

# Report sulle criticità della macchina Metasploitable

Analisi suddivisa in sezione semplificata e approfondita

## Parte 1: Analisi semplice e chiara

La macchina Metasploitable rappresenta una piattaforma vulnerabile ideata per l'apprendimento e la pratica della sicurezza informatica. Tuttavia, essa presenta numerose criticità che possono essere sfruttate nel corso di attività di verifica e simulazione. Si riportano di seguito alcune delle principali vulnerabilità:

- **Accesso remoto:** La piattaforma include servizi quali FTP e SSH che accettano credenziali predefinite, facilitando l'accesso non autorizzato.
- **Database non protetti:** MySQL e PostgreSQL risultano configurati in maniera non sicura e sono facilmente soggetti a compromissione.
- **Applicazioni web vulnerabili:** Sono presenti applicazioni web che manifestano vulnerabilità comuni, tra cui SQL injection e cross-site scripting.
- **Servizi obsoleti:** Numerosi pacchetti e software non sono aggiornati, aumentando il rischio di exploit conosciuti.

Tali vulnerabilità rendono la piattaforma uno strumento eccellente per simulare scenari di attacco, evidenziando al contempo i rischi derivanti dal mancato aggiornamento o da configurazioni inadeguate, che possono verificarsi in ambienti reali.

## Parte 2: Analisi articolata e approfondita

La macchina Metasploitable costituisce un ambiente volutamente vulnerabile, concepito per l'analisi di tecniche offensive e difensive nella sicurezza informatica. Si propone di seguito un'analisi dettagliata delle criticità riscontrate.

### Servizi di rete

La piattaforma ospita diversi servizi di rete esposti, come SSH (porta 22), FTP (porta 21) e Telnet (porta 23). Questi:

- Utilizzano credenziali predefinite, quali "msfadmin/msfadmin", che consentono accessi non autorizzati.
- Non implementano cifrature moderne per la trasmissione dei dati, esponendo le comunicazioni a potenziali vulnerabilità.

L'esposizione di tali servizi evidenzia il rischio di attacchi basati su brute force o man-in-the-middle.

## Database vulnerabili

I database MySQL e PostgreSQL inclusi nella piattaforma:

- Permettono l'accesso tramite credenziali standard senza limitazioni di rete.
- Non adottano misure di protezione contro query malevole, quali SQL injection.

Queste vulnerabilità simulano configurazioni errate comunemente riscontrabili in ambienti di produzione.

## Applicazioni web non sicure

Le applicazioni web integrate, come Mutillidae e DVWA (Damn Vulnerable Web Application), sono progettate per dimostrare vulnerabilità frequenti, tra cui:

- SQL injection: Consentono agli utenti di eseguire query arbitrarie contro il database.
- Cross-Site Scripting (XSS): Permettono l'inserimento di script malevoli, con conseguente compromissione delle sessioni e dei dati degli utenti.
- File inclusion: Rivelano vulnerabilità che permettono il caricamento di file arbitrari sul server.

Tali criticità sottolineano l'importanza della validazione degli input e della corretta configurazione dei server web.

## Pacchetti e sistemi obsoleti

Numerosi pacchetti software installati sulla piattaforma risultano obsoleti, inclusi versioni non supportate di Apache e Samba. Questo:

- Incrementa la probabilità di exploit noti.
- Costituisce un esempio di gestione carente della manutenzione software.

La configurazione obsoleta evidenzia i rischi derivanti dal mancato aggiornamento dei sistemi, un problema frequentemente trascurato nelle infrastrutture operative.

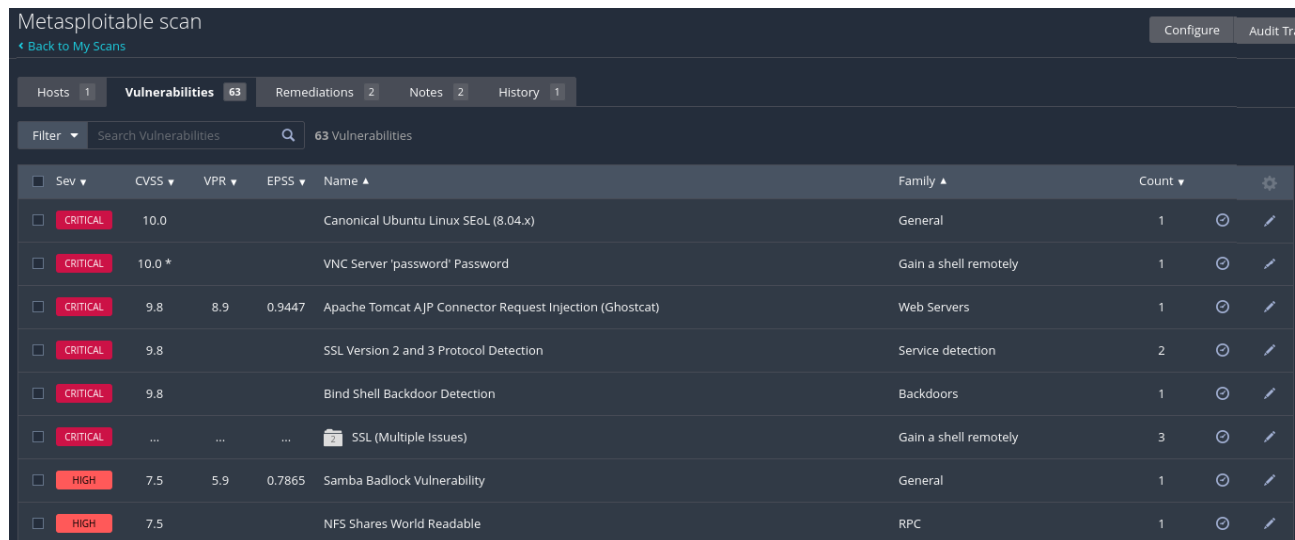
## Conclusioni

Nonostante sia concepita come ambiente di test, Metasploitable si dimostra estremamente utile per comprendere le implicazioni delle configurazioni errate e dell'utilizzo di software obsoleto. Le vulnerabilità rilevate rappresentano scenari realistici che possono essere mitigati adottando le seguenti misure:

- Una gestione accurata degli accessi e delle credenziali.
- L'implementazione tempestiva di patch e aggiornamenti.
- La validazione continua dei sistemi e delle applicazioni.

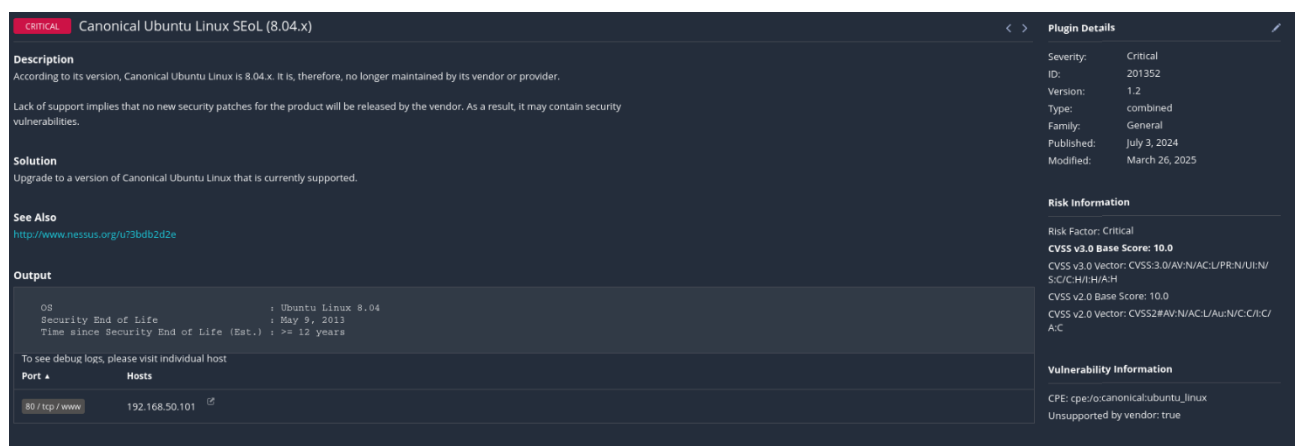
Il presente report evidenzia l'importanza della sicurezza informatica quale priorità assoluta per qualsiasi organizzazione tecnologica.

Fatte queste conclusioni sulla macchina Metasploitable inizio col risolvere le criticità trovate dopo una scansione basica con “Nessus”



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1

Iniziamo con la prima criticità ossia “Canonical Ubuntu Linux SEoL (8.04.x)”. Dopo averci cliccato vedremo tutte le caratteristiche della suddetta criticità



Canonical Ubuntu Linux SEoL (8.04.x)		Plugin Details
<b>Description</b> According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.		Severity: Critical ID: 201352 Version: 1.2 Type: combined Family: General Published: July 3, 2024 Modified: March 26, 2025
<b>Solution</b> Upgrade to a version of Canonical Ubuntu Linux that is currently supported.		<b>Risk Information</b> Risk Factor: Critical CVSS v3.0 Base Score: 10.0 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/CH/I/H/A/H CVSS v2.0 Base Score: 10.0 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/C/I/A/C
<b>See Also</b> <a href="http://www.nessus.org/u73bde2d2e">http://www.nessus.org/u73bde2d2e</a>		<b>Vulnerability Information</b> CPE: cpe/o:canonical:ubuntu_linux Unsupported by vendor: true
<b>Output</b> <pre>OS : Ubuntu Linux 8.04 Security End of Life : May 9, 2013 Time since Security End of Life (Est.) : &gt;= 12 years</pre> To see debug logs, please visit individual host		
<b>Port</b>	<b>Hosts</b>	
80 / tcp / www	192.168.50.101	

Questa criticità è dovuta alla mancanza di aggiornamenti per la versione obsoleta, come mostrato dall'immagine. Nessus propone una soluzione valida: aggiornare la macchina a una versione più recente e supportata con costanti aggiornamenti.

## Secondo errore

Spostiamo invece l'attenzione sulla seconda criticità presentata da Nessus, ossia "VNC Server 'password' Password"

The screenshot shows a Nessus scan result for a critical vulnerability titled "VNC Server 'password' Password". The description states that the VNC server is secured with a weak password, allowing an unauthenticated attacker to gain control. The solution is to secure the VNC service with a strong password. The output shows a successful login using the password "password". The risk information indicates a critical risk factor and a CVSS v2.0 base score of 10.0. The vulnerability information shows it was published on August 29, 2012, and modified on September 24, 2015.

Port	Hosts
5900 / tcp / vnc	192.168.50.101

La criticità risiede nella semplicità della password del server VNC. Infatti, questa risulterà quasi obsoleta, vista la sua inclusione in quasi tutte le liste utilizzate per attacchi di tipo Brute Force o comunque facilmente intuibile poiché si tratta della password predefinita.

### Cos'è VNC (Virtual Network Computing)?

VNC è un sistema che permette di controllare a distanza un altro computer tramite un'interfaccia grafica (GUI), come se l'utente fosse fisicamente presente davanti al monitor. In altre parole, VNC consente di visualizzare il desktop di un altro computer e interagire con mouse e tastiera da remoto.

### Come funziona tecnicamente?

- Un server VNC gira sulla macchina da controllare (ad esempio, la VM Metasploitable).
- Un client VNC (viewer) si connette a tale indirizzo IP, solitamente sulla porta 5900 (o 5901, 5902).
- La sessione può essere trasmessa su una rete locale o su internet se mal configurata.

### Perché è una vulnerabilità?

- Utilizzo di password deboli o predefinite (es. password, 1234).
- Mancanza di cifratura del traffico, rendendolo intercettabile.
- Assenza di restrizioni di accesso solo agli IP autorizzati.

### Come risolvere questa criticità?

- Aprire la macchina Metasploitable.
- Eseguire il seguente comando:

```
sudo iptables -A INPUT -p tcp --dport 5900 -j DROP
```

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5900 -j DROP
msfadmin@metasploitable:~$
```

Il comando indicato bloccherà la porta "5900" rilevata in errore senza modificare o disinstallare alcun componente.

## Terzo errore

The screenshot shows a Nessus scan result for the 'Apache Tomcat AJP Connector Request Injection (Ghostcat)' vulnerability. The severity is 'Critical'. The description states that a file read/inclusion vulnerability was found in the AJP connector, allowing an unauthenticated attacker to read web application files. The solution is to 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. The 'See Also' section lists several Nessus and Red Hat advisories. The 'Output' section shows a hex dump of the exploit request. The 'Plugin Details' section on the right provides additional information: Severity: Critical, ID: 134862, Version: 1.51, Type: remote, Family: Web Servers, Published: March 24, 2020, Modified: February 12, 2025. The 'VPR Key Drivers' section lists threat metrics: Threat Recency: 30 to 120 days, Threat Intensity: Very Low, Exploit Code Maturity: High, Age of Vuln: 730 days +, Product Coverage: Very High, CVSSv3 Impact Score: 5.9, Threat Sources: No recorded events. The 'Risk Information' section shows a Vulnerability Priority Rating (VPR) of 8.9, an Exploit Prediction Scoring System (EPSS) of 0.9447, and a Risk Factor of High. The CVSS v3.0 Base Score is 9.8. The CVSS v3.0 Vector is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H. The CVSS v3.0 Temporal Vector is CVSS:3.0/E:H/RL:O/R:C/C. The CVSS v3.0 Temporal Score is 9.4. The CVSS v2.0 Base Score is 7.5. The CVSS v2.0 Temporal Score is 6.5. The CVSS v2.0 Vector is CVSS2#AV:N/AC:L/Au:N/C:P/PL:P/A:P. The CVSS v2.0 Temporal Vector is CVSS2#E:H/RL:O/R:C/C.

Il terzo errore è "Apache Tomcat AJP Ghostcat (CVE-2020-1938)". Apache Tomcat (versioni <9.0.31, <8.5.51, <7.0.100) ha un bug nel connettore AJP (Apache JServer Protocol).

Il connettore AJP è attivo di default. Un attaccante può sfruttarlo per leggere file arbitrari o, in alcuni casi, eseguire codice.

Rimedi:

- Aggiornare Tomcat alla versione 9.0.31 o superiore.
- Disabilitare il connettore AJP nel file server.xml.
- Limitare l'accesso a 127.0.0.1

**<Connector port="8009" protocol="AJP/1.3" address="127.0.0.1" redirectPort="8443" />**

Una volta trovata questa riga, bisogna commentarla o disabilitarla.

Nota: Metasploitable è volutamente vulnerabile, quindi i pacchetti non si aggiornano facilmente. Tuttavia, la soluzione sopra indicata è valida se ci si presentasse la stessa criticità su un server reale.

## Quarto errore

CRITICAL

SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of "strong cryptography".

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>  
<http://www.nessus.org/u7906c7e95>  
<http://www.nessus.org/u7247c4540>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.nessus.org/u75d15ba70>  
<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://tools.ietf.org/html/rfc7507>  
<https://tools.ietf.org/html/rfc7568>

Plugin Details

Severity: Critical  
ID: 20007  
Version: 1.34  
Type: remote  
Family: Service detection  
Published: October 12, 2005  
Modified: April 4, 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

Vulnerability Information

In the news: true

Output

```

- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

  Name                Code      KEX      Auth      Encryption          MAC
  -----
EXP-RC2-CBC-MD5      RSA(512)  RSA      RC2-CBC(40)      MD5      export
EXP-RC4-MD5          RSA(512)  RSA      RC4(40)          MD5      export
more...

To see debug logs, please visit individual host
Port  Hosts
25 / tcp / smtp  192.168.50.101

- SSLv3 is enabled and the server supports at least one cipher.
  Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

  Name                Code      KEX      Auth      Encryption          MAC
  -----
EXP-RSA-RSA-CBC-MD5  RSA      RSA      RSA      3DES-CBC(168)      RSA
more...

To see debug logs, please visit individual host
Port  Hosts
5432 / tcp / postgresql  192.168.50.101

```

Il quarto errore è dovuto al fatto che Metasploitable accetta connessioni di tipo SSL Version 2 e 3, protocolli attualmente considerati obsoleti e insicuri. Questi protocolli sono vulnerabili a vari attacchi come POODLE, DROW, ecc.

Perché rappresenta un problema?

- SSLv2 e SSLv3 non garantiscono più la sicurezza dei dati.
- Sono facilmente intercettabili o forzabili da un attaccante man-in-the-middle.
- Tutti i sistemi moderni utilizzano TLS 1.2 o TLS 1.3.

Metasploitable è una macchina progettata per essere volutamente vulnerabile. Un metodo per risolvere il problema è bloccare il traffico sulle porte insicure (es. 443). In questo caso, come ci segnala anche Nessus, le porte sospette sono esattamente la porta 25 e la porta 5432, si può impartire alla macchina Metasploitable il comando:

**sudo iptables -A INPUT -p tcp -dport 25 -j DROP**

```
sudo iptables -A INPUT -p tcp --dport 5432 -j DROP
```

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 25 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5432 -j DROP
```

questo servirà a chiudere le porte sospette, infatti come vedremo nel report successivo l'errore non si ripresenterà.

## Quinto Errore

The screenshot shows a Nessus scan result for the 'Bind Shell Backdoor Detection' plugin. The status is 'CRITICAL'. The description 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 suggests: 'Verify if the remote host has been compromised, and reinstall the system if necessary.' The output shows a successful connection to 192.168.50.101 on port 1524, resulting in a root shell. The risk information indicates a critical risk factor and a CVSS v3.0 base score of 9.8.

La quinta criticità segnala che è stato individuato un servizio di tipo "Bind Shell" sulla macchina. Questo implica che un attaccante possa connettersi direttamente a una porta TCP della macchina e ottenere accesso remoto con shell, senza necessità di autenticazione.

## Cosa significa Bind Shell?

Un Bind Shell è una backdoor che apre una porta sulla macchina bersaglio e rimane in ascolto. Quando un attaccante si collega a quella porta, ottiene una shell (accesso terminale remoto).

Meta è dotata intenzionalmente di backdoor, quindi:

- È comune che ci sia sempre una bind shell in ascolto.
- Non esiste un metodo ufficiale per rimuoverla, se non modificando lo startup o ricompilando la macchina.

È comunque possibile disattivare temporaneamente una porta sospetta utilizzando il comando:

```
sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
```

Nonostante le ripetute scan effettuate, purtroppo le seguenti criticità non mi si sono presentate



Ho deciso di proporre una soluzione per risolvere la criticità segnalata. L'immagine mostra un problema nel sistema che condivide informazioni su directory tramite NFS, rendendole visibili anche a utenti non autorizzati, con conseguente accesso a file sensibili.

Soluzione:

1. Visualizza le condivisioni NFS con: `cat /etc/exports`
2. Modifica il file per limitare l'accesso con: `sudo nano /etc/exports`
3. Cambia righe come: `/home *(rw, no_root_squash) in: /home 192.168.50.101 (rw, sync, no_root_squash, no_subtree_check)` per limitare l'accesso alla macchina locale.
4. Riavvia NFS con: `sudo exportfs -ra` per applicare i cambiamenti.

Mentre la seconda criticità riguarda il servizio rexecd, questo permette l'esecuzione remota di comandi ma invia tutto in chiaro (senza cifratura)

Una soluzione sarebbe:

- Verificare che rexecd sia attiva attraverso il comando: `netstat -tulpn | grep rexecd`
- Disabilitare temporaneamente il servizio (fino al riavvio) attraverso il comando: `sudo service openbsd-inetd stop.`

La seconda soluzione per disattivarlo definitivamente sarebbe:

- Verificare che rexecd sia attiva attraverso il comando: `netstat -tulpn | grep rexecd`
- Modificare il file `/etc/inetd.conf` attraverso il comando: `sudo nano /etc/inetd.conf`
- Cercare la riga: `rexec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd`
- Dopodiché commentare la riga col simbolo `"#"`

**Nota Bene:** le soluzioni sopraelencate possono essere imprecise o errate data la non conferma dei passaggi scritti.

In allegato i due PDF delle scansioni effettuate da nessus: