

Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. **Screenshot e spiegazione dei passaggi della remediation** - **RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

4

Sev ▼	Score ▼	Name ▲
<input type="checkbox"/> CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/> CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/> CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/> CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/> CRITICAL	9.8	Bind Shell Backdoor Detection

VULNERABILITA' 61708 :

CRITICAL 10.0* - 61708 VNC Server 'password' Password

VNC Server 'password' Password

CRITICAL Nessus Plugin ID 61708

Information Dependencies Dependents Changelog

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

SOLUZIONE:

La soluzione consiste nel modificare la password “debole” con una password “forte”

```
metasploit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:4088 (3.9 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:106 errors:0 dropped:0 overruns:0 frame:0
TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:20749 (20.2 KB) TX bytes:20749 (20.2 KB)

msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# uncpasswd
Using password file /root/.unc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

Seconda Criticità

CRITICAL 10.0 - 171340 Apache Tomcat SEoL (<= 5.5.x)

Apache Tomcat SEoL (<= 5.5.x)

CRITICAL Nessus Plugin ID 171340

Information Dependencies Dependents Changelog

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

See Also

<https://tomcat.apache.org/tomcat-55-eol.html>

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.50.101
```

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

```
(root@kali)-[/home/kali]
# nmap --script auth 192.168.50.101 -sS
```

8180/tcp open unknown

| http-default-accounts:

| [Apache Tomcat] at /manager/html/

| tomcat:tomcat

| [Apache Tomcat Host Manager] at /host-manager/html/

| tomcat:tomcat

MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)

Post-scan script results:

| creds-summary:

| 192.168.50.101:

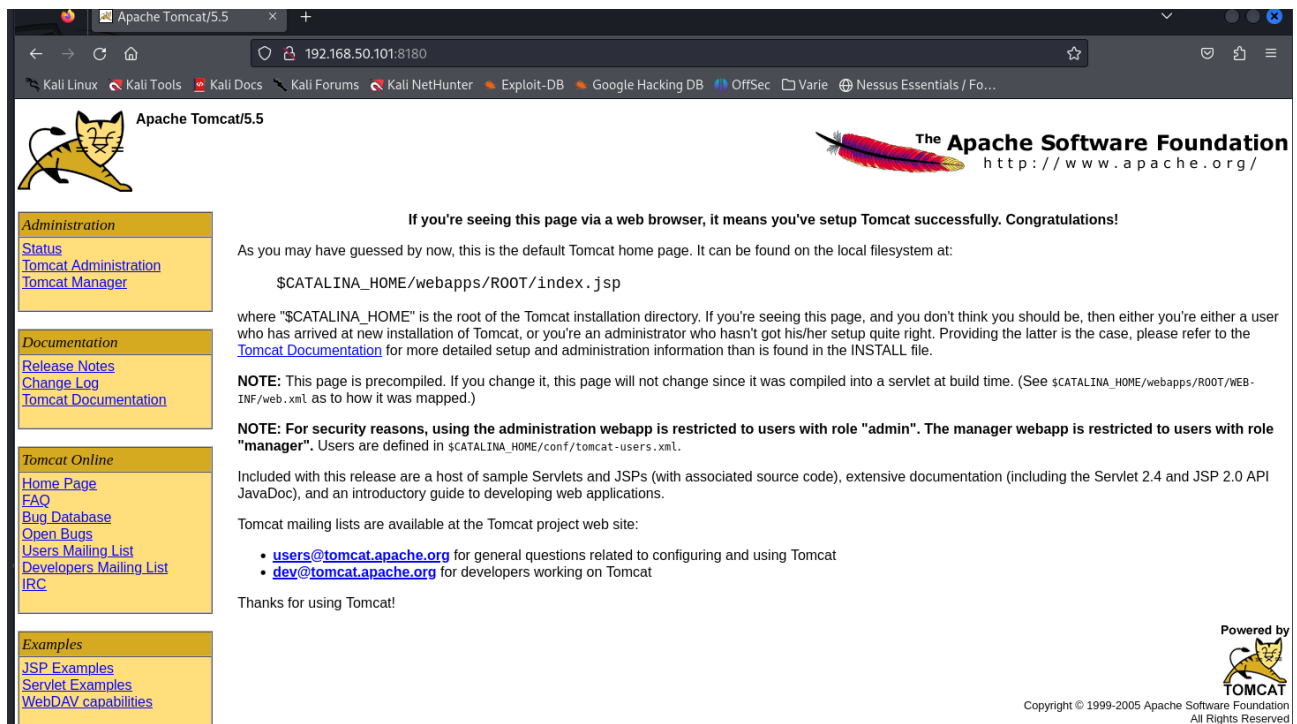
| 8180/nil:

| tomcat:tomcat - Valid credentials

| tomcat:tomcat - Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 44.21 seconds

<http://192.168.50.101:8180/>



Accesso con credenziali tomcat : tomcat

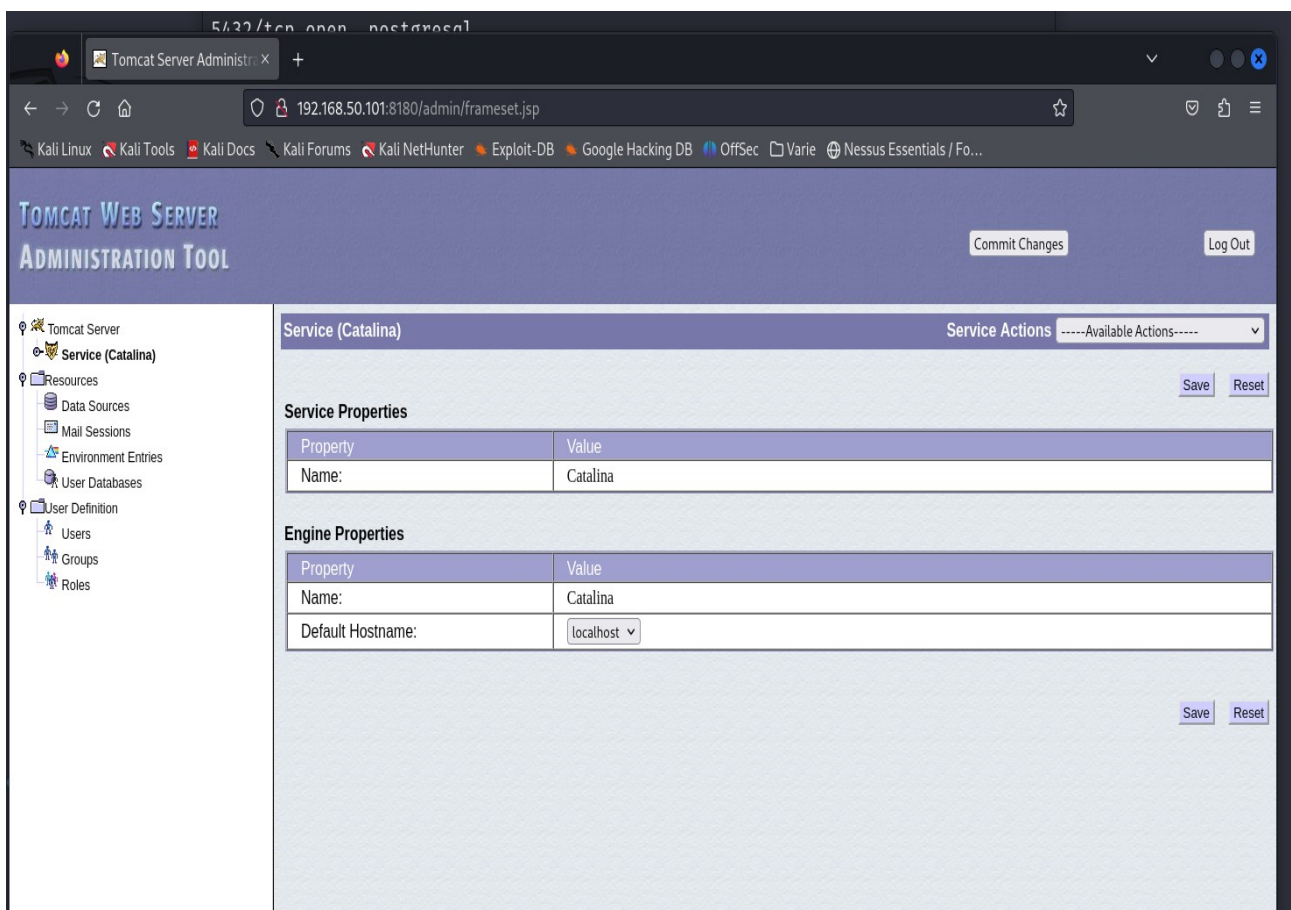


The image shows the login interface of the Tomcat Web Server Administration tool. It has a dark red background with the title 'TOMCAT WEB SERVER ADMINISTRATION T O O L' in a stylized font. Below the title, there are two input fields: 'User Name' with the value 'tomcat' and 'Password' with masked characters '.....'. At the bottom, there are two buttons: 'Login' and 'Reset'.

TOMCAT WEB SERVER
ADMINISTRATION
T O O L

User Name

Password



The image shows the main interface of the Tomcat Web Server Administration tool in a web browser. The browser address bar shows the URL '192.168.50.101:8180/admin/frameset.jsp'. The interface has a dark blue header with the title 'TOMCAT WEB SERVER ADMINISTRATION TOOL' and buttons for 'Commit Changes' and 'Log Out'. On the left, there is a sidebar menu with categories: 'Tomcat Server' (containing 'Service (Catalina)'), 'Resources' (containing 'Data Sources', 'Mail Sessions', 'Environment Entries', 'User Databases'), and 'User Definition' (containing 'Users', 'Groups', 'Roles'). The main content area displays the configuration for the 'Service (Catalina)'.

5422/tomcat-admin-postgresql

Tomcat Server Administration X

192.168.50.101:8180/admin/frameset.jsp

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Varie Nessus Essentials / Fo...

TOMCAT WEB SERVER
ADMINISTRATION TOOL

Commit Changes Log Out

Tomcat Server

- Service (Catalina)

Resources

- Data Sources
- Mail Sessions
- Environment Entries
- User Databases

User Definition

- Users
- Groups
- Roles

Service (Catalina) Service Actions -----Available Actions-----

Save Reset

Service Properties

Property	Value
Name:	Catalina

Engine Properties

Property	Value
Name:	Catalina
Default Hostname:	localhost

Save Reset

Cambio password amministratore con una piu forte.

The screenshot shows the Tomcat Web Server Administration Tool interface. On the left is a navigation tree with categories like Tomcat Server, Service (Catalina), Resources, Data Sources, Mail Sessions, Environment Entries, User Databases, User Definition, Users, Groups, and Roles. The main panel is titled 'Edit Existing User Properties' and contains a 'User Properties' section with fields for 'User Name' (tomcat), 'Password' (masked with dots), and 'Full Name'. Below this are two tables: 'Group Name' and 'Role Name'. The 'Role Name' table has columns for 'Role Name' and 'Description', with roles 'admin', 'manager', 'role1', and 'tomcat' listed. The 'admin' and 'manager' roles are checked. At the bottom right of the role table is a 'Save' button.

Group Name	Description

Role Name	Description
<input checked="" type="checkbox"/> admin	
<input checked="" type="checkbox"/> manager	
<input type="checkbox"/> role1	
<input checked="" type="checkbox"/> tomcat	

Localizzazione file tomcat-users.xml su Metasploitable :

```
root@metasploitable:/home/msfadmin# locate tomcat-users.xml
/etc/tomcat5.5/tomcat-users.xml
root@metasploitable:/home/msfadmin# cd /etc/tomcat5.5/
root@metasploitable:/etc/tomcat5.5# ls
Catalina          context.xml      server-minimal.xml  tomcat-users.xml
Catalina.policy   logging.properties  server.xml          web.xml
Catalina.properties  policy.d        tomcat5.5
root@metasploitable:/etc/tomcat5.5# cat tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="admin"/>
  <role rolename="tomcat"/>
  <role rolename="manager"/>
  <role rolename="role1"/>
  <user username="tomcat" password="TOM159cat!" fullName="" roles="admin,manager,tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
</tomcat-users>
root@metasploitable:/etc/tomcat5.5#
```

Modifica admin

The screenshot shows the GNU nano 2.0.7 text editor editing the file 'tomcat-users.xml'. The XML content is visible, showing roles 'admin-gui', 'tomcat', 'manager', and 'role1'. The 'admin-gui' role is being modified. The bottom status bar shows various keyboard shortcuts like 'Get Help', 'WriteOut', 'Read File', etc.

```
<tomcat-users>
  <role rolename="admin-gui"/>
  <role rolename="tomcat"/>
  <role rolename="manager"/>
  <role rolename="role1"/>
  <user username="tomcat" password="TOM159cat!" fullName="" roles="admin,manager,tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
</tomcat-users>
```

```

root@metasploitable:/etc/tomcat5.5#
root@metasploitable:/etc/tomcat5.5# cat tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="admin-gui"/>
  <role rolename="tomcat"/>
  <role rolename="manager"/>
  <role rolename="role1"/>
  <user username="tomcat" password="TOM159cat!" fullName="" roles="admin,manager,tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
</tomcat-users>
root@metasploitable:/etc/tomcat5.5#

```

Risultato finale delle modifiche per migliorare la sicurezza generale di Tomcat

Terza criticità:

CRITICAL

9.8

-

51988

Bind Shell Backdoor Detection

```

File Actions Edit View Help
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 09:52 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00052s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```


Con “netcat” vediamo che la backdoor è funzionante (porta 1524)

```
(root@kali)-[/home/kali]
# nc 192.168.50.101 1524
root@metasploitable:/# msfadmin
bash: msfadmin: command not found
root@metasploitable:/# whoami
root
root@metasploitable:/# netstat -an | grep 192.168.50.101
tcp        0      0 192.168.50.101:53      0.0.0.0:*               LISTEN
tcp        0      0 192.168.50.101:1099    192.168.50.100:35304    CLOSE_WAIT
tcp        0      0 192.168.50.101:1524    192.168.50.100:55272    ESTABLISHE
D
udp        0      0 192.168.50.101:137     0.0.0.0:*
udp        0      0 192.168.50.101:138     0.0.0.0:*
udp        0      0 192.168.50.101:53      0.0.0.0:*
root@metasploitable:/#
```

Utilizzando il comando “fuser” tenteremo di chiudere quella determinata porta per evitare un futuro utilizzo della backdoor.

```
root@metasploitable:/# fuser -k -n tcp 1524
1524/tcp:          4520  6270
```

```
(root@kali)-[/home/kali]
#
```

Scansione con “nmap” per verificare che la porta sia effettivamente chiusa

```
root@kali:~# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 10:12 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 35.15 seconds
```

Purtoppo non è una soluzione definitiva, dato che al riavvio di Metasploitable la porta si riattiva e con essa la backdoor.

Quarta vulnerabilità:

CRITICAL

10.0*

5.9

11356

NFS Exported Share Information Disclosure

NFS Exported Share Information Disclosure

CRITICAL

Nessus Plugin ID 11356

Information

Dependencies

Dependents

Changelog

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Modifichiamo il file EXPORTS:

Questo fa sì che SOLO i file nel percorso specificato siano condivisi e SOLO con tutta la rete interna di metasploitable.

```
dpkg
e2fsck.conf
emacs
environment
esound
event.d
exports
fdmount.conf
firefox-3.0
fonts
fstab
ftphroot
ftpusers
fuse.conf
gai.conf
gconf
gdm
groff
group
group-
grub.d
gshadow
gshadow-
gssapi_mech.conf
root@metasploitable:/etc#
mailname
manpath.config
mediaprm
menu
menu-methods
mime.types
mke2fs.conf
modprobe.d
modules
motd
motd.tail
mtab
mysql
nanorc
network
networks
nsswitch.conf
opt
pam.conf
pam.d
pango
passwd
passwd-
pcmcia
sudoers
su-to-rootrc
sysctl.conf
syslog.conf
terminfo
timezone
tomcat5.5
ucf.conf
udev
ufw
unreal
updatedb.conf
update-manager
vim
vsftpd.conf
w3m
wgetrc
wpa_supplicant
X11
xinetd.conf
xinetd.d
zsh_command_not_found
```



```
# /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)
#
/usr/share 192.168.50.0/24(ro, sync, squash_root, check_subtree)_
```

^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