

W12 D4 BENCHMARK

abbiamo effettuato la scansione con il software nessus sulla macchina metasploitable 2 sono (con indirizzo ip 192.168.1.7)state trovate 114 vulnerabilità

Filter

Search Vulnerabilities

68 Vulnerabilities

<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/> CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1		
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1		
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1		
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1		
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/> HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1		
<input type="checkbox"/> HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1		
<input type="checkbox"/> HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1		
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1		
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	General	28		
<input type="checkbox"/> MIXED	ISC Bind (Multiple Issues)	DNS	5		

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 9:53 AM

End:

Today at 10:31 AM

Elapsed:

38 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

dal report sotto riportato sono state trovate 9 vulnerabilità con classificazione CRITICAL in base al CVSS Score

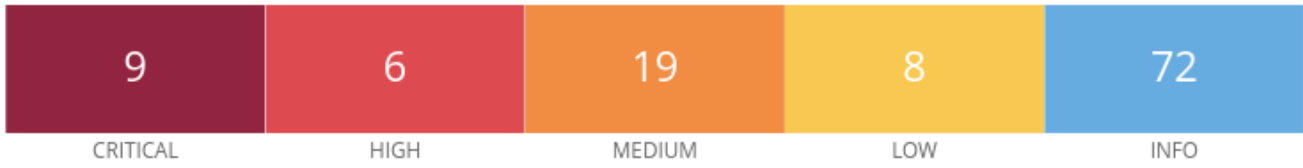
Il CVSS Score (Common Vulnerability Scoring System) è un sistema standardizzato per valutare la gravità delle vulnerabilità informatiche. Assegna un punteggio numerico da 0 a 10, dove un punteggio più alto indica una vulnerabilità più grave.

Oltre al punteggio numerico, il CVSS Score include anche una classificazione che categorizza le vulnerabilità in base alla loro gravità:

- **Bassa:** Impatto minimo o nullo sul sistema.
- **Media:** Danni moderati al sistema.
- **Alta:** Danni significativi al sistema.
- **Critica:** Gravi danni o compromissione completa del sistema.

Il CVSS Score è solo uno strumento per valutare la gravità di una vulnerabilità. Altri fattori, come il contesto specifico e le risorse disponibili per la mitigazione, devono essere presi in considerazione quando si prendono decisioni su come affrontare una vulnerabilità.

192.168.1.7



Vulnerabilities

Total: 114

lanciamo il comando nmap da Kali per vedere le porte aperte

```

(kali㉿kali)-[~]
$ sudo nmap -sS -v -O 192.168.1.7
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 10:15 CEST
Initiating ARP Ping Scan at 10:15
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 10:15, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:15
Completed Parallel DNS resolution of 1 host. at 10:15, 0.00s elapsed
Initiating SYN Stealth Scan at 10:15
Scanning Host-003.homenet.telecomitalia.it (192.168.1.7) [1000 ports]
Discovered open port 5900/tcp on 192.168.1.7
Discovered open port 139/tcp on 192.168.1.7
Discovered open port 111/tcp on 192.168.1.7
Discovered open port 22/tcp on 192.168.1.7
Discovered open port 80/tcp on 192.168.1.7
Discovered open port 53/tcp on 192.168.1.7
Discovered open port 3306/tcp on 192.168.1.7
Discovered open port 21/tcp on 192.168.1.7
Discovered open port 445/tcp on 192.168.1.7
Discovered open port 25/tcp on 192.168.1.7
Discovered open port 23/tcp on 192.168.1.7
Discovered open port 513/tcp on 192.168.1.7
Discovered open port 8180/tcp on 192.168.1.7
Discovered open port 8009/tcp on 192.168.1.7
Discovered open port 1099/tcp on 192.168.1.7
Discovered open port 2049/tcp on 192.168.1.7
Discovered open port 1524/tcp on 192.168.1.7
Discovered open port 6667/tcp on 192.168.1.7
Discovered open port 5432/tcp on 192.168.1.7
Discovered open port 514/tcp on 192.168.1.7
Discovered open port 6000/tcp on 192.168.1.7
Discovered open port 512/tcp on 192.168.1.7
Discovered open port 2121/tcp on 192.168.1.7
Completed SYN Stealth Scan at 10:15, 0.05s elapsed (1000 total ports)
Initiating OS detection (try #1) against Host-003.homenet.telecomitalia.it (192.168.1.7)
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.00081s latency).
Completed SYN Stealth Scan at 10:15, 0.05s elapsed (1000 total ports)
Initiating OS detection (try #1) against Host-003.homenet.telecomitalia.it (192.168.1.7)
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:DE:81:F6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.014 days (since Sat May 11 09:55:20 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)

```

di seguito le vulnerabilità trattate

CRITICAL 10.0* - 61708 VNC Server 'password' Password

Scan Summary Hosts 1 Vulnerabilities 68 Remediations 3 Notes 1 History 3

CRITICAL VNC Server 'password' Password

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution
Secure the VNC service with a strong password.

Output
No output recorded.

To see debug logs, please visit individual host

Port	Hosts
5900 / tcp / vnc	192.168.1.7

Plugin Details

Severity: Critical
ID: 61708
Version: \$Revision: 1.2 \$
Type: remote
Family: Gain a shell remotely
Published: August 29, 2012
Modified: September 24, 2015

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true
Exploited by Nessus: true

lanciando il comando da kali come sotto riportato e inserendo la password password avremo pieno accesso alla macchina metasploitable 2 dove per esempio possiamo lanciare il comando ip a e possiamo vedere l'indirizzo ip della macchina in analisi 192.168.1.7

The screenshot shows a Kali Linux terminal window on the left and a TightVNC window on the right. The terminal window displays the command `wncviewer 192.168.1.7` and the output of the VNC connection, including the password 'password' and the desktop name 'root's X desktop (metasploitable:0)'. The TightVNC window shows the desktop environment of metasploitable2, with a terminal window open displaying the command `ip a` and its output, which includes the IP address 192.168.1.7.

rimediamo, come sotto riportato, cambiando la password

```

msfadmin@metasploitable:~$ sudo vncpasswd
[sudo] password for msfadmin:
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$

```

in seguito chiuderemo anche la porta del servizio 5900

2

CRITICAL 10.0* 5.9 11356 NFS Exported Share Information Disclosure

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```

The following NFS shares could be mounted :
+ /
+ Contents of / :
- .
- ..
- bin
- boot
more...

```

To see debug logs, please visit individual host

Port	Hosts
2049 / udp / rpc-nfs	192.168.1.7

Plugin Details

Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSv3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C

lanciamo il seguente comando

```
nano /etc/exports
```

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#                to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
#
# *(rw,sync,no_root_squash,no_subtree_check)

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

inseriamo l'ip della macchina 192.168.1.7 in modo da impedire l'accesso a altri utenti

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

/etc/exports: the access control list for filesystems which may be exported
                to NFS clients.  See exports(5).

Example for NFSv2 and NFSv3:
/srv/homes      hostname1(rw,sync) hostname2(ro,sync)

Example for NFSv4:
/srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
/srv/nfs4/homes gss/krb5i(rw,sync)

192.168.1.7(rw,sync,no_root_squash,no_subtree_check)
```

CRITICAL

Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```

Nessus was able to execute the command "id" using the
following request :

..... snip .....

This produced the following truncated output (limited to 10 lines) :
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
..... snip .....

```

To see debug logs, please visit individual host

Port	Hosts
1524 / tcp / wild_shell	192.168.1.7

Plugin Details

Severity: Critical

ID: 51988

Version: 1.10

Type: remote

Family: Backdoors

Published: February 15, 2011

Modified: April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

in questa vulnerabilità basta collegarci a metasploitable 2 alla porta 1524 con il comando netcat

```

(kali@kali)-[~]
$ nc 192.168.1.7 1524
root@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
        inet6 ::1/128 scope host
            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:de:81:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.7/24 brd 192.168.1.255 scope global eth0
        inet6 fe80::a00:27ff:fede:81f6/64 scope link
            valid_lft forever preferred_lft forever
root@metasploitable:/#

```

per avere direttamente una connessione come root

dalla precedente scansione con nmap

1524/tcp open ingreslock

la porta 1524 risulta aperta

facendo una rapida ricerca ho trovato il seguente sito

http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-0203/Scansione_servizi_rete/SAINT_DOCS/tutorials/vulnerability/Vulnerability_Exploits.html

dove si possono modificare i parametri di ingreslock al file inetd.conf

```
GNU nano 2.0.7          File: /etc/inetd.conf          Modified
#<off># netbios-ssn      stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
telnet                  stream  tcp    nowait  telnetd  /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp              stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp                   dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec                   stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
#ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

andremo a commentare l'ultima riga con #

```
#ingreslock stream tcp nowait root /bin/bash bash -i
```

andando a lanciare nuovamente il comando netcat e di seguito nmap sulla porta 1524 il servizio non sarà + raggiungibile e la porta risulta chiusa

```
(kali@kali)-[~]
$ nc 192.168.1.7 1524
(UNKNOWN) [192.168.1.7] 1524 (ingreslock) : Connection refused
```



```

(kali@kali)-[~]
$ sudo nmap -sV -v 192.168.1.7 -p 1524
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 15:53 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 15:53
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 15:53, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:53
Completed Parallel DNS resolution of 1 host. at 15:53, 0.00s elapsed
Initiating SYN Stealth Scan at 15:53
Scanning Host-003.homenet.telecomitalia.it (192.168.1.7) [1 port]
Completed SYN Stealth Scan at 15:53, 0.01s elapsed (1 total ports)
Initiating Service scan at 15:53
NSE: Script scanning 192.168.1.7.
Initiating NSE at 15:53
Completed NSE at 15:53, 0.00s elapsed
Initiating NSE at 15:53
Completed NSE at 15:53, 0.00s elapsed
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.00040s latency).

PORT      STATE SERVICE      VERSION
1524/tcp  closed ingreslock
MAC Address: 08:00:27:DE:81:F6 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (68B)

```

4

analogamente possiamo rimediare alla seguente vulnerabilità

HIGH

7.5*

5.9

10205

rlogin Service Detection

HIGH

rlogin Service Detection

< >

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
513 / tcp / rlogin	192.168.1.7

andando a commentare il file inetd.conf alla riga login

```
#login      stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rls
```

di seguito le scansioni di nmap prima e dopo la modifica

```

(kali@kali)-[~]
$ sudo nmap -sV -v 192.168.1.7 -p 513
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 16:17 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 16:17
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 16:17, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:17
Completed Parallel DNS resolution of 1 host. at 16:17, 0.00s elapsed
Initiating SYN Stealth Scan at 16:17
Scanning Host-003.homenet.telecomitalia.it (192.168.1.7) [1 port]
Discovered open port 513/tcp on 192.168.1.7
Completed SYN Stealth Scan at 16:17, 0.02s elapsed (1 total ports)
Initiating Service scan at 16:17
Scanning 1 service on Host-003.homenet.telecomitalia.it (192.168.1.7)
Completed Service scan at 16:17, 6.13s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.7.
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.00034s latency).

PORT      STATE SERVICE VERSION
513/tcp   open  login   OpenBSD or Solaris rlogind
MAC Address: 08:00:27:DE:81:F6 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.46 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

```

```

(kali@kali)-[~]
$ sudo nmap -sV -v 192.168.1.7 -p 513
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 16:30 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 16:30
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 16:30, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:30
Completed Parallel DNS resolution of 1 host. at 16:30, 0.00s elapsed
Initiating SYN Stealth Scan at 16:30
Scanning Host-003.homenet.telecomitalia.it (192.168.1.7) [1 port]
Completed SYN Stealth Scan at 16:30, 0.23s elapsed (1 total ports)
Initiating Service scan at 16:30
NSE: Script scanning 192.168.1.7.
Initiating NSE at 16:30
Completed NSE at 16:30, 0.00s elapsed
Initiating NSE at 16:30
Completed NSE at 16:30, 0.00s elapsed
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.00049s latency).

PORT      STATE SERVICE VERSION
513/tcp   filtered login   OpenBSD or Solaris rlogind
MAC Address: 08:00:27:DE:81:F6 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
Raw packets sent: 3 (116B) | Rcvd: 1 (28B)

```

dove si nota che la porta 513 è prima aperta e poi chiusa

5

HIGH

7.5

5.9

90509

Samba Badlock Vulnerability

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

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.1.7

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

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
139 / tcp / smb	192.168.1.13

andando a scansionare con nmap una delle due porte dove si trova il servizio

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -v 192.168.1.7 -p 445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 16:07 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 16:07
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 16:07, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:07
Completed Parallel DNS resolution of 1 host. at 16:07, 0.00s elapsed
Initiating SYN Stealth Scan at 16:07
Scanning Host-003.homenet.telecomitalia.it (192.168.1.7) [1 port]
Discovered open port 445/tcp on 192.168.1.7
Completed SYN Stealth Scan at 16:07, 0.02s elapsed (1 total ports)
Initiating Service scan at 16:07
Scanning 1 service on Host-003.homenet.telecomitalia.it (192.168.1.7)
Completed Service scan at 16:07, 6.09s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.7.
Initiating NSE at 16:07
Completed NSE at 16:07, 0.00s elapsed
Initiating NSE at 16:07
Completed NSE at 16:07, 0.00s elapsed
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.00049s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:DE:81:F6 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

andremo a modificare il firewall di metasploitable 2

con i seguenti comandi

dove da prima abiliteremo il firewall

```
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
```

e in seguito con i comandi

ufw deny 139

ufw deny 445

ufw deny 5900

disabiliteremo le porte

quii di seguito le regole del firewall

```
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

To Action From
--
445:tcp DENY Anywhere
445:udp DENY Anywhere
139:tcp DENY Anywhere
139:udp DENY Anywhere
5900:tcp DENY Anywhere
5900:udp DENY Anywhere
Anywhere ALLOW 192.168.1.0/24
```

riavviamo la macchina

lanciamo il precedente comando di nmap da kali sulla porta 445 presa in esame

```
(kali@kali)-[~]
$ sudo nmap -sV -v 192.168.1.7 -p 445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 16:30 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 16:30
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 16:30, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:30
Completed Parallel DNS resolution of 1 host. at 16:30, 0.00s elapsed
Initiating SYN Stealth Scan at 16:30
Scanning Host-003.homenet.telecomitalia.it (192.168.1.7) [1 port]
Completed SYN Stealth Scan at 16:30, 0.22s elapsed (1 total ports)
Initiating Service scan at 16:30
NSE: Script scanning 192.168.1.7.
Initiating NSE at 16:30
Completed NSE at 16:30, 0.00s elapsed
Initiating NSE at 16:30
Completed NSE at 16:30, 0.00s elapsed
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.00046s latency).

PORT      STATE      SERVICE      VERSION
445/tcp    filtered  microsoft-ds
MAC Address: 08:00:27:DE:81:F6 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
Raw packets sent: 3 (116B) | Rcvd: 1 (28B)
```


e la scansione su tutte le porte

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV --reason -v 192.168.1.13
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-12 22:28 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 22:28
Scanning 192.168.1.13 [1 port]
Completed ARP Ping Scan at 22:28, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:28
Completed Parallel DNS resolution of 1 host. at 22:28, 0.00s elapsed
Initiating SYN Stealth Scan at 22:28
Scanning Host-003.homenet.telecomitalia.it (192.168.1.13) [1000 ports]
Discovered open port 22/tcp on 192.168.1.13
Discovered open port 111/tcp on 192.168.1.13
Discovered open port 23/tcp on 192.168.1.13
Discovered open port 80/tcp on 192.168.1.13
Discovered open port 25/tcp on 192.168.1.13
Discovered open port 3306/tcp on 192.168.1.13
Discovered open port 21/tcp on 192.168.1.13
Discovered open port 2121/tcp on 192.168.1.13
Discovered open port 6000/tcp on 192.168.1.13
Discovered open port 2049/tcp on 192.168.1.13
Discovered open port 512/tcp on 192.168.1.13
Discovered open port 8180/tcp on 192.168.1.13
Discovered open port 514/tcp on 192.168.1.13
Discovered open port 8009/tcp on 192.168.1.13
Discovered open port 1099/tcp on 192.168.1.13
Discovered open port 5432/tcp on 192.168.1.13
Discovered open port 6667/tcp on 192.168.1.13
Completed SYN Stealth Scan at 22:29, 1.23s elapsed (1000 total ports)
Initiating Service scan at 22:29
Scanning 17 services on Host-003.homenet.telecomitalia.it (192.168.1.13)
Completed Service scan at 22:30, 62.78s elapsed (17 services on 1 host)
NSE: Script scanning 192.168.1.13.
Initiating NSE at 22:30
Completed NSE at 22:30, 0.07s elapsed
Initiating NSE at 22:30
Completed NSE at 22:30, 0.03s elapsed
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.13)
Host is up, received arp-response (0.00053s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE      SERVICE      REASON      VERSION
21/tcp    open      ftp          syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open      ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open      telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open      smtp        syn-ack ttl 64 Postfix smtpd
80/tcp    open      http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open      rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   filtered  netbios-ssn no-response
445/tcp   filtered  microsoft-ds no-response
512/tcp   open      exec?       syn-ack ttl 64
514/tcp   open      tcpwrapped  syn-ack ttl 64
1099/tcp  open      java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
2049/tcp  open      nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open      ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open      mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
5432/tcp  open      postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  filtered  vnc         no-response
6000/tcp  open      X11         syn-ack ttl 64 (access denied)
6667/tcp  open      irc         syn-ack ttl 64 UnrealIRCd
8009/tcp  open      ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open      http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:DE:81:F6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

effettuiamo un ultima scansione con nessus e vediamo che le vulnerabilità trattate non sono piu' presenti

Scan Summary

Hosts1

Vulnerabilities55

Remediations2

History10

Filter

Search Vulnerabilities

55 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detecti...	Backdoors	1		
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsu...	General	1		
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connect...	Web Servers	1		
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol ...	Service detection	2		
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1		
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	26		
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5		
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Det...	Service detection	2		
<input type="checkbox"/>	MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1		

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 10:39 PM

End:

Today at 11:17 PM

Elapsed:

39 minutes

Vulnerabilities

Critical

High

Medium

Low

Info