

Scansione metasploitable con Nessus Vulnerability scanner

The screenshot shows a Nessus scan report titled "scan1" for host 192.168.50.101. The report includes a table of contents and a summary bar chart showing the distribution of vulnerabilities by severity: Critical (10), High (6), Medium (23), Low (5), and Info (128).

Severity	Count
Critical	10
High	6
Medium	23
Low	5
Info	128

The screenshot shows the Nessus interface displaying a list of vulnerabilities for scan "scansione2". The list includes the following entries:

Severity	Score	Name	Plugin ID	Count
Critical	10.0 *	NFS Export...	RPC	1
Critical	10.0	Unix Opera...	General	1
Critical	10.0 *	VNC Server...	Gain a shell remotely	1
Critical	9.8	Apache To...	Web Servers	1
Critical	9.8	Bind Shell ...	Backdoors	1
High	7.5	NFS Shares...	RPC	1
High	7.5	Samba Bad...	General	1
Medium	6.5	TLS Versio...	Service detection	2
Medium	5.9	SSL DROW...	Misc.	1

The interface also displays "Scan Details" and a "Vulnerabilities" pie chart.

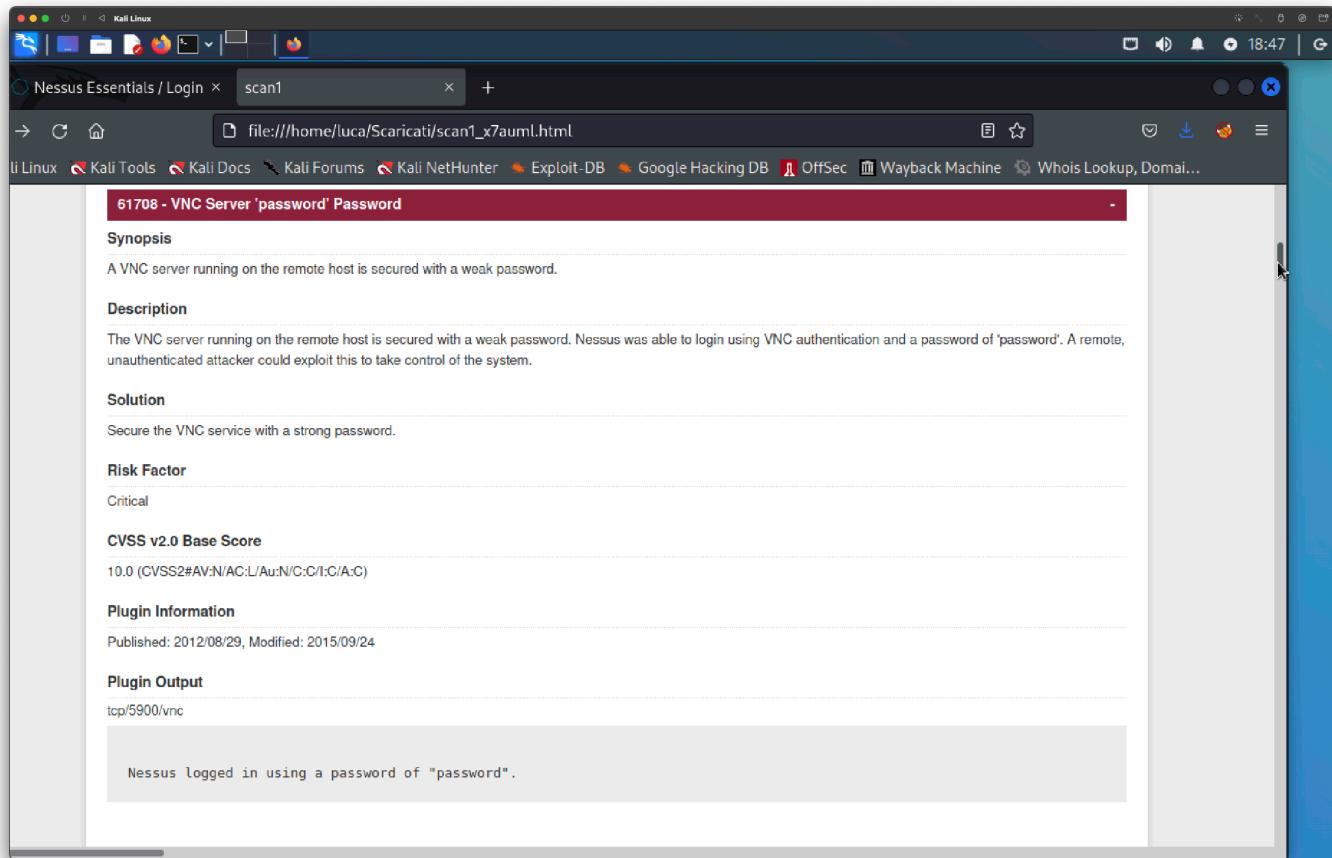
Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 1:42 PM
- End: Today at 2:12 PM
- Elapsed: 30 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Dopo aver rilevato le vulnerabilità di metasploitable andiamo a trovare delle soluzioni per correggere le vulnerabilità più critiche



Come si può vedere dalla foto sopra siamo andati a correggere la prima vulnerabilità siamo andati a implementare la password tramite terminale da metasploitable con i

```
Creating default startup script /home/msfadmin/.vnc/xstartup
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log

msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd .vnc
root@metasploitable:/home/msfadmin/.vnc# lx
bash: lx: command not found
root@metasploitable:/home/msfadmin/.vnc# vncpassword
bash: vncpassword: command not found
root@metasploitable:/home/msfadmin/.vnc# vncpass
bash: vncpass: command not found
root@metasploitable:/home/msfadmin/.vnc# ls
metasploitable:1.log metasploitable:1.pid passwd  xstartup
root@metasploitable:/home/msfadmin/.vnc# psswd
bash: psswd: command not found
root@metasploitable:/home/msfadmin/.vnc# vncpsswd
bash: vncpsswd: command not found
root@metasploitable:/home/msfadmin/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin/.vnc#
```

Dopo aver corretto la vulnerabilità VNC Server ‘password’ Password possiamo vedere nella foto sotto come la vulnerabilità è stata eliminata

The screenshot shows the Nessus Essentials interface on a Kali Linux desktop. The main window displays a scan titled "scansione3" with 50 vulnerabilities found. The vulnerabilities are listed in a table with columns for Severity (Sev), Score, Name, Family, and Count. The severity levels shown are Critical, High, Mixed, and Medium. The "Scan Details" panel on the right indicates the scan was completed successfully with a basic network policy and took 31 minutes. A pie chart in the "Vulnerabilities" section shows the distribution of severity levels.

Poi siamo andati a correggere la seconda vulnerabilità bind shell backdoor detection

The screenshot shows a web browser displaying the details of a specific vulnerability. The URL is file:///home/luca/Scaricati/scan1_x7auml.html. The page title is "51988 - Bind Shell Backdoor Detection". The content includes sections for Synopsis, Description, Solution, Risk Factor, CVSS v3.0 Base Score, CVSS v2.0 Base Score, Plugin Information, and Plugin Output. The "Synopsis" section states: "The remote host may have been compromised." The "Description" section states: "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." The "Solution" section suggests: "Verify if the remote host has been compromised, and reinstall the system if necessary." The "CVSS v3.0 Base Score" is 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). The "CVSS v2.0 Base Score" is 10.0 (CVSS2:AV:N/AC:L/Au:N/C:L/I:C/A:C). The "Plugin Information" section shows the plugin was published on 2011/02/15 and modified on 2022/04/11. The "Plugin Output" section shows the command "id" was executed and returned "tcp/1524/wild_shell".

La vulnerabilità bind shell backdoor detection è stata corretta grazie alla giunta di un firewall sulla porta 1534

```
● ● ○ ○ ○ Metasploitable
Default policy changed to 'deny'
(be sure to update your rules accordingly)
root@metasploitable:~# ufw deny 1524
Rules updated
root@metasploitable:~#
root@metasploitable:~# ufw

Usage: ufw COMMAND

Commands:
enable                                Enables the firewall
disable                               Disables the firewall
default ARG                           set default policy to ALLOW or DENY
logging ARG                           set logging to ON or OFF
allow/deny RULE                        allow or deny RULE
delete allow/deny RULE                 delete the allow/deny RULE
status                                 show firewall status
version                                display version information

root@metasploitable:~# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:~# ufw deny 1524
Rules updated
root@metasploitable:~#
```

Come si vede dalla foto sotto la vulnerabilità bind shell backdoor detection è stata eliminata

The screenshot shows the Nessus Essentials application running on Kali Linux. The main window displays a scan titled "scansione4" with 60 vulnerabilities found. The left sidebar shows navigation options like "My Scans", "All Scans", and "Terrascan". The right side panel provides "Scan Details" including the policy (Basic Network Scan), status (Completed), and a summary of the scan duration. A "Vulnerabilities" section includes a pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Severity	Count
Critical	10
High	7
Medium	27
Low	3
Info	2

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 5:57 PM
- End: Today at 6:27 PM
- Elapsed: 30 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Sono riuscito a togliere anche la vulnerabilità apache tomcat ajp connector request injection (ghostcat) sempre grazie al firewall

The screenshot shows a web browser window on a Kali Linux desktop. The address bar indicates the page is file:///home/luca/Scaricati/scan1_x7auml.html. The main content is a Nessus scan report for a specific vulnerability:

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis
There is a vulnerable AJP connector listening on the remote host.

Description
A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

See Also
<http://www.nessus.org/u?8ebe6246>
<http://www.nessus.org/u?7ae287adb>
<http://www.nessus.org/u?7bc3d54e>
<https://access.redhat.com/solutions/4851251>
<http://www.nessus.org/u?d218234>
<http://www.nessus.org/u?d772531>
<http://www.nessus.org/u?2aa1d6bf>
<http://www.nessus.org/u?3b5af27e>
<http://www.nessus.org/u?9dab109f>
<http://www.nessus.org/u?7eacf70>

Solution
Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Risk Factor
High

CVSS v3.0 Base Score
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H)

Dopo aggiunta del firewall la vulnerabilità è stata tolta come si può vedere nella foto qui sotto

The screenshot shows the Nessus interface on a Kali Linux desktop. The left sidebar shows 'My Scans' selected. The main area displays the results of a scan named 'scansione5'. The table shows the following data:

Sev	Score	Name	Family	Count
Critical	10.0 *	NFS Exported Share Inform...	RPC	1
Critical	10.0	Unix Operating System Uns...	General	1
Critical	...	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	...	ISC Bind (Multiple Issu...	DNS	5
Medium	5.3	SMB Signing not required	Misc.	1
Mixed	...	SSL (Multiple Issues)	General	12

Scan Details

Policy: Basic Network Scan
Status: Stopping
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:30 PM

Vulnerabilities

A pie chart shows the distribution of vulnerability types: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Risultato finale delle vulnerabilità rimaste

