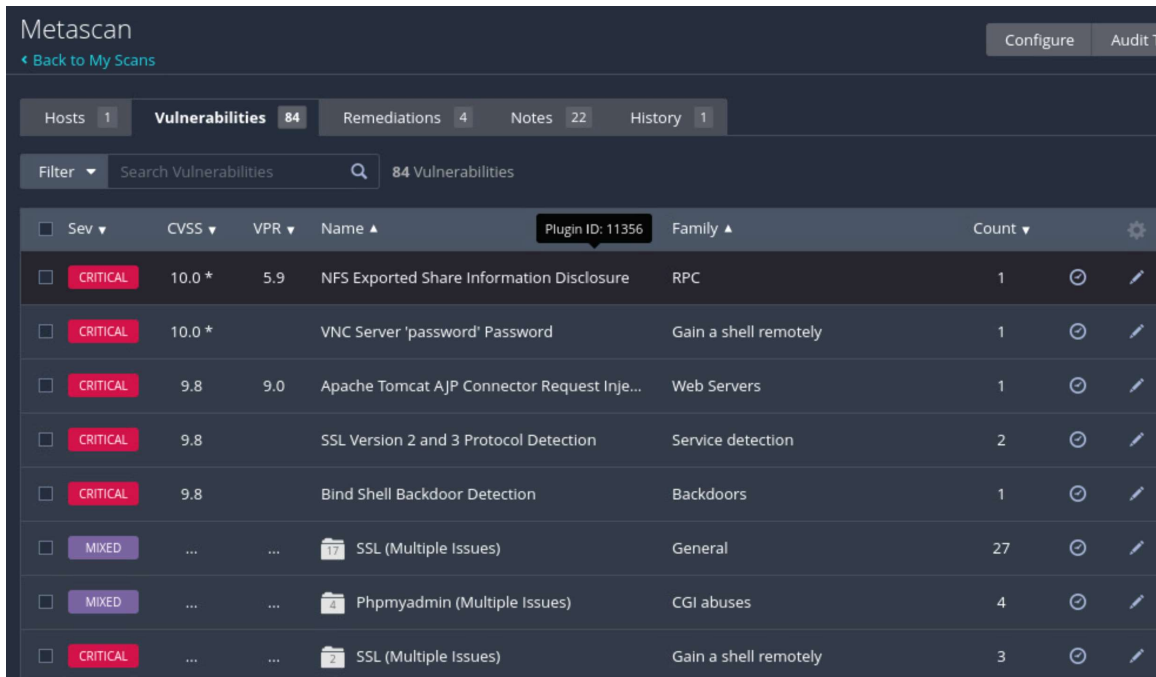


Vulnerabilita' Identificate da Nessus:



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Inje...	Web Servers	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	SSL (Multiple Issues)	General	27
MIXED	Phpmyadmin (Multiple Issues)	CGI abuses	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3

Risoluzione "NFS Exported Share Information Disclosure"

1. Modifica del file /etc/exports e rimozione della riga che consente di montare la root del sistema:

```
# /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)
~
~
~
~
~
~
~
```

2. Riavvio del sistema per rendere attive le modifiche.

Risoluzione "VNC Server 'password' password"

1. Occorre eseguire il comando "vncpasswd" per rimpiazzare la password di default con una password piu' robusta:

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ _
```

Risoluzione "Apache Tomcat AJP Connector Request Injection (Ghostcat)"

1. Modifichiamo il file /etc/tomcat5.5/server.xml e commentiamo la riga che definisce un connettore AJP:

```
-->
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. -->
<!--
<Connector port="8082"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
      enableLookups="false" acceptCount="100" connectionTimeout="20000"
      proxyPort="80" disableUploadTimeout="true" />
-->
```

2. Riavviamo il servizio del web server tomcat o la macchina metasploitable per rendere attive le modifiche.

Risoluzione "SSL Version 2 and 3 Protocol Detection"

Nessus rileva il problema sui servizi che usufruiscono delle porte 25 e 5432. Da netstat cerchiamo i servizi per poterne modificare le configurazioni:

```
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep :25
tcp        0      0 0.0.0.0:25 0.0.0.0:*        LISTEN
4973/master
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep :5432
tcp        0      0 0.0.0.0:5432 0.0.0.0:*        LISTEN
4818/postgres
tcp6       0      0 :::5432    :::*              LISTEN
4818/postgres
```

nel nostro caso si tratta del server PostgreSQL e del servizio Postfix per l'invio di messaggi di posta elettronica (SMTP):

```
msfadmin@metasploitable:~$ ps -eF | grep 4973
root      4973      1  0 1353 1728  0 Jul05 ?        00:00:03 /usr/lib/postfix
/master
postfix   4979  4973  0 1365 1800  0 Jul05 ?        00:00:00 qmgr -l -t fifo
-u
postfix   19226 4973  0 1355 1648  0 12:53 ?        00:00:00 pickup -l -t fif
o -u -c
msfadmin 19389 19325 0 751 756  0 14:21 tty1    00:00:00 grep 4973
postfix   20984 4973  0 1447 2456  0 Jul12 ?        00:00:00 tlsmgr -l -t uni
x -u -c
msfadmin@metasploitable:~$
```

la risoluzione del problema richiede pertanto di modificare le configurazioni dei due servizi.

1. PostgreSQL:

Modifichiamo il file di configurazione del server PostgreSQL DB in:

`/etc/postgresql/8.3/main`

occorre disabilitare il supporto SSL in quanto la versione 8.3 di PostgreSQL non supporta lo standard TLSv1.2 che risolverebbe la vulnerabilit  in questione:

```

#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_min_protocol_version = 'TLSv1.2'
#ssl_ciphers = 'TLSv1.2:!aNULL'      # allowed SSL ciphers
#                                # (change requires restart)
#password_encryption = on

```

i due parametri commentati sarebbero quelli utilizzati in versioni di PostgreSQL piu' recenti.

2. *Postfix:*

Modifichiamo il file di configurazione in /etc/postfix/main.cf:

```

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

smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, TLSv1.2
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, TLSv1.2
smtpd_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, TLSv1.2
smtp_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, TLSv1.2
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

```

Riavviamo il servizio.

Risoluzione "Bind shell backdoor detection":

In questo caso nessus identifica una backdoor attiva con accesso root sulla porta 1524.
Utilizzando netstat:

```
msfadmin@metasploitable:~$ sudo netstat -tlunp | grep :1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*           LISTEN
5010/xinetd
msfadmin@metasploitable:~$
```

il processo che esegue la backdoor e' quello con PID 5010 (xinetd). Ricercando su internet:

<https://packetstormsecurity.com/files/26161/pure-xinetd-backdoor.c.html>
<https://packetstormsecurity.com/files/26161/pure-xinetd-backdoor.c.html>

oppure:

<https://elhacker.info/Cursos/Computer%20and%20Network%20Hacking%20Mastery%20Practical%20Techniques/9.%20Attacks%20on%20Operating%20Systems/3.%20Entering%20the%20system%20by%20the%20backdoor.pdf>

per trovare come questo servizio possa essere utilizzato per la definizione di una backdoor.

Siccome xinetd e' la versione X server di inetd verificiamo entrambi i file di configurazione. Per xinetd.conf:

```
msfadmin@metasploitable:~$ cat /etc/xinetd.conf
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    # Please note that you need a log_type line to be able to use log_on_success
    # and log_on_failure. The default is the following :
    # log_type = SYSLOG daemon info
}

includedir /etc/xinetd.d
```

e la cartella di configurazione /etc/xinetd.d:

```
msfadmin@metasploitable:/etc/xinetd.d$ ls -al
total 32
drwxr-xr-x  2 root root 4096 2012-05-20 14:17 .
drwxr-xr-x 94 root root 4096 2024-07-30 10:10 ..
-rw-r--r--  1 root root  798 2007-12-03 19:16 chargen
-rw-r--r--  1 root root  660 2007-12-03 19:16 daytime
-rw-r--r--  1 root root  549 2007-12-03 19:16 discard
-rw-r--r--  1 root root  580 2007-12-03 19:16 echo
-rw-r--r--  1 root root  727 2007-12-03 19:16 time
-rw-r--r--  1 root root  576 2012-05-20 14:17 vsftpd
msfadmin@metasploitable:/etc/xinetd.d$
```

possiamo analizzare file per file, ma questi sembrano legittimi e non hanno include per richiamare file malevoli.

Per inetd.conf:

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbi
n/smbd
telnet                  stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
netd
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbi
n/in.ftpd
tftp                   dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tft
pd /srv/tftp
shell                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
d
login                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlo
gind
exec                   stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rex
ecd
#ingreslock stream tcp nowait root /bin/bash bash -i
-
-
-
-
-
-
-
msfadmin@metasploitable:~$ sudo vi /etc/inetd.conf
```

la riga con il comando /bin/bash bash -i sembra essere quella indirizzata ad aprire una sessione di bash. Commentiamo la riga e riavviamo la distro.

Verifica della risoluzione delle criticita'.

Per verificare che le criticita' siano state risolte, eseguiamo nuovamente la scansione con Nessus sul target per verificare che gli elementi CRITICAL siano stati eliminati:

Metascan / 192.168.50.100
[← Back to Hosts](#)

Vulnerabilities 66

Filter Search Vulnerabilities 66 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	1
HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses	1
HIGH	7.5		Samba Badlock Vulnerability	General	1
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	1
MEDIUM	5.9		SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9		SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1

A fronte degli interventi correttivi intrapresi, l'unica criticita' non eliminata e' quella relativa al server smtp postfix. Probabilmente a causa disud

```

root@metasploitable:~# postconf | grep protocols
inet_protocols = ipv4
lmtp_tls_mandatory_protocols = SSLv3, TLSv1
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, TLSv1.2
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, TLSv1.2
root@metasploitable:~# _

```

Aggiungiamo anche la riga per i protocolli lmtp e riavviamo i servizi.