Vulnerability Assessment Report

Executive Summary

Il presente report descrive un'attività di vulnerability assessment condotta su un sistema **Metasploitable**, utilizzando **Nessus** come strumento di scansione. L'analisi ha evidenziato un numero elevato di vulnerabilità, molte delle quali classificate come critiche. Tra queste, tre vulnerabilità ad alto impatto sono state selezionate e correttamente remediate. Una successiva scansione di verifica ha confermato l'efficacia delle contromisure applicate, mostrando una riduzione concreta della superficie di attacco.

Contesto e Scansione Iniziale

L'attività di assessment è stata eseguita sul seguente target:

- **Indirizzo IP:** 192.168.51.101
- **Sistema Operativo:** Linux Kernel 2.6 su Ubuntu 8.04

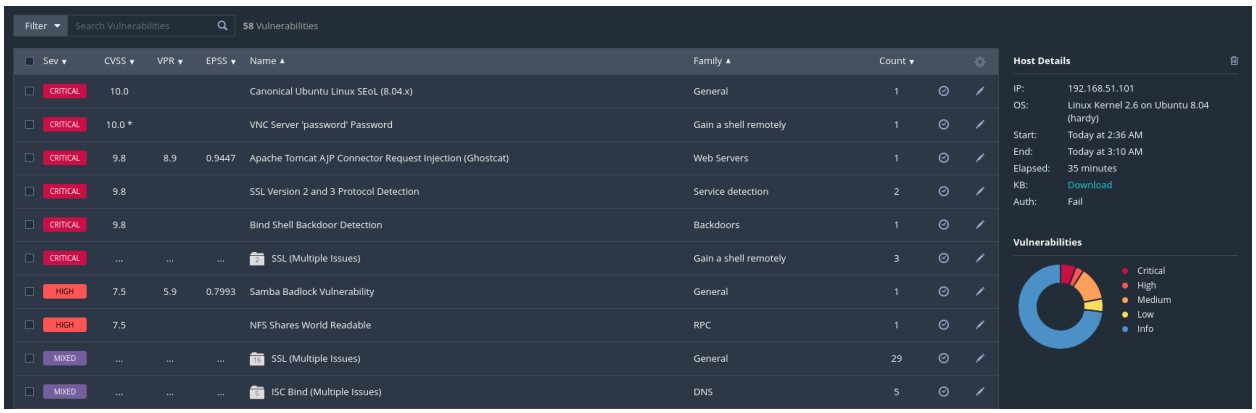
La scansione iniziale ha rilevato **217 vulnerabilità complessive**, tra cui **9 vulnerabilità critiche**, riconducibili principalmente a servizi obsoleti, configurazioni deboli e presenza di meccanismi di accesso remoto non sicuri.

Vulnerabilità Critiche Identificate

Le principali vulnerabilità critiche emerse includono:

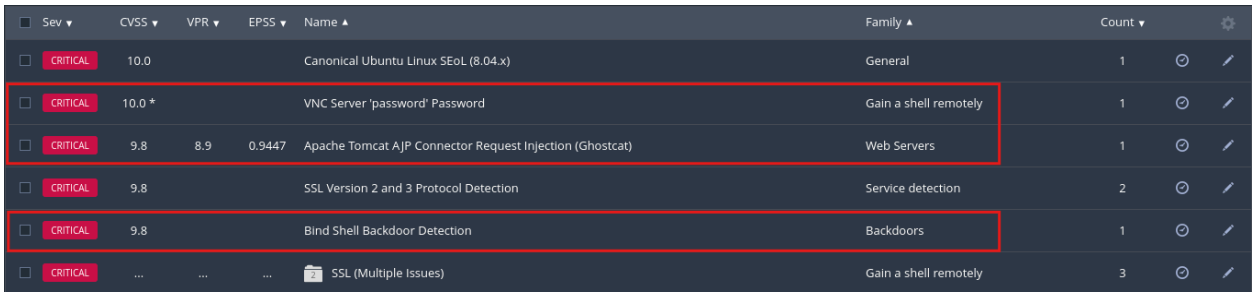
- **Canonical Ubuntu Linux SEoL (8.04.x)** – CVSS 10.0
  Il sistema operativo risulta End-of-Life e non più supportato, esponendo il sistema a vulnerabilità note e non patchate.
- **SSL Version 2 and 3 Protocol Detection** – CVSS 9.8
  Presenza di protocolli SSL obsoleti e intrinsecamente vulnerabili.
- **SSL (Multiple Issues)**
  Vulnerabilità multiple legate alla configurazione SSL/TLS, rilevate in tre istanze distinte.
- **VNC Server con password di default** – CVSS 10.0
  Il servizio VNC era protetto dalla password predefinita "password", consentendo accesso remoto non autorizzato.
- **Apache Tomcat AJP Connector – Ghostcat** – CVSS 9.8
  Vulnerabilità che consentiva request injection tramite il protocollo AJP, con potenziale lettura di file arbitrari ed esecuzione di codice.

- **Bind Shell Backdoor Detection** – CVSS 9.8
  Presenza di una bind shell backdoor attiva sulla porta 1524.



Attività di Remediation

Tra le vulnerabilità critiche identificate, ne sono state selezionate tre per l'attività di remediation, in quanto rappresentavano vettori di attacco diretti e ad altissimo impatto.



VNC Server – Password di Default

Il servizio VNC utilizzava una password debole e nota. La mitigazione è stata effettuata modificando la password tramite il comando `vncpasswd` e impostando una credenziale robusta, eliminando la possibilità di accesso non autorizzato.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ _
```

Apache Tomcat AJP Connector (Ghostcat)

Il connettore AJP di Tomcat, in ascolto sulla porta 8009, è stato disabilitato intervenendo sul file di configurazione `/opt/apache-tomcat-5.5.25/conf/server.xml`. La riga relativa al connettore AJP è stata commentata, rimuovendo definitivamente il servizio vulnerabile.

```
  <!-- Define an AJP 1.3 Connector on port 8009 -->
 <!-- <Connector port="8009"
            enableLookups="false" redirectPort="8443" protocol="AJP/1.3"> -->
  <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
  <!-- See proxy documentation for more information about using this. -->
  <!--
  <Connector port="8082"
            maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
            enableLookups="false" acceptCount="100" connectionTimeout="20000"
            proxyPort="80" disableUploadTimeout="true" />
  -->
```

Bind Shell Backdoor

È stata individuata una bind shell associata al servizio **Ingreslock** sulla porta 1524.

```
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep 1524
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4483/xinetd
```

La remediation ha previsto la rimozione della configurazione del servizio dal file `/etc/inetd.conf`, commentando la riga incriminata e riavviando il servizio `openbsd-inetd`.

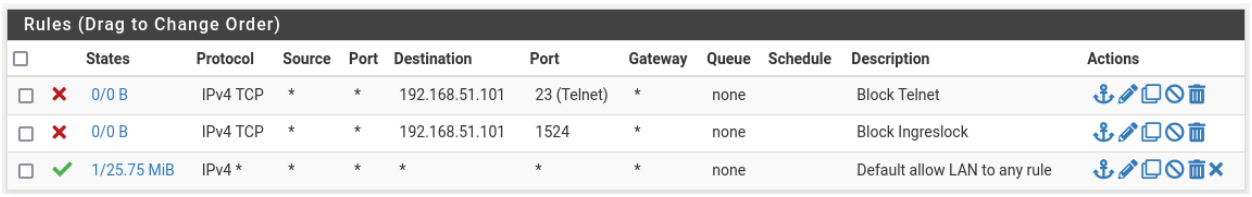
```
  GNU nano 2.0.7            File: /etc/inetd.conf                      Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

Rafforzamento tramite Firewall

Per aumentare ulteriormente il livello di sicurezza e adottare un approccio di **defense in depth**, sono state configurate specifiche regole firewall:

- Blocco del servizio **Telnet** (porta 23)
- Blocco del servizio **Ingreslock** (porta 1524)
- Mantenimento della regola di default che consente il traffico LAN

Queste regole garantiscono che, anche in caso di riattivazione accidentale dei servizi vulnerabili, essi non risultino accessibili dall'esterno.

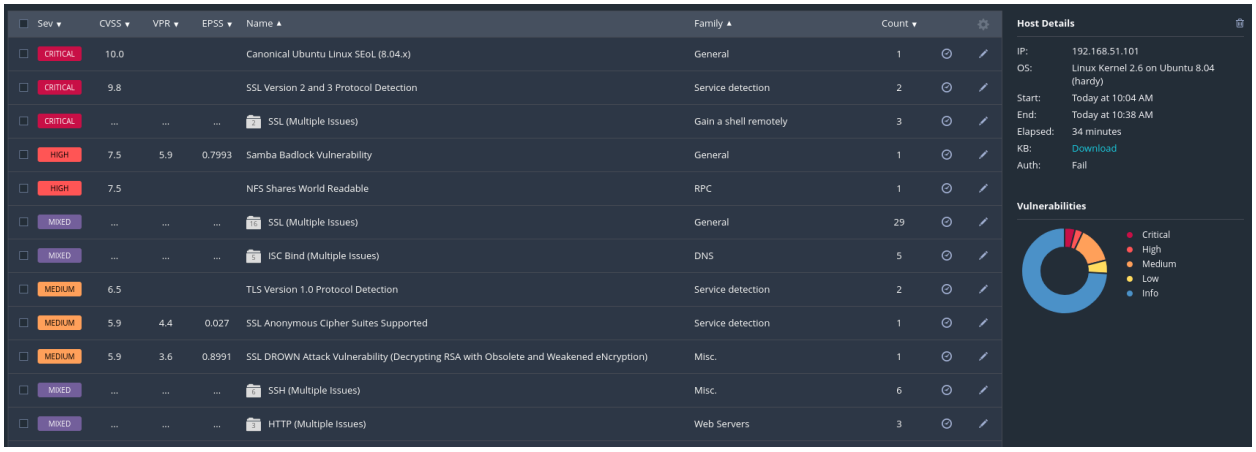


Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗	0/0 B	IPv4 TCP	*	*	192.168.51.101	23 (Telnet)	*	none		Block Telnet	
☐	✗	0/0 B	IPv4 TCP	*	*	192.168.51.101	1524	*	none		Block Ingreslock	
☐	✓	1/25.75 MiB	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule	

Scansione Post-Remediation

Una nuova scansione è stata effettuata per verificare l'efficacia delle mitigazioni:



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	SSL (Multiple Issues)	General	29
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	3

Host Details

IP: 192.168.51.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 10:04 AM
End: Today at 10:38 AM
Elapsed: 34 minutes
KB: Download
Auth: Fail

Vulnerabilities

Critical
High
Medium
Low
Info

La scansione finale ha rilevato **213 vulnerabilità totali**, confermando che le tre vulnerabilità critiche precedentemente remediate (e il servizio Telnet attivo) non sono più presenti.

Riduzione del Rischio

Le vulnerabilità mitigate rappresentavano i principali vettori di compromissione del sistema. La loro rimozione ha eliminato:

- l'accesso diretto al desktop remoto tramite VNC;
- la possibilità di file disclosure ed esecuzione di codice remoto via Ghostcat;
- l'accesso shell non autenticato tramite bind shell.

Nel complesso, la superficie di attacco del sistema è stata significativamente ridotta.

Conclusioni e Raccomandazioni

L'attività di vulnerability assessment ha raggiunto con successo gli obiettivi prefissati, consentendo di identificare le principali criticità, applicare remediation efficaci e verificarne i risultati tramite rescanning.

Si raccomanda, tuttavia, di intraprendere ulteriori azioni strutturali per migliorare la postura di sicurezza complessiva:

- aggiornare il sistema operativo a una versione supportata;
- effettuare un hardening completo di SSL/TLS, disabilitando SSLv2 e SSLv3;
- rivedere le configurazioni di Samba e NFS;
- implementare un processo di patch management regolare;
- pianificare attività di monitoring e scanning periodico.

Lessons Learned

L'esperienza evidenzia l'importanza di un approccio metodico al vulnerability management, nonché il valore della verifica post-remediation. Inoltre, l'integrazione di controlli firewall si conferma un elemento fondamentale per una strategia di sicurezza multilivello.

Data: 14 Dicembre 2025
Redatto da: Nicola Guidi