

Report finale M3 Remediations Meta Manini Sara

Indice generale

Introduzione.....	2
Remediation 1.....	2
Remediation 2.....	4
Remediation 3.....	5
Remediation 4.....	6
Remediation 5.....	8
Conclusioni.....	9

Introduzione

In questo report andremo ad applicare delle remediations per alcune delle vulnerabilità critiche emerse nella scansione fatta in precedenza.

Le remediations non saranno in molti casi quelle suggerite da Nessus ma saranno degli interventi ad hoc eseguiti sui file di configurazione dei servizi della macchina in esame, si è inoltre fatto in modo che le azioni eseguite fossero permanenti anche a seguito del riavvio della macchina.

Remediation 1

Vulnerabilità: 134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat).

Tipo di remediation: Regola firewall.

Procedimento:

- **Step 1:** Dalla macchina Metasploitable 2 eseguire il comando `iptables -I INPUT -p tcp --dport 8009 -j DROP`.

```
root@metasploitable:~# iptables -I INPUT -p tcp --dport 8009 -j DROP
```

- **Step 2:** Controllare se la regola è stata creata correttamente con il comando `iptables -L`.

```
root@metasploitable:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:8009
DROP      tcp  --  anywhere              anywhere              tcp dpt:8009

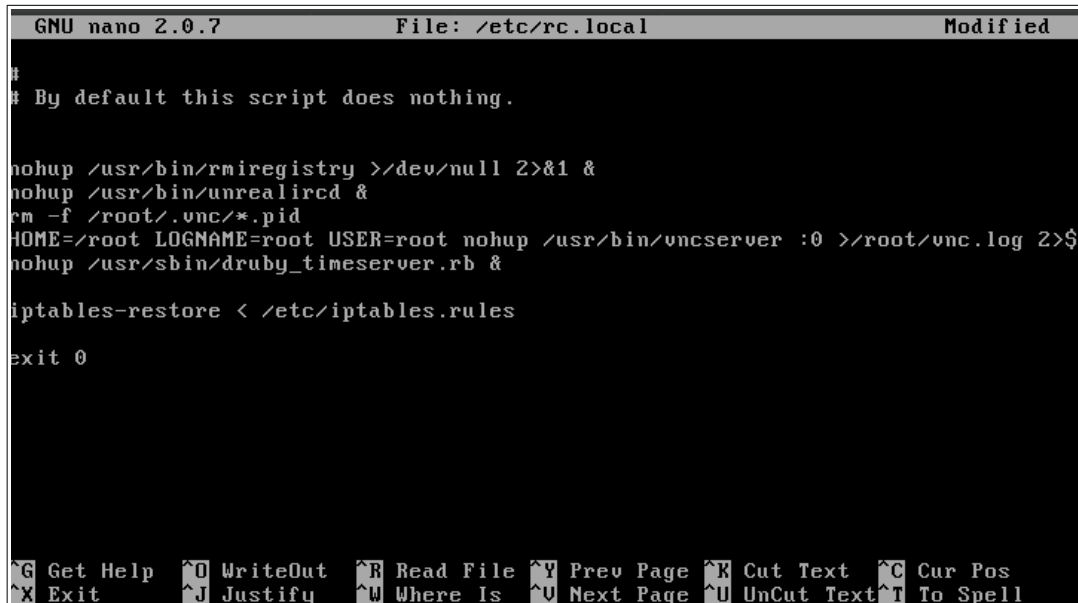
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:~#
```

- **Step 3:** Per salvare la regola, eseguire il comando `iptables-save > /etc/iptables.rules`.

```
root@metasploitable:~# iptables-save > /etc/iptables.rules
```

- **Step 4:** Per rendere la regola permanente al riavvio della macchina, modificare il file `/etc/rc.local` immettendo il file contenente la regola nella modalità che segue.



```
GNU nano 2.0.7      File: /etc/rc.local      Modified
#
# By default this script does nothing.

nohup /usr/bin/rmiregistry >>/dev/null 2>&1 &
nohup /usr/bin/unrealircd &
rm -f /root/.vnc/*.pid
HOME=/root LOGNAME=root USER=root nohup /usr/bin/vncserver :0 >/root/vnc.log 2>$
nohup /usr/sbin/druby_timeserver.rb &

iptables-restore < /etc/iptables.rules

exit 0

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

Esito remediation: Tramite regola firewall abbiamo bloccato il traffico sulla porta 8009, su cui è presente l'AJP connector vulnerabile.

Remediation 2

Vulnerabilità: 51988 - Bind Shell Backdoor Detection.

Tipo di remediation: Modifica file di sistema.

Procedimento:

- **Step 1:** Accedere al file `/etc/inetd.conf` e commentare la riga di `ingreslock`.

```
GNU nano 2.0.7      File: /etc/inetd.conf      Modified
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet               stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                dgram   udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tf$
shell               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login              stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

- **Step 2:** riavviare il servizio `xinetd` con il comando `/etc/init.d/xinetd restart` per applicare le modifiche.

```
root@metasploitable:~# /etc/init.d/xinetd restart
* Stopping internet superserver xinetd      [ OK ]
* Starting internet superserver xinetd      [ OK ]
```

Esito remediation: A causa della riga finale `ingreslock stream tcp nowait root /bin/bash bash -i`, potenziali attori malintenzionati possono facilmente avviare una shell con privilegi di root utilizzando strumenti come Meterpreter e Netcat. Commentando questa riga non è più possibile farlo.

Remediation 3

Vulnerabilità: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness.

Tipo di remediation: Rigenerazione chiavi SSH.

Procedimento:

- **Step 1:** Rigenerare la chiave RSA con il seguente comando
ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key.

```
root@metasploitable:~# ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key
Generating public/private rsa key pair.
/etc/ssh/ssh_host_rsa_key already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
79:e7:bf:cb:e0:55:db:63:e9:02:43:92:2e:b7:0c:26 root@metasploitable
root@metasploitable:~# _
```

- **Step 2:** Rigenerare la chiave DSA con il seguente comando
ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key.

```
root@metasploitable:~# ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key
Generating public/private dsa key pair.
/etc/ssh/ssh_host_dsa_key already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
ac:70:19:8d:a9:43:46:9a:3a:a6:70:cf:98:08:e3:3d root@metasploitable
root@metasploitable:~# _
```

- **Step 3:** Riavviare il servizio SSH con il comando */etc/init.d/ssh restart*.

```
root@metasploitable:~# /etc/init.d/ssh restart
* Restarting OpenBSD Secure Shell server sshd [ OK ]
root@metasploitable:~# _
```

Esito remediation: Le chiavi SSH rigenerate non sono affette dalla precedente vulnerabilità.

Remediation 4

Vulnerabilità: 20007 - SSL Version 2 and 3 Protocol Detection.

Tipo di remediation: Disattivazione SSL v2 e v3.

Procedimento per la porta 25:

- **Step 1:** Accedere al file `/etc/postfix/main.cf` e modificarlo come da figura. In questo modo disattiveremo il protocollo SSL ed attiveremo al suo posto la modalità TLS encrypt.

```
GNU nano 2.0.7      File: /etc/postfix/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_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtpd_tls_security_level = encrypt
smtpd_tls_protocols = !SSLv2, !SSLv3
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for

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

- **Step 2:** Riavviare il servizio SMTP con il comando `/etc/init.d/postfix restart`.

```
root@metasploitable:~# sudo /etc/init.d/postfix restart
* Stopping Postfix Mail Transport Agent postfix      [ OK ]
* Starting Postfix Mail Transport Agent postfix      [ OK ]
root@metasploitable:~# _
```

Procedimento per la porta 5432:

- **Step 1:** Disattivare il protocollo SSL modificando il file `/etc/postgresql/8.3/main/postgresql.conf`.

```
GNU nano 2.0.7  File: /etc/postgresql/8.3/main/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 restart)
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 = off                                             # (change requires restart)
password_encryption = on
db_user_namespace = off
```

- **Step 2:** Riavviare il servizio di postgresql con il comando `/etc/init.d/postgresql-8.3 restart`.

```
root@metasploitable:~# /etc/init.d/postgresql-8.3 restart
* Restarting PostgreSQL 8.3 database server
root@metasploitable:~# _ [ OK ]
```

Esito remediation: Disattivando il servizio SSL sulle porte 25 e 5432 abbiamo eliminato i protocolli vulnerabili.

Remediation 5

Vulnerabilità: 61708 - VNC Server 'password' Password.

Tipo di remediation: Cambio password server VNC.

Procedimento:

- **Step 1:** Eseguire il comando `vncpasswd` con i permessi di root attivati ed immettere una nuova password sia per il server VNC, sia per la versione view-only del servizio. Spostandoci sulla vm di Kali ed eseguendo il comando `vncviewer <IP metasploitable> : <porta servizio VNC>` possiamo verificare se la password è stata cambiata correttamente provando a connetterci al server VNC.

```
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#
```

Esito remediation: La password è stata cambiata ed è ora sicura.

Conclusioni

Le remediations eseguite non sono procedure standard o consigliate per la risoluzione delle vulnerabilità, ma sono state necessarie in quanto la macchina Metasploitable 2 è studiata per essere estremamente vulnerabile e quindi non è possibile collegarla ad internet per eseguire aggiornamenti di sistema (o dei servizi) o per applicare patch di sicurezza come suggerito da Nessus a monte della scansione.