

Oggi abbiamo
usato il tool
Nessus per fare
una scansione
vulnerabilità
sulla nostra
macchina
Metasploitable,
IP 192.168.32.101

Ha trovato tanti
vulnerabilità, di
cui andremo a
rimediare cuatro.

Meta / 192.168.32.101

[Back to Hosts](#)

Configure

Vulnerabilities 57

Filter Search Vulnerabilities 57 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported Share Information Dis...	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported...	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
CRITICAL	9.8		Apache Tomcat AJP Connector Requ...	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5		Samba Badlock Vulnerability	General	1
MIXED	15 SSL (Multiple Issues)	General	28
MIXED	5 ISC Bind (Multiple Issues)	DNS	5


Host Details

IP: 192.168.32.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Start: Today at 5:37 AM

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

La prima vulnerabilità trovata è un sistema di Network File Sharing (NFS) pubblica, che può essere accesa per utenti non autorizzati che poi avranno il potere di fare molte cose, come vedere informazioni sensibili, modificare i file, fare privilege escalation, e anche inserire malware.

Meta / Plugin #11356

[← Back to Vulnerabilities](#)

Configure

Vulnerabilities 57

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
  adxom
more...
```

To see debug logs, please visit individual host

Port ▲

Hosts

2049 / udp / rpc-nfs

192.168.32.101



Plugin Details

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

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

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 1, 1985

Exploitable With

Metasploit (NFS Mount Scanner)

Un'altra
vulnerabilità
critica trovata e
la nostra
password molto
debole al server
VNC. Nessus è
riuscito ad
indovinare questa
password.
Possiamo
risolvere questo
rischio cambiando
ad una password
più forte e
sicura.

Meta / Plugin #61708

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch ▾

Report

Export ▾

Vulnerabilities 65

CRITICAL VNC Server 'password' Password

< >

Plugin Details

✎

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

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port ▲

Hosts

5900 / tcp / vnc

192.168.32.101

🔗

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

Una backdoor di bind shell è un tipo di software dannoso che apre una porta su nostra macchina meta, in attesa di una connessione in entrata da un utente malintenzionato. Crea una shell collegata a una porta specifica, consentendo all'aggressore di ottenere accesso e controllo non autorizzati sul sistema compromesso.

Ovviamente queste e uno dei rischi più critici che possiamo avere dentro nostra macchina

Meta / Plugin #51988

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

Vulnerabilities 65

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 :

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	192.168.32.101 🔗

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

Samba è un tipo di server hosted per la nostra macchina linux che consente una comunicazione tra una database SAM e un cliente. Metasploitable ha una versione vecchia di cui si ha trovato un rischio di sicurezza che consente l'intercettazione di traffico per parte di un attaccante fungendo di man-in-the-middle

Meta / Plugin #90509

[← Back to Vulnerabilities](#)

ConfigureAudit TrailLaunch▼ReportExport▼

Vulnerabilities65

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	192.168.32.101 🔗

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): 6.7
Risk Factor: Medium