

Exploit Critici post scansione con Nessus:

The screenshot displays the Nessus web interface within a virtual machine. The main content area shows a 'Metasploit scan' report with a table of vulnerabilities. The table columns are: Severity, CVSS, VPR, Name, Family, and Count. The vulnerabilities listed include NFS Exported Share Information Disclosure, Unix Operating System Unsupported Version Detection, VNC Server 'password' Password, SSL Version 2 and 3 Protocol Detection, Bind Shell Backdoor Detection, Apache Tomcat (Multiple Issues), SSL (Multiple Issues), Samba Badlock Vulnerability, NFS Shares World Readable, ISC Bind (Multiple Issues), and TLS Version 1.0 Protocol Detection. On the right, the 'Scan Details' panel shows the policy 'Basic Network Scan', status 'Completed', severity base 'CVSS v3.0', scanner 'Local Scanner', start time 'Today at 11:55 AM', end time 'Today at 12:23 PM', and elapsed time '27 minutes'. Below this is a 'Vulnerabilities' pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0	...	Unix Operating System Unsupported Version Detection	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	...	Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1
HIGH	7.5	...	NFS Shares World Readable	RPC	1
MIXED	ISC Bind (Multiple Issues)	General	28
MIXED	SSL (Multiple Issues)	DNS	5
MEDIUM	6.5	...	TLS Version 1.0 Protocol Detection	Service detection	2

NFS Exported Share Information Disclosure

NFS Exported Share Information Disclosure

Language: English ▾

CRITICAL Nessus Plugin ID 11356

Information

Dependencies

Dependents

Changelog

Synopsis

It is possible to access NFS shares on the remote host.

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.

Plugin Details

Severity: Critical

ID: 11356

File Name: nfs_mount.nasl

Version: 1.21

Type: remote

Family: RPC

Published: 3/12/2003

Updated: 8/30/2023

Supported Sensors: Nessus

Per risolvere questa vulnerabilità, l'unica possibilità che non sono andato a testare sarebbe aggiornare il sistema applicando la patch NFS jumbo (Patch-ID# 100173-13), disponibile sul sito Web di Sun Microsystems.

VNC Server 'password' Password

VNC Server 'password' Password

Language: English ▾

CRITICAL Nessus Plugin ID 61708

Information

Dependencies

Dependents

Changelog

Synopsis

A VNC server running on the remote host is secured with a weak 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.

Plugin Details

Severity: Critical

ID: 61708

File Name:
vnc_password_password.nasl

Version: Revision: 1.2

Type: remote

Family: [Gain a shell remotely](#)

Published: 8/29/2012

Updated: 9/24/2015

Supported Sensors:
Nessus

Il problema in questione è CHE la password utilizzata per autenticarsi su un server VNC è "Password".

Il VNC, acronimo di Virtual Network Computing, è un protocollo che consente di controllare e visualizzare il desktop di un computer da un altro

Per risolvere abbiamo cambiato semplicemente la Password da linea di comando usando il comando "vncpasswd".

Dopo il Sistema chiederà due volte di inserire la password per conferma e basterà inserire una nuova password e premere invio.

Bind Shell Backdoor Detection

Bind Shell Backdoor Detection

Language: English ▾

CRITICAL Nessus Plugin ID 51988

Information

Dependencies

Dependents

Changelog

Synopsis

The remote host may have been compromised.

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.

Plugin Details

Severity: Critical

ID: 51988

File Name:
wild_shell_backdoor.nasl

Version: 1.10

Type: remote

Family: Backdoors

Published: 2/15/2011

Updated: 4/11/2022

Configuration: Enable thorough checks

Supported Sensors:
Nessus

In questo caso ho determinato grazie a Nessus che la porta interessata dalla Backdoor era la 1524, quindi sono andato successivamente ad impostare una regola nel firewall che andasse a bloccare e non a rigettare il tentativo di connessione alla porta. Successivamente per conferma ho lanciato il comando nmap sulla porta 1524 per vedere che la porta

risultasse filtrata. Per vedere se il problema è stato risolto è bastato rifare la scansione su Nessus e confrontare il primo risultato della scansione con il secondo risultato con la regola del firewall applicata.

The screenshot shows the MetasploitScan interface within a Kali Linux virtual machine. The browser displays the URL `https://kali.8834/#/scans/reports/5/vulnerabilities`. The interface is divided into several sections:

- Hosts:** 1
- Vulnerabilities:** 62
- Remediations:** 2
- Notes:** 4
- History:** 3

The main table lists 62 vulnerabilities. The first few rows are:

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0	...	Unix Operating System Unsupported Version Detection	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	...	Bind Shell Backdoor Detection	Backdoors	1
MEDIUM	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1
HIGH	7.5	...	NFS Shares World Readable	RPC	1
MEDIUM	SSL (Multiple Issues)	General	28
MEDIUM	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5	...	TLS Version 1.0 Protocol Detection	Service detection	2

On the right, the **Scan Details** section shows:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 11:55 AM
- End: Today at 12:23 PM
- Elapsed: 27 minutes

Below this is a **Vulnerabilities** donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

The screenshot shows the pfSense Firewall Rules configuration page. The browser displays the URL `https://192.168.50.1/firewall_rules.php?if=lan`. The page has a warning at the top: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager."

The page is titled **Firewall / Rules / LAN**. A green message box states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress."

Below the message, the **Rules (Drag to Change Order)** table is shown. The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/1.16 MB	*	*	*	LAN Address	443	*	*	*	Anti-Logout Rule	⚙️
✗ 0/120 B	IPv4 TCP	*	*	192.168.49.101	1524	*	*	none		⬇️ ⬆️ ⬇️ ⬆️ ⬇️ ⬆️
✓ 1/367.30 MB	IPv4 *	LAN subnets	*	*	*	*	*	none	Default allow LAN to any rule	⬇️ ⬆️ ⬇️ ⬆️ ⬇️ ⬆️
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	⬇️ ⬆️ ⬇️ ⬆️ ⬇️ ⬆️

At the bottom of the table, there are buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

The footer of the page states: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license."

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -p 1524 192.168.49.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 14:25 CET  
Nmap scan report for 192.168.49.101  
Host is up (0.0030s latency).  
  
PORT      STATE      SERVICE  
1524/tcp  filtered  ingreslock  
  
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds  
  
(kali@kali)-[~]  
$
```

