Progetto Modulo M3 – Maria Ludovica Tartaglia

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.

Svolgimento:

Come prima cosa, effettuiamo una scansione attraverso il software Nessus per ricercare tutte le vulnerabilità presenti nella macchina. Scarichiamo poi il report che viene generato a scansione effettuata, e controlliamo le vulnerabilità riscontrate. Come segnala lo screenshot successivo, scelgo tre vulnerabilità critiche da risolvere:

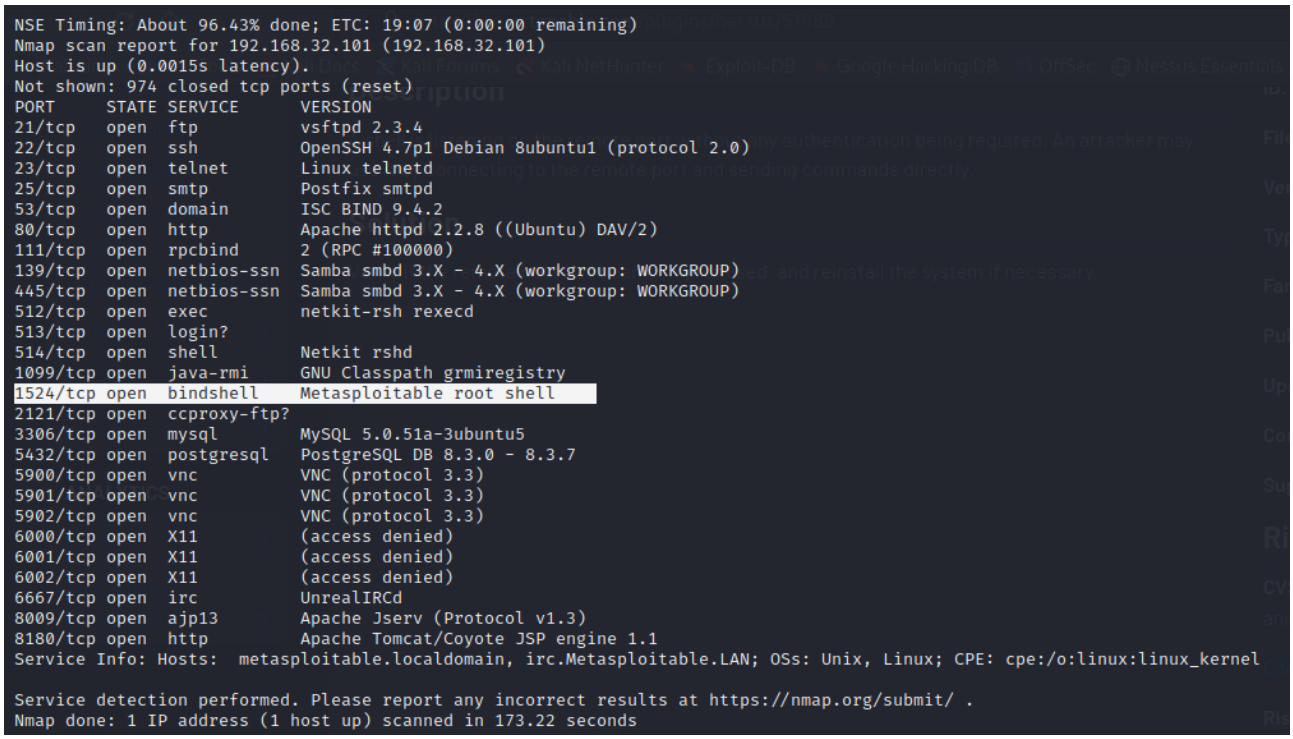
Vulnerabilities — Total: 102

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

- *Bind Shell Backdoor Detection*

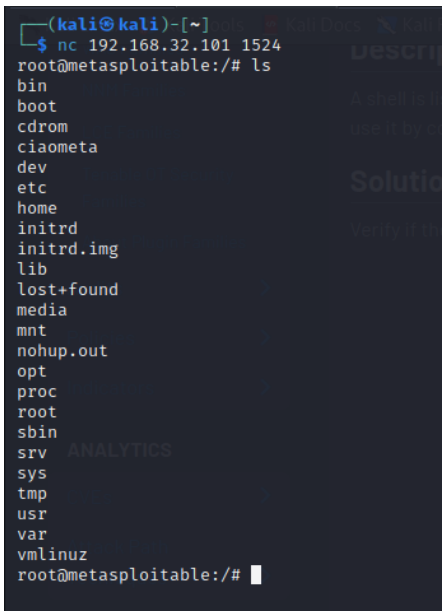
Come ci suggerisce la descrizione, una shell si trova in listening sulla porta senza che sia necessario richiedere alcuna autenticazione. Per risolvere la problematica, si può creare una regola firewall che impedisca l'accesso alla porta in questione.

Per prima cosa, verifichiamo attraverso una scansione Nmap sulla macchina Kali quali siano le porte aperte presenti sulla macchina Metasploitable. Lanciamo sul terminale di Kali il comando **sudo nmap -sV 192.168.32.101 -p-**, che ci riporterà quanto segue:



```
NSE Timing: About 96.43% done; ETC: 19:07 (0:00:00 remaining)
Nmap scan report for 192.168.32.101 (192.168.32.101)
Host is up (0.0015s latency).
Not shown: 974 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
2121/tcp open  ccproxy-ftp?
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)
5901/tcp open  vnc          VNC (protocol 3.3)
5902/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6001/tcp open  X11          (access denied)
6002/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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; 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 173.22 seconds
```

Vediamo che il servizio Bind shell si trova sulla porta 1524. Con il comando **netcat 192.168.32.101 1524** lanciato su Kali, effettuiamo una scansione sulla porta come nello screen seguente, dimostrando di poter accedere alla porta senza problemi:



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.32.101 1524
root@metasploitable:/# ls
bin
boot
cdrom
ciaometa
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

Andiamo quindi ad impostare una regola su Metasploitable utilizzando il software Iptables, che ci permetterà di configurare un firewall per impedire l'accesso alla porta 1524. Scriveremo quindi la stringa **iptables -I INPUT -p tcp –dport 1524 -j DROP** come mostrato nello screen che segue.

```
root@metasploitable:/# iptables -I INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/# _
```

Una volta impostata la regola, effettuiamo un controllo incrociato dalla macchina Kali, riutilizzando il comando netcat. Come mostrato in seguito, la porta risulta a questo punto inaccessibile.

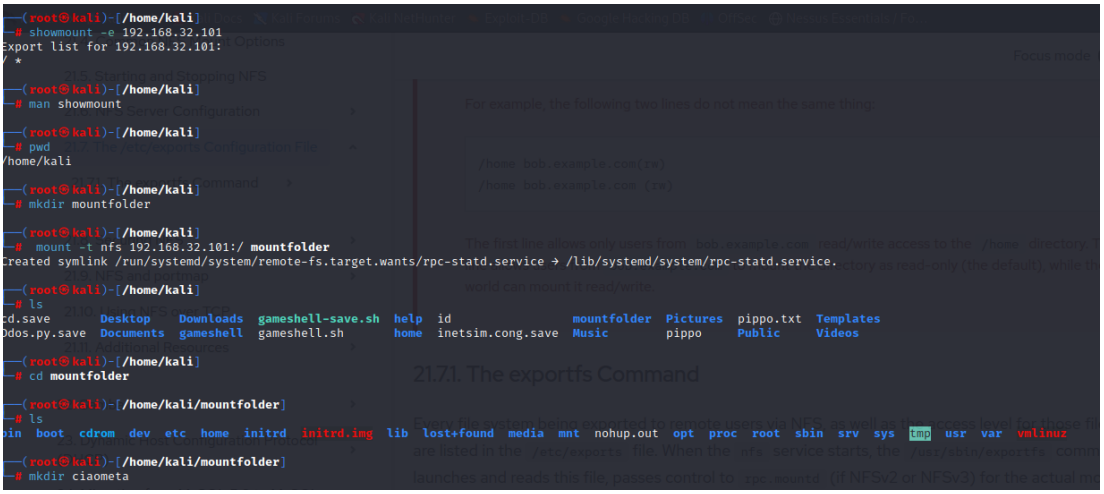
```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.32.101 1524
(UNKNOWN) [192.168.32.101] 1524 (ingreslock) : Connection timed out
```

- *NSF Exported Share Information Disclosure*

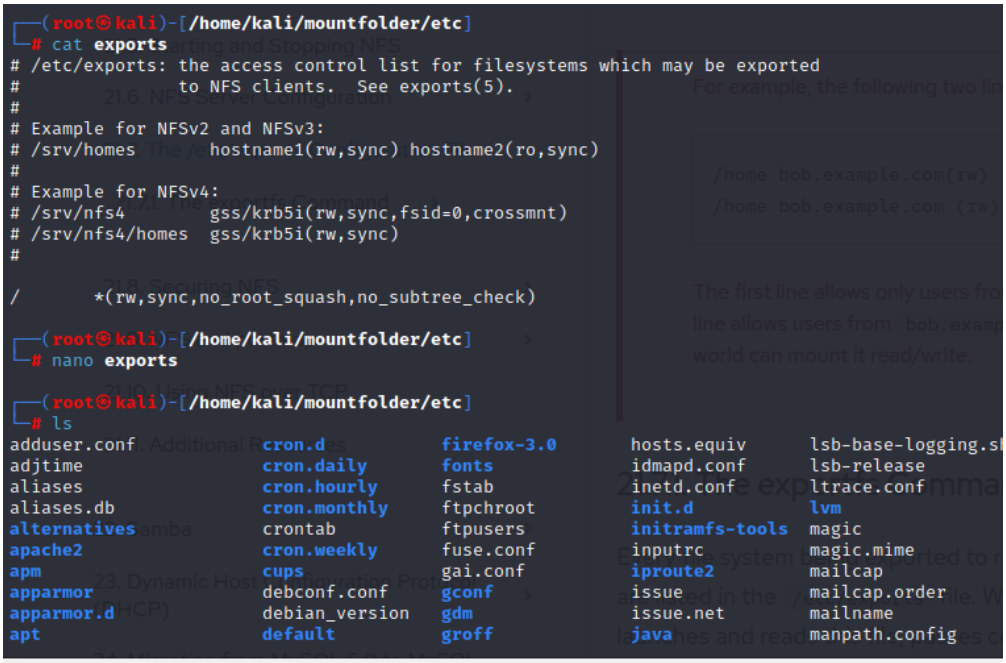
La seconda vulnerabilità che andiamo ad analizzare e risolvere è questa. Come da descrizione, notiamo che il problema si pone perché è possibile accedere ai file di NSF, e quindi un potenziale hacker potrebbe leggere, ed anche sovrascrivere, i file suddetti. In questo caso si deve pertanto stabilire che solo utenti autorizzati possano montare la cartella contenente i file in questione.
Per prima cosa andiamo con il comando **man exports** a leggere il manuale di funzionamento dei file NSF che è possibile esportare.

```
EXPORTS(5)                  Linux File Formats Manual                  EXPORTS(5)

NAME
       exports - NFS file systems being exported (for Kernel based NFS)

SYNOPSIS
       /etc/exports

DESCRIPTION
       The  file  /etc/exports serves as the access control list for file sys-
       tems which may be exported to NFS clients.  It is used  by  exportfs(8)
       to  give  information  to  mountd(8)  and  to the kernel based NFS file
       server daemon nfsd(8).

       The file format is similar to the SunOS exports file.  Each  line  con-
       tains  an  export  point  and  a  whitespace-separated  list of clients
       allowed to mount the file system at that point. Each listed client  may
       be  immediately  followed  by  a parenthesized, comma-separated list of
       export options for that client. No whitespace is  permitted  between  a
       client and its option list.

       Also, each line may have one or more specifications for default options
       after the path name, in the form of a dash ("-") followed by an  option
       list.  The  option list is used for all subsequent exports on that line
 Manual page exports(5) line 1
```

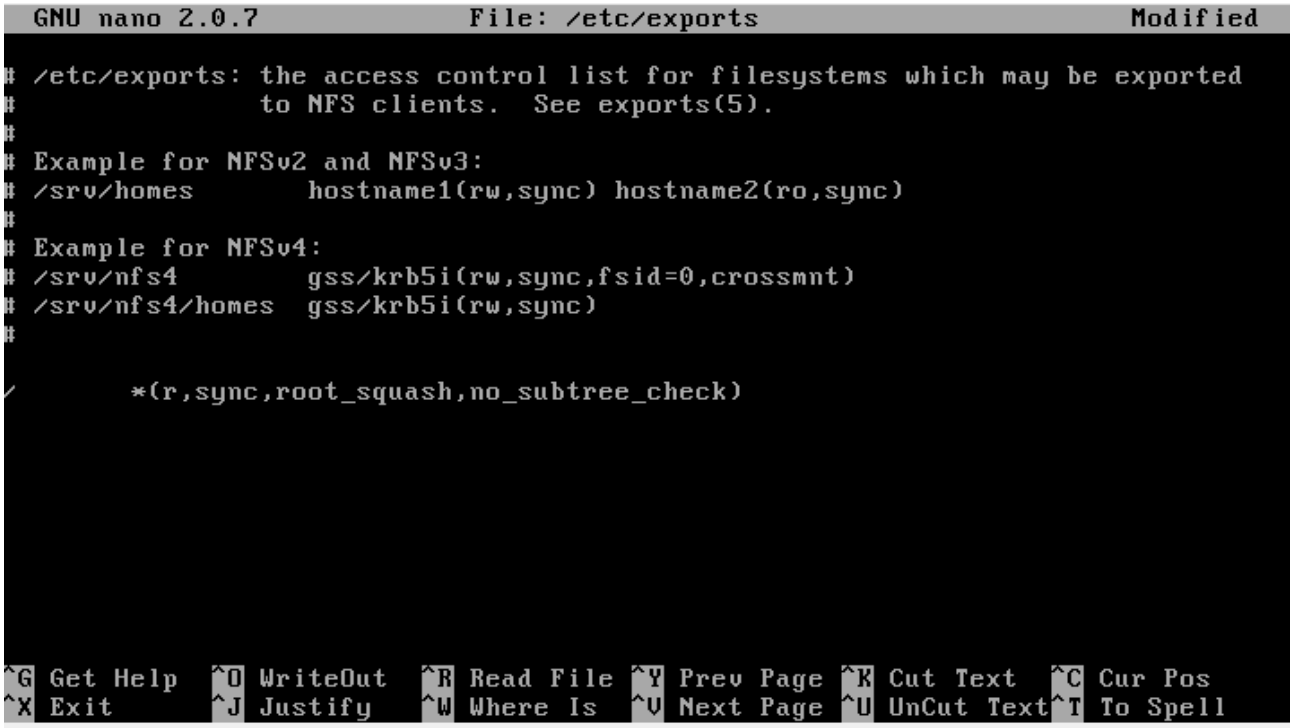
Dalla macchina Kali, lanciamo il comando **showmount -e 192.168.32.101** per vedere tutte le cartelle che sono montate su file e che vengono visualizzate. Proviamo poi a creare noi stessi una cartella all'interno del file:



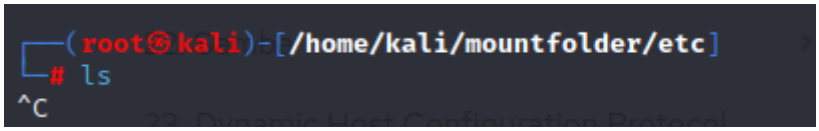
Spostandoci all'interno della cartella appena creata, nella sezione /etc, con il comando **cat exports** vediamo che tutti i file presenti all'interno possono essere sia letti che riscritti, come ci suggeriva la scansione effettuata.



Ci spostiamo sulla macchina Metasploitabile e con il comando **sudo nano /etc/exports** andiamo a modificare l'ultima riga come da screenshot seguente, di modo da eliminare la possibilità di accedere ai file



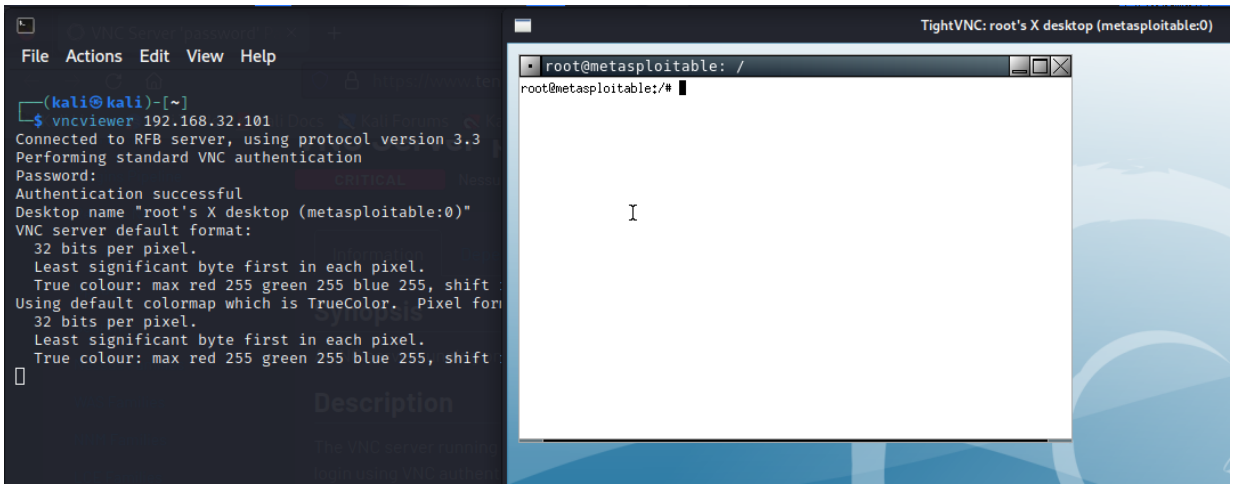
A questo punto, ritornando sulla macchina Kali, se proviamo ad accedere nuovamente ai file, scopriremo che il comando **ls** non restituirà nessuna possibilità di vedere i file all'interno:



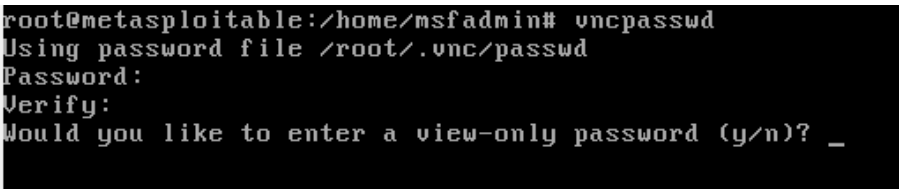
- *VNC Server 'password' Password*

In questa vulnerabilità vediamo come il server VCN abbia una password troppo debole, che permetterebbe facilmente l'accesso ad un utente non autorizzato, in grado poi di prendere il controllo del sistema.

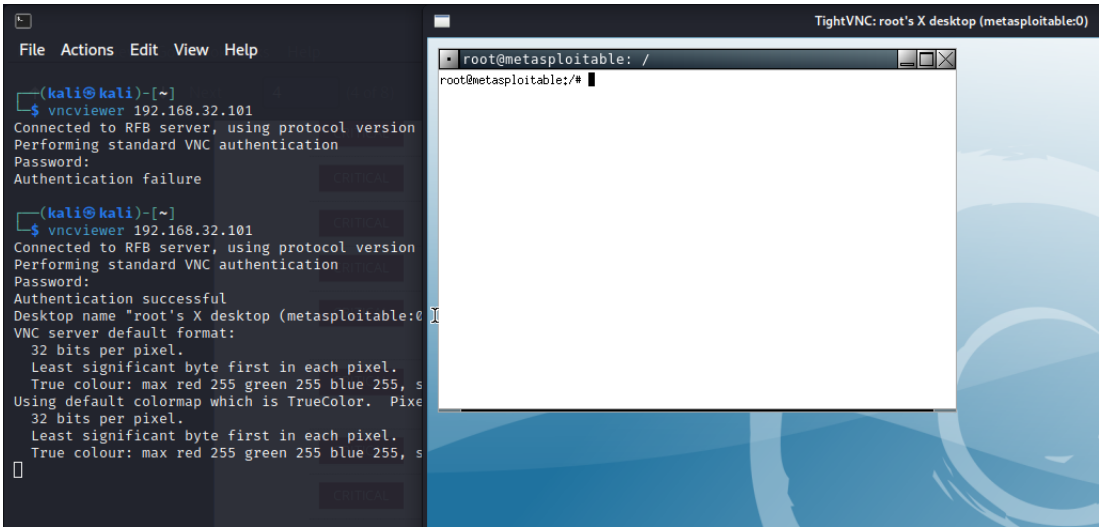
Per prima cosa andiamo ad operare in modalità root sulla macchina Metasploitable con il comando **sudo su**. Una volta effettuato ciò, sulla macchina Kali andiamo a lanciare **vncviewer 192.168.32.101**, che ci permetterà di accedere da remoto a Metasploitable. Inserendo la password "password" vediamo che ci viene permesso l'accesso al sistema senza problemi.



Torniamo su Metasploitable, e inserendo il comando **vncpasswd** cambiamo la password con una più sicura:



A questo punto, torniamo su Kali, rilanciamo nuovamente vncpasswd. Verifichiamo che tentando di inserire la vecchia password "password" il sistema rifiuterà l'accesso. Inserendo invece la nuova password più sicura, l'accesso sarà consentito:



Risoluzione e scansione di conferma:

A questo punto, abbiamo risolto tre vulnerabilità rilevate dal software Nessus.
Andiamo per correttezza e completezza, come richiesto, ad effettuare una nuova scansione con il tool suddetto, di modo da verificare la corretta risoluzione delle vulnerabilità.
Lo screenshot che segue lo va a dimostrare:

Vulnerabilities Total: 102

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

*Bonus track**

Nel controllare le vulnerabilità residue e quelle correttamente risolte, notiamo un fatto curioso: nell'esperire la remediation relativa alla vulnerabilità critica di NSF, notiamo che è stata risolta anche una seconda vulnerabilità, di severità alta, presente nella scansione effettuata prima dell'applicazione delle risoluzioni:

HIGH	7.5	-	42256	NFS Shares World Readable

Notiamo come, effettuata la seconda scansione, la vulnerabilità in questione non risulti più essere tra quelle individuate:

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	6.5	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