

# S5/L5

---

# NESSUS

---

# \* REPORT

---

Vulnerability scanning e resolution

# Table of Contents

---

Introduzione

---

Risultati Prima Scansione

---

Analisi delle Vulnerabilità

---

Risoluzione

---

Risultati Seconda Scansione e Conclusioni

# Introduzione

Il presente report illustra la procedura adottata per la scansione di sicurezza del sistema Metasploitable, con l'obiettivo di identificare e mitigare da due a quattro vulnerabilità di livello critico o elevato. In seguito alla scansione iniziale e all'identificazione delle principali minacce, sono state implementate specifiche azioni di rimedio, comprese misure di configurazione delle regole firewall. Successivamente, è stata eseguita una seconda scansione per valutare l'efficacia degli interventi confrontando i risultati con quelli iniziali. Tale processo dimostra come interventi mirati possano migliorare la sicurezza del sistema.

## Risultati da ottenere

- Scansione e Analisi dei Rischi:** Condurre una scansione completa di sicurezza sul sistema Metasploitable per identificare le vulnerabilità critiche e ad alto rischio. Analizzare i rischi associati a tali vulnerabilità, comprendendo il potenziale impatto e le probabilità di sfruttamento.
- Implementazione di Contromisure:** Sviluppare e applicare misure di mitigazione specifiche per ciascuna delle vulnerabilità identificate.
- Valutazione dell'Efficacia delle Contromisure:** Rieseguire la scansione del sistema dopo l'implementazione delle contromisure per verificarne l'efficacia. Confrontare i risultati pre e post-intervento per determinare il grado di riduzione del rischio.
- Rapporto e Raccomandazioni:** Fornire un'analisi dettagliata dei risultati della scansione e delle azioni di rimedio, concludendo con raccomandazioni per ulteriori miglioramenti della sicurezza o per il mantenimento delle misure implementate.

# Risultati prima scansione

## # Classificazione Risultati

## Priority

Rappresentano il massimo rischio per la sicurezza del sistema. Queste possono essere sfruttate dagli attaccanti per compromettere completamente il sistema, ottenere accesso illimitato o causare danni significativi. È imperativo affrontare queste vulnerabilità con la massima priorità per evitare gravi conseguenze per la sicurezza.

CRITICAL

Costituiscono rischi seri per la sicurezza del sistema. Queste possono permettere agli attaccanti di ottenere accesso privilegiato o eseguire attacchi severi. È cruciale risolvere queste vulnerabilità tempestivamente per proteggere il sistema e i dati sensibili.

HIGH

Rappresentano un rischio significativo, anche se non critico, per la sicurezza del sistema. Possono consentire agli attaccanti di ottenere un certo livello di accesso non autorizzato o di compromettere la sicurezza in modi meno gravi. È comunque importante affrontare queste vulnerabilità in modo tempestivo.

MEDIUM

Generalmente rappresentano rischi minori o limitati. Possono includere problemi che hanno un impatto ridotto sulla sicurezza complessiva del sistema. Anche se queste vulnerabilità possono richiedere azioni correttive, non sono normalmente urgenti.

LOW

Vengono segnalate come informazioni le vulnerabilità meno importanti o quelle non considerate dallo scan effettuato.

INFO

**192.168.50.100**

8

4

16

7

69

CRITICAL

HIGH

MEDIUM

LOW

INFO

# Analisi delle Vulnerabilità

Dalla scansione di sicurezza sono state identificate diverse vulnerabilità, incluse alcune di livello critico che rappresentano un serio rischio per il sistema. Sono state selezionate e analizzate in dettaglio quattro di queste vulnerabilità critiche, descritte nel paragrafo seguente.

CRITICAL

9.8

9.0

134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)

La vulnerabilità riguarda un AJP connector che consente a un attaccante remoto non autenticato di leggere file dell'applicazione web o, se consentito, di caricare codice malevolo per ottenere l'esecuzione remota di codice (RCE).

## ★ Uso malevolo

Un attaccante potrebbe leggere file sensibili dell'applicazione o caricare codice malevolo tramite file JSP per assumere il controllo del server, compromettendo la sicurezza e l'integrità del sistema.

## ★ Risoluzione

Per risolvere questa vulnerabilità, è consigliabile aggiornare il software, disabilitare o proteggere l'AJP connector, filtrare e validare l'input, implementare un monitoraggio per rilevare attività sospette e utilizzare un firewall.

CRITICAL

9.8

-

51988 Bind Shell Backdoor Detection

L'host remoto potrebbe essere stato compromesso e presenta una shell in ascolto su una porta remota senza richiedere alcuna autenticazione.

## ★ Uso malevolo

Un attaccante potrebbe connettersi alla porta remota e inviare comandi direttamente alla shell, ottenendo così un accesso non autorizzato al sistema compromesso.

## ★ Risoluzione

Per risolvere questa vulnerabilità, è necessario identificare e rimuovere la shell compromessa. Inoltre, è fondamentale aggiornare e configurare correttamente il software per prevenire future intrusioni.

# Analisi delle Vulnerabilità

Dalla scansione di sicurezza sono state identificate diverse vulnerabilità, incluse alcune di livello critico che rappresentano un serio rischio per il sistema. Sono state selezionate e analizzate in dettaglio quattro di queste vulnerabilità critiche, descritte nel paragrafo seguente.

**CRITICAL** 10.0\* 5.9 11356 NFS Exported Share Information Disclosure

È possibile accedere alle condivisioni NFS sull'host remoto.

## \* Uso malevolo

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare questa situazione per leggere (e eventualmente scrivere) file sull'host remoto.

## \* Risoluzione

Per mitigare questa vulnerabilità, è consigliabile configurare correttamente le autorizzazioni di accesso alle condivisioni NFS, limitando l'accesso solo agli utenti autorizzati e implementando le misure di sicurezza appropriate.

**CRITICAL**

10.0\*

-

61708

VNC Server 'password' Password

Il server VNC in esecuzione sull'host remoto è protetto da una password debole.

## \* Uso malevolo

Un attaccante potrebbe sfruttare questa debolezza della password per accedere al server VNC e ottenere il controllo del sistema.

## \* Risoluzione

Per risolvere questa vulnerabilità, è necessario cambiare la password del server VNC utilizzando una password forte e complessa

# Risoluzione

## APACHE TOMCAT AJP CONNECTOR REQUEST INJECTION

La vulnerabilità riguarda un AJP connector che consente a un attaccante remoto non autenticato di leggere file dell'applicazione web o, se consentito, di caricare codice malevolo per ottenere l'esecuzione remota di codice (RCE).

CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
----------	-----	-----	--------	--

```
└$ nmap 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 06:50 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0067s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

Per risolvere questa vulnerabilità, è stata applicata una regola firewall con l'obiettivo di filtrare l'accesso alla porta 8009, che è associata al protocollo AJP13.

Questa azione è stata intrapresa per prevenire eventuali attacchi che potrebbero sfruttare questa porta aperta.

6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	filtered	ajp13

Per verificare l'efficacia della regola firewall applicata, è stato eseguito nuovamente un comando nmap dal terminale di Kali.

La porta 8009 non risulta più aperta ("open"), ma appare come "filtered". Questo indica che il firewall sta correttamente bloccando l'accesso alla porta, mitigando così la vulnerabilità precedentemente identificata.

Inoltre è consigliato l'aggiornamento all'ultima versione di apache.

# Risoluzione

## BIND SHELL BACKDOOR DETECTION

L'host remoto potrebbe essere stato compromesso e presenta una shell in ascolto su una porta remota senza richiedere alcuna autenticazione.

CRITICAL 9.8 - 51988 Bind Shell Backdoor Detection

```
$ sudo nmap -sS -p 512-32768 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 07:12 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00043s latency).
Not shown: 32240 closed tcp ports (reset)
PORT      STATE SERVICE
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
3306/tcp   open  mysql
3632/tcp   open  distccd
5432/tcp   open  postgresql
5900/tcp   open  vnc
6000/tcp   open  X11
6667/tcp   open  irc
6697/tcp   open  ircs-u
8009/tcp   open  ajp13
8180/tcp   open  unknown
8787/tcp   open  msgsrvr
MAC Address: 08:00:27:6D:5F:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.73 seconds
```

Per verificare l'apertura delle porte su un sistema compromesso metasploitable, il team ha eseguito il comando nmap dal terminale di Kali Linux, specificando l'indirizzo IP del sistema da analizzare. Questa operazione ha permesso di identificare la porta 1524, associata al servizio ingreslock, e di verificarne lo stato.

Successivamente, dal terminale del metasploit, il team ha chiuso la porta sospetta. Utilizzando il comando netstat, hanno individuato il processo che stava utilizzando la porta 1524. Identificato il PID del processo, hanno usato il comando kill per terminare il processo in esecuzione e chiudere la porta.

```
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep 1524
tcp        0      0 0.0.0.0:1524          0.0.0.0:*
LISTEN
4493/xinetd
msfadmin@metasploitable:~$ sudo kill 4493
msfadmin@metasploitable:~$
```

Per confermare l'efficacia delle azioni intraprese, il team ha tentato una nuova connessione alla porta precedentemente chiusa. Utilizzando i comandi nmap e nc, hanno verificato che la porta 1524 non risultasse più aperta, ma che la connessione venisse rifiutata, mostrando il messaggio di "connection refused".

```
(kali㉿kali)-[~]
$ sudo nmap -sS -p 1524 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 07:22 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00040s latency).

PORT      STATE SERVICE
1524/tcp  closed ingreslock
MAC Address: 08:00:27:6D:5F:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds

(kali㉿kali)-[~]
$ nc 192.168.50.100 1524
(UNKNOWN) [192.168.50.100] 1524 (ingreslock) : Connection refused
```

Era anche possibile applicare una regola firewall per mitigare questa vulnerabilità, bloccando l'accesso alla porta 1524 direttamente a livello di rete. Questa misura avrebbe aggiunto un ulteriore livello di sicurezza al sistema.

# Risoluzione

## NFS EXPORTED SHARE INFORMATION DISCLOSURE

È possibile accedere alle condivisioni NFS sull'host remoto.

CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
----------	-------	-----	-------	---

```
GNU nano 2.0.7          File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,async,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,async)
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

Per risolvere la vulnerabilità relativa all'accesso non autorizzato alle condivisioni NFS, è stata adottata una configurazione accurata dei file NFS, in modo che solo gli utenti autorizzati possano usufruire del servizio.

Innanzitutto, è stato rimosso dal file di configurazione /etc/exports ogni riferimento che permettesse l'accesso globale con privilegi elevati. Questa rimozione ha garantito che solo gli utenti specificatamente autorizzati possano accedere alle risorse NFS.

Successivamente, è stato applicato il parametro root\_squash a tutte le esportazioni NFS. Questa configurazione impedisce agli utenti root sui client NFS di mantenere privilegi elevati sul server NFS. In dettaglio, il parametro root\_squash mappa le richieste root in arrivo da un client NFS a un utente meno privilegiato sul server, generalmente l'utente nobody.

```
GNU nano 2.0.7          File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,async,no_root_squash) hostname2(ro,async,no_root_squash)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,async,fsid=0,crossmnt,no_root_squash)
# /srv/nfs4/homes  gss/krb5i(rw,async,no_root_squash)
#
```

# Risoluzione

## VNC SERVER "PASSWORD" PASSWORD

Il server VNC in esecuzione sull'host remoto è protetto da una password debole.

CRITICAL	10.0*	-	61708	VNC Server 'password' Password
----------	-------	---	-------	--------------------------------

```
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
```

Per risolvere questa vulnerabilità, il team ha deciso di modificare la password predefinita del server VNC direttamente dal terminale del sistema metasploitable. Hanno utilizzato il comando **vncpasswd** con privilegi di root. Il processo prevedeva l'impostazione di una nuova password più sicura, e in questo caso è stata scelta **"Gatt1n1!"**.

Una volta avviato il comando **vncpasswd**, il sistema ha richiesto l'inserimento della nuova password e la sua conferma. Successivamente, è stato chiesto se si desiderava impostare una password per la sola visualizzazione, opzione alla quale il team ha risposto negativamente per garantire che la password permettesse sia l'accesso che il controllo completo.

La modifica della password è stata effettuata con successo.

# Risultato seconda scansione e conclusioni

## Prima Scansione



## Seconda Scansione



La seconda scansione di sicurezza ha evidenziato una riduzione marcata del numero di rischi rilevati, passando da dieci a cinque. Questo calo rappresenta un chiaro indicatore dell'efficacia delle misure correttive implementate.

La seconda scansione di sicurezza ha confermato l'efficacia delle misure correttive implementate, riducendo significativamente il numero di rischi rilevati. L'analisi dettagliata e il report fornito da Nessus hanno permesso di sviluppare un piano d'azione mirato per affrontare le vulnerabilità critiche e migliorare la sicurezza complessiva del sistema.

La manutenzione continua e l'installazione regolare degli aggiornamenti restano fondamentali per garantire una protezione costante contro le minacce informatiche.

\* Thank you!

