

SCANSIONE METASPLOITABLE.

Nella task di oggi ci è stato richiesto di effettuare vari tipi di scansione sulla nostra Metasploitable. Per tutte le scansioni mi sono avvalso del tool Nmap.

I metodi di scansione erano del tipo:

- TCP
- SYN
- Os Detected

Tutte effettuate con successo.

TCP SCAN

La prima scansione che è stata effettuata è una scansione di tipo TCP, ovvero creando un canale diretto completando il 3-way-handshake. Per fare ciò sono stati utilizzati i parametri << -sT >> , per effettuare la chiamata di tipo TCP, << -p >> per scansionare solo le porte well-know (0-1023):

```
(kali@kali)~$ sudo nmap -sT -p 0-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 09:56 EST
Nmap scan report for 192.168.50.101
Host is up (0.00019s 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:AC:A6:3F (Oracle VirtualBox virtual NIC)
```

FONTE SCAN	DESTINAZIONE SCAN	PORTA	SERVIZIO
192.168.50.100	192.168.50.101	23	telnet
192.168.50.100	192.168.50.101	25	smtp
192.168.50.100	192.168.50.101	53	domain
192.168.50.100	192.168.50.101	80	http
192.168.50.100	192.168.50.101	111	rpcbind
192.168.50.100	192.168.50.101	139	netbios-ssn
192.168.50.100	192.168.50.101	445	microsoft-ds
192.168.50.100	192.168.50.101	512	exec
192.168.50.100	192.168.50.101	513	login
192.168.50.100	192.168.50.101	514	shell

SYN SCAN

Per il SYN SCAN sono stati utilizzati i parametri << -sS >> e << -p>>.

La scansione SYN è più “” discreta “” rispetto alla classica TCP, in quanto il 3-way-handshake non sarà completato, infatti alla chiusura della comunicazione non otterremo un pacchetto ACK ma un pacchetto RST (reset).

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 0-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 09:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.000065s 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:AC:A6:3F (Oracle VirtualBox virtual NIC)
```

FONTE SCAN	DESTINAZIONE SCAN	PORTA	SERVIZIO
192.168.50.100	192.168.50.101	23	telnet
192.168.50.100	192.168.50.101	25	smtp
192.168.50.100	192.168.50.101	53	domain
192.168.50.100	192.168.50.101	80	http
192.168.50.100	192.168.50.101	111	rpcbind
192.168.50.100	192.168.50.101	139	netbios-ssn

OS DETECTED SCAN

Infine è stata effettuata una scansione di tipo Os Detected con il parametro << -A >>. Questo tipo di scansione ci permette di avere molte più informazioni su ogni porta come:

- Status
- Versione utilizzata
- Hostkey dell'ssh
- Versioni supportate
- Tipologia di server in uso

Questo tipo di scansione è fondamentale nel nostro ambito, in quanto conoscere la versione di un Database o il tipo di kernel ci permetterà di scoprire più facilmente le vulnerabilità ad esso associate:

```

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
|_ssl2:
|_    SSLv2 supported
|_ciphers:
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSM
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       35710/tcp  mountd
|_    100005  1,2,3       60677/udp  mountd
|_    100021  1,3,4       35420/udp  nlockmgr
|_    100021  1,3,4       48046/tcp  nlockmgr
|_    100024  1           39356/udp  status
|_    100024  1           47804/tcp  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:AC:A6:3F (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:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_smb-security-mode:
|_    account_used: guest
|_    authentication_level: user
|_    challenge_response: supported
|_    message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-os-discovery:
|_    OS: Unix (Samba 3.0.20-Debian)
|_    Computer name: metasploitable
|_    NetBIOS computer name:
|_    Domain name: localdomain
|_    FQDN: metasploitable.localdomain
|_    System time: 2022-11-10T09:52:17-05:00
|_clock-skew: mean: 2h30m00s, deviation: 3h32m08s, median: 0s

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.31 ms 192.168.50.101

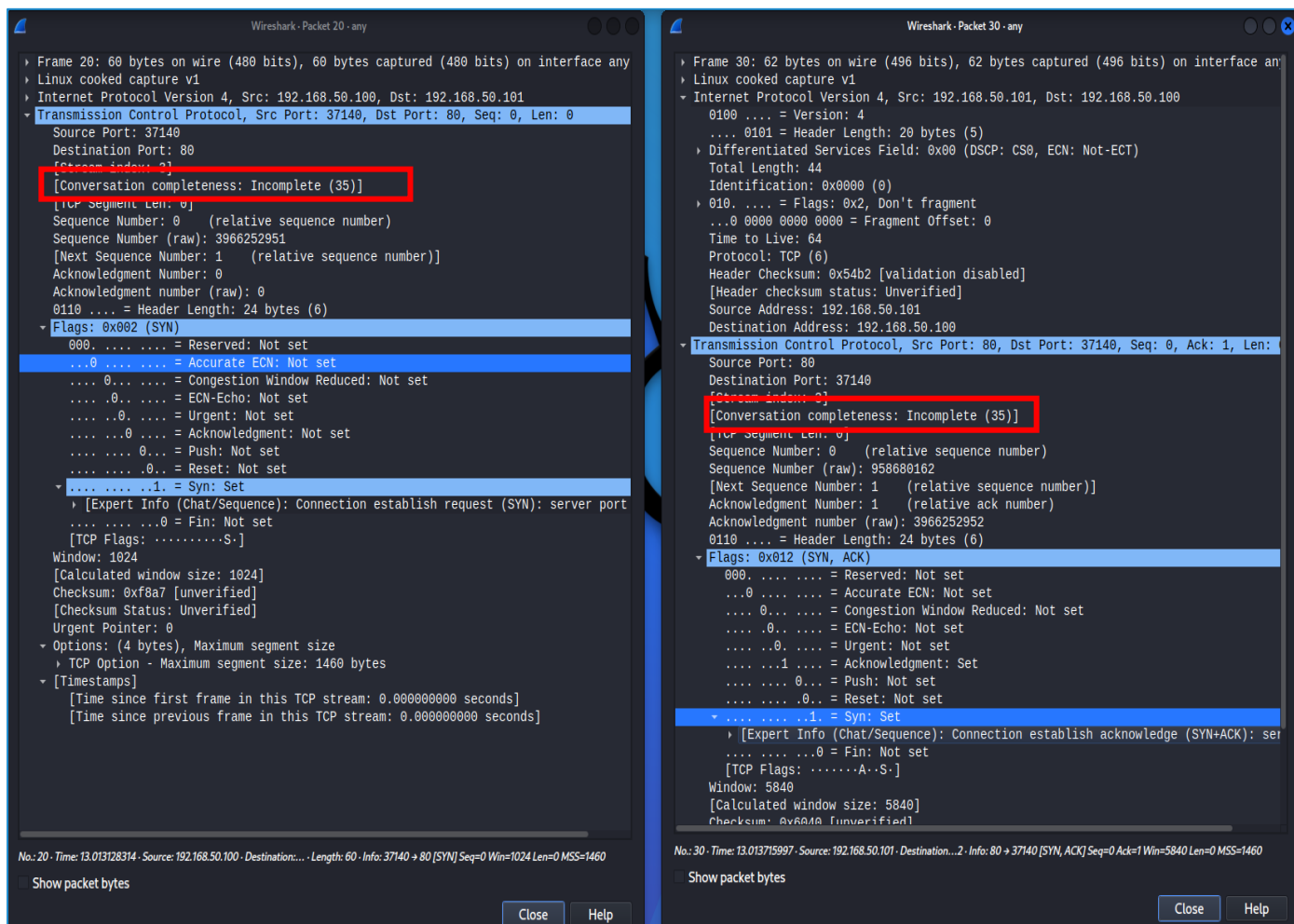
```

WIRESHARK

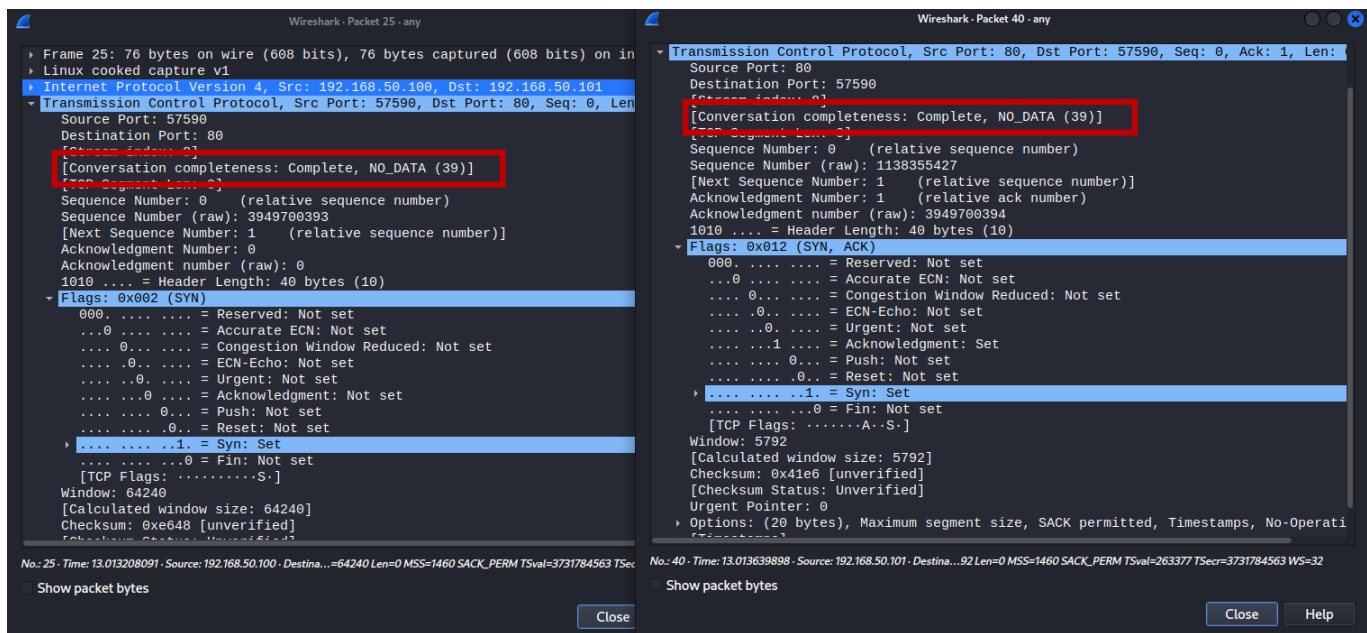
Come ultimo procedimento è stato utilizzato Wireshark per studiare il comportamento dei pacchetti tramite la richiesta TCP e SYN.

Difatti come affermato in precedenza, anche il suddetto tool ci mostra come “”Conversazione”” risulta Incompleta nel metodo SYN analogamente risulta, invece, completa nel metodo TCP

ANALISI COMUNICAZIONE PORTA 80 METODO SYN:



ANALISI COMUNICAZIONE PORTA 80 METODO TCP:



Di seguito riportati gli screen della cattura pacchetti con relativa comunicazione (si prenda sempre in esame porta 80):

METODO SYN:

36	13.014881991	192.168.50.100	192.168.50.101	TCP	58 48965 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
37	13.014887114	192.168.50.100	192.168.50.101	TCP	58 48965 → 334 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
38	13.014892108	192.168.50.100	192.168.50.101	TCP	58 48965 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39	13.014896597	192.168.50.100	192.168.50.101	TCP	58 48965 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	13.014921428	192.168.50.100	192.168.50.101	TCP	58 48965 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	13.014940141	192.168.50.100	192.168.50.101	TCP	58 48965 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	13.014944462	192.168.50.100	192.168.50.101	TCP	58 48965 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43	13.014963717	192.168.50.100	192.168.50.101	TCP	58 48965 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	13.014969306	192.168.50.100	192.168.50.101	TCP	58 48965 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	13.014975551	192.168.50.100	192.168.50.101	TCP	58 48965 → 678 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	13.015037695	192.168.50.101	192.168.50.100	TCP	60 111 → 48965 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
47	13.015037747	192.168.50.101	192.168.50.100	TCP	60 80 → 48965 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
48	13.015037775	192.168.50.101	192.168.50.100	TCP	60 554 → 48965 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	13.015037805	192.168.50.101	192.168.50.100	TCP	60 995 → 48965 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
50	13.015043780	192.168.50.100	192.168.50.101	TCP	54 48965 → 111 [RST] Seq=1 Win=0 Len=0
51	13.015050594	192.168.50.100	192.168.50.101	TCP	54 48965 → 80 [RST] Seq=1 Win=0 Len=0

METODO TCP:

15	13.016032781	192.168.50.100	192.168.50.101	TCP	74 55806 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1866393777 TSecr=0 WS=128
16	13.016035456	192.168.50.100	192.168.50.101	TCP	74 50260 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1866393777 TSecr=0 WS=128
17	13.016040502	192.168.50.100	192.168.50.101	TCP	74 47252 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1866393777 TSecr=0 WS=128
18	13.016095101	192.168.50.100	192.168.50.101	TCP	74 50376 → 119 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1866393777 TSecr=0 WS=128
19	13.016174857	192.168.50.101	192.168.50.100	TCP	60 80 → 55806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	13.016174114	192.168.50.101	192.168.50.100	TCP	74 80 → 55806 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=309838 TSecr=1866393777 WS=32
21	13.016174137	192.168.50.101	192.168.50.100	TCP	74 445 → 50268 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=309838 TSecr=1866393777 WS=32
22	13.016174159	192.168.50.101	192.168.50.100	TCP	60 135 → 47252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	13.016174183	192.168.50.101	192.168.50.100	TCP	60 119 → 50376 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	13.016189585	192.168.50.100	192.168.50.101	TCP	66 55806 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1866393777 TSecr=309838