCP       60 14441 → 39150 [RST, ACK]
  264 36.024581036  192.168.1.113   192.168.1.100   TCP       60 5925 → 55588 [RST, ACK] S
  265 36.024581058  192.168.1.113   192.168.1.100   TCP       60 1048 → 54286 [RST, ACK] S
  266 36.024581081  192.168.1.113   192.168.1.100   TCP       60 10082 → 41482 [RST, ACK]
  267 36.024581104  192.168.1.113   192.168.1.100   TCP       60 10024 → 46504 [RST, ACK]
  268 36.024619216  192.168.1.113   192.168.1.100   TCP       60 57797 → 47326 [RST, ACK]
  269 36.024619263  192.168.1.113   192.168.1.100   TCP       60 2107 → 58004 [RST, ACK] S
  270 36.024619285  192.168.1.113   192.168.1.100   TCP       60 5811 → 34392 [RST, ACK] S
  271 36.024619307  192.168.1.113   192.168.1.100   TCP       60 8290 → 54566 [RST, ACK] S
  272 36.024619330  192.168.1.113   192.168.1.100   TCP       60 1152 → 37090 [RST, ACK] S
  273 36.024619353  192.168.1.113   192.168.1.100   TCP       60 18988 → 48268 [RST, ACK]
  274 36.024619375  192.168.1.113   192.168.1.100   TCP       60 2191 → 38622 [RST, ACK] S
  275 36.024619398  192.168.1.113   192.168.1.100   TCP       60 1059 → 34652 [RST, ACK] S
  276 36.024632085  192.168.1.113   192.168.1.100   TCP       60 617 → 33092 [RST, ACK] Se
  277 36.024632114  192.168.1.113   192.168.1.100   TCP       60 10626 → 59668 [RST, ACK]
  278 36.024632136  192.168.1.113   192.168.1.100   TCP       60 6502 → 41906 [RST, ACK] S
  279 36.024632159  192.168.1.113   192.168.1.100   TCP       60 6510 → 49664 [RST, ACK] S
  280 36.024632182  192.168.1.113   192.168.1.100   TCP       60 6101 → 39192 [RST, ACK] S
  281 36.024632203  192.168.1.113   192.168.1.100   TCP       60 51103 → 40634 [RST, ACK]
  282 36.024632226  192.168.1.113   192.168.1.100   TCP       60 4567 → 43832 [RST, ACK] S
  283 36.024632248  192.168.1.113   192.168.1.100   TCP       60 8300 → 53562 [RST, ACK] S
  284 36.024692555  192.168.1.113   192.168.1.100   TCP       60 24 → 57128 [RST, ACK] Seq
  285 36.024692615  192.168.1.113   192.168.1.100   TCP       60 8649 → 37692 [RST, ACK] S
  286 36.024692638  192.168.1.113   192.168.1.100   TCP       60 636 → 40266 [RST, ACK] Se
  287 36.024692670  192.168.1.113   192.168.1.100   TCP       60 3367 → 59240 [RST, ACK] S
  288 36.040423134  192.168.1.100   192.168.1.113   TCP       74 52920 → 3011 [SYN] Seq=0
  289 36.040511484  192.168.1.100   192.168.1.113   TCP       74 35460 → 1112 [SYN] Seq=0
  290 36.040608913  192.168.1.100   192.168.1.113   TCP       74 45794 → 2717 [SYN] Seq=0
  291 36.040696724  192.168.1.100   192.168.1.113   TCP       74 46320 → 42510 [SYN] Seq=0
```

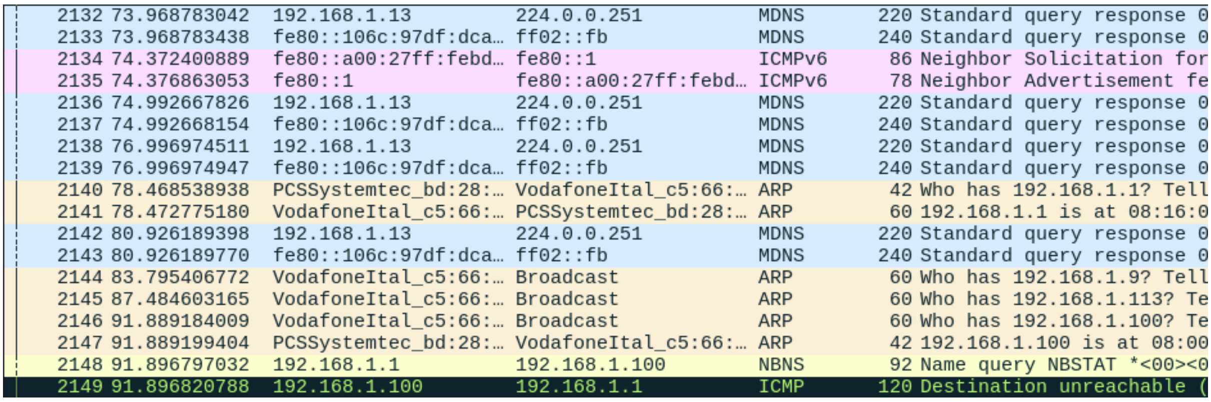
```
› Frame 1: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface eth0, id 0
› Ethernet II, Src: ca:40:8f:5b:16:01 (ca:40:8f:5b:16:01), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
› Internet Protocol Version 4, Src: 192.168.1.3, Dst: 224.0.0.251
› User Datagram Protocol, Src Port: 5353, Dst Port: 5353
› Multicast Domain Name System (query)
```

SYN REQUEST:



```
2088 36.357924598  192.168.1.3          224.0.0.251          MDNS      124 Standard query 0x0000 PTR
2089 36.360314197  fe80::1c74:7657:f60… ff02::fb             MDNS      144 Standard query 0x0000 PTR
2090 37.393063761  192.168.1.3          224.0.0.251          MDNS      154 Standard query 0x0000 PTR
2091 37.393064123  fe80::1c74:7657:f60… ff02::fb             MDNS      174 Standard query 0x0000 PTR
2092 40.356719455  192.168.1.3          224.0.0.251          MDNS      154 Standard query 0x0000 PTR
2093 40.356719789  fe80::1c74:7657:f60… ff02::fb             MDNS      174 Standard query 0x0000 PTR
2094 41.073678096  fe80::1              fe80::a00:27ff:febd… ICMPv6     86 Neighbor Solicitation for
2095 41.073705146  fe80::a00:27ff:febd… fe80::1              ICMPv6     78 Neighbor Advertisement fe
2096 42.731158844  Intel_7f:aa:49       Broadcast            ARP        60 Who has 192.168.1.1? Tell
2097 42.737080446  VodafoneItal_c5:66:… Intel_7f:aa:49       ARP        60 192.168.1.1 is at 08:16:0
2098 42.916905617  192.168.1.1          224.0.0.1            IGMPv2     60 Membership Query, general
2099 44.249685314  VodafoneItal_c5:66:… Broadcast            ARP        60 Who has 192.168.1.9? Tell
2100 46.910667349  192.168.1.10         224.0.0.251          MDNS      124 Standard query 0x0000 PTR
2101 46.910667943  fe80::14cd:f2b5:280… ff02::fb             MDNS      144 Standard query 0x0000 PTR
2102 47.834298832  192.168.1.10         224.0.0.251          MDNS      154 Standard query 0x0000 PTR
2103 47.935182675  fe80::14cd:f2b5:280… ff02::fb             MDNS      174 Standard query 0x0000 PTR
2104 50.396612634  VodafoneItal_c5:66:… Broadcast            ARP        60 Who has 192.168.1.113? Te
2105 50.906104724  192.168.1.10         224.0.0.251          MDNS      154 Standard query 0x0000 PTR
2106 50.906783104  fe80::14cd:f2b5:280… ff02::fb             MDNS      174 Standard query 0x0000 PTR
2107 52.052861054  Intel_7f:aa:49       Broadcast            ARP        60 Who has 192.168.1.1? Tell
2108 52.057316602  VodafoneItal_c5:66:… Intel_7f:aa:49       ARP        60 192.168.1.1 is at 08:16:0
2109 53.374686665  192.168.1.8          239.255.255.250      SSDP      218 M-SEARCH * HTTP/1.1
2110 54.391650629  192.168.1.8          239.255.255.250      SSDP      218 M-SEARCH * HTTP/1.1
2111 54.596653600  VodafoneItal_c5:66:… Broadcast            ARP        60 Who has 192.168.1.100? Te
2112 54.596668547  PCSSystemtec_bd:28:… VodafoneItal_c5:66:… ARP        42 192.168.1.100 is at 08:00
2113 54.600174908  192.168.1.1          192.168.1.100        NBNS       92 Name query NBSTAT *<00><0
2114 54.600199957  192.168.1.100        192.168.1.1          ICMP      120 Destination unreachable (
```

UDP REQUEST:



```
2132 73.968783042  192.168.1.13         224.0.0.251          MDNS      220 Standard query response 0
2133 73.968783438  fe80::106c:97df:dca… ff02::fb             MDNS      240 Standard query response 0
2134 74.372400889  fe80::a00:27ff:febd… fe80::1              ICMPv6     86 Neighbor Solicitation for
2135 74.376863053  fe80::1              fe80::a00:27ff:febd… ICMPv6     78 Neighbor Advertisement fe
2136 74.992667826  192.168.1.13         224.0.0.251          MDNS      220 Standard query response 0
2137 74.992668154  fe80::106c:97df:dca… ff02::fb             MDNS      240 Standard query response 0
2138 76.996974511  192.168.1.13         224.0.0.251          MDNS      220 Standard query response 0
2139 76.996974947  fe80::106c:97df:dca… ff02::fb             MDNS      240 Standard query response 0
2140 78.468538938  PCSSystemtec_bd:28:… VodafoneItal_c5:66:… ARP        42 Who has 192.168.1.1? Tell
2141 78.472775180  VodafoneItal_c5:66:… PCSSystemtec_bd:28:… ARP        60 192.168.1.1 is at 08:16:0
2142 80.926189398  192.168.1.13         224.0.0.251          MDNS      220 Standard query response 0
2143 80.926189770  fe80::106c:97df:dca… ff02::fb             MDNS      240 Standard query response 0
2144 83.795406772  VodafoneItal_c5:66:… Broadcast            ARP        60 Who has 192.168.1.9? Tell
2145 87.484603165  VodafoneItal_c5:66:… Broadcast            ARP        60 Who has 192.168.1.113? Te
2146 91.889184009  VodafoneItal_c5:66:… Broadcast            ARP        60 Who has 192.168.1.100? Te
2147 91.889199404  PCSSystemtec_bd:28:… VodafoneItal_c5:66:… ARP        42 192.168.1.100 is at 08:00
2148 91.896797032  192.168.1.1          192.168.1.100        NBNS       92 Name query NBSTAT *<00><0
2149 91.896820788  192.168.1.100        192.168.1.1          ICMP      120 Destination unreachable (
```

Conclusioni:

In condizioni normali, nmap riesce ad effettuare solo lo scan completo TCP, inviando un grande quantità di pacchetti. Negli altri due casi il s.o. target nega lo scan, in quanto risulta molto più invasivo e metterebbe a repentaglio informazioni sensibili per un possibile attacco. Effettuando prove inverse ho invece notato che i pacchetti che invia l'attaccante nei confronti del target con le scansioni UDP e SYN sono molti di più di quelli mostrati in Kali linux, superando di molto lo scan TCP e non mantenendo quindi un basso profilo.