Gabriele Di giampietro **Data 10/11/2022**

Obbiettivo: Effettuare tramite la comunicazione di due macchine virtuali le scansioni TCP, SYN e con il comando "switch" di "nmap" sulle porte well-know, analizzandone le differenze.

Premessa: abbiamo messo in comunicazione interna due VM Kali (ip:192.168.50.100), Metasploitable (ip:192.168.50.101).

Prima scansione (TCP)

Utilizzando il comando "nmap" andiamo a scannerizzare il nostro ip target:192.168.50.101 con la funzione sT, ottenendo così una scansione più invasiva in quanto recupera le informazioni sulle porte aperte che troviamo, attraverso il SYN >> SYN/ACK>>ACK<< che vediamo attraverso la cattura dei paccheti in "wireshark". Inoltre troviamo sulle porte well-know scansionate (filtriamo nel comando di nmap -p 0-1023) 12 servizi attivi.

Come possiamo vedere nelle figure seguenti, ci sono le porte aperte scansionate con "nmap" e le relative risposte SYN ACK catturate con "wireshark" (possiamo notare anche gli ip di source e destination):

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 0-1023 192.168.50.101 -sT
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 09:55 EST
Nmap scan report for 192.168.50.101
Host is up (0.0040s 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

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```

tcp.port==513SS

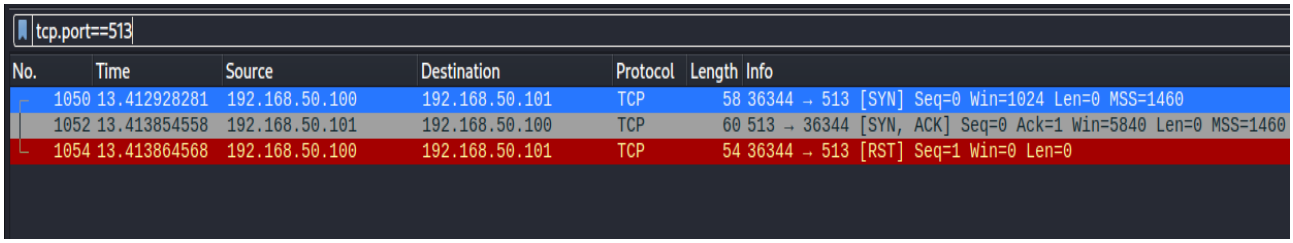
No.	Time	Source	Destination	Protocol	Length	Info
131	13.015170464	192.168.50.100	192.168.50.101	TCP	74	47368 → 513 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=
138	13.015640951	192.168.50.101	192.168.50.100	TCP	74	513 → 47368 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
139	13.015662181	192.168.50.100	192.168.50.101	TCP	66	47368 → 513 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2990655160 TSec
232	13.024778494	192.168.50.100	192.168.50.101	TCP	66	47368 → 513 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2990655169

Seconda scansione (SYN)

Nella seconda scansione riproponiamo gli stessi passaggi della prima solo che in questo caso dobbiamo operare dal root, quindi dopo avere utilizzato il comando “sudo su” da root andiamo ad utilizzare nmap ma questa volta utilizzanto la funzione sS, detta anche SYN, una scansione meno invasiva infatti dopo aver verificato le porte aperte chiude la comunicazione, notiamo questa differenza sulla cattura di pacchetti con “wireshark” che dopo l’invio della risposta SYN e SYN/ACK non abbiamo nessuna informazione e la comunicazione viene chiusa come possiamo vedere dalla stringa rossa subito dopo la verifica di SYN/ACK. Anche in questo caso abbiamo 12 servizi.

Come possiamo vedere dalle figure seguenti otteniamo soltanto la certezza delle porte aperte:

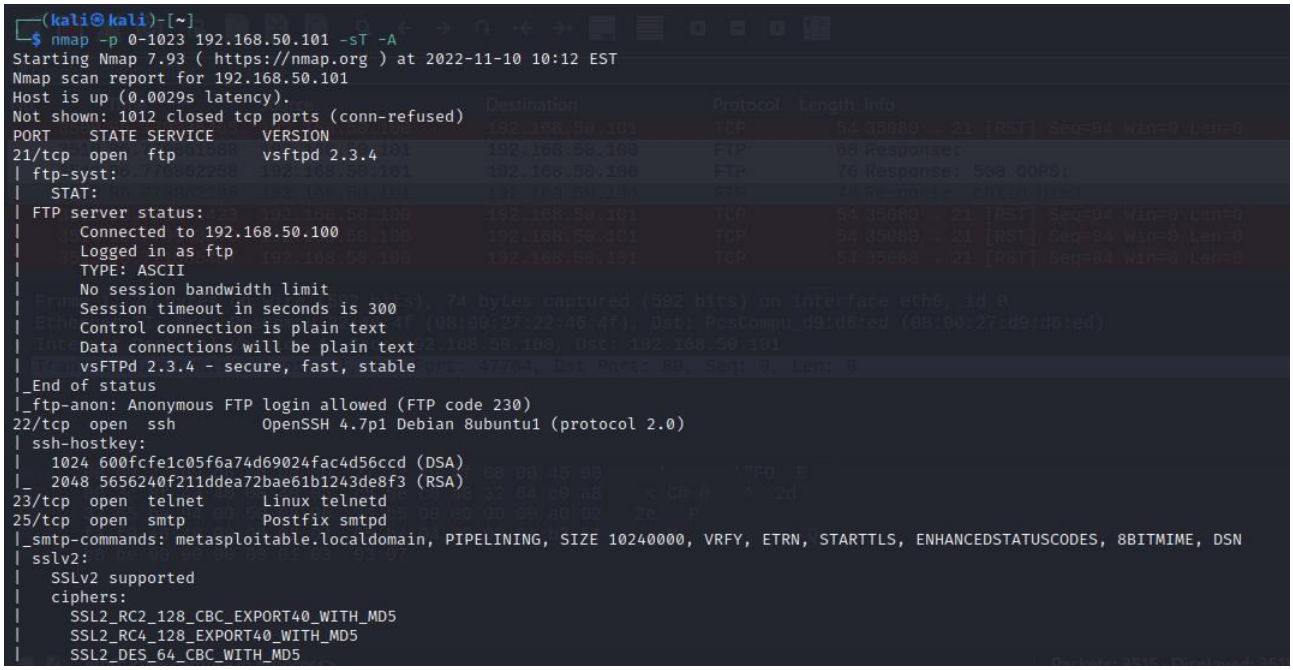
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -p0-1023  192.168.50.101 -sS
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 10:02 EST
Nmap scan report for 192.168.50.101
Host is up (0.00097s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    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:D9:D6:ED (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds
```



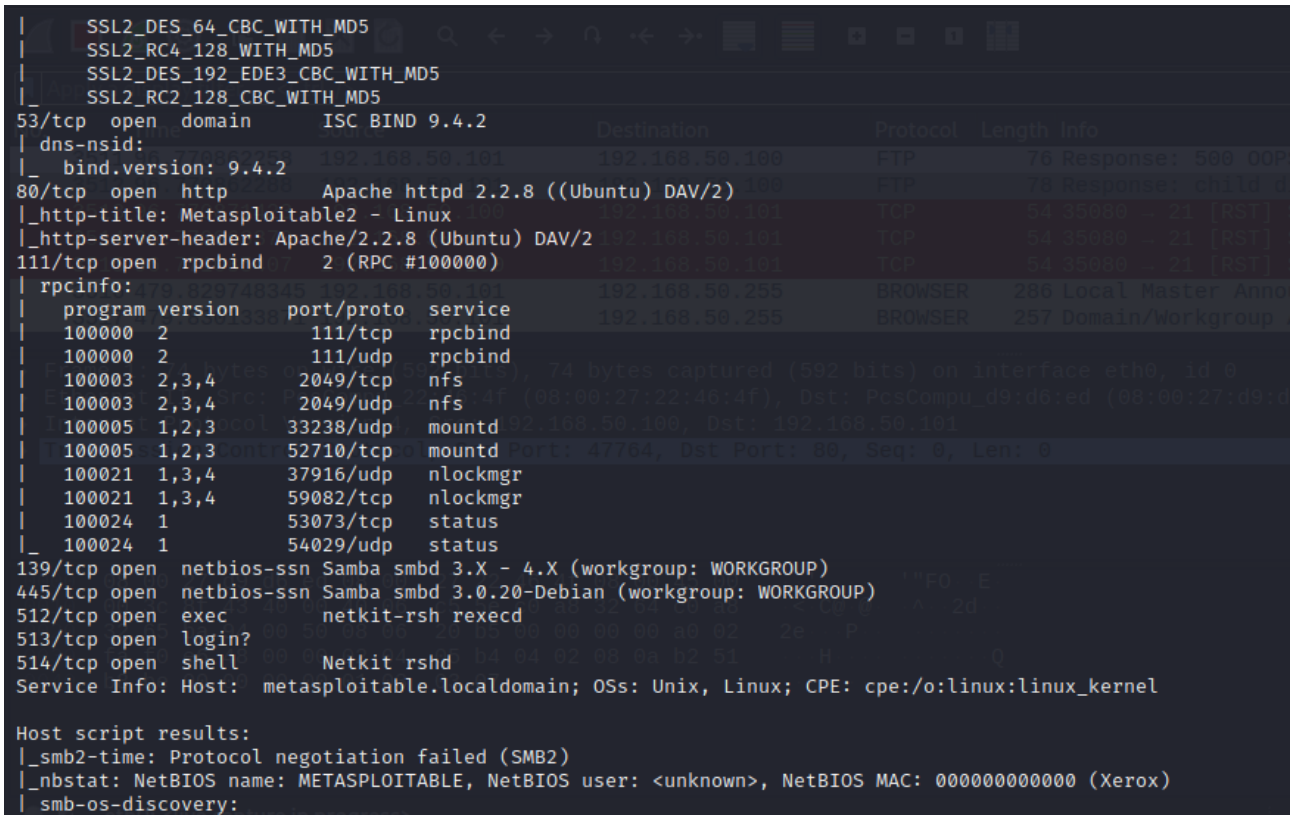
Ultima scansione (Switch –A)

Nell'ultima scansione utilizziamo la funzione di "nmap" -A detta switch che ci dà una scansione ancora più dettagliata, ovvero scansiona anche il range della singola porta con tutte le risposte che vengono inviate tra source e destination; abbiamo sempre 12 servizi attivi.

Come possiamo vedere nelle figure seguenti, abbiamo molte più informazioni per ogni porta aperta (ho effettuato una scansione con funzione sT per completezza):



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 0-1023 192.168.50.101 -sT -A
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 10:12 EST
Nmap scan report for 192.168.50.101
Host is up (0.0029s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
```



```
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_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-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      33238/udp   mountd
|   100005  1,2,3      52710/tcp   mountd
|   100021  1,3,4      37916/udp   nlockmgr
|   100021  1,3,4      59082/tcp   nlockmgr
|   100024  1          53073/tcp   status
|_  100024  1          54029/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
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
```

```
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-11-10T10:13:56-05:00
|_clock-skew: mean: 2h30m08s, deviation: 3h32m17s, median: 1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.20 seconds
```

Pacchetti di catturati su wireshark su una singola porta aperta in questo caso la 513: