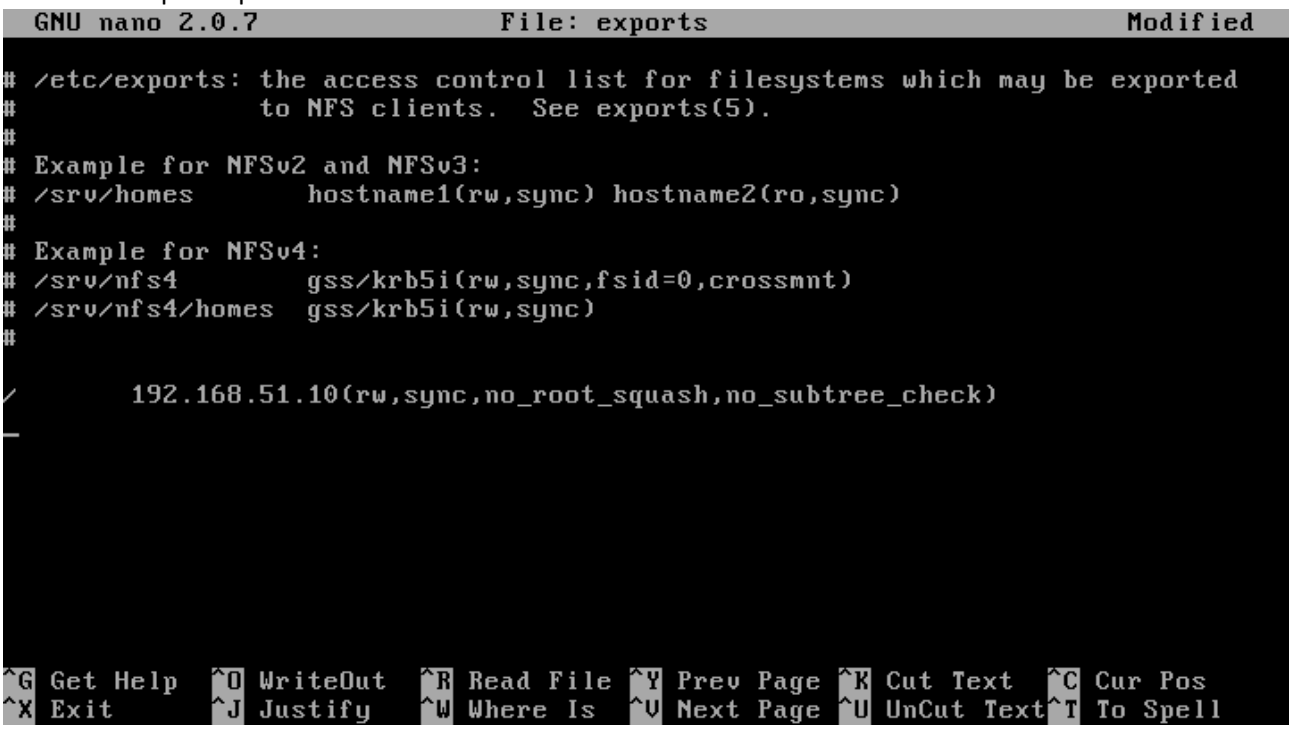
ESERCITAZIONE FINE MODULO 3
BARRECA MONICA

Risolvere criticità rilevate con Nessus

1. **NFS Exported Share Information Disclosure**
2. **VNC Server 'password' Password**
3. **Apache Tomcat AJP Connector Request Injection (Ghostcat)**
4. **Bind Shell Backdoor Detection**
5. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness / SSL Version 2 and 3 Protocol Detection**

1. Per risolvere la prima criticità ho modificato il file /etc/exports autorizzando solo la macchina Meta con tutte le opzioni per l'utilizzo del servizio NFS.



2. Per risolvere la seconda criticità ho lanciato il comando sudo su per autenticarmi come root e poi lanciato il comando vncpasswd che mi ha permesso di modificare la password del servizio.

ESERCITAZIONE FINE MODULO 3
BARRECA MONICA

```
metasploitable login: msfadmin
Password:
Last login: Sat Jan 13 08:37:04 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for 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
root@metasploitable:/home/msfadmin# _
```

3. La terza criticità è stata risolta modificando il file di configurazione contenuto in /etc/tomcat5.5/ server.xml ho disabilitato il connettore AJP sulla porta 8009 in quanto dopo una serie di ricerche ho evinto che in tutte le versioni successive del servizio questo connettore è stato dismesso poiché obsoleto.

```
  GNU nano 2.0.7                File: server.xml                          Modified

                        noCompressionUserAgents="gozilla, traviata"
                        compressableMimeType="text/html,text/xml"
        -->

    <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
    <!--
    <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
    -->

    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <!-- <Connector port="8009"
               enableLookups="false" redirectPort="8443" protocol="AJP/1.3" /> $
_
    <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
    <!-- See proxy documentation for more information about using this. -->
    <!--

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

4. Per la quarta criticità ho modificato il file sshd.config indicando come porta per il servizio ssh la 1524 invece che la standard 22 e richiedendo la login con la password per poter accedere:

ESERCITAZIONE FINE MODULO 3
BARRECA MONICA

```
  GNU nano 2.0.7              File: sshd_config                         Modified

# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 1524
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
  GNU nano 2.0.7              File: sshd_config                         Modified


# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

ESERCITAZIONE FINE MODULO 3
BARRECA MONICA

```
  GNU nano 2.0.7                File: sshd_config                          Modified


# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
UseLogin yes

#MaxStartups 10:30:60
#Banner /etc/issue.net

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

5. Per le criticità legate ai servizi ssh/ssl ho usato due strade:
   la più semplice, utilizzando il firewall per droppare la richieste in entrata sulle porte che utilizzavano quei servizi (compresa la 1524)

```
                               extended match (may load extension)
  --numeric     -n             numeric output of addresses and ports
  --out-interface -o [!] output name[+]
                               network interface name ([+] for wildcard)
  --table       -t table       table to manipulate (default: `filter')
  --verbose     -v             verbose mode
  --line-numbers               print line numbers when listing
  --exact       -x             expand numbers (display exact values)
[!] --fragment  -f             match second or further fragments only
  --modprobe=<command>         try to insert modules using this command
  --set-counters PKTS BYTES    set the counter during insert/append
[!] --version   -V             print package version.
root@metasploitable:/# iptables -S
iptables v1.3.8: Unknown arg `-S'
Try `iptables -h' or 'iptables --help' for more information.
root@metasploitable:/# iptables -S [INPUT]
iptables v1.3.8: Unknown arg `-S'
Try `iptables -h' or 'iptables --help' for more information.
root@metasploitable:/# iptables -I INPUT -p ssl --dport 5432 -j DROP
iptables v1.3.8: unknown protocol `ssl' specified
Try `iptables -h' or 'iptables --help' for more information.
root@metasploitable:/# iptables -I INPUT -p tcp --dport 5432 -j DROP
root@metasploitable:/# iptables -I INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/# iptables -I INPUT -p tcp --dport 25 -j DROP
root@metasploitable:/# _
```

   La seconda (ma non so se corretta) ho modificato i file di configurazione dei servizi su quelle porte così che non utilizzassero più i protocolli ssl

ESERCITAZIONE FINE MODULO 3
BARRECA MONICA

```
  GNU nano 2.0.7                File: main.cf


# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# TLS parameters
#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
                              [ Read 39 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
  GNU nano 2.0.7            File: postgresql.conf

max_connections = 100                   # (change requires restart)
# Note:  Increasing max_connections costs ~400 bytes of shared memory per
# connection slot, plus lock space (see max_locks_per_transaction).  You might
# also need to raise shared_buffers to support more connections.
#superuser_reserved_connections = 3     # (change requires restart)
unix_socket_directory = '/var/run/postgresql'           # (change requires rest$
#unix_socket_group = ''                 # (change requires restart)
#unix_socket_permissions = 0777         # begin with 0 to use octal notation
                                        # (change requires restart)
#bonjour_name = ''                      # defaults to the computer name
                                        # (change requires restart)

# - Security and Authentication -

#authentication_timeout = 1min          # 1s-600s
ssl = false                             # (change requires restart)
#ssl_ciphers = 'ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH:'     # allowed SSL ciphers
                                        # (change requires restart)
#password_encryption = on
#db_user_namespace = off

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```