

REMEDIATION

VNC SERVER 'PASSWORD' PASSWORD

Per risolvere questa vulnerabilità bisogna impostare una nuova password più sicura per il server VNC.

Per fare ciò, da terminale, eseguo il comando 'sudo su' per avere tutti i privilegi da amministratore; successivamente eseguo il comando 'vncserver' per avviare il server VNC.; a questo punto con il comando 'vncpasswd' mi viene data la possibilità di inserire una nuova password; scelgo quindi la password 9!*%38!B tramite un tool online di creazione password sicure che comprende numeri, simboli e caratteri. Avrei voluto inserire una password più lunga per avere una maggiore sicurezza, ma veniva accettata solo una password di massimo otto caratteri.

```
root@metasploitable:/home/msfadmin# vncserver
New 'X' desktop is metasploitable:1
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:1.log
root@metasploitable:/home/msfadmin# _
```

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

NFS EXPORTED SHARE INFORMATION DISCLOSURE

Per risolvere questa vulnerabilità bisogna limitare gli host che possono accedere alle cartelle condivise.

Per fare ciò, tramite il comando 'cd /etc' mi sposto nella directory etc e guardo tutte le directory/file presenti al suo interno con il comando 'ls -A'; apro quindi il file exports per poterlo modificare con il comando 'nano exports'; nell'ultima riga aggiungo '192.168.50.100/24' per far sì che solo la rete interna possa accedere alle cartelle esportate e salvo il file modificato.

```
root@metasploitable:~# cd /etc
root@metasploitable:/etc# ls -A_
```

```
dpkg
e2fsck.conf
emacs
environment
esound
event.d
exports
fdmount.conf
firefox-3.0
fonts
fstab
ftphroot
ftputers
fuse.conf
gai.conf
gconf
gdm
groff
group
group-
grub.d
gshadow
gshadow-
gssapi_mech.conf
mailname
nanpath.config
mediaprm
menu
menu-methods
mime.types
nke2fs.conf
modprobe.d
modules
nord
nord.tail
ntab
mysql
nanorc
network
networks
nsswitch.conf
opt
pam.conf
pam.d
pango
passwd
passwd-
pcmcia
ssl
sudoers
su-to-rootrc
sysctl.conf
syslog.conf
terminfo
timezone
tomcat5.5
ucf.conf
udev
ufw
unreal
updatedb.conf
update-manager
vim
vsftpd.conf
w3m
wgetrc
wpa_supplicant
X11
xinetd.conf
xinetd.d
zsh_command_not_found
root@metasploitable:/etc# nano exports
```

```
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)
#
# * (rw,sync,no_root_squash,no_subtree_check)
```

```
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)
#
# * 192.168.50.100/24 (rw,sync,no_root_squash,no_subtree_check)
```



BIND SHELL BACKDOOR DETECTION

Per risolvere questa vulnerabilità bisogna chiudere la porta a cui è associato il servizio incriminato. Per fare ciò, guardando il report della scansione di Nessus, noto che la porta da chiudere è la 1524; per una ulteriore verifica, da Kali eseguo una scansione con nmap sulla porta 1524 con il comando 'nmap -sV -p 1524 192.168.50.101' che mi conferma quanto riportato da Nessus riportando inoltre il servizio e la sua versione; a questo punto, da terminale su Meta eseguo il comando 'iptables -I INPUT -p tcp --dport 1524 -j DROP' per aggiungere una nuova regola di firewall per bloccare il traffico in entrata sulla porta 1524 utilizzando il firewall di linux iptables; eseguo quindi il comando 'iptables -L' per verificare la presenza della nuova regola. Per avere una verifica prima di eseguire una nuova scansione con Nessus, eseguo nuovamente nmap su Kali che, correttamente, mi restituisce lo stato della porta come filtrata e non fornisce informazioni riguardo il servizio in ascolto.

| Port ▲ | Hosts |
|-------------------------|----------------|
| 1524 / tcp / wild_shell | 192.168.50.101 |

```
(kali@kali)-[~]
$ nmap -sV -p 1524 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 15:39 BST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
PORT      STATE SERVICE VERSION
1524/tcp  open  bindshell Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

```
META 2
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin# _
```

```
(kali@kali)-[~]
$ nmap -sV -p 1524 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 17:28 BST
Nmap scan report for 192.168.50.101
Host is up (0.00076s latency).
PORT      STATE SERVICE VERSION
1524/tcp  filtered ingreslock

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```