Vulnerability scan and remediation

Andrea Volterra

Target: Metasploitable

SCANSIONE NESSUS PRELIMINARE

192.168.1.115

Vulnerabilities Total: 106

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
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

VULNERABILITY REMEDIATION METASPLOITABLE

CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure

La directory root viene rimossa tramite commento sulla riga relativa nel file exports

```
  GNU nano 2.0.7                File: /etc/exports                      Modified

# /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)

                              [ Read 12 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
```

CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection

Avvio prima il servizio SSL

```
msfadmin@metasploitable:~$ sudo a2enmod ssl
Module ssl installed; run /etc/init.d/apache2 force-reload to enable.
msfadmin@metasploitable:~$
```

Per poi modificare il file ssl.conf, disabilitando il protocollo SSL per attivare il TLS

```
  GNU nano 2.0.7      File: /etc/apache2/mods-enabled/ssl.conf        Modified

#SSLSessionCache         dbm:/var/run/apache2/ssl_scache
SSLSessionCache        shmcb:/var/run/apache2/ssl_scache(512000)
SSLSessionCacheTimeout  300

#   Semaphore:
#   Configure the path to the mutual exclusion semaphore the
#   SSL engine uses internally for inter-process synchronization.
SSLMutex  file:/var/run/apache2/ssl_mutex

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
#   enable only secure ciphers:
SSLCipherSuite HIGH:MEDIUM:!ADH

# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol all +TLSv1

</IfModule>

^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
```

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

Imposto la regola firewall che rifiuta il traffico sulla porta 1524 con il comando:

iptables -A INPUT -p tcp –dport 1524 -j DROP

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?

root@metasploitable:/etc/init.d# iptables-save > fwrules
root@metasploitable:/etc/init.d# cat fwrules
# Generated by iptables-save v1.3.8 on Fri May 12 14:18:41 2023
*filter
:INPUT ACCEPT [18107:1947090]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [15122:2395097]
-A INPUT -p tcp -m tcp --dport 1524 -j DROP
COMMIT
# Completed on Fri May 12 14:18:41 2023
root@metasploitable:/etc/init.d#
```

E salvo la regola nel file fwrules all’interno della directory /etc/init.d

Per caricare la regola ad ogni boot modifico il file rc.local inserendo la stringa

Iptables-restore </etc/init.d/fwrules

```
  GNU nano 2.0.7             File: /etc/rc.local

#
# By default this script does nothing.

loadkeys it
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/init.d/fwrules

exit 0
_

^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
```

Disattivo anche i servizi shell, telnet e exec commentandoli sul file inetd.conf nella directory /etc/

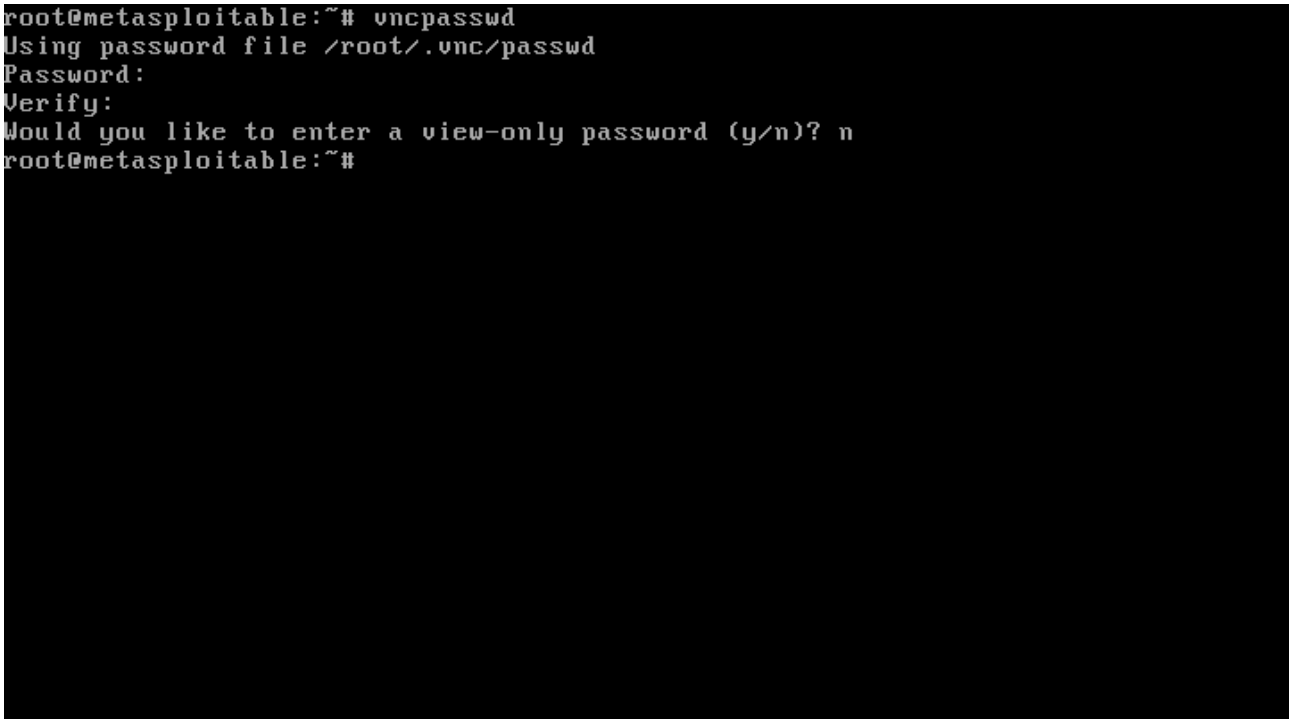
```
  GNU nano 2.0.7             File: /etc/inetd.conf

#<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

                        [ Read 8 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
```

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Per risolvere la vulnerabilità della password di VNC modifico il file passwd nella directory /root/.VNC/



VULNERABILITY SCAN POST FIX

192.168.1.115

5	3	17	5	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
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)
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service