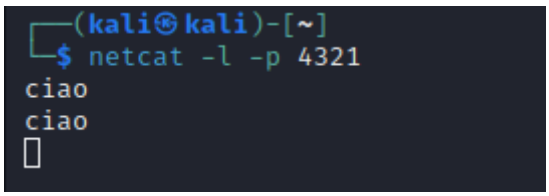
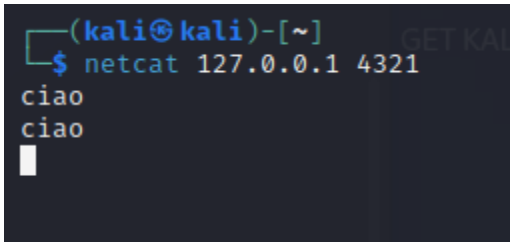
UTILIZZO DEL COMANDO NETCAT

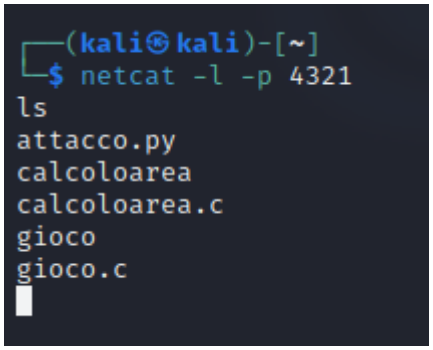
Eserc. 17/07/2023

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

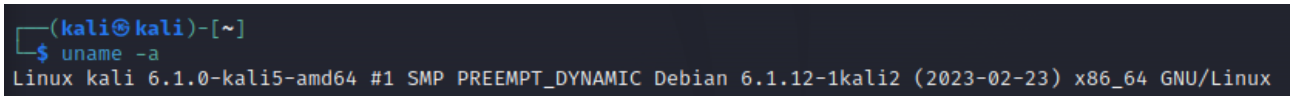


Dopo con il comando Netcat 127.0.0.1(ip locale della macchina) 4321 creiamo una situazione di Client/Server dove noi siamo in ascolto (con il comando utilizzato in precedenza) e ogni richiesta fatta sul server noi riusciamo a visualizzarla sul terminale.

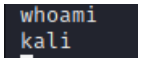




Dopo aver verificato la connessione procediamo a utilizzare il comando uname -a per avere informazioni sul sistema utilizzato.



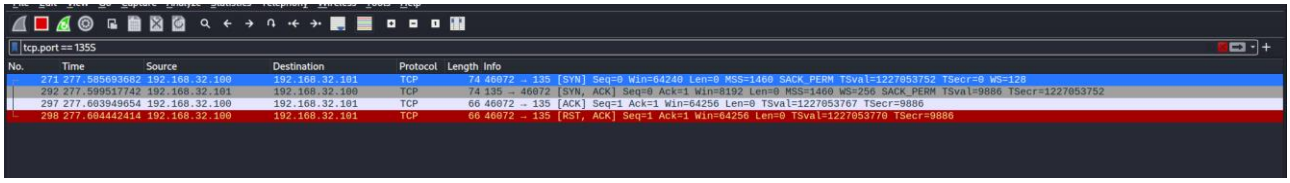
Mentre per verificare il nome utente utilizziamo il comando whoami



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

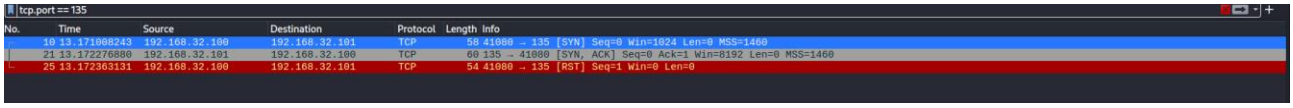
Qui utilizziamo nmap -sT, un metodo aggressivo che va a creare effettivamente un canale di comunicazione per recuperare informazioni sul servizio in ascolto.

```
┌──(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
```



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 comuicazione.

```
┌──(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)
```



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: 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
```