nessus

192.168.1.10

9	9	32	7	89
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 146

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
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)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password
HIGH	8.8	70728	Apache PHP-CGI Remote Code Execution

Risoluzione criticitá 51988

```
msfadmin@metasploitable:~$ ufw default ALLOW
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw default ALLOW
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ ufw DENY 1524
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw DENY 1524
Rules updated
```

Su Metasploitable sono state abilitate tutte le connessioni in entrata con $ ufw default ALLOW poi con $ ufw DENY 1524 viene negata qualsiasi connessione in ingresso verso la porta 1524 e in fine abilitati i firewall $ ufw enable.

Risoluzione criticità 11356

```
  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,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

/mnt/newdisk 192.168.1.10(rw,sync,no_root_squash,no_subtree_check)
```

Aggiungere i permessi solamente alla macchina host nel file che si trova in /etc/exports quindi come all'ultima riga aggiungere solamente l'IP della macchina host /mnt/newdisk IP , il problema é che mancava la configurazione.

Risoluzione criticità 61780

```
root@metasploitable:/# cd home/
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# cd
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# ls -a
.               .config      .gconf           .profile        .ssh
..              Desktop      .gconfd          .purple         .vnc
.bash_history   .filezilla   .gstreamer-0.10  reset_logs.sh   vnc.log
.bashrc         .fluxbox     .mozilla         .rhosts         .Xauthority
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log  metasploitable:1.log  passwd
metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/.vnc# cd passwd
bash: cd: passwd: Not a directory
root@metasploitable:~/.vnc# vncpass
bash: vncpass: command not found
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/.vnc# _
```

```
root@metasploitable:~/.vnc# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:~/.vnc#
```

Entrando come root e nella home o $ cd && ls -a vediamo il file .vnc, entriamo in $ cd .vnc. Cambiamo sia la password dell'host che di VNC, con i comandi $ passwd per cambiare la pass host e $ vncpasswd. Poi si esegue un riavvio e la criticità è terminata. Qui sotto lo scan finale

192.168.1.10

5	3	17	5	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 100

SEVERITY	CVSS V3.0	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