

## Descrizione:

In questa fase, sono state implementate una serie di azioni correttive per mitigare le vulnerabilità identificate nella scansione iniziale. Di seguito vengono presentati gli screenshot e una spiegazione dei passaggi seguiti per la remediation.

## Passaggi della Remediation:

### → VNC Server 'password' Password:

- ◆ È stata cambiata la password con una più sicura, tramite il comando 'vncpasswd'. In seguito è stato eseguito un riavvio del servizio VNC.

### → NFS Exported Share Information Disclosure:

- ◆ Per poter mettere in sicurezza, è stato modificato il file di esportazione NFS /etc/exports (mostrato nell'immagine seguente). Inoltre è stata creata una directory( /var/nfsshare ) da esportare che è stata aggiunta all' host a cui è consentito l'accesso.

```
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)
#
#
# /var/nfsshare 192.168.50.100(rw,sync,no_subtree_check)
```

### → Bind Shell Backdoor Detection:

- ◆ Per mettere in sicurezza, è stata creata una regola firewall per la porta 1524. Di seguito, l'immagine con le seguenti regole applicate

```
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ingreslock
DROP       tcp  -- anywhere              anywhere               tcp dpt:ingreslock
Chain FORWARD (policy ACCEPT)
```

### → SSL v. 2.0 e v. 3.0 Protocol Detection:

- ◆ Sono state effettuate varie operazioni. Per quanto riguarda la porta 5432(PostgreSQL), tramite un editor di testo all'interno del file `postgresql.conf` in cui è stata modificata la riga `listen_address`, che si trova nel percorso `/etc/postgresql/<version>/main/`; nella stessa directory(`/main/`) è stato modificato, sempre tramite editor di testo il file `pg_hba.conf` aggiungendo una riga (presente nell'immagine seguente).

```
GNU nano 2.0.7   File: /etc/postgresql/8.3/main/postgresql.conf

                                # (change requires restart)
ident_file = '/etc/postgresql/8.3/main/pg_ident.conf'  # ident configuration f$
                                # (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
external_pid_file = '/var/run/postgresql/8.3-main.pid'           # write an extr$
                                # (change requires restart)

#-----
# CONNECTIONS AND AUTHENTICATION
#-----

# - Connection Settings -

listen_addresses = 'localhost,192.168.50.100'          # what IP address(es) t$
                                # comma-separated list of addresses;
                                # defaults to 'localhost' only;
                                # use '*' for all (IPv4 or IPv6; see
                                # 'listen_ipv6' for details)
```

(postgresql.conf)

```
GNU nano 2.0.7   File: /etc/postgresql/8.3/main/pg_hba.conf

# (autovacuum, daily cronjob, replication, and similar tasks).
#
# Database administrative login by UNIX sockets
local   all             postgres                                ident sameuser
# TYPE  DATABASE  USER  CIDR-ADDRESS              METHOD
# "local" is for Unix domain socket connections only
local   all             all                                ident sameuser
# IPv4 local connections:
host    all             all             0.0.0.0/0                  md5
# IPv6 local connections:
host    all             all             ::0/0                      md5
host    all             all             192.168.50.100/32         md5
```

(pg\_hba.conf)

- ◊ Per quanto riguarda la porta 25 (SMTP), tramite editor di testo è stata modificata la riga `inet.interfaces` all'interno del file `main.cf` nella directory `/etc/postfix/`.

```
GNU nano 2.0.7      File: /etc/postfix/main.cf

smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = metasploitable.localdomain
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = metasploitable.localdomain, localhost.localdomain, , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = loopback-only
```

- ◊ Eseguite le precedenti azioni, è stato eseguito un riavvio.

## Risultati della Remediation:

Tutte le azioni di remediation sono state documentate e verificate. Successivamente è stata eseguita una nuova scansione per verificare la veridicità delle problematiche risolte.