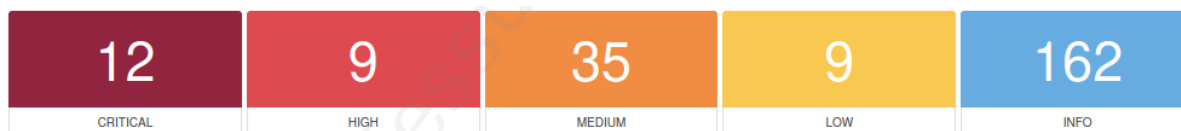


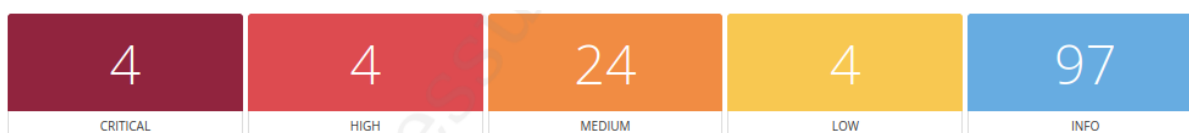
# Remediation Report:

Report effettuato da Anatoliy Prysyzhnyuk (04.06.2023)

## Prima scansione delle vulnerabilità:



## Scansione finale delle vulnerabilità:



**NFS Exported Share Information Disclosure:** Ho implementato misure per prevenire l'accesso non autorizzato alle informazioni sensibili contenute nelle condivisioni NFS.

**CRITICAL** NFS Exported Share Information Disclosure

**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.

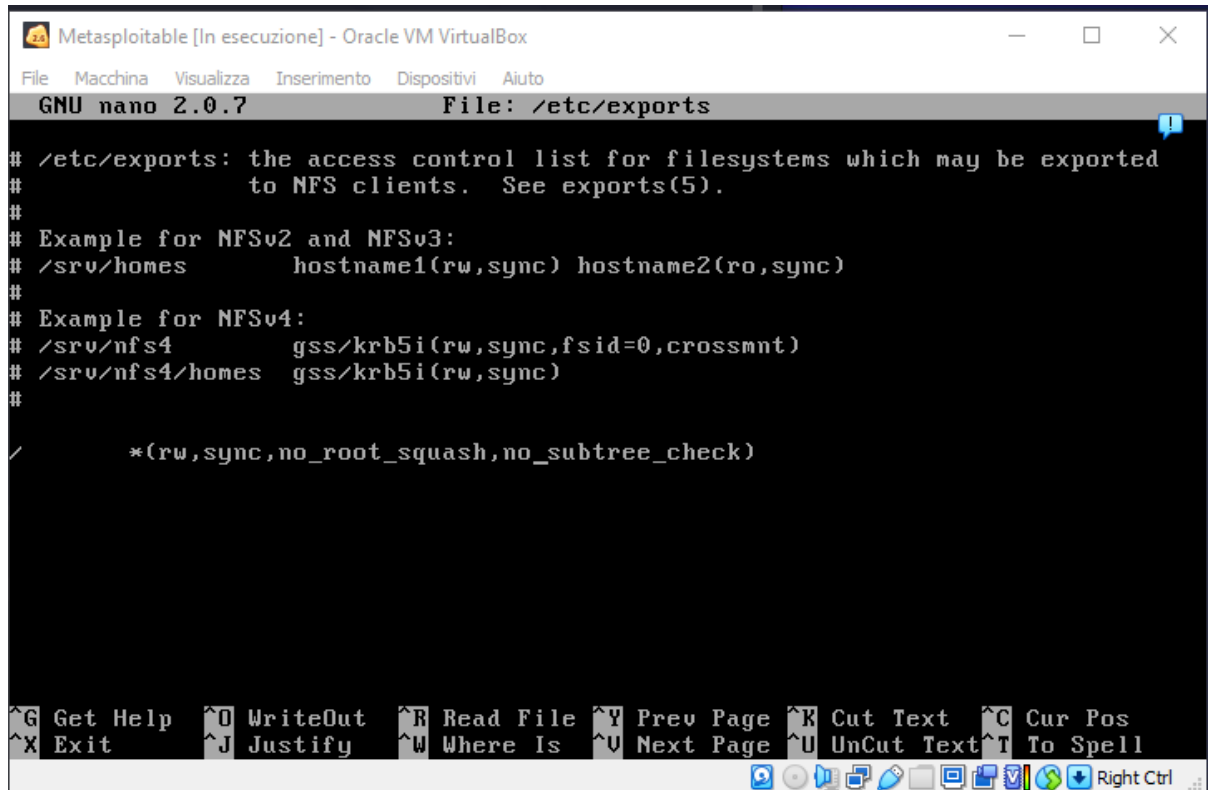
**Output**  

```
The following NFS shares could be mounted :  
  
+ /  
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom  
- dev  
- etc  
- home  
- initrd  
- initrd.img  
- lib  
- lost+found  
- media  
- mnt  
- nohup.out  
- opt  
- proc  
- root  
- sbin  
- srv  
- sys
```

Sulla VM (Virtual Machine) di Metasploitable ho eseguito il seguente comando:

“sudo nano /etc/exports:”

Nell'immagine sotto, vediamo come era settata la configurazione all'inizio:

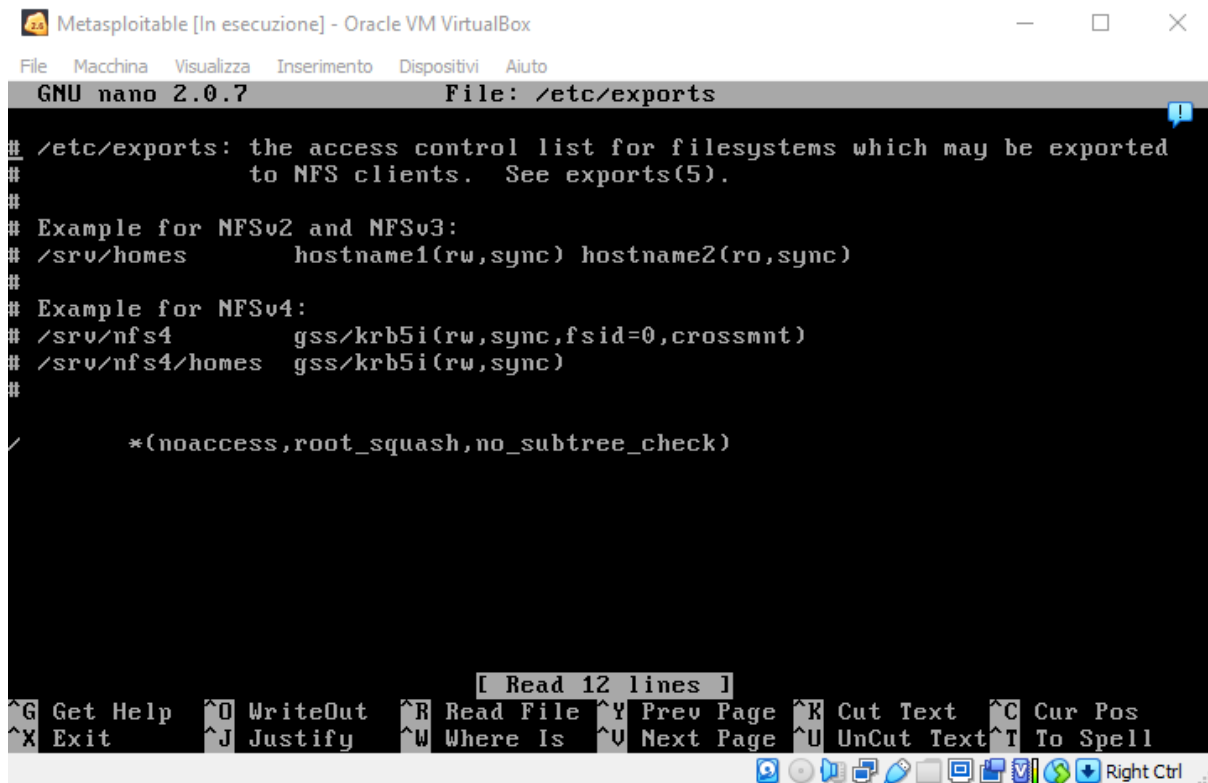


```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports

# /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)
```

Dopodichè la cambiai, come vediamo nello screen sottostante:

Precisamente cambiai i permessi, togliendo rw (read and write) e sync, ho tolto anche il “no” nel “no\_root\_squash”.



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports

# /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)
#
/*(noaccess, root_squash, no_subtree_check)
```

Per confermare le modifiche: Ctrl O + Ctrl X, dopodichè “sudo reboot” per riavviare la macchina.

**Bind Shell Backdoor Detection:** Ho rimosso una potenziale backdoor che consentiva l'accesso non autorizzato al sistema.

Metasploitable Basic Scan / Plugin #51988		
<a href="#">← Back to Vulnerabilities</a>		
Vulnerabilities 92		
CRITICAL Bind Shell Backdoor Detection		
<b>Description</b> <p>A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.</p>		
<b>Solution</b> <p>Verify if the remote host has been compromised, and reinstall the system if necessary.</p>		
<b>Output</b> <pre>Nessus was able to execute the command "id" using the following request :  This produced the following truncated output (limited to 10 lines) : ----- snip ----- root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root) root@metasploitable:/# ----- snip -----</pre>		
To see debug logs, please visit individual host		
Port ▲	Hosts	
1524 / tcp / wild_shell	192.168.50.101 	

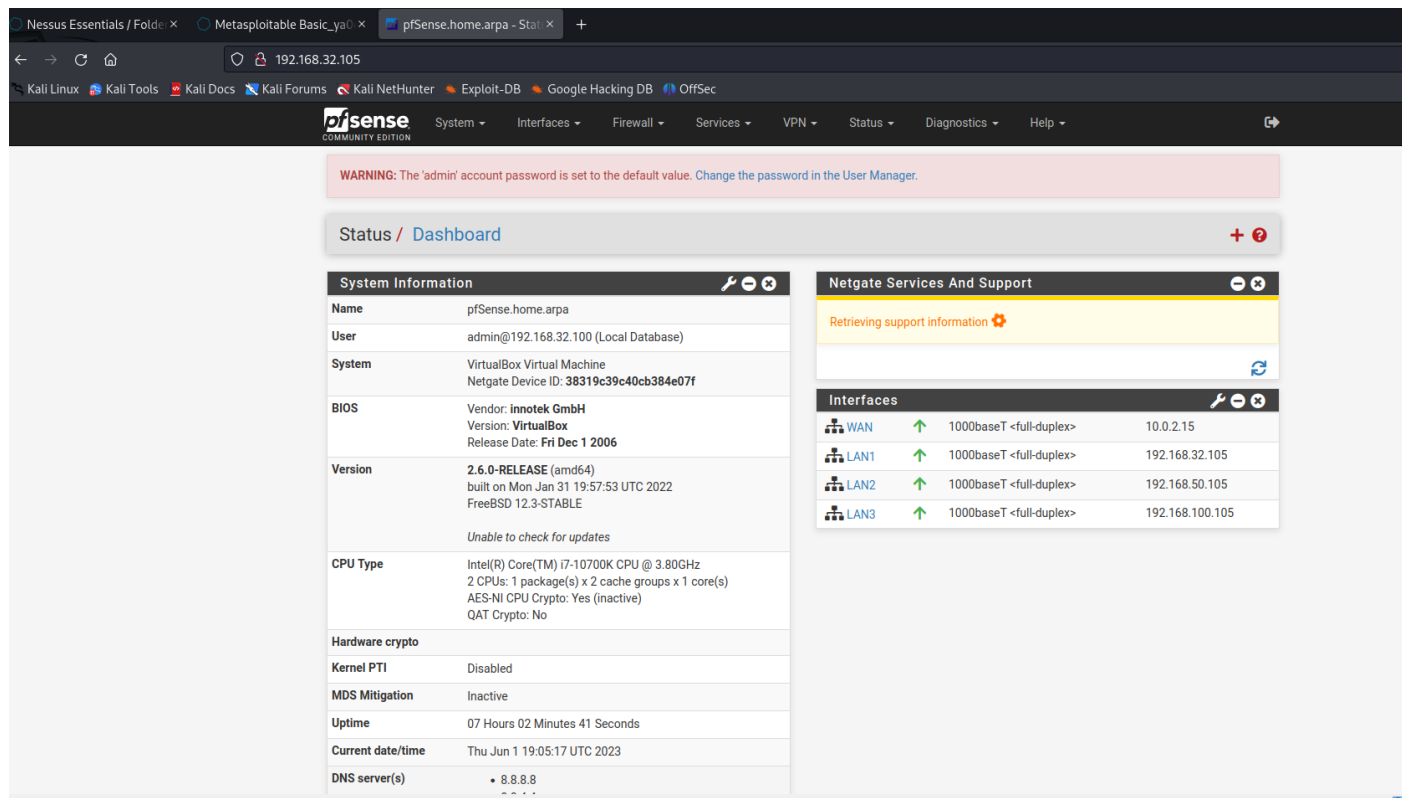
La porta rilevata aperta era la: 1524;

Effettuai il comando “nmap -sV -p 1524 192.168.50.101” per controllare la versione e se fosse aperta codesta porta, come vediamo, la porta era aperta:

```
(kali㉿kali)-[//]
$ nmap -sV -p 1524 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 13:13 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0047s latency).
PORT      STATE SERVICE      VERSION
1524/tcp  open  bindshell    Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

Utilizzo Pfsense come Firewall per bloccare l'accesso e l'uscita di pacchetti da quella determinata porta



Setto il blocco su “Action”, determino il protocollo “TCP”, la Destination, precisamente la porta 1524 per l’IP di Metasploitable (192.168.50.101);  
Salvo la configurazione.

192.168.32.105/firewall\_rules\_edit.php?id=0

### Edit Firewall Rule

**Action** Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** LAN1  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which IP protocol this rule should match.

### Source

**Source** ☐ Invert match any Source Address /

[Display Advanced](#)

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

### Destination

**Destination** ☐ Invert match Single host or alias 192.168.50.101 /

**Destination Port Range** (other) 1524 (other) 1524  
From Custom To Custom

Specify the destination port or port range for this rule. The “To” field may be left empty if only filtering a single port.

Eseguo di nuovo il comando “nmap -sV -p 1524 192.168.50.101” per verificare se la configurazione sia andata a buon fine:

```
(kali㉿kali)-[/]
$ nmap -sV -p 1524 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 13:18 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0071s latency).

PORT      STATE      SERVICE      VERSION
1524/tcp   filtered  ingreslock

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

Da come vediamo, ho settato bene il firewall di PfSense, da ora, la porta 1524 è filtrata.

**VNC Server “password” Password:** la password settata sul Server VNC era molto debole, dunque per risolvere questa criticità ho tolto l’accesso a quel Server, trovando la directory in cui c’era il file di configurazione della password, effettuando un `ls -A`, per trovare file nascosti, venni a trovarlo nella directory “.vnc”, dopodichè l’ho rimosso con il comando: “`rm passwd`”

Metasploitable Basic Scan / Plugin #61708

[Back to Vulnerabilities](#)

Vulnerabilities 92

CRITICAL VNC Server 'password' 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.

**Output**

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

```
msfadmin@metasploitable:/$ ls
bin    dev    initrd    lost+found    nohup.out    root    sys    var
boot   etc    initrd.img  media        opt          sbin    tmp    vmlinuz
cdrom  home  lib       mnt          proc         srv     usr

msfadmin@metasploitable:/$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/# cd / root
root@metasploitable:/# ls
bin    dev    initrd    lost+found    nohup.out    root    sys    var
boot   etc    initrd.img  media        opt          sbin    tmp    vmlinuz
cdrom  home  lib       mnt          proc         srv     usr

root@metasploitable:/# cd root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log  metasploitable:1.log  passwd
metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/.vnc# rm passwd
root@metasploitable:~/.vnc# ls
metasploitable:0.log  metasploitable:1.log  xstartup
metasploitable:0.pid  metasploitable:2.log
root@metasploitable:~/.vnc# _
```

**rexecd Service Detection:** Ho disabilitato il servizio rexecd per prevenire possibili attacchi e accessi non autorizzati.

#### 10203 - rexecd Service Detection

##### Synopsis

The rexecd service is running on the remote host.

##### Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.

However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

##### Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

##### Risk Factor

Critical

##### VPR Score

6.7

##### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

##### References

CVE CVE-1999-0618

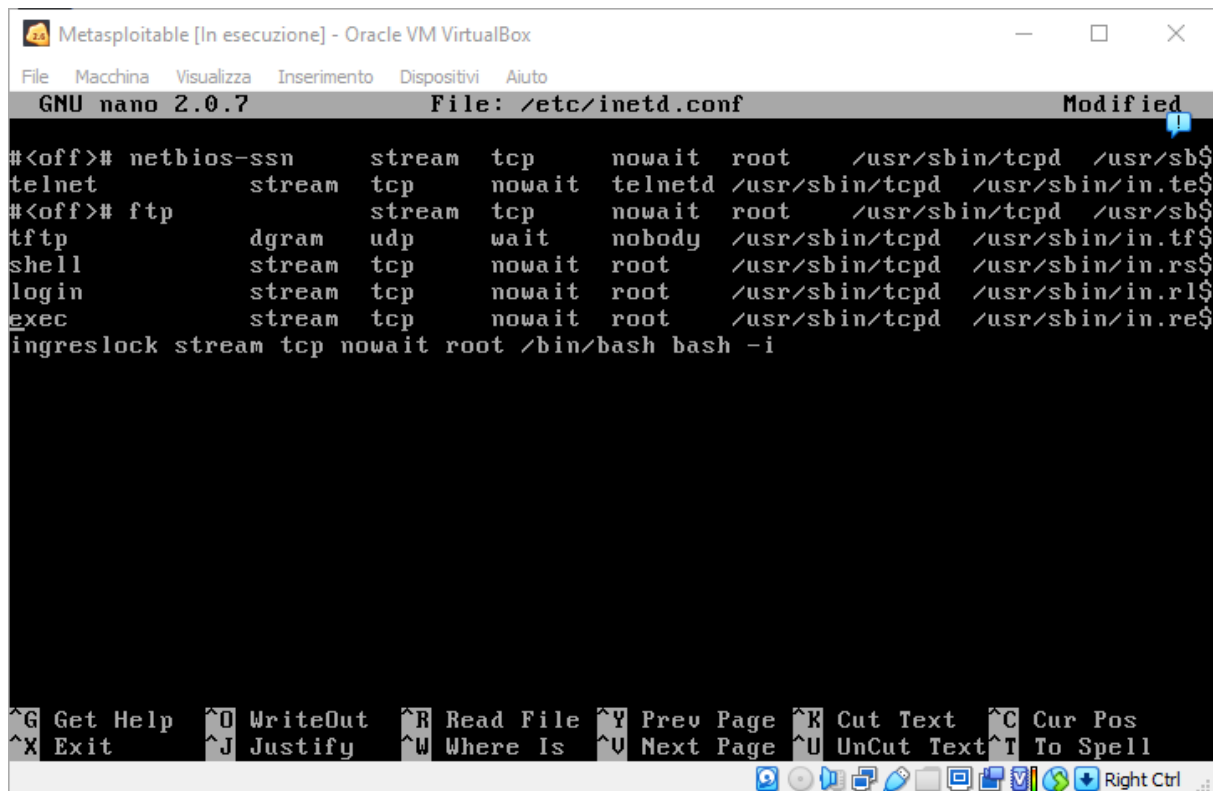
##### Plugin Information

Published: 1999/08/31, Modified: 2018/08/13

##### Plugin Output

tcp/512/rexecd

Disabilitando la linea "exec" in /etc/inetd.conf



Metasploitable [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

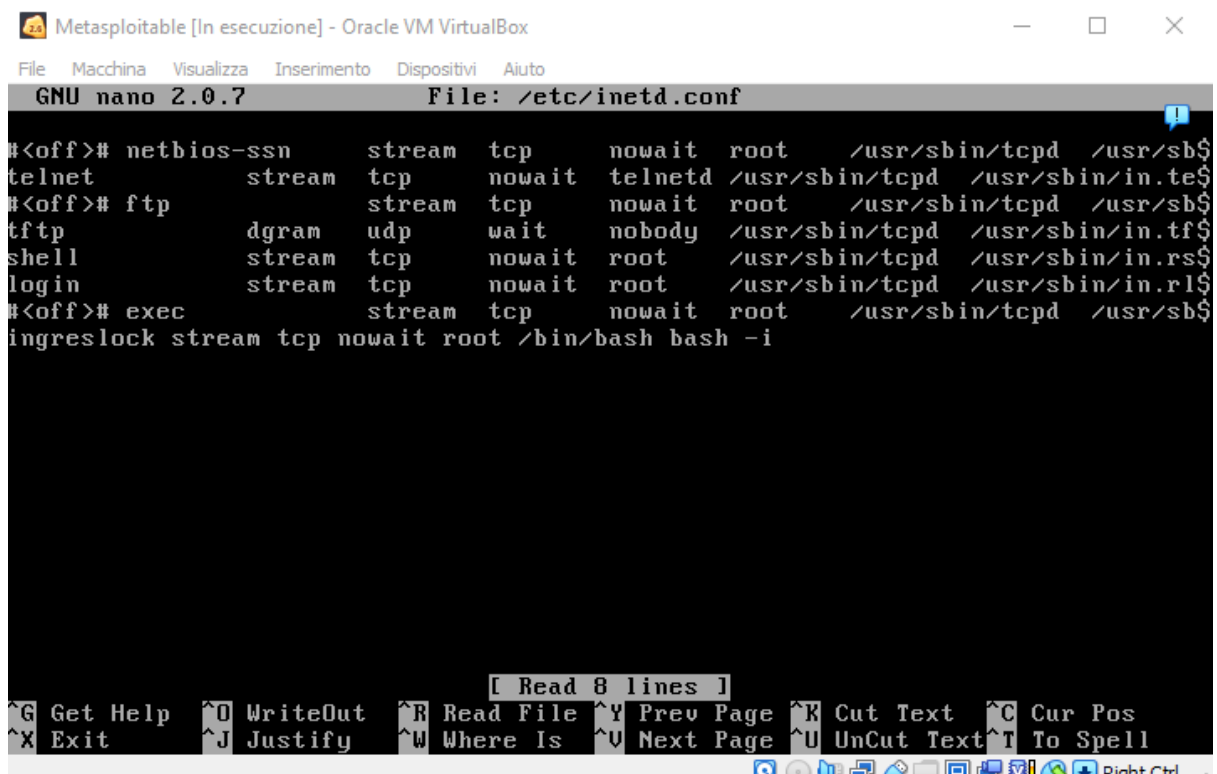
GNU nano 2.0.7 File: /etc/inetd.conf Modified

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
telnet      stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/inetd.$
#<off># ftp          stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
tftp        dgram   udp      wait     nobody  /usr/sbin/tcpd  /usr/sbin/inetd.$
shell       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
login       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
exec        stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
ingreslock  stream  tcp      nowait  root    /bin/bash bash -i
```

^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

Right Ctrl

Da come vediamo, metto: “#<off>#” accanto ad “exec”:



Metasploitable [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: /etc/inetd.conf

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
telnet      stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/inetd.$
#<off># ftp          stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
tftp        dgram   udp      wait     nobody  /usr/sbin/tcpd  /usr/sbin/inetd.$
shell       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
login       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
#<off># exec        stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/inetd.$
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

Right Ctrl

## Unix Operating System Unsupported Version Detection:

Dobbiamo scaricare l'ISO da <https://wiki.ubuntu.com/Releases> con la versione aggiornata, immettere l'ISO nella nuova macchina virtuale e la criticità sarà risolta.

Metasploitable Scan Dopo / Plugin #33850

[← Back to Vulnerabilities](#)

Vulnerabilities 55

**CRITICAL** Unix Operating System Unsupported Version Detection

**Description**

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

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

**Solution**

Upgrade to a version of the Unix operating system that is currently supported.

**Output**

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.50.101 <a href="#">🔗</a>

## Apache Tomcat Web Server: disabilitato tale servizio;

Metasploitable Scan Dopo / Plugin #171340

[← Back to Vulnerability Group](#)

Hosts 1 Vulnerabilities 55 Remediations 2 Notes 3 History 1

**CRITICAL** Apache Tomcat Web Server SEoL (<= 5.5.x)

**Description**

According to its version, the Apache Tomcat web server is 5.5.x or earlier. It is, therefore, 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**

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

**See Also**

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



Mi collego con “telnet” da Kali a Metasploitable, per avere una visione migliore

[illegible]

Cerco dove si trova tomcat:

Lo trovo su “cd /etc/init.d” denominato “tomcat5.5”

```

msfadmin@metasploitstable:/etc$ cd init
init.d/          initramfs-tools/
msfadmin@metasploitstable:/etc$ cd init.d
msfadmin@metasploitstable:/etc/init.d$ ls
apache2          keyboard-setup    pcmciautils      ssh
apparmor          killprocs         portmap          stop-bootlogd
atd              klogd            postfix         stop-bootlogd-single
bind9            loopback         postgresql-8.3   syslogd
bootclean        module-init-tools pppd-dns        tomcat5.5
bootlogd         mountall-bootclean.sh procps          udev
bootmisc.sh      mountall.sh      proftpd         udev-finish
checkfs.sh       mountdevsubfs.sh rc              ufw
checkroot.sh     mountkernfs.sh   rc.local        umountfs
console-screen.sh mountnfs-bootclean.sh rcS            umountnfs.sh
console-setup    mountoverflowtmp README          umountroot
cron            mtab.sh         reboot         urandom
distcc          mysql           rmnologin      waitnfs.sh
dns-clean       mysql-ndb       rsync          wpa-ifupdown
glibc.sh        mysql-ndb-mgm  samba         x11-common
halt            networking     screen-cleanup xinetd
hostname.sh     nfs-common     sendsigs       xserver-xorg-input-wacom
hwclockfirst.sh nfs-kernel-server single
hwclock.sh      openbsd-inetd  skeleton
msfadmin@metasploitstable:/etc/init.d$
-----
cron.daily      idmapd.conf    opt            su-to-rootrc
cron.hourly    inetd.conf     pam.conf       sysctl.conf
cron.monthly   init.d         pam.d         syslog.conf
crontab        initramfs-tools pango         terminfo
cron.weekly    inputrc       passwd        timezone
cups           iproute2      passwd-       tomcat5.5
debconf.conf   issue         pcmcia        ucf.conf
debian_version issue.net      perl          udev
default        java          php5          ufw
defoma         jvm           popularity-contest.conf unreal
deluser.conf   jvm.d         postfix       updatedb.conf
depmod.d       kernel-img.conf postgresql     update-manager

```

Per risolvere codesta vulnerabilità, disabilitiamo il servizio di Tomcat con “sudo /etc/init.d/tomcat5.5 stop”:

```
msfadmin@metasploitable:/etc/init.d$ sudo /etc/init.d/tomcat5.5 stop
[sudo] password for msfadmin:
* Stopping Tomcat servlet engine tomcat5.5
... done.
```

Disattivando il servizio di Tomcat risolviamo anche altre vulnerabilità, come:  
Non abbiamo più la necessità di aggiornare il tomcat server alla versione più recente.

#### **CRITICAL** Apache Tomcat AJP Connector Request Injection (Ghostcat)

##### **Description**

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

##### **Solution**

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

##### **See Also**

<http://www.nessus.org/u?8e6246>  
<http://www.nessus.org/u?4e287adb>  
<http://www.nessus.org/u?cbc3d54e>  
<https://access.redhat.com/security/cve/CVE-2020-1745>  
<https://access.redhat.com/solutions/4851251>  
<http://www.nessus.org/u?dd218234>  
<http://www.nessus.org/u?dd772531>  
<http://www.nessus.org/u?2a01d6bf>  
<http://www.nessus.org/u?3b5af27e>  
<http://www.nessus.org/u?9dab109f>  
<http://www.nessus.org/u?5eafc70>

## Debian OpenSSH/OpenSSL Package (Anche OpenVPN): ho risolto l'OpenSSH;

Metasploitable Scan Dopo / Plugin #32321

[← Back to Vulnerability Group](#)

Hosts 1

Vulnerabilities 55

Remediations 2

Notes 3

History 1

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

**Description**

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

**Solution**

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

**See Also**

<http://www.nessus.org/u?107f9bdc>  
<http://www.nessus.org/u?f14f4224>

Accedo a Metasploitable tramite la console della macchina virtuale.

Verifico la presenza di chiavi SSH nella directory ~/.ssh

Sono presenti file come id\_rsa e id\_rsa.pub, che sono le chiavi SSH.

```
msfadmin@metasploitable:~$ ls ~/.ssh
authorized_keys  id_rsa  id_rsa.pub
msfadmin@metasploitable:~$ rm ~/.ssh/id_rsa*
msfadmin@metasploitable:~$ ls ~/.ssh
authorized_keys
```

Le elimino con ~/.ssh/id\_rsa\* (con il jolly comprendo tutti i simili)

Creo nuove key

```
msfadmin@metasploitable:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/msfadmin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/msfadmin/.ssh/id_rsa.
Your public key has been saved in /home/msfadmin/.ssh/id_rsa.pub.
The key fingerprint is:
6c:48:af:84:ab:84:d4:2b:40:86:e0:bd:a1:db:bd:19 msfadmin@metasploitable
```