

UTILIZZO DEL COMANDO NETCAT

Eserc. 17/07/2023

Utilizziamo il comando Netcat -l(listen) -p(port) 4321 per entrare in ascolto sulla porta 4321.

```
(kali㉿kali)-[~]  
$ netcat -l -p 4321  
ciao  
ciao  
█
```

Dopo con il comando Netcat 127.0.0.1(ip locale della macchina) 4321 creiamo una situazione di Client/Server dove noi siamo in ascolto (con il comando utilizzato in precedenza) e ogni richiesta fatta sul server noi riusciamo a visualizzarla sul terminale.

```
(kali㉿kali)-[~]  
$ netcat 127.0.0.1 4321  
ciao  
ciao  
█
```

```
(kali㉿kali)-[~]  
$ netcat -l -p 4321  
ls  
attacco.py  
calcoloarea  
calcoloarea.c  
gioco  
gioco.c  
█
```

Dopo aver verificato la connessione procediamo a utilizzare il comando `uname -a` per avere informazioni sul sistema utilizzato.

```
(kali㉿kali)-[~]  
$ uname -a  
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) x86_64 GNU/Linux
```

Mentre per verificare il nome utente utilizziamo il comando `whoami`

```
whoami  
kali  
█
```

Adesso, grazie a Wireshark andiamo a verificare i vari tipi di connessioni:

Qui utilizziamo nmap -sT, un metodo aggressivo che va a creare effettivamente un canale di comunicazione per recuperare informazioni sul servizio in ascolto.

```
(kali㉿kali)-[~/Desktop/eseguibili]
└─$ nmap -sT 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-26 13:57 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0027s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
```

tcp.port == 1355

No.	Time	Source	Destination	Protocol	Length	Info
271	277.585693682	192.168.32.100	192.168.32.101	TCP	74	46072 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1227053752 TSecr=0 WS=128
292	277.599537742	192.168.32.101	192.168.32.100	TCP	74	135 → 46072 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=9886 TSecr=1227053752
297	277.603949654	192.168.32.100	192.168.32.101	TCP	66	46072 → 135 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1227053767 TSecr=9886
298	277.604442414	192.168.32.100	192.168.32.101	TCP	66	46072 → 135 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1227053770 TSecr=9886

Qui utilizziamo nmap -sS, un metodo meno aggressivo che dopo aver verificato che ci sia il canale di comunicazione e aver ricevuto il pacchetto SYN/ACK non va a concludere il 3-way-handshake.

Appurato lo stato della porta termina la comunicazione.

```
(kali㉿kali)-[~/Desktop/eseguibili]
└─$ sudo nmap -sS 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-26 14:10 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0020s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:98:03:97 (Oracle VirtualBox virtual NIC)
```

tcp.port == 135

No.	Time	Source	Destination	Protocol	Length	Info
10	13.171068243	192.168.32.100	192.168.32.101	TCP	58	41080 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	13.172276880	192.168.32.101	192.168.32.100	TCP	60	135 → 41080 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
25	13.172363131	192.168.32.100	192.168.32.101	TCP	54	41080 → 135 [RST] Seq=1 Win=0 Len=0

Infine utilizziamo il metodo nmap -A, un metodo molto aggressivo per riuscire ad acquisire più informazioni possibili, facendo più rumore sulla rete, ma avendo tutti i dettagli di cui potremmo avere bisogno.

```
(kali㉿kali)-[~/Desktop/eseguibili]
$ nmap -A 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-26 14:17 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0025s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WINDOWS; OS: Windows; CPE: o:microsoft:windows

Host script results:
|_ clock-skew: mean: -40m02s, deviation: 1h09m16s, median: -2s
|_ nbstat: NetBIOS name: WINDOWS, NetBIOS user: <unknown>, NetBIOS MAC: 080027980397 (Oracle VirtualBox virtual NIC)
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   210:
|_     Message signing enabled but not required
|_ smb2-time:
|   date: 2023-07-26T18:18:39
|_   start_date: 2023-07-26T17:56:48
|_ smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:o:microsoft:windows_7::sp1
|   Computer name: Windows
|   NetBIOS computer name: WINDOWS\x00
|   Workgroup: WORKGROUP\x00
|_   System time: 2023-07-26T20:18:39+02:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.49 seconds
```

tcp.port == 139					
No.	Time	Source	Destination	Protocol	Length Info
38	15.82244035	192.168.32.100	192.168.32.101	TCP	74 58410 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1228234122 TSecr=0 WS=128
42	13.826371612	192.168.32.101	192.168.32.100	TCP	74 139 → 58410 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=127929 TSecr=1228234122
45	13.826390987	192.168.32.100	192.168.32.101	TCP	66 58410 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1228234125 TSecr=127929
72	13.839185959	192.168.32.100	192.168.32.101	TCP	66 58410 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1228234137 TSecr=127929
2030	13.455671844	192.168.32.100	192.168.32.101	TCP	74 58422 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1228234554 TSecr=0 WS=128
2036	13.457939359	192.168.32.101	192.168.32.100	TCP	74 139 → 58422 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=127972 TSecr=1228234554
2040	13.458019453	192.168.32.100	192.168.32.101	TCP	66 58422 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1228234556 TSecr=127972
2058	19.501723638	192.168.32.100	192.168.32.101	NBSS	84 NBSS Continuation Message
2067	19.507942539	192.168.32.101	192.168.32.100	NBSS	71 Negative session response, Unspecified error
2076	19.515585436	192.168.32.100	192.168.32.101	TCP	66 58422 → 139 [FIN, ACK] Seq=19 Ack=7 Win=64256 Len=0 TSval=1228240614 TSecr=128576
2077	19.516964397	192.168.32.100	192.168.32.101	TCP	74 58438 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1228240614 TSecr=0 WS=128
2082	19.517234972	192.168.32.101	192.168.32.100	TCP	66 139 → 58422 [ACK] Seq=7 Ack=20 Win=66560 Len=0 TSval=128577 TSecr=1228240614
2085	19.518349153	192.168.32.101	192.168.32.100	TCP	74 139 → 58438 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=128577 TSecr=1228240614
- Frame 38: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0					
Section number: 1					
Interface id: 0 (eth0)					
Encapsulation type: Ethernet (1)					
0000 08 00 27 98 03 97 08 00 27 de 8e 39 08 0000 00 3c 93 82 40 00 40 06 e5 1f c0 a8 200020 20 65 e4 2a 00 8b c2 bb 6e 69 00 00 000000 fa f0 c2 48 00 00 02 04 05 b4 04 02 080000 5d 8a 00 00 00 00 01 63 63 67					