REPORT NMAP SCANS

Il test di oggi consiste nell'effettuare delle scansioni tramite il tool Nmap che è per l'appunto un port-scanner ovvero uno strumento che ci viene utile per la scansione di reti siano esse locali come vedremo nell'esempio, che di grandi dimensioni.
Si possono anche inserire degli Ip singoli o gruppi di Ip, così come porte singole o range di porte.
Per ogni tipo di scansione si possono utilizzare insieme al comando nmap, che in alcuni casi torna utile lanciare con sudo per i privilegi che si ottengono, si possono utilizzare moltissimi switch che ci vengono descritti brevemente lanciando il comando nmap.

Le scansioni richieste sono:

1) la prima che è una *host discovery* andremo a farla tramite l'utilizzo dello switch **-sn**, che serve per effettuare un ping scan ovvero verificare tramite ping senza effettuare una vera e propria scansione quali sono gli host attivi su una rete.

2) la seconda tramite gli switch **-sT** e **-sS** che apparengono invece alla categoria *scan techniques*, appunto tecniche di scan. Queste si distinguono tra loro per la metodologia di azione: -sT ad esempio è la tencnica più invasiva in quanto per verificare se una porta è aperta nmap *effettua tutti e tre i passaggi del 3-way-handshake* facendosi rilevare dal server target; al contrario -sS chiamata anche SYN scan, è una tecnica meno invasiva perchè invece di effettuare tutti i passaggi del 3-way-handshake una volta ricevuto il pacchetto *SYN/ACK* dal server target e aver confermato quindi che la porta sia aperta termina subito la comunicazione inviando un pacchetto *RST (reset)*.
Sembrerebbe inutile quindi utilizzare -sT ma dobbiamo tenere a mente che nel suo "rumore" oltre allo stato della porta riesce a portare a casa anche ulteriori informazioni sul servizio in ascolto.
L'applicazione dell'uno o dell'altro quindi dipende sempre dall'obbiettivo che si ha.

3) la terza invece tramite l'utilizzo dello switch **-A** che sta per aggressive scan option appartiene invece alla categoria *Misc*, cioè *opzioni miscellanee*. Queste sono altre funzioni molto importanti ma che non hanno trovato spazio nelle altre categorie. Questa tecnica *attiva contemporaneamente l'OS detection (-o), il version scanning (-sV), lo script scanning (-sC) e il traceroute (--traceroute)*, senza bisogno di dover ripetere scansioni separate per ognuna di essi e riportando di conseguenza una grandissima quantità di informazioni.

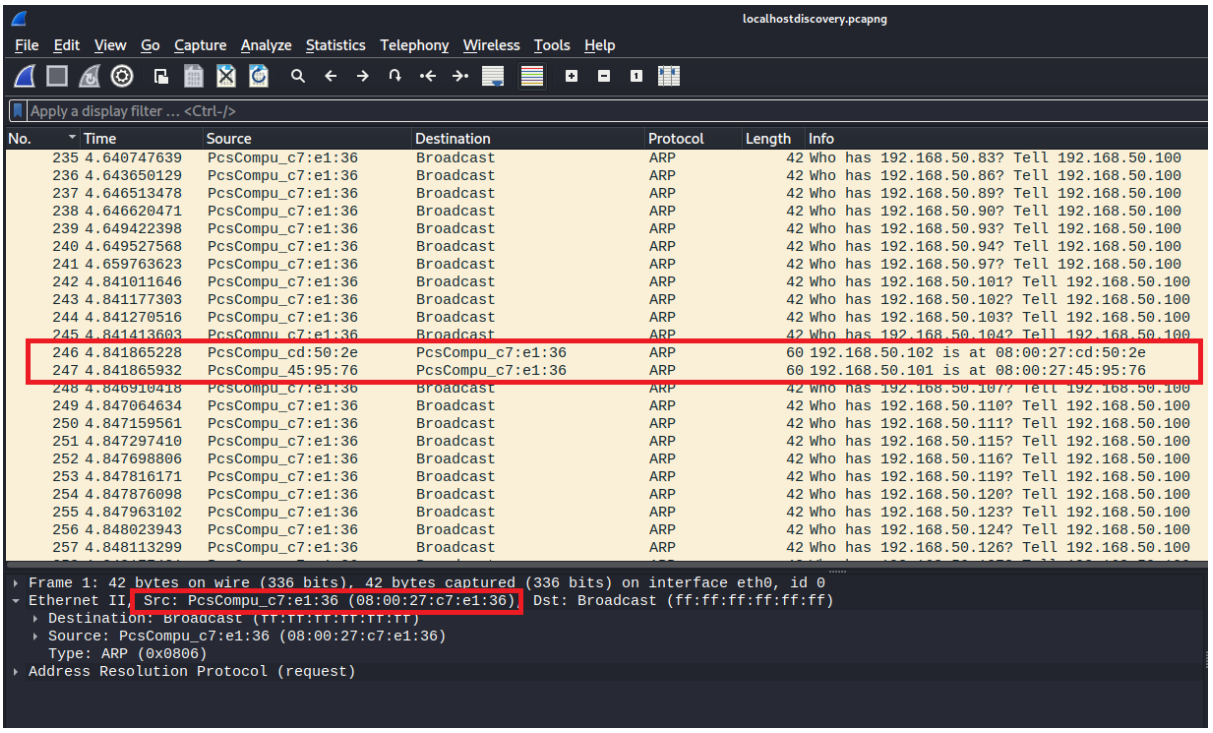
Andiamo ad analizzare caso per caso, riportando sia il risultato della scansione tramite nmap che i pacchetti catturati tramite il software Wireshark.

SCANSIONE CON SWITCH -sN / HOST DISCOVERY SU LAN

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.50.0/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 07:37 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00086s latency).
MAC Address: 08:00:27:45:95:76 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.102
Host is up (0.00078s latency).
MAC Address: 08:00:27:CD:50:2E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 32.43 seconds
```

Screen di Nmap dove vediamo il comando nmap seguito dall'Ip di rete con la notazione CIDR e poi la risposta al ping di tre host, uno con IP 192.168.50.101, uno con IP 192.168.50.102 e l'ultimo con IP 192.168.50.100; ognuno con annesso il MAC address e la Network Interface Card che in questo caso è di Virtual Box.



Screen di Wireshark dove vediamo la scansione più nel dettaglio notando come Nmap vada a mandare la richiesta tramite protocollo ARP dall' IP 192.168.50.0 fino all' IP 192.168.50.255 fino a quando non incontra i due IP che rispondono comunicando anche i rispettivi MAC. In evidenza nei riquadri rossi il source in basso e le risposte dei due host.

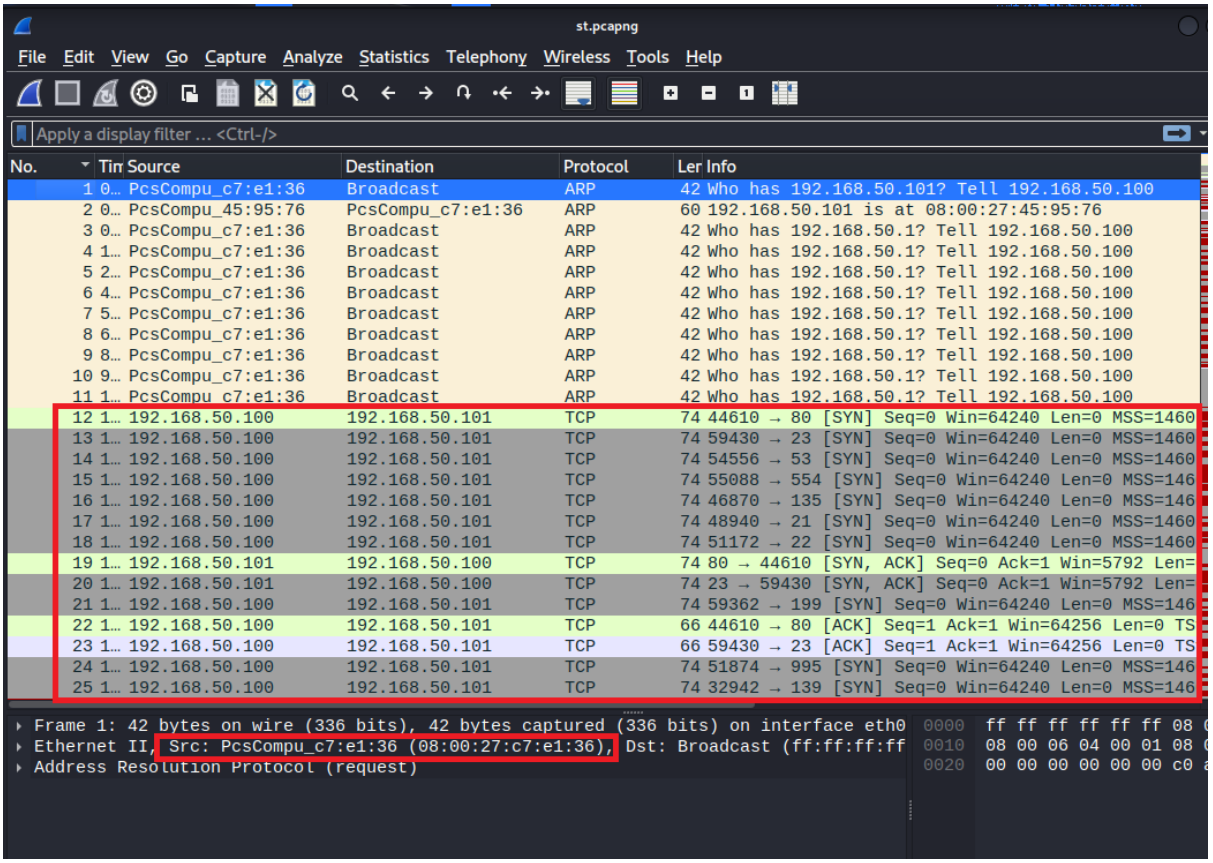
SCANSIONE CON SWITCH -sT / TCP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -p 0-1023

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 03:53 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s 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: 08:00:27:45:95:76 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

Screen di Nmap dove oltre all'IP bersaglio indichiamo anche il numero di porte che vogliamo andare a controllare. Nello specifico viene riportato che la porta 1012 risulta chiusa e la connessione viene rifiutata; poi segue un elenco delle porte con annesso numero di porta, stato e servizio in esecuzione. In questo caso sul client bersaglio abbiamo 12 servizi in esecuzione.



Screen di Wireshark dove vediamo la scansione più nel dettaglio notando come dopo aver verificato tramite il protocollo ARP relativi IP e MAC address del destinatario, si passi alla parte della comunicazione tramite il protocollo TCP (rettangolo in rosso) e si assite al completamente di tutti i passaggi del 3-way-handshake (sequenza SYN - SYN/ACK - ACK) tipica dello switch -sT. Inoltre in basso si nota sempre il source (rettangolo in rosso).

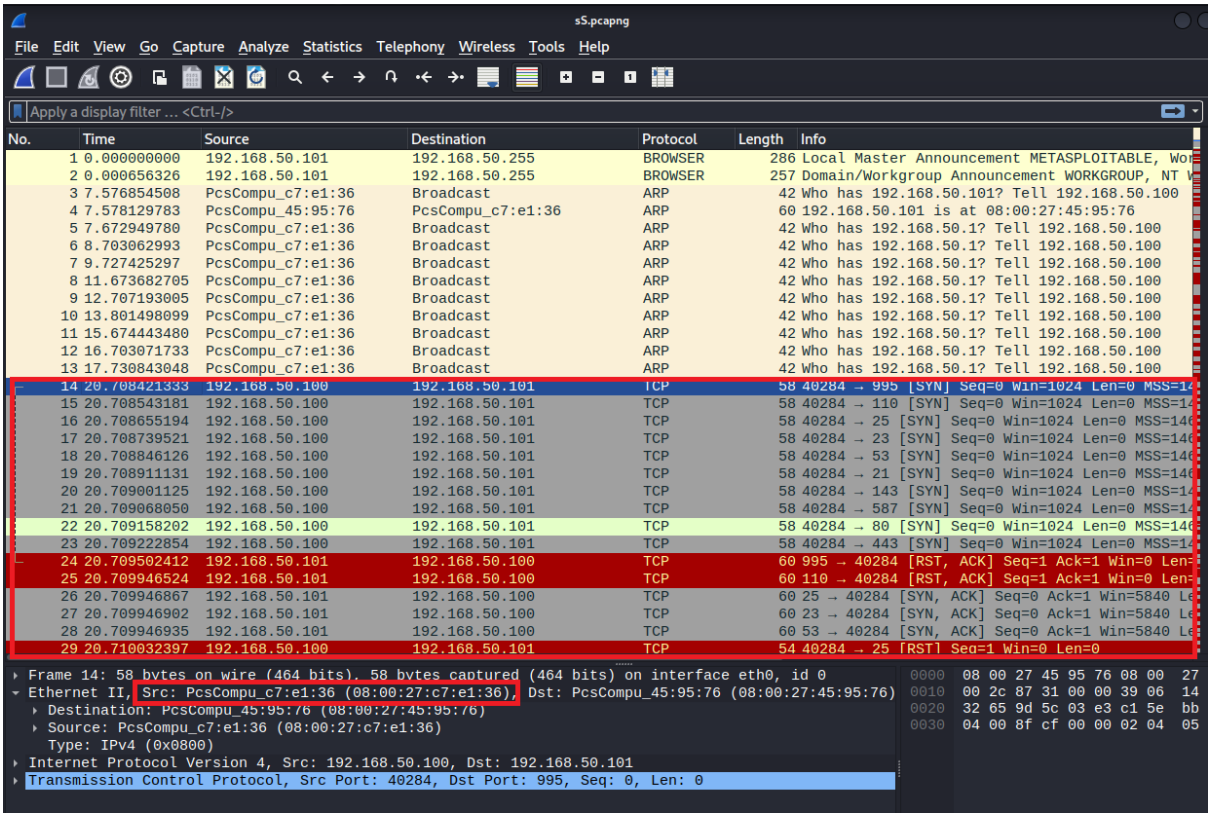
SCANSIONE CON SWITCH -sS / SYN

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS  192.168.50.101 -p 0-1023

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 03:53 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0018s 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: 08:00:27:45:95:76 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

Screen di Nmap dove oltre all'IP bersaglio indichiamo anche il numero di porte che vogliamo andare a controllare. Nello specifico viene riportato che la porta 1012 risulta chiusa e la connessione a differenza dello switch -sT non viene rifiutata bensì viene resettata; poi segue un elenco delle porte con annesso numero di porta, stato e servizio in esecuzione. In questo caso sul client bersaglio abbiamo 12 servizi in esecuzione.



Screen di Wireshark dove vediamo la scansione più nel dettaglio notando come in primis intervenga il protocollo BROWSER che va ad identificare anche che si tratta di un client Metasploitable, e dopo aver verificato tramite il protocollo ARP relativi IP e MAC address del destinatario, si passi alla parte della comunicazione tramite il protocollo TCP (rettangolo in rosso) ma questa volta vediamo come i passaggi del 3-way-handshake non vegano portati a termine bensi venga inviato un pacchetto RST ovvero di reset della comunicazione tipico dello switch -sS. Inoltre in basso si nota sempre il source (rettangolo in rosso).

SCANSIONE CON SWITCH -A / Aggressive

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A  192.168.50.101 -p 0-1023

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 03:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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      46708/tcp   mountd
|   100005  1,2,3      57915/udp   mountd
|   100021  1,3,4      33518/tcp   nlockmgr
|   100021  1,3,4      36820/udp   nlockmgr
|   100024  1          42594/tcp   status
|_  100024  1          53969/udp   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        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:45:95:76 (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: Host:  metasploitable.localdomain; 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: 2023-05-18T03:57:03-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h00m03s, deviation: 2h49m47s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.50.101

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 99.27 seconds
```

Screen di Nmap dove notiamo questa volta una quantità di informazioni maggiore di gran lunga rispetto alle precedenti in quanto questa scansione come anticipato prima riporta informazioni sul sistema operativo; colleziona altre informazioni interrogando le porte aperte con delle probe ognuno dei quali ha un valore assegnato tra 1 e 9; esegue poi una serie di script di default ed infine effettua un traceroute ovvero determina il percorso fatto fino al client bersaglio.

P.s. tutte le informazioni sono state prese dal sito www.nmap.org