

Dopo aver effettuato una scansione con Nessus sulla macchina Metasploitable notiamo che ci vengono restituite le vulnerabilità principali della macchina in ordine di criticità.

The screenshot shows the Tenable Nessus Essentials web interface. The main content area displays a scan report for 'ESERCIZIO 2'. The 'Vulnerabilities' tab is active, showing a list of vulnerabilities sorted by severity. The table includes columns for Severity, CVSS, VPR, Name, Family, and Count. The vulnerabilities are listed in descending order of severity, with 'CRITICAL' items at the top. A 'Scan Details' sidebar on the right provides information about the scan policy, status, and duration. A 'Vulnerabilities' donut chart is also visible, showing the distribution of vulnerability severities.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0	+	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		Apache Tomcat AJP Connector Request Injection (GHOSTcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	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	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5

Vediamo di seguito alcune modalità per gestire 3 di queste vulnerabilità di livello critico.

## 1) "NFS EXPORTED SHARE INFORMATION DISCLOSURE"

Qui ci viene detto che la porta 2049, su cui è attivo il protocollo Network File System (Protocollo usato per la condivisione dei dati) è vulnerabile. Possiamo utilizzare un firewall per bloccare le connessioni con altri host e prevenire attacchi tramite il comando: "iptables -A INPUT -p tcp -dport 2049 -j DROP". Impostando questo comando la porta verrà bloccata e il traffico ad essa associato sarà interrotto, impedendo eventuali attacchi.

The screenshot displays the Nessus Essentials interface for a vulnerability scan. The main window shows the details for 'ESERCIZIO / Plugin #11356', which is 'NFS Exported Share Information Disclosure'. The description states: 'At least one of the NFS shares exported by the remote server could be mounted by the scanning host. A read (and possibly write) files on remote host.' The solution suggests: 'Configure NFS on the remote host so that only authorized hosts can mount its remote shares.' The output section lists the following NFS shares that could be mounted:

- Contents of / :
- bin
- boot

A terminal window is overlaid on the Nessus window, showing a Metasploit session. The user logs in as 'msfadmin' and runs the command 'iptables -A INPUT -p tcp -dport 2049 -j DROP'.

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

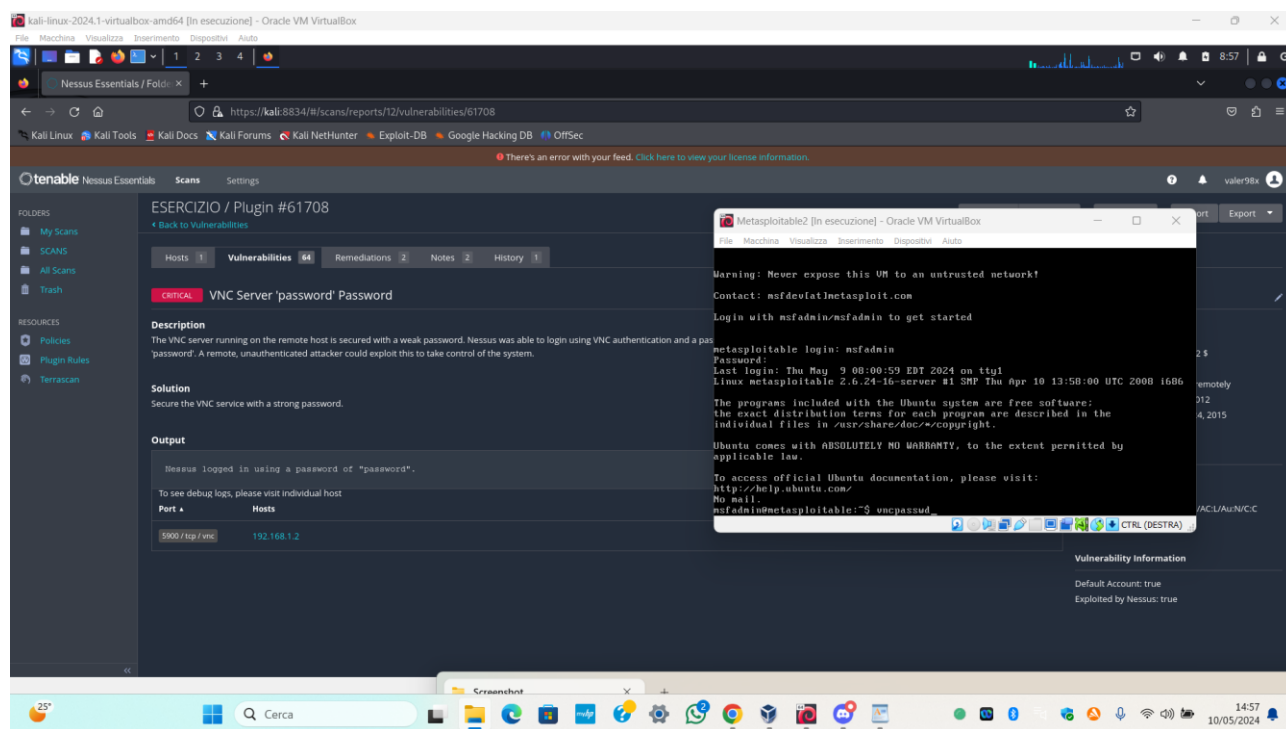
Vulnerability Information:

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

Exploitable With:

## 2) “VNC server ‘password’ Password”

Nessus ci comunica che la password associata al servizio VNC server è molto debole. Il programma di scanning, infatti, ha effettuato un tentativo di accesso remoto alla macchina Metasploitable, riuscendo ad aggirare facilmente la password (ovvero “password”). In questo caso basterà semplicemente cambiare la password VNC con una più complessa (per esempio xTn6ChM5).



### 3) “Bind shell backdoor detection”

Si tratta della concreta possibilità che un malintenzionato crei una backdoor ed inizi a controllare a distanza la nostra macchina. Dallo scan di rete effettuato con kali, vediamo che alla porta 1524 è associato il servizio ingreslock (che gestisce e coordina l'accesso di più utenti al database).

Supponiamo di essere l'unico utente ad accedere alla macchina Metasploitable (dunque il servizio diventa di utilità trascurabile); è possibile, in questo caso, disattivare il servizio stesso. Utilizziamo il comando “sudo systemctl stop ingreslock”.

The screenshot displays the Nessus Essentials interface with a vulnerability report for 'Bind Shell Backdoor Detection' on the host 'Metasploitable2'. The report includes a description of the vulnerability, a solution to verify the host, and a truncated output of the scan. In the foreground, a terminal window shows the command 'sudo systemctl stop ingreslock' being executed on the Metasploitable2 host.

**Vulnerability Details:**

- Hosts:** 1
- Vulnerabilities:** 64
- Remediations:** 2
- Notes:** 2
- History:** 1

**Description:** A shell is listening on the remote port without any authentication being required. An attacker may use it to send 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 -----
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
----- snip -----
```

**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/AU:N/S:C/H:HA/H
- CVSS v2.0 Base Score:** 10.0
- CVSS v2.0 Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/A:C/A:C

Per essere sicuri di aver sistemato le vulnerabilità effettuiamo una nuova scansione.

The screenshot displays the Nessus Essentials web interface within a Kali Linux virtual machine. The browser address bar shows the URL `https://kali8834/#/scans/reports/18/vulnerabilities`. The interface is titled "Esercizio 3" and includes tabs for "Configure", "Audit Trail", "Launch", "Report", and "Export".

The main content area shows a table of vulnerabilities under the "Vulnerabilities" tab. The table has columns for "Sev", "CVSS", "VPR", "Name", "Family", and "Count". The vulnerabilities listed include:

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9		SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9		SSL DROWN Attack Vulnerability (Decryptor RSA with Obsolete and Weakened eEncryption)	Misc	1
MIXED	...	...	SSH (Multiple Issues)		
MIXED	...	...	HTTP (Multiple Issues)		

On the right side, the "Scan Details" panel shows the following information:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: May 10 at 4:38 PM
- End: May 10 at 5:03 PM
- Elapsed: 25 minutes

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

The bottom of the image shows the Kali Linux desktop environment with the taskbar and system tray.