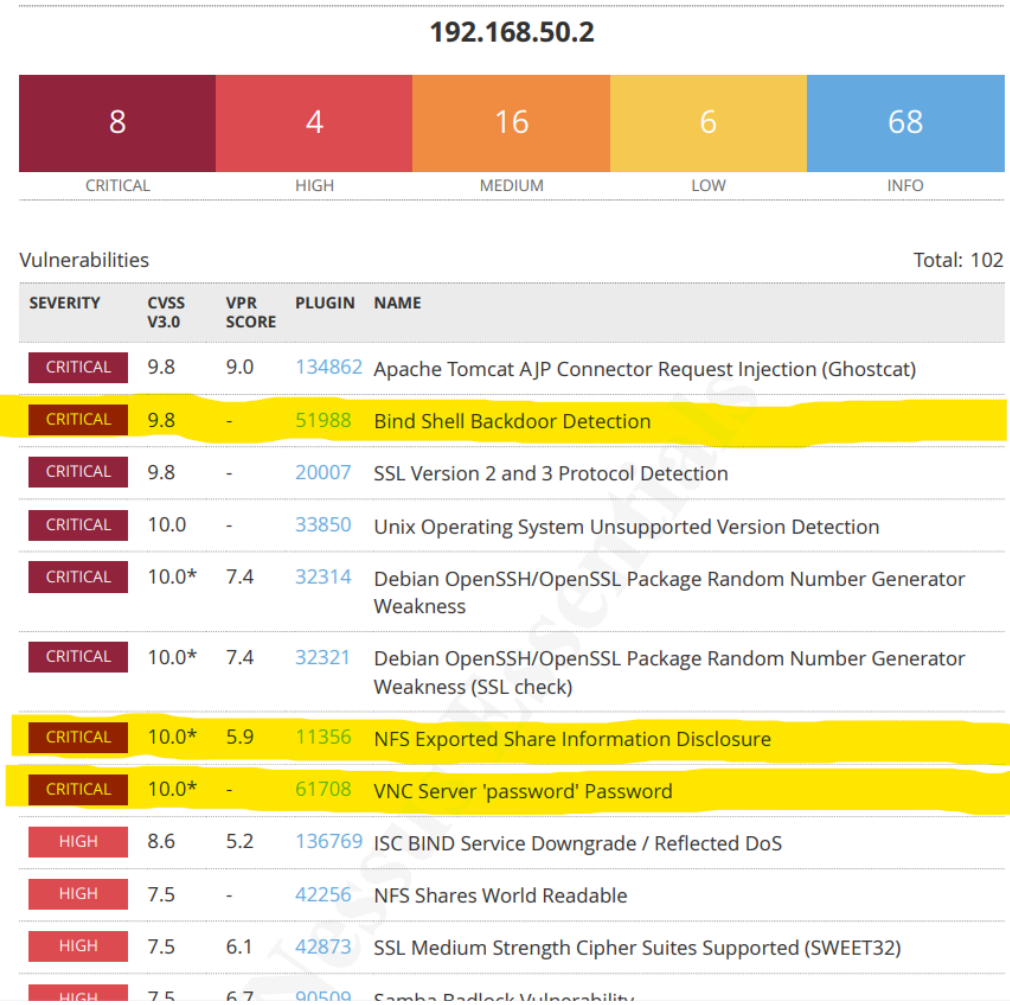
PROGETTO W12D4

Di Florin Eugen Peticaru

Il progetto di questo modulo ci richiede una scansione con il servizio **Nessus** sulla macchina di *Metasploitable* per rilevare e correggere eventuali vulnerabilità, per iniziare quindi avviamo una scansione di tipo basic e notiamo i seguenti errori (per comodità verranno mostrati solo gli errori critici dei quali saranno evidenziati quelli che proveremo a risolvere durante il progetto);



192.168.50.2

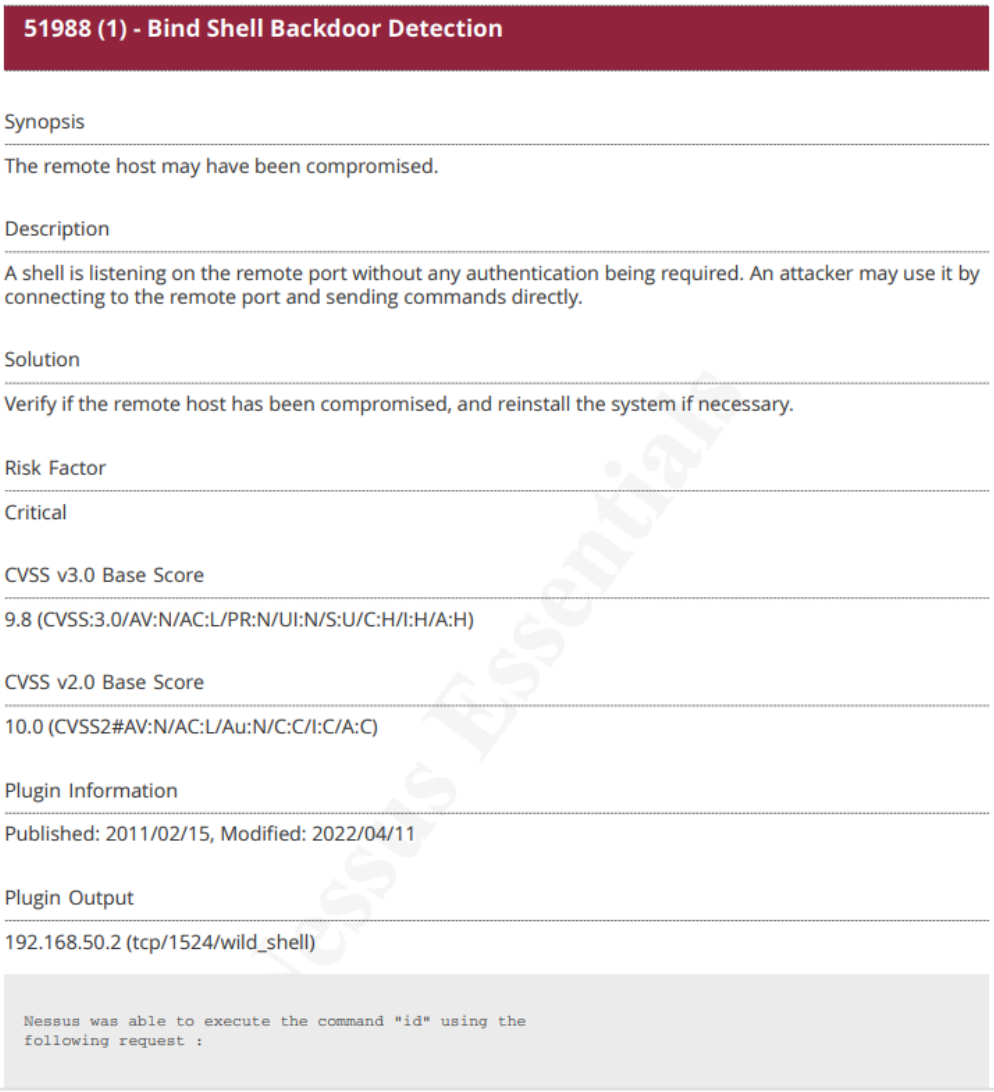
8	4	16	6	68
CRITICAL	HIGH	MEDIUM	LOW	INFO

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
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

Spiegazione vulnerabilità

Bind Shell Backdoor Detection



51988 (1) - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

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.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

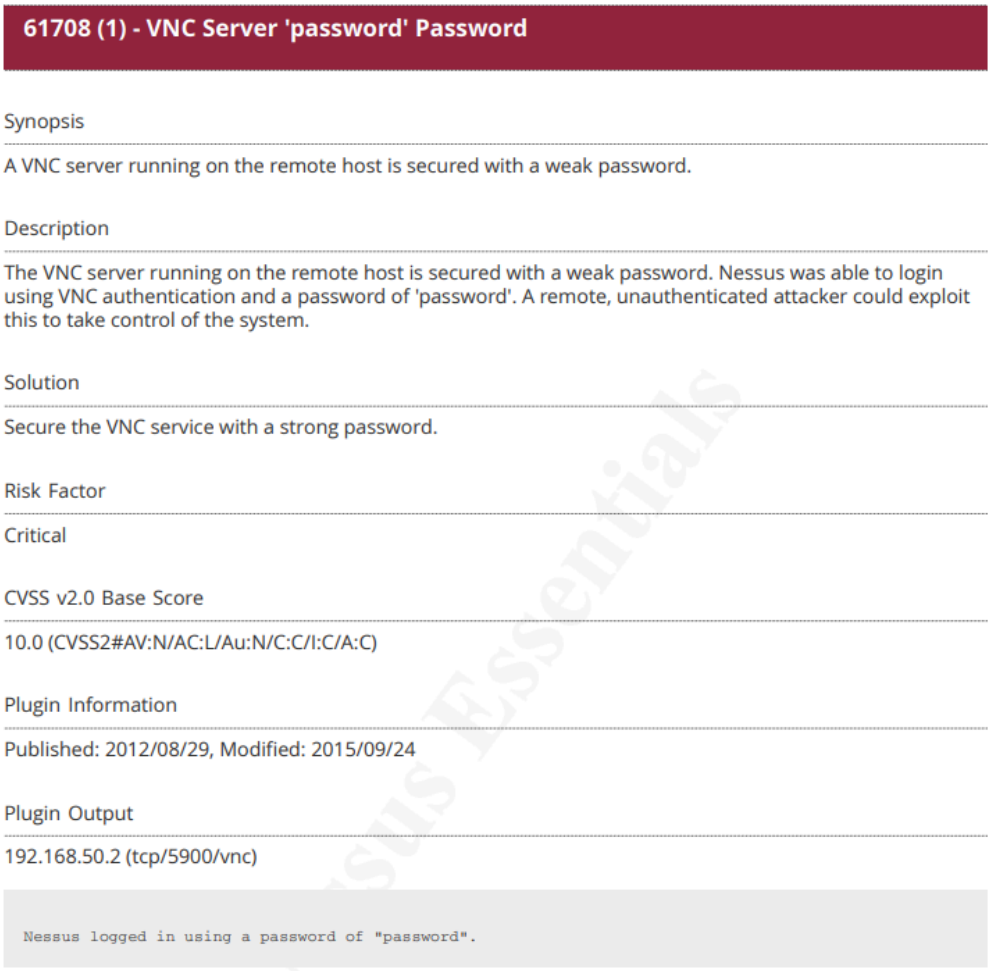
Plugin Output

192.168.50.2 (tcp/1524/wild_shell)

```
Nessus was able to execute the command "id" using the
following request :
```

Questa criticità ci attenziona sul fatto che una qualsiasi macchina remota potrebbe collegarsi a *Metasploitable* dato che è presente un *listener* in ascolto sulla porta **1524** che potrebbe portare a un rischio di collegamento senza necessità di autenticazione e conseguentemente dare la possibilità di modificare i file presenti sul sistema.

VNC Server password



61708 (1) - VNC Server 'password' Password

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.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

192.168.50.2 (tcp/5900/vnc)

```
Nessus logged in using a password of "password".
```


Questa criticità ci dice che il server *VNC* presente sulla macchina di *Metasploitable* è a rischio di exploit anche di tipo *brute force* poichè la password impostata è ancora quella di default cioè ***password*** quindi siamo a rischio di accesso e modifiche ai file di sistema.

NFS Exported share information disclosure

11356 (1) - NFS Exported Share Information Disclosure

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.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2023/08/30

Plugin Output

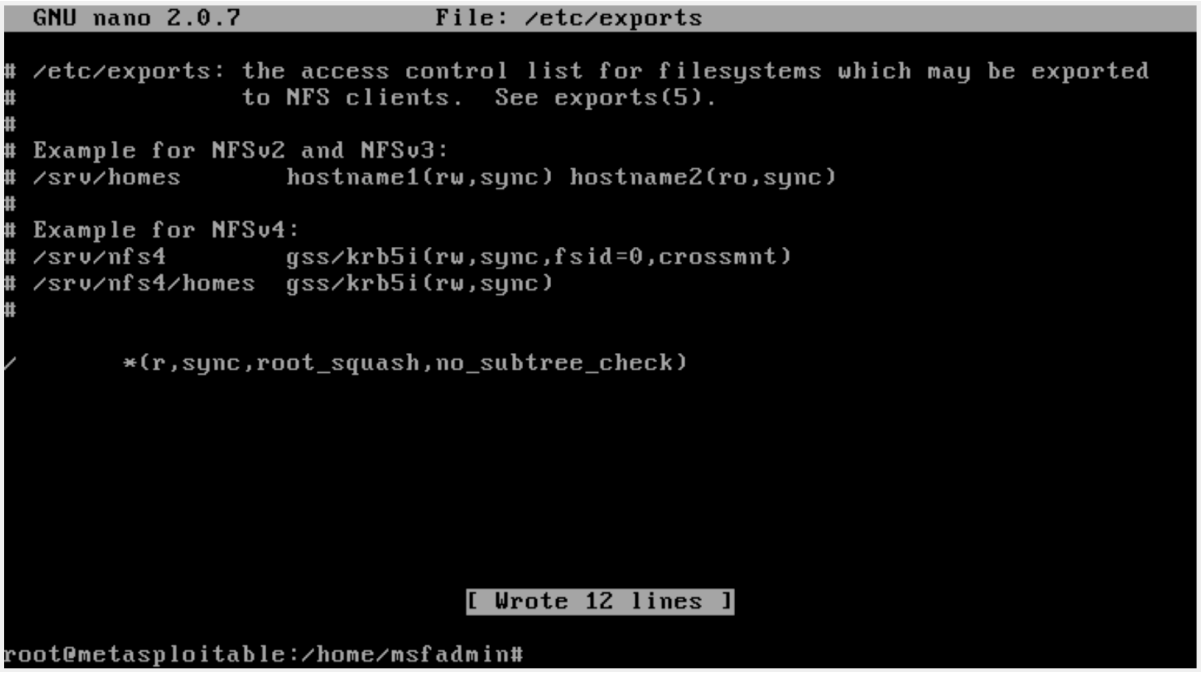
Questa criticità ci mostra che chiunque tenti ad accedere al servizio di *NFS* è in grado di entrare e poter modificare oltre a leggere i file presenti sul sistema.

Remediation actions

Vediamo adesso quali azioni possiamo intraprendere per risolvere le criticità sopra citate;

NFS Exported share information disclosure

Iniziamo con la risoluzione della criticità di *NFS* entriamo quindi dalla macchina di *Metasploitable* nel file di configurazione grazie al comando ***Sudo nano /etc/exports*** che ci permetterà di modificare i permessi;



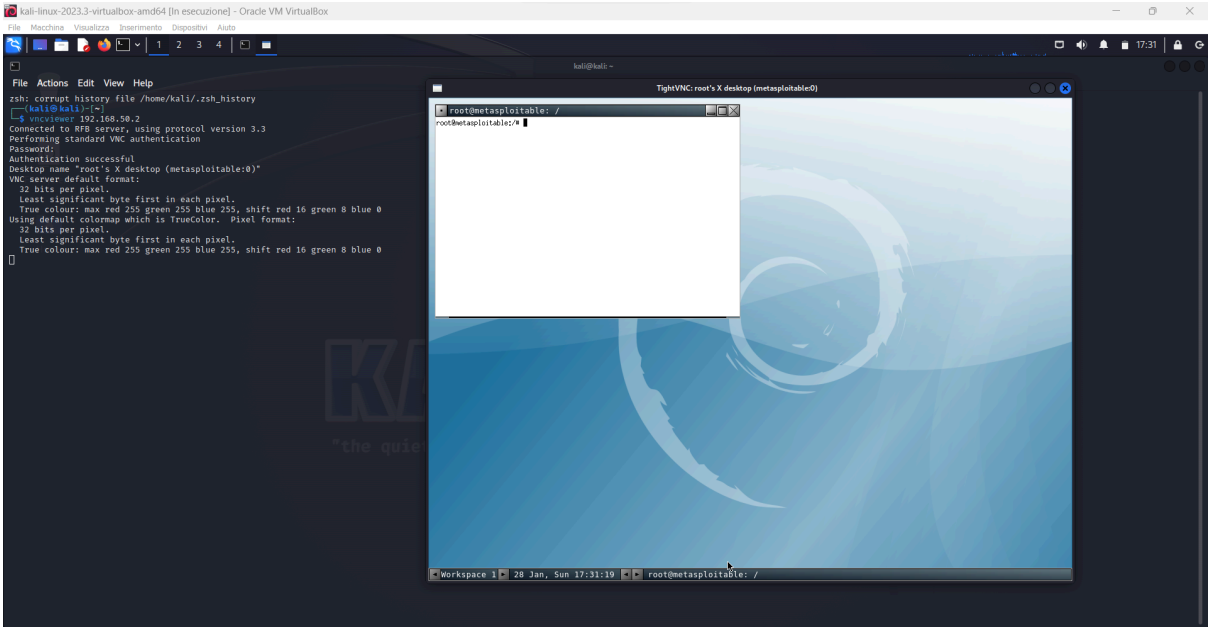
Modifichiamo quindi i permessi lasciando solamente quelli di lettura e richiedendo l'autenticazione come root per poter accedere alla directory, modificando l'opzione da ***no_ root_ squash*** a ***root_ squash.***

VNC Server password

Continuiamo con il risolvere la seconda criticità ovvero la password di VNC, sempre dalla macchina di *Metasploitable* eseguiamo il comando ***vncpasswd*** e in seguito inseriamo la nuova password e la conferma di essa per poterla cambiare come nell'immagine che segue:

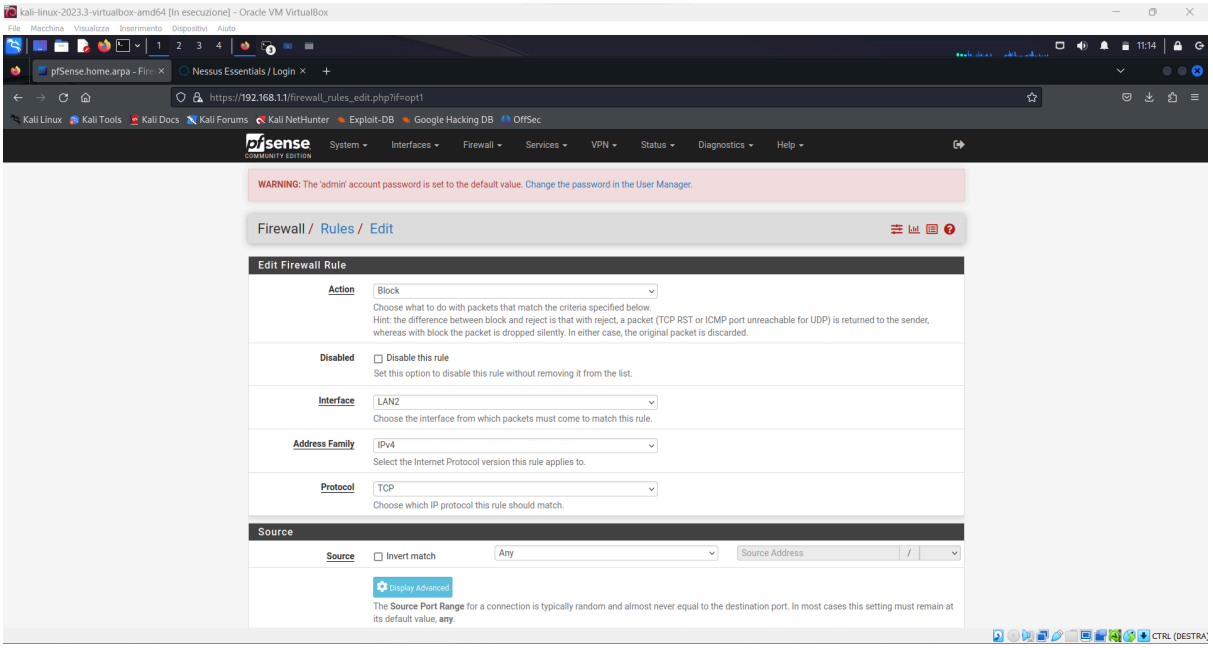
```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# msfadmin
bash: msfadmin: command not found
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

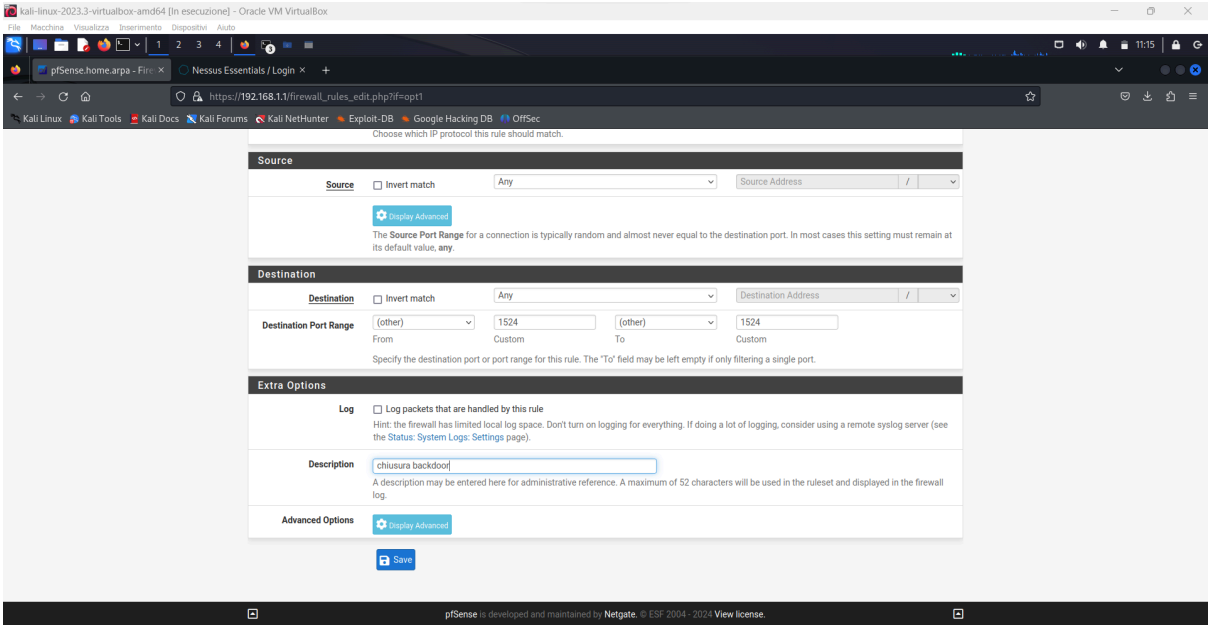
per poter confermare che la password è stata cambiata dal terminale di kali eseguiamo il comando ***vncviewer 192.168.50.2*** (che è l'indirizzo ip di *Metasploitable*) e per potervi accedere ci chiederà l'inserimento della password e se è stata modificata con successo riusciremo ad accedervi



Bind Shell Backdoor Detection

L'ultima criticità che tenteremo di risolvere per questo progetto è il listener sulla porta 1524 inizialmente configurando una regola di firewall da pfsense che blocca tutto il traffico su quella porta

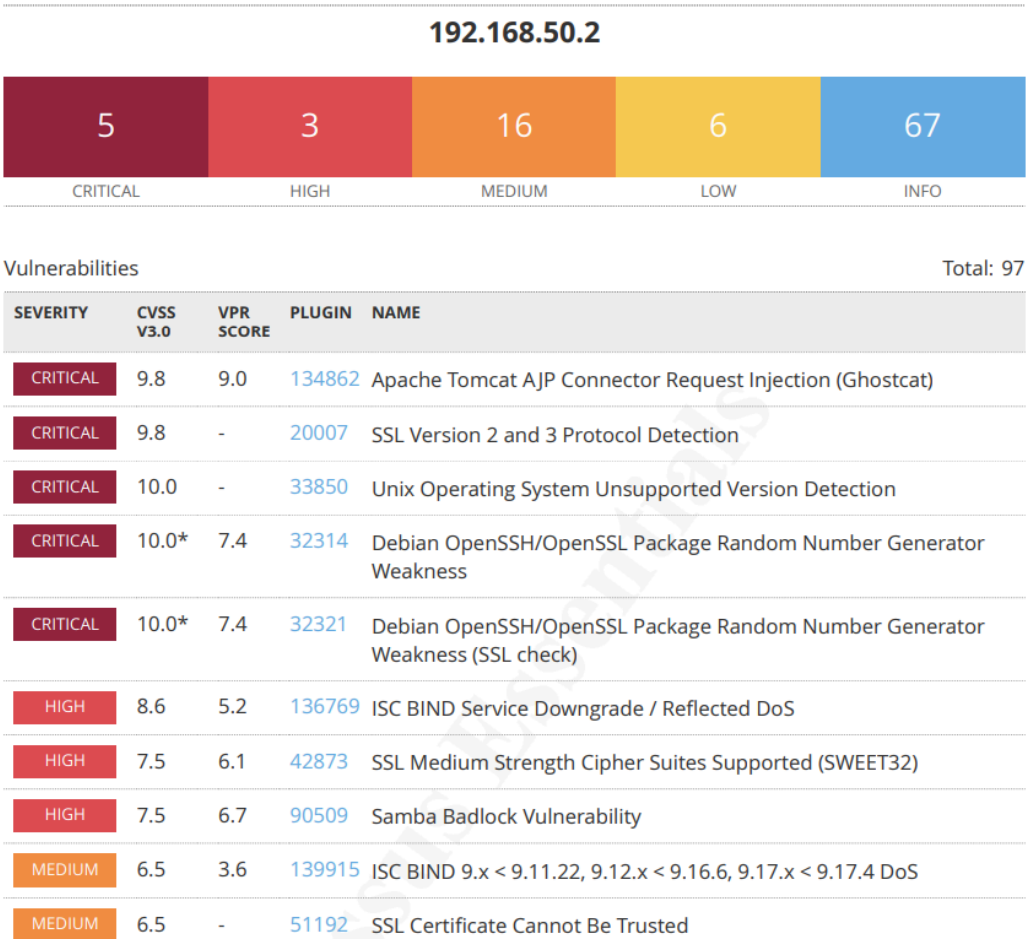




E in seguito da *Metasploitable* con il comando ***sudo iptables -I INPUT -p tcp –dport 1524 -j DROP***

```
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 1524 -j DRO
P
```

Scansione post remediation



192.168.50.2

5	3	16	6	67
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 97

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	-	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
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

A seguito di tutte le remediation action che abbiamo intrapreso per risolvere le criticità scelte possiamo rieseguire una scansione con il tool *Nessus* per notare (come riportato nell'immagine sopra) che ciò che abbiamo fatto ha avuto successo ed ora quelle criticità non sono più presenti.