

REMEDIATION META

ERNESTO ROBLES



STRUMENTI UTILIZZATI

Lo strumento utilizzato per la scansione delle vulnerabilità è Nessus sviluppato da Tenable Network Security.

DISPOSITIVI COINVOLTI

Macchina Kali ip: 192.168.1.60

Macchina Metasploitable ip: 192.168.1.67



RISOLUZIONE VULNERABILITIES

In questo report vengono illustrate alcune risoluzioni effettuate su alcune delle 70 vulnerabilità trovate con Nessus:

NFS Exported Share Information Disclosure
(CRITICAL)

VNC Server ‘password’ Password **(CRITICAL)**

Bind Shell Backdoor Detection **(CRITICAL)**

rlogin Service Detection **(High)**

rsh Service Detection **(High)**

Unencrypted Telnet Server **(High)**

Vulnerabilities 70				
	Sev	CVSS	VPR	Name
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure
<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
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)
<input type="checkbox"/>	MIXED	Apache Tomcat (Multiple Issues)
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable
<input type="checkbox"/>	HIGH	7.5 *	6.7	rlogin Service Detection
<input type="checkbox"/>	HIGH	7.5 *	6.7	rsh Service Detection
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability

SOLUZIONI

Per risolvere alcune di queste vulnerabilità è stato attivato il firewall su Metasploitable con i seguenti comandi:

`ufw default ALLOW`(abilito connessioni in entrata)

`ufw enable`(attivo il firewall).

Bind Shell Backdoor Detection (CRITICAL):

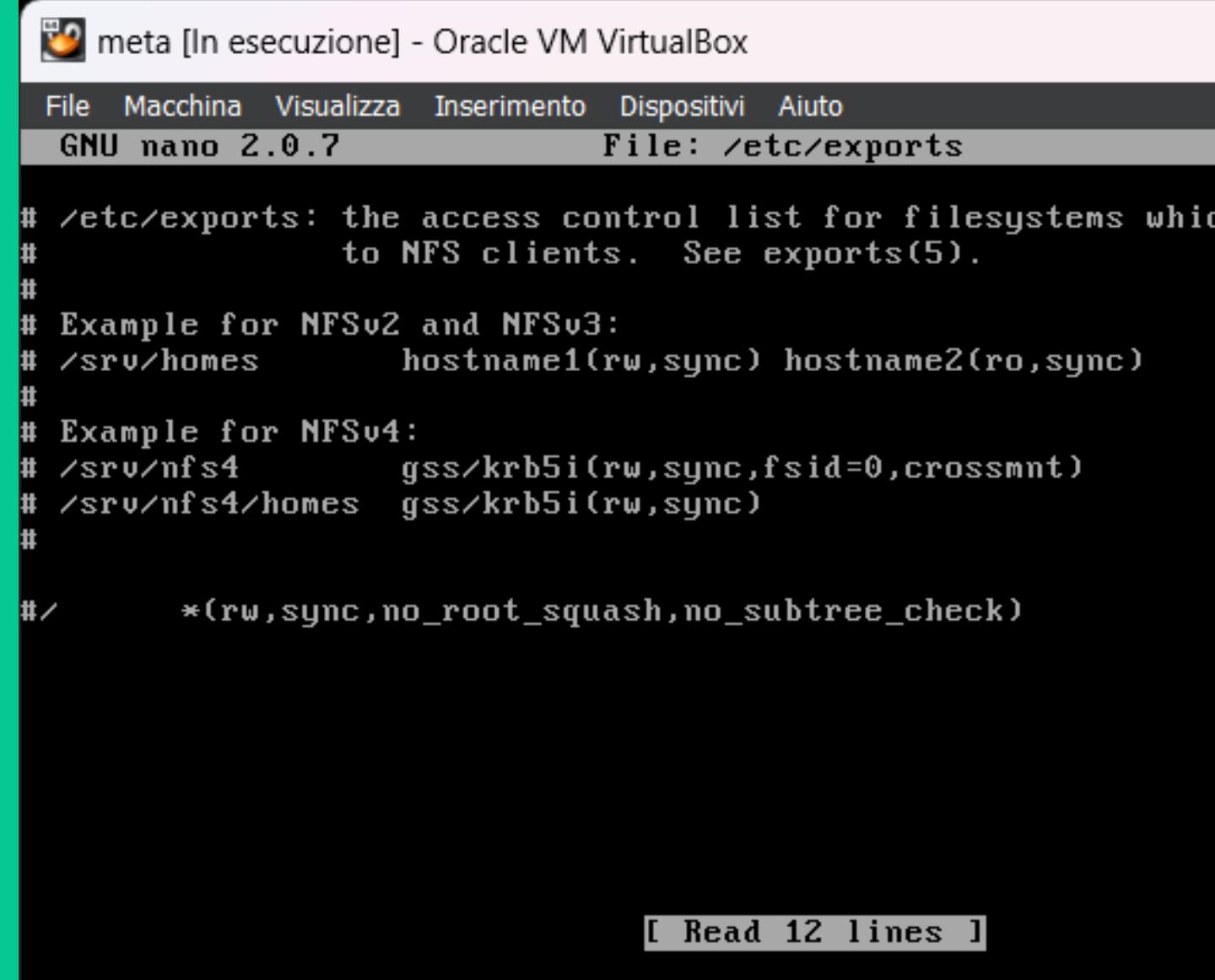
Dopo aver verificato che l'host non fosse compromesso, attraverso l'uso del firewall di Metasploitable si aggiunge una regola per negare tutto il traffico in arrivo sulla porta 1524 con il comando “`ufw deny 1524`”.

NFS Exported Share Information Disclosure (CRITICAL):

Al'interno del file di configurazione del servizio è stato tolto il permesso a tutti di potervi accedere senza credenziali con i comandi:

`sudo nano /etc/exports` (modifica del file)

`sudo /etc/init.d/nfs-kernel-server start` (avvio del servizio).



```
meta [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
#               are 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)

[ Read 12 lines ]
```

SOLUZIONI

VNC Server ‘password’ Password (CRITICAL):

Poichè la password del servizio era troppo debole, è stata modificata con una più sicure per farlo sono stati usati i comandi:

sudo su (per l'utente root)

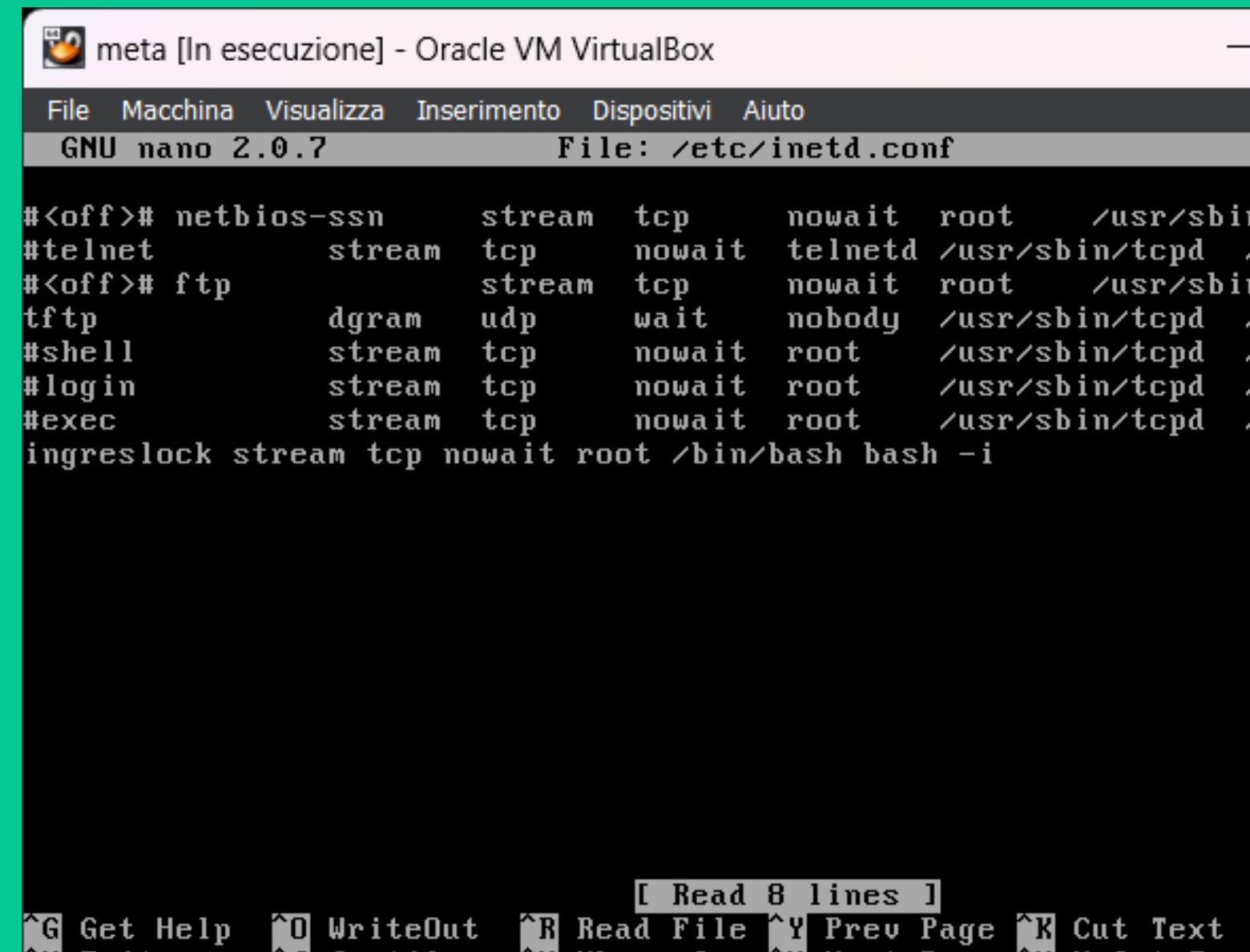
vnc passwd(per impostare la nuova password)

vncserver -kill:1(cessiamo il servizio)

vncserver (viene fatto ripartire con le impostazioni nuove)

rlogin Service Detection (High):

Modificando il file **inetd.conf** è stato tolto l'accesso e permesso di scrittura ai file di login usando il comando “**sudo nano /etc/inetd.conf**”.



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

SOLUZIONI

rsh Service Detection (High):

Modificando il file `inetd.conf` è stato tolto l'accesso e permesso di scrittura ai file di login usando il comando “`sudo nano /etc/inetd.conf`”.

Unencrypted Telnet Server (High):

E’ preferibile disattivare il servizio telnet commentando il servizio nel file `inetd.conf` oppure attraverso l’uso del firewal di Metasploitable si aggiunge una regola per negare tutto il traffico in arrivo sulla porta 23 con il comando “`ufw deny 23`”.

X Server Detection (Low):

Attraverso l’uso del firewal di Metasploitable si aggiunge una regola per negare tutto il traffico in arrivo sulla porta 6000 con il comando “`ufw deny 6000`”.

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

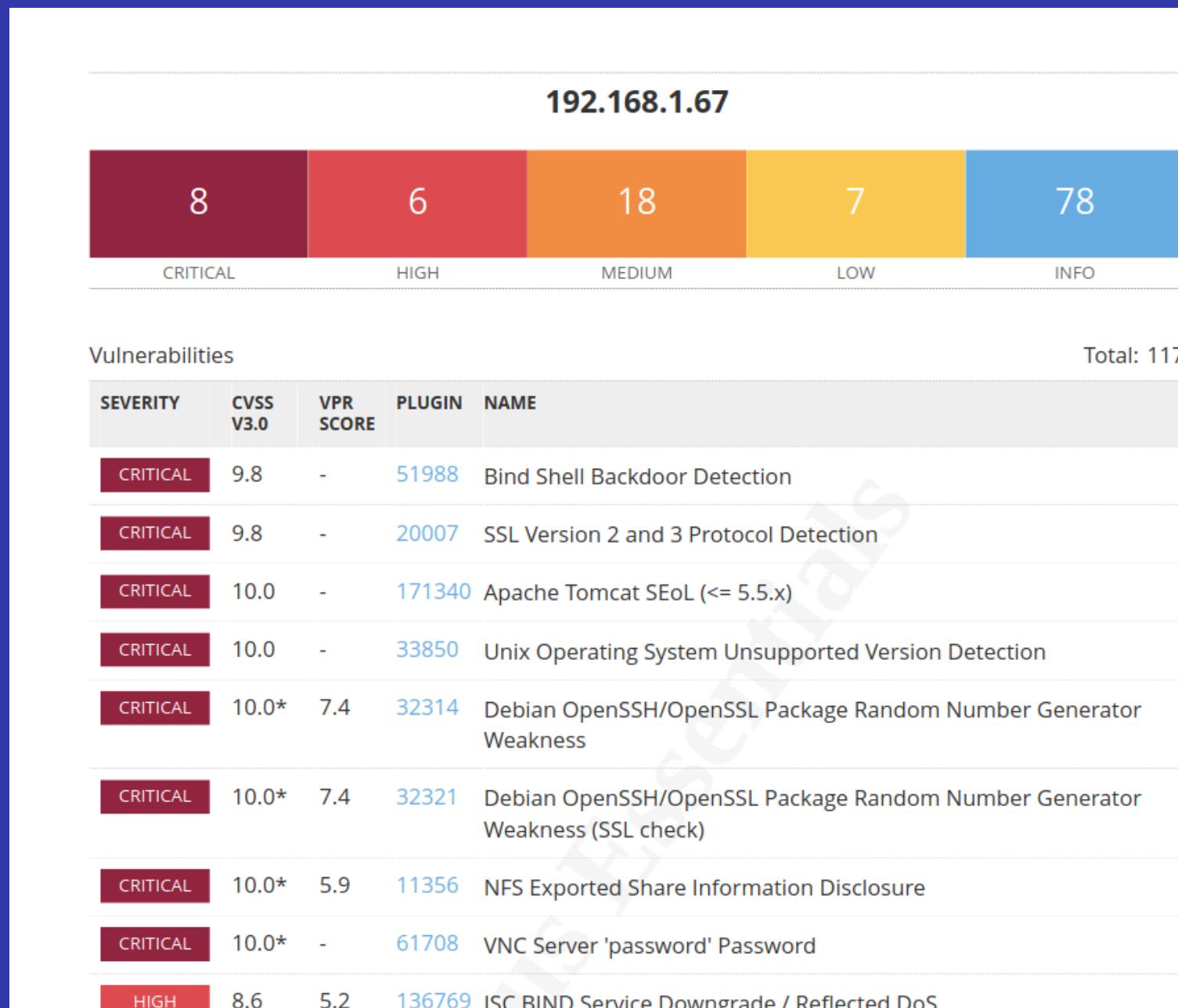
RISOLUZIONE VULNERABILITIES

In questo report viene illustrato il resoconto
dopo l'applicazione di determinate
risoluzioni effettuate su alcune delle 70
vulnerabilità trovate con Nessus in
precedenza ora scese a 59 totali

scansionefine2 / 192.168.1.67				
Back to Hosts				
Vulnerabilities 59				
Filter ▾		Search Vulnerabilities		59 Vulnerabilities
□	Sev ▾	CVSS ▾	VPR ▾	Name ▾
□	Critical	10.0		Unix Operating System Unsupported Version Detection
□	Mixed	Apache Tomcat (Multiple Issues)
□	Critical	SSL (Multiple Issues)
□	Mixed	SSL (Multiple Issues)
□	High	7.5	6.7	Samba Badlock Vulnerability
□	Mixed	SSL (Multiple Issues)
□	Mixed	ISC Bind (Multiple Issues)
□	Medium	6.5		TLS Version 1.0 Protocol Detection
□	Medium	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
□	Mixed	SSH (Multiple Issues)
□	Mixed	HTTP (Multiple Issues)
□	Mixed	SMB (Multiple Issues)
□	Mixed	TLS (Multiple Issues)

GRAFICO VULNERABILITIES

Graffico iniziale senza implementazione
delle soluzioni alle vulnerabilità



Graffico finale con implementazione
delle soluzioni alle vulnerabilità

