



Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Svolgimento :

Architettura :

PfSense : 10.x.y.z scheda di rete in NAT

192.168.1.1 scheda di rete gateway per la macchina kali

192.168.2.1 scheda di rete gateway per la macchina meta

Kali : scheda di rete interna 192.168.1.100

Meta : scheda di rete interna 192.168.2.199

Partendo dal report della volta precedente prendiamo in esame le seguenti vulnerabilità, per le quali proponiamo una soluzione ai fini di migliorare la sicurezza del ns target.

CRITICAL

10.0*

-

61708

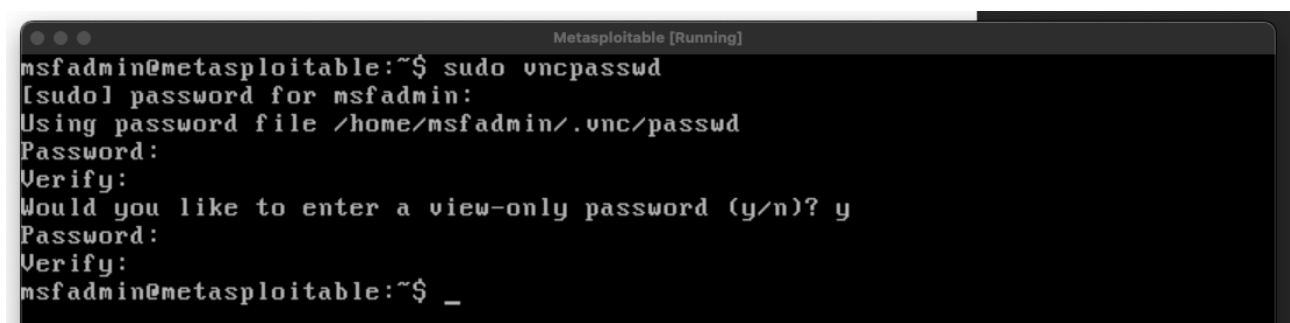
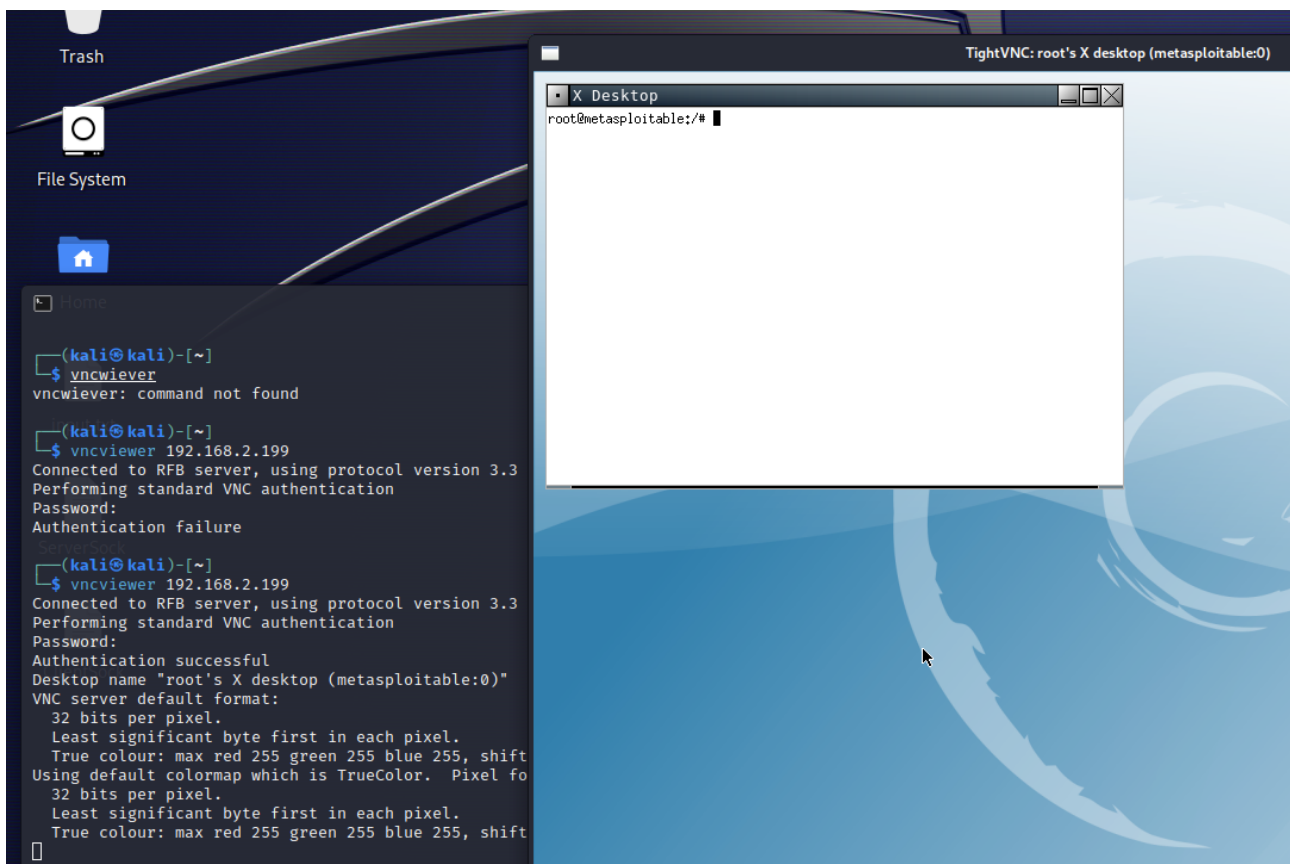
VNC Server 'password' Password

Per questa vulnerabilità collegandoci dal terminale della ns macchina Kali Linux e facendo il comando `vncviewer <ip target>` possiamo accedere al server vnc utilizzando la password `<password >`.

Per sistemare questa vulnerabilità dalla macchina meta eseguiamo il comando `vncpasswd` ed abbiamo a proporre una password più sicura.

Nel primo screen si vede il fallimento dell'autenticazione utilizzando la precedente password e l'autenticazione con successo utilizzando quella nuova.

Nel secondo screen si vede il cambio password dalla macchina meta.



CRITICAL

10.0*

5.9

11356

NFS Exported Share Information Disclosure

Per la risoluzione di questa vulnerabilità si parte dal link contenuto all'interno del report

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.

Atterrando su questa pagina si può copiare e “googlare” la solutions

Solution

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

Il primo risultato restituito da google contiene all'interno il percorso del file che dobbiamo editare per andare a correggere questa vulnerabilità sulla macchina meta



LinuxQuestions.org

<https://www.linuxquestions.org> > ... · [Traduci questa pagina](#) ⋮

How To Make NFS Share only accessible to specific ...

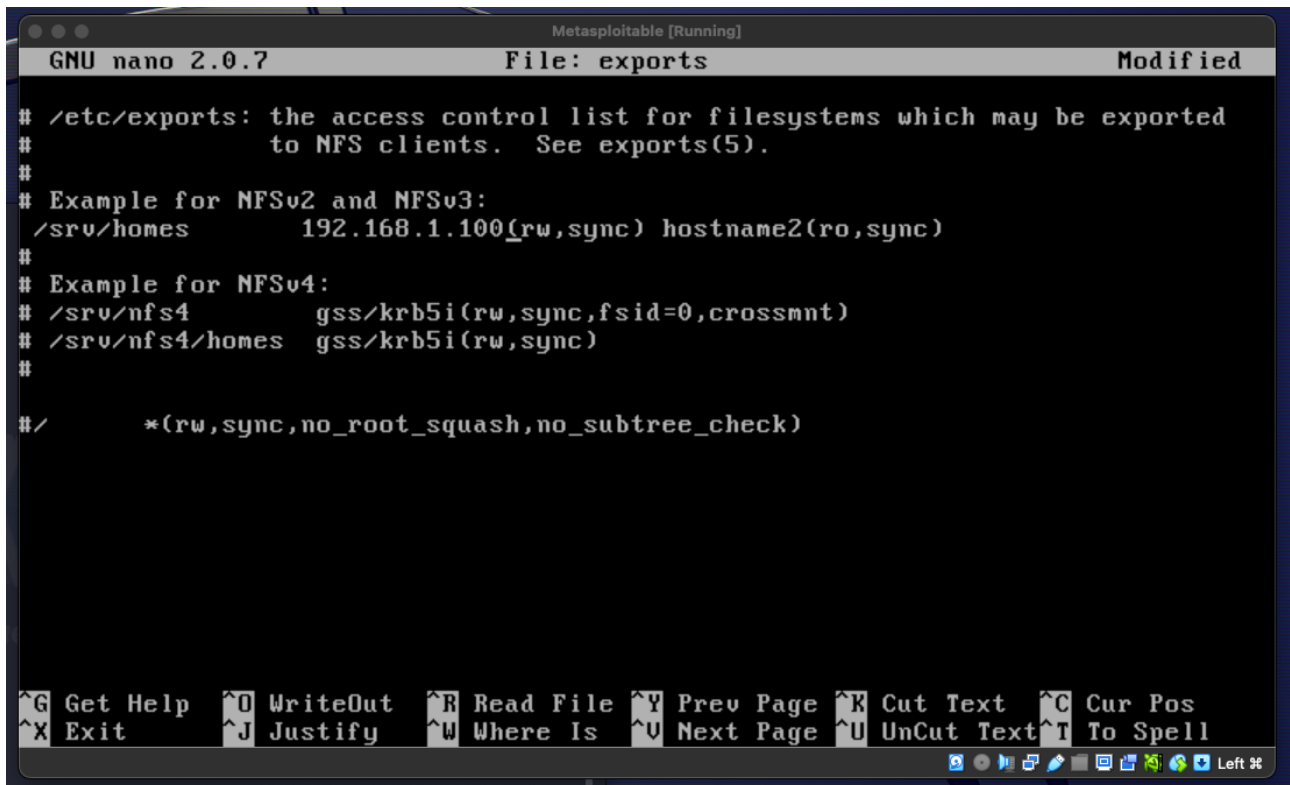
27 ago 2015 — **Configure NFS on the remote host so that only authorized hosts can mount its remote shares.** Any help is really appreciated. Thanks in ...

The file /etc/exports on the NFS server controls this. If you type "man exports" you should see documentation on how to configure this file.

La modifica di questa file arriva direttamente dagli esempi in esso contenuti.

Si commenta l'ultima riga che contiene l'asterisco dove tutto è consentito e viene decommentata la riga che presenta come esempio l'hostname.

Inseriamo come indirizzo quello della ns macchina Kali.



```
GNU nano 2.0.7 File: 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 192.168.1.100(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)
```

CRITICAL

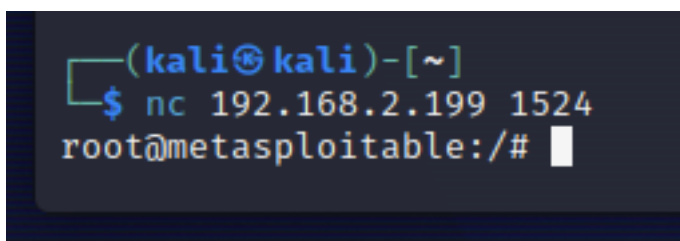
9.8

-

51988

Bind Shell Backdoor Detection

In questa vulnerabilità collegandoci con una netcat alla porta 1524 della macchina meta otteniamo una connessione root senza che ci venga chiesta l'autenticazione.



```
(kali@kali)-[~]
$ nc 192.168.2.199 1524
root@metasploitable:/#
```

Per fixare questo problema è stata utile la documentazione di "ufficiale" di metasploitable 2 che accanto alla porta 1524 parla di ingreslock



Rapid7

<https://docs.rapid7.com/metasploit> · [Traduci questa pagina](#) · [...](#)

Metasploitable 2 Exploitability Guide

The following command line will scan all TCP ports on the **Metasploitable 2** instance: ... port 1524. The ingreslock port was a popular choice a decade ago for ...

[Services](#) · [Unix Basics](#) · [Backdoors](#) · [Unintentional Backdoors](#)

```
1 root@ubuntu:~# nmap -p0-65535 192.168.99.131
2
3 Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-31 21:14 PDT
4 Nmap scan report for 192.168.99.131
5 Host is up (0.00028s latency).
6 Not shown: 65506 closed ports
7 PORT      STATE SERVICE
8 21/tcp    open  ftp
9 22/tcp    open  ssh
10 23/tcp    open  telnet
11 25/tcp    open  smtp
12 53/tcp    open  domain
13 80/tcp    open  http
14 111/tcp   open  rpcbind
15 139/tcp   open  netbios-ssn
16 445/tcp   open  microsoft-ds
17 512/tcp   open  exec
18 513/tcp   open  login
19 514/tcp   open  shell
20 1099/tcp  open  rmiregistry
21 1524/tcp  open  ingreslock
22 2049/tcp  open  nfs
23 2121/tcp  open  ccproxy-ftp
24 3306/tcp  open  mysql
25 3632/tcp  open  distccd
26 5432/tcp  open  postgresql
27 5900/tcp  open  vnc
28 6000/tcp  open  X11
29 6667/tcp  open  irc
30 6697/tcp  open  unknown
31 8009/tcp  open  ajp13
32 8180/tcp  open  unknown
33 8787/tcp  open  unknown
34 39292/tcp open  unknown
35 43729/tcp open  unknown
36 44813/tcp open  unknown
37 55852/tcp open  unknown
38 MAC Address: 00:0C:29:9A:52:C1 (VMware)
```

Cercando info su ingreslock si trova questa risorsa su youtube

<https://www.youtube.com/watch?v=FuwWjWt75dM>

Dove viene editato il file inetd.conf

Utilizzando l'editor di testo nano andiamo a commentare l'ultima riga del file in modo da chiudere la porta e la vulnerabilità.

Una seconda soluzione poteva essere la chiusura della porta dal firewall.

```
msfadmin@metasploitable:/$ cat /etc/inetd.conf
#<off># netbios-ssn      stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
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/sbin/
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:/$
```

L'ultima riga del file è ora commentata e non consente più la connessione sulla porta 1524

```
(kali@kali)-[~]
$ nc 192.168.2.199 1524
(UNKNOWN) [192.168.2.199] 1524 (ingreslock) : Connection refused
```

CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
----------	-----	---	--------	--

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

Queste due vulnerabilità riguardano la versione troppo datata di Apache Tomcat

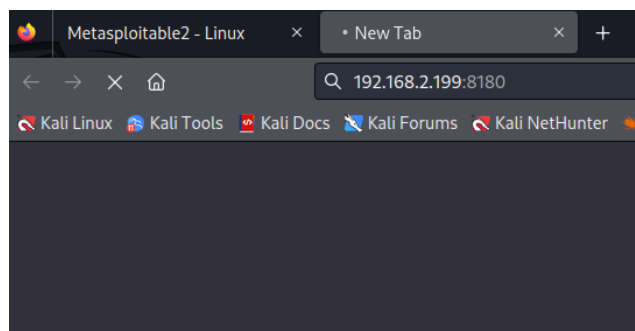
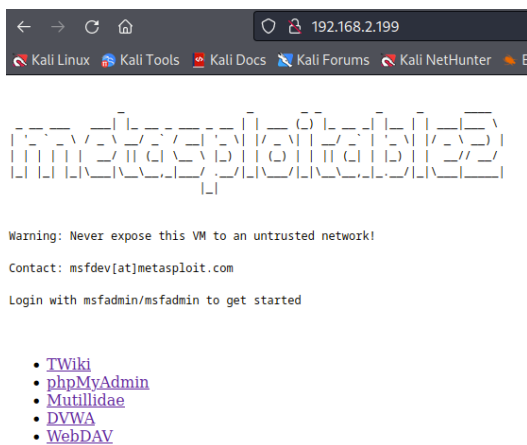
Per raggiungere il servizio partiamo con l'avvio del server apache2 su meta

```
msfadmin@metasploitable:/$ sudo /etc/init.d/apache2 restart
[sudo] password for msfadmin:
* Restarting web server apache2                                [ OK ]
msfadmin@metasploitable:/$ sudo /etc/init.d/apache2 start
* Starting web server apache2
httpd (pid 5279) already running                                [ OK ]
msfadmin@metasploitable:/$ _
```

Ora raggiungiamo il servizio partendo dalla macchina Kali e dal browser web digitiamo ip meta porta 8180



**** Il servizio Tomcat viene bloccato dalla regola firewall ma la vulnerabilità rimane nel report ****



** Le versioni SSLv2 e SSLv3 vengono disabilitate nel file ssl.conf ma la vulnerabilità permane **

```
Metasploitable [Running]
GNU nano 2.0.7 File: 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 -SSLv2 -SSLv3_

</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
```