




S5/L5 Epicode Cybersecurity

Vulnerability Remediation




Indice:

- Elenco vulnerabilità
- Risoluzione vulnerabilità 1
- Risoluzione vulnerabilità 2
- Risoluzione vulnerabilità 3
- Conclusioni

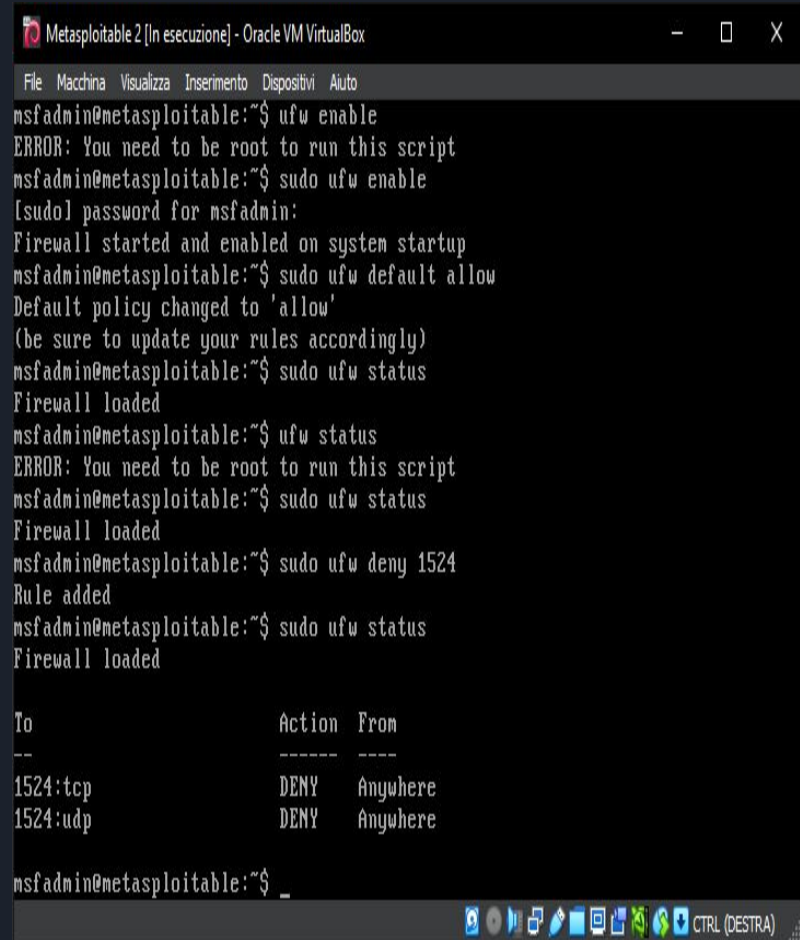


Nell'esercizio di oggi viene richiesto di rimediare ad alcune vulnerabilità presenti sulla macchina Metasploitable. Andiamo quindi ad effettuare una scansione con Nessus e scegliamo quali risolvere.

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password




La prima vulnerabilità che andremo a risolvere è una possibile backdoor presente nel sistema. Per farlo accediamo a Metasploitable, prendiamo i permessi di root tramite il comando 'sudo' e creiamo una nuova regola nel firewall di sistema tramite il comando 'ufw deny 1524', dove ufw corrisponde al firewall e 1524 alla porta che stiamo chiudendo per prevenire la possibile backdoor che Nessun ci indica come vulnerabilità.




```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ ufw enable
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded
msfadmin@metasploitable:~$ ufw status
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

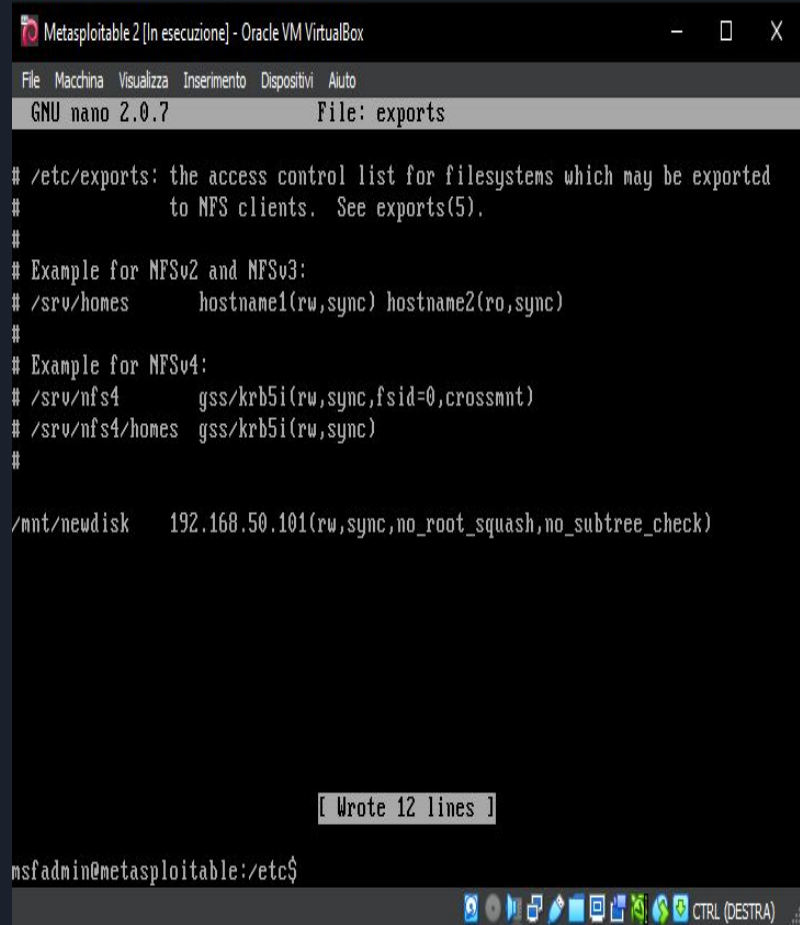
To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere

msfadmin@metasploitable:~$ _
```





La seconda vulnerabilità a cui porremo rimedio è “NFS Exported Share Information Disclosure”, un protocollo che permette agli utenti di condividere file e cartelle tra macchine diverse. Per farlo, modifichiamo il file ‘exports’ tramite il comando ‘nano’ + nome del file, permettendo una eventuale modifica successiva soltanto agli utenti autorizzati.




```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7                               File: 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     192.168.50.101(rw,sync,no_root_squash,no_subtree_check)


[ Wrote 12 lines ]

msfadmin@metasploitable:/etc$
```

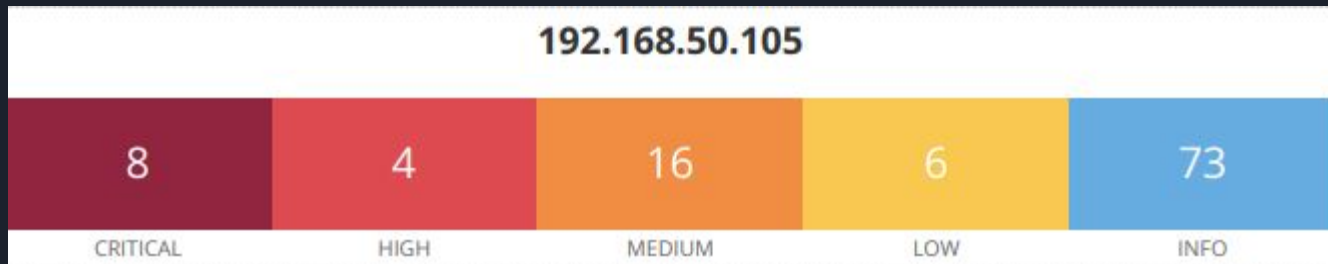


La terza vulnerabilità a cui porremo rimedio è una password debole su un sistema di desktop sharing noto come VNC (Virtual Network Computing), che utilizza la porta 5900. Avendo sempre i permessi di root, utilizziamo il comando 'vncpasswd' per cambiare la password in una più complicata, così da rendere più difficile l'accesso remoto.

```
root@metasploitable:/home/msfadmin# ls -la
.                  .distcc           .mysql_history    .sudo_as_admin_successful
..                .esercizio.py.swp .profile          vulnerable
.bash_history     .gconf            .rhosts
clientbackdoor.py .gconfd           .ssh
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```



Effettuati tutti i passaggi sopra elencati, avviamo un'altra scansione su Nessus per verificare se le vulnerabilità siano state risolte. Se tutto sarà andato per il verso giusto, il numero di vulnerabilità passerà da questo



a questo. Ciò ci dimostra che le nostre azioni siano state effettuate correttamente e tutto è andato a buon fine, risolvendo in totale 4 criticità.

