ANDREA CUORE

10-11-2022

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.

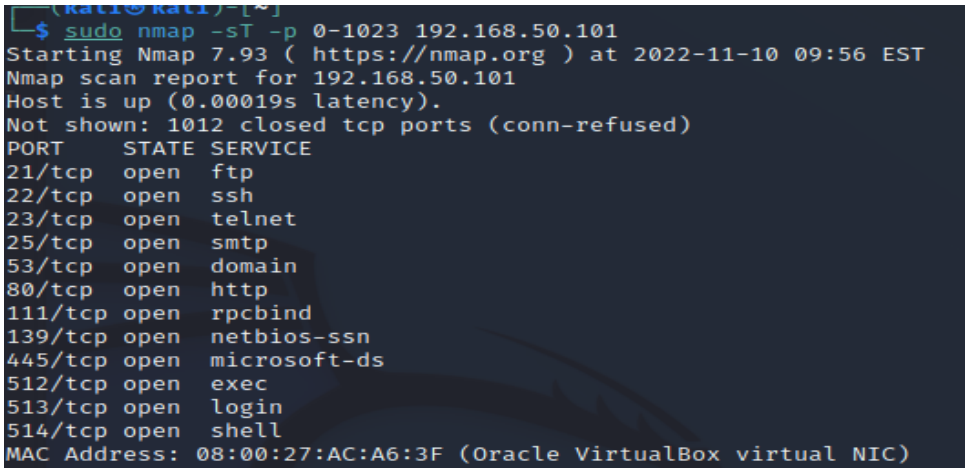
I metodi di scansione erano del tipo:

- 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):

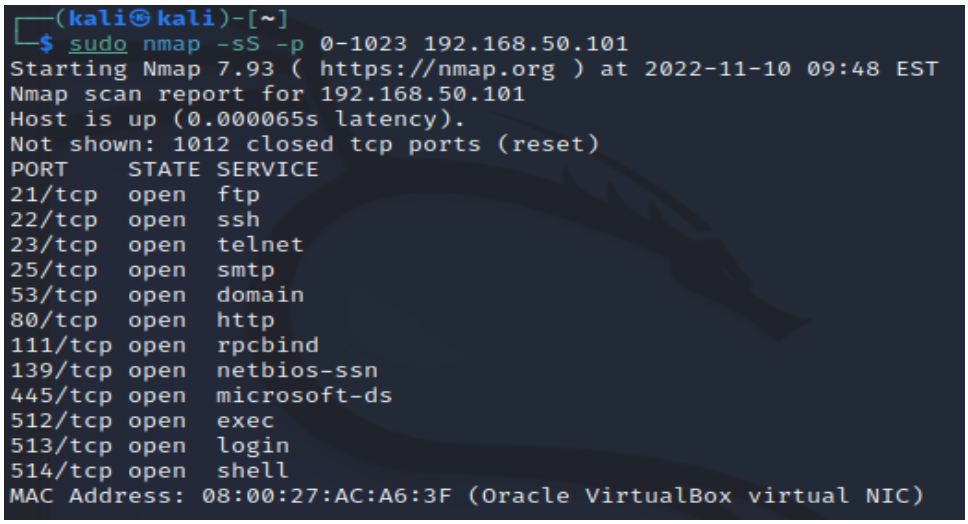


FONTE SCAN	DESTINAZIONE SCAN	PORTA	SERVIZIO
192.168.50.100	192.168.50.101	23	telnet
192.168.50.100	192.168.50.101	25	smtp
192.168.50.100	192.168.50.101	53	domain
192.168.50.100	192.168.50.101	80	http
192.168.50.100	192.168.50.101	111	rpcbind
192.168.50.100	192.168.50.101	139	netbios-ssn
192.168.50.100	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 otteremo un pacchetto ACK ma un pacchetto RST (reset).



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
| sslv2:
|   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, 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      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
```

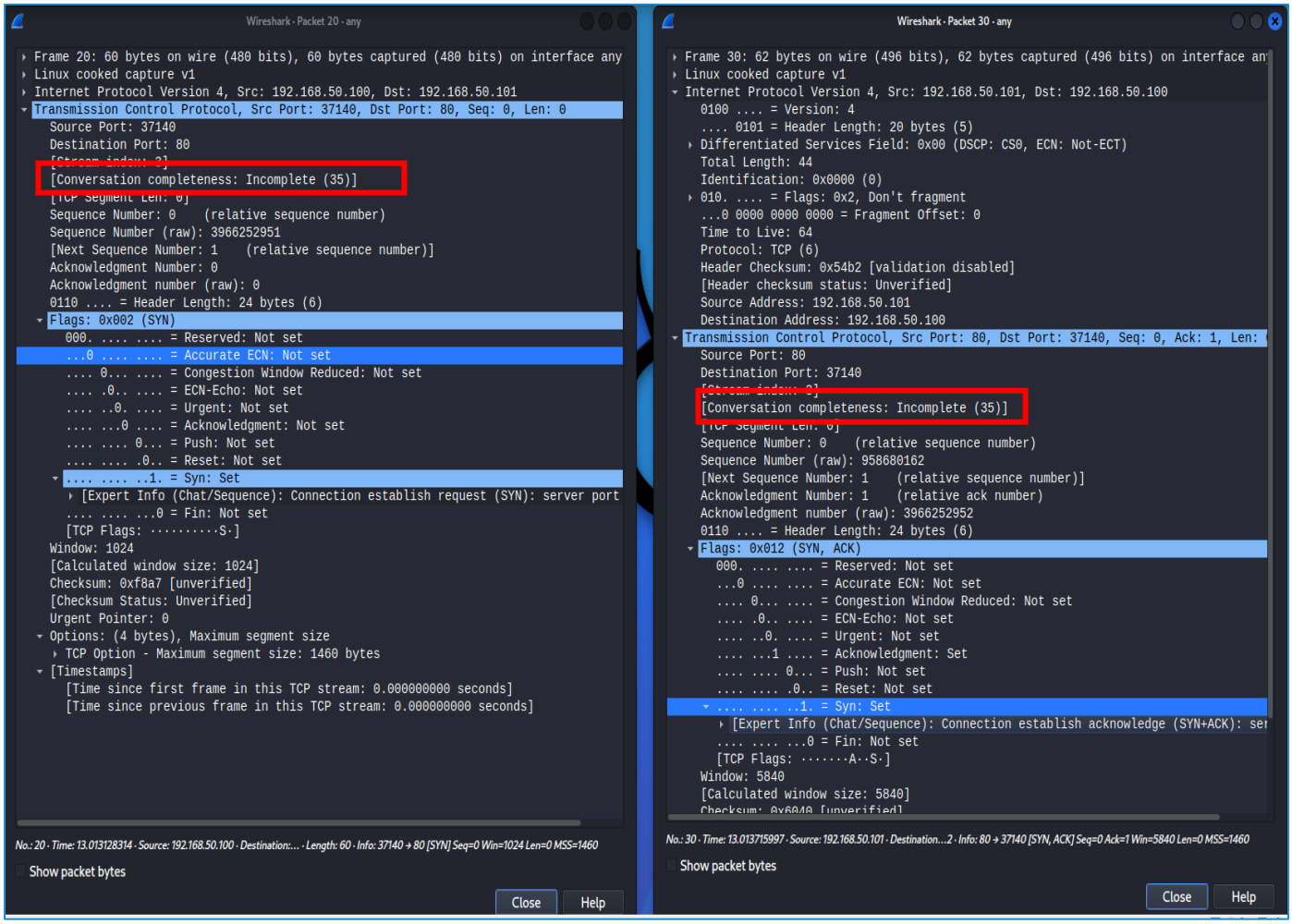
```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:AC:A6:3F (Oracle VirtualBox 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

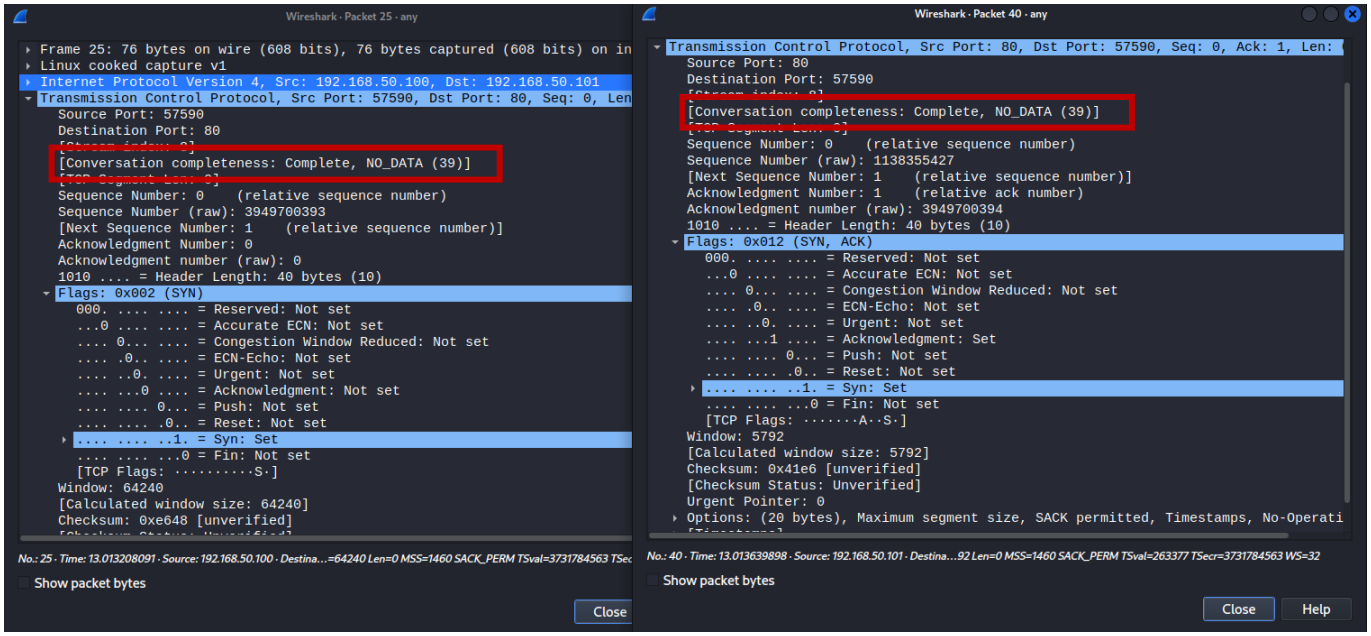
Come ultimo procedimento è stato utilizzato Wireshark per studiare il comportamento dei pacchetti tramite la richiesta TCP e SYN.

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

ANALISI COMUNICAZIONE PORTA 80 METODO SYN:

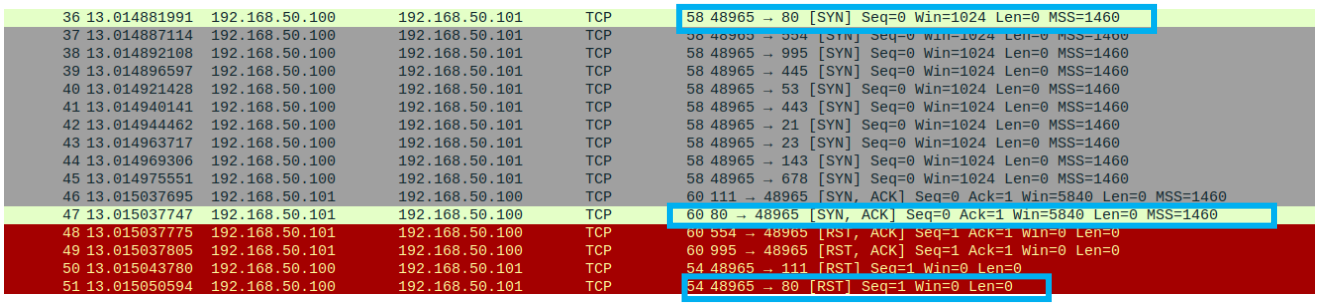


ANALISI COMUNICAZIONE PORTA 80 METODO TCP:



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

METODO SYN:



METODO TCP: