



EPICODE SET-5

# FIX VULNERABILITA

NESSUS

---



Vulnerabilities Total: 107

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN NAME	
CRITICAL	9.8	-	<a href="#">134862</a> Apache Tomcat AJP Connector Request Injection (Ghostcat)	
CRITICAL	9.8	-	<a href="#">51988</a> Bind Shell Backdoor Detection	
CRITICAL	9.8	-	<a href="#">20007</a> SSL Version 2 and 3 Protocol Detection	
CRITICAL	10.0	-	<a href="#">33850</a> Unix Operating System Unsupported Version Detection	
CRITICAL	10.0*	-	<a href="#">32314</a> Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
CRITICAL	10.0*	-	<a href="#">32321</a> Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
CRITICAL	10.0*	-	<a href="#">11356</a> NFS Exported Share Information Disclosure	
CRITICAL	10.0*	-	<a href="#">61708</a> VNC Server 'password' Password	
HIGH	8.6	-	<a href="#">136769</a> ISC BIND Service Downgrade / Reflected DoS	
HIGH	7.5	-	<a href="#">42256</a> NFS Shares World Readable	
HIGH	7.5	-	<a href="#">42873</a> SSL Medium Strength Cipher Suites Supported (SWEET32)	
HIGH	7.5	-	<a href="#">90509</a> Samba Badlock Vulnerability	
MEDIUM	6.5	-	<a href="#">139915</a> ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	
MEDIUM	6.5	-	<a href="#">51192</a> SSL Certificate Cannot Be Trusted	
MEDIUM	6.5	-	<a href="#">57582</a> SSL Self-Signed Certificate	
MEDIUM	6.5	-	<a href="#">104743</a> TLS Version 1.0 Protocol Detection	
MEDIUM	5.9	-	<a href="#">136808</a> ISC BIND Denial of Service	
MEDIUM	5.9	-	<a href="#">31705</a> SSL Anonymous Cipher Suites Supported	

# PRIMO SCAN

Possiamo notare che Nessus effettuerà una scansione completa, restituendo tutte le vulnerabilità rilevate e ordinandole dal più critico al meno critico.

In giallo sono evidenziate tre fallo del sistema che andremo a correggere.

# TARGET

192.168.50.101 = MetaSploit

# NFS EXPORTED SHARE INFORMATION DISLOSURE

PROBLEM 1

## Cosa è?

Il problema riguarda la configurazione di condivisioni NFS (Network File System) su un server remoto. NFS consente a dispositivi sulla rete di accedere e condividere risorse di file.

Questo è un problema di sicurezza, poiché potenzialmente un attaccante potrebbe sfruttare questa configurazione per accedere ai file sul server remoto.

# CORREZIONE

```
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)
#
# /home *(ro)

# Example for NFSv4:
# /srv/nfs4      gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
# / *(rw,sync,no_root_squash,no_subtree_check)
```

**Si dovrà andare con meta a cambiare un  
parametro nella configurazione di NFS**

Questo problema è facilmente risolvibile aggiungendo un semplice #, il quale serve a commentare e quindi a non rendere pubblico il percorso desiderato

# VNC SERVER 'PASSWORD' PASSWORD

PROBLEM 2

## Cosa è?

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad effettuare l'accesso utilizzando l'autenticazione VNC e una password di 'password'. Un aggressore remoto e non autenticato potrebbe sfruttare ciò per prendere il controllo del sistema.

# CORREZIONE

```
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:~$
```

## Password debole

Questo problema è facilmente risolvibile. Basta cambiare la password in questione con un'altra più sicura

COMANDO PER IL CAMBIO PASSWORD = vncpasswd

# BIND SHELL BACKDOOR DETECTION

PROBLEM 3

## Cosa è?

Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla collegandosi alla porta remota e inviando comandi direttamente.

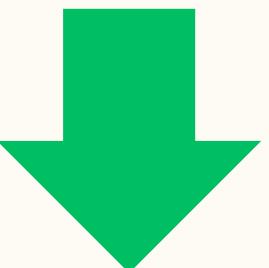
# CORREZIONE

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rules updated
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To                         Action  From
--                         ----  ---
1524/tcp                   DENY   Anywhere
1524/udp                   DENY   Anywhere
```

## FireWall

Per risolvere questo problema dovremmo creare una regola sul Firewall per bloccare il traffico su una specifica porta. Quindi andremo a configurare un Firewall



## **UFW ENABLE**

attiva il firewall sul sistema.

## **UFW DEFAULT ALLOW**

Questo comando imposta la politica predefinita del firewall per consentire il traffico. In altre parole, se il firewall riceve una connessione per la quale non è stata specificata alcuna regola, la permette per impostazione predefinita.

## **UFW DENY 1524**

Questo comando aggiunge una regola al firewall per bloccare il traffico sulla porta 1524

5

3

16

6

73

CRITICAL

HIGH

MEDIUM

LOW

INFO

## Vulnerabilities

Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	-	136808	ISC BIND Denial of Service
MEDIUM	5.9	-	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	-	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	11213	HTTP TRACE / TRACK Methods Allowed

# SECONDO SCAN

Dopo aver apportato tutte le correzioni ai diversi file di configurazione, nel secondo scan non risulteranno più le vulnerabilità precedenti.