M3 D8

ESERCIZIO

GIORNO 5 – PROGETTO

Scansione completa da Kali con tool Nessus verso la macchina virtuale Metasploitable.
Diverse criticità e vulnerabilità sono state trovate, dalle più gravi alle meno importanti (raffigurate con colore rosso le principali dove porre rimedio fino alle azzurre – le più innocue).

Obiettivo: Provare ad implementare delle azioni di rimedio (remediation actions) e verificare che le vulnerabilità siano state fixate.

PUNTO 1:

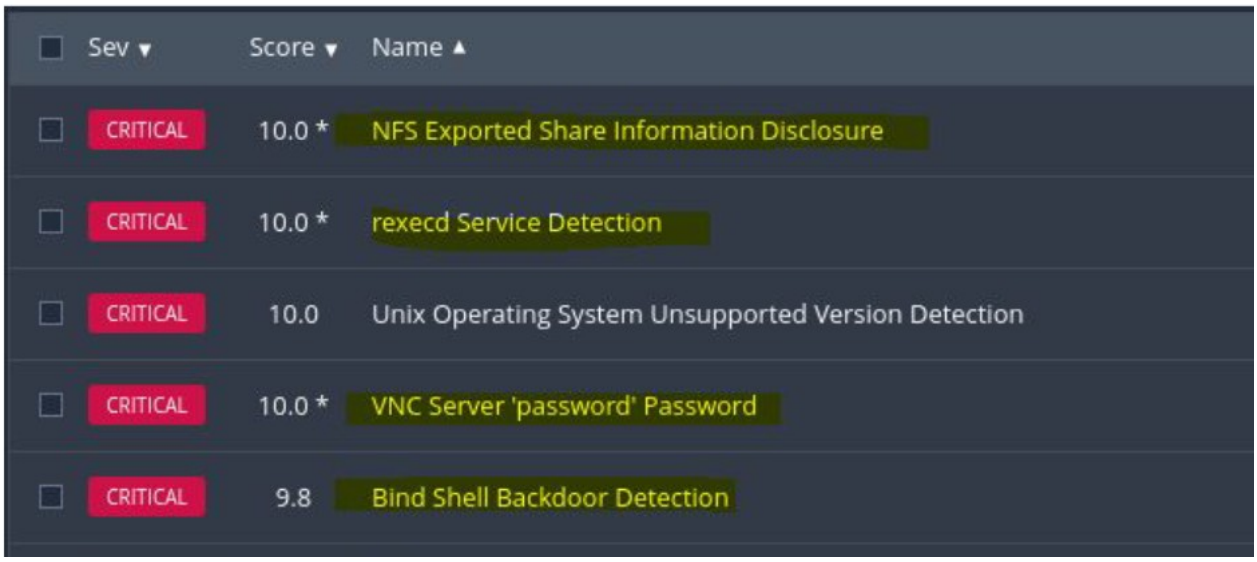
Elenco delle vulnerabilità trovate, specialmente le più gravi da segnalare, e riportate sul report (specialmente report tecnico dove segnalare il problema e possibile azione correttiva da implementare).

Vulnerabilities — Total: 106

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

PUNTO 2:

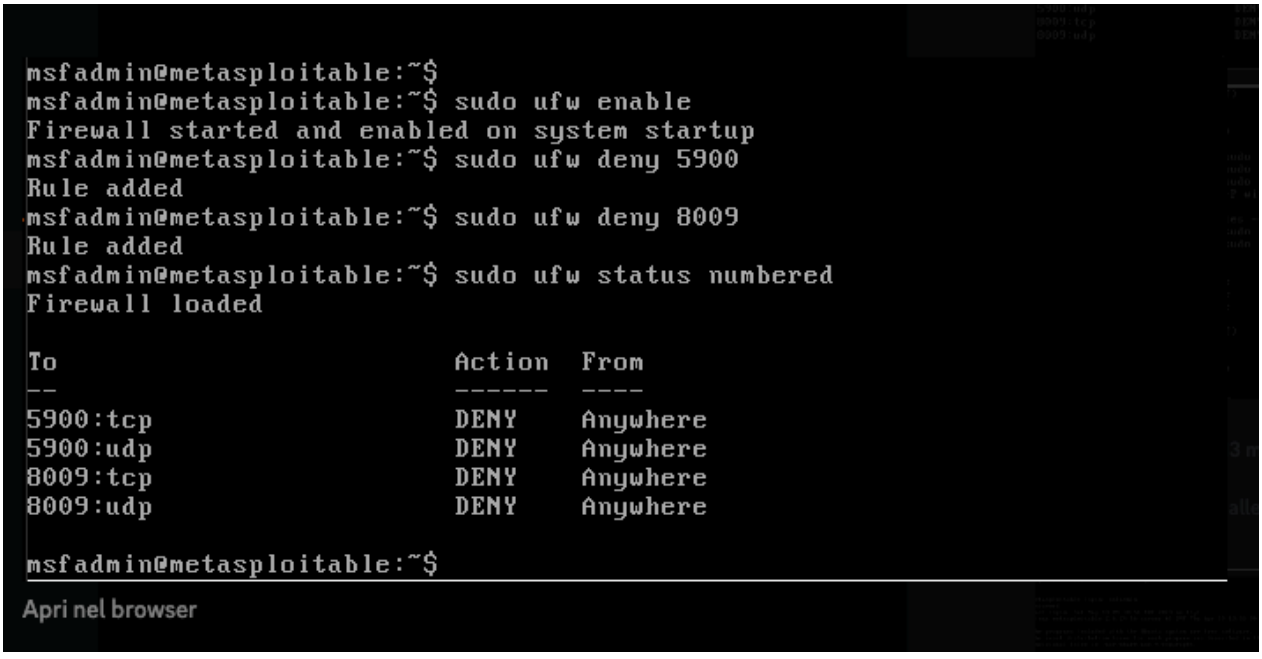
Analizzare le varie vulnerabilità e provare a porre azioni di rimedio su Metasploitabe.
Le vulnerabilità analizzate hanno un' alta criticità e sono riportate in tabella.



Sev	Score	Name
CRITICAL	10.0 *	NFS Exported Share Information Disclosure
CRITICAL	10.0 *	rexecd Service Detection
CRITICAL	10.0	Unix Operating System Unsupported Version Detection
CRITICAL	10.0 *	VNC Server 'password' Password
CRITICAL	9.8	Bind Shell Backdoor Detection

SETTAGGIO REGOLA FIREWALL
(scansione ci aveva dato una data porta aperta e noi col firewall Metaspl la filtriamo)

Comando da Metaspl: sudo ufw enable / sudo ufw deny

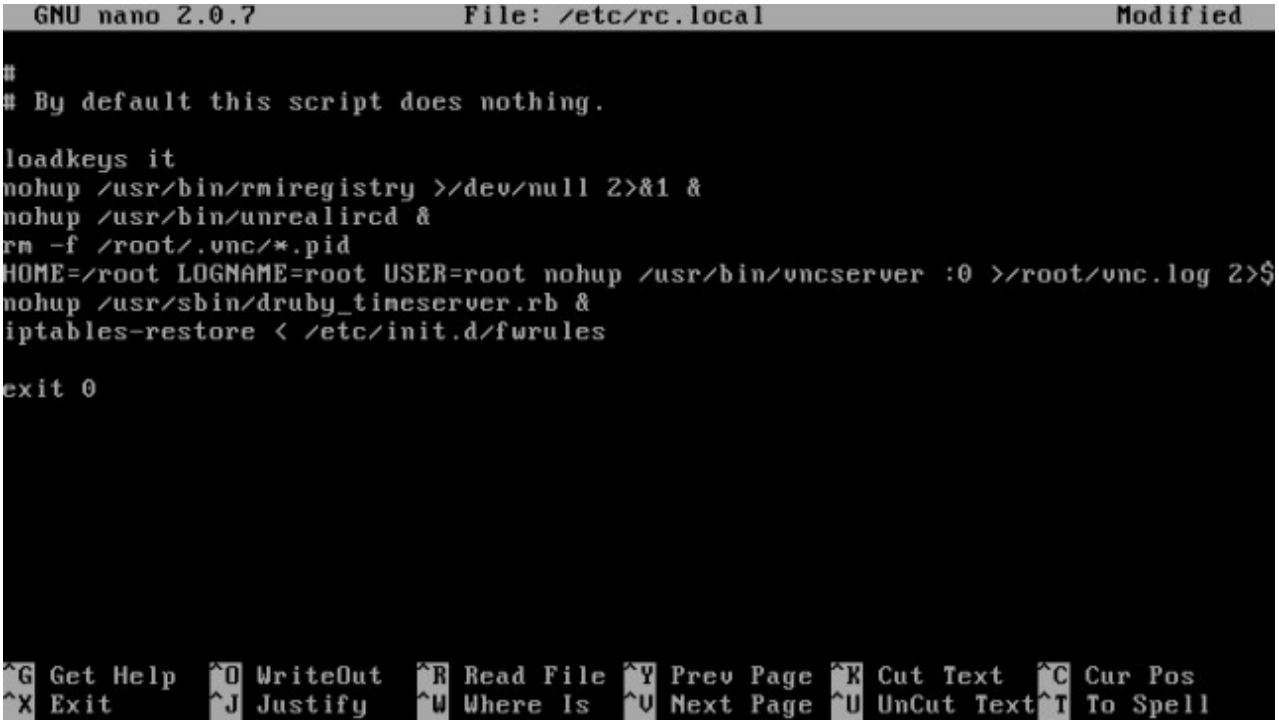


```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw deny 5900
Rule added
msfadmin@metasploitable:~$ sudo ufw deny 8009
Rule added
msfadmin@metasploitable:~$ sudo ufw status numbered
Firewall loaded

To                         Action  From
--                         ------  ----
5900:tcp                   DENY    Anywhere
5900:udp                   DENY    Anywhere
8009:tcp                   DENY    Anywhere
8009:udp                   DENY    Anywhere

msfadmin@metasploitable:~$
```

Apri nel browser

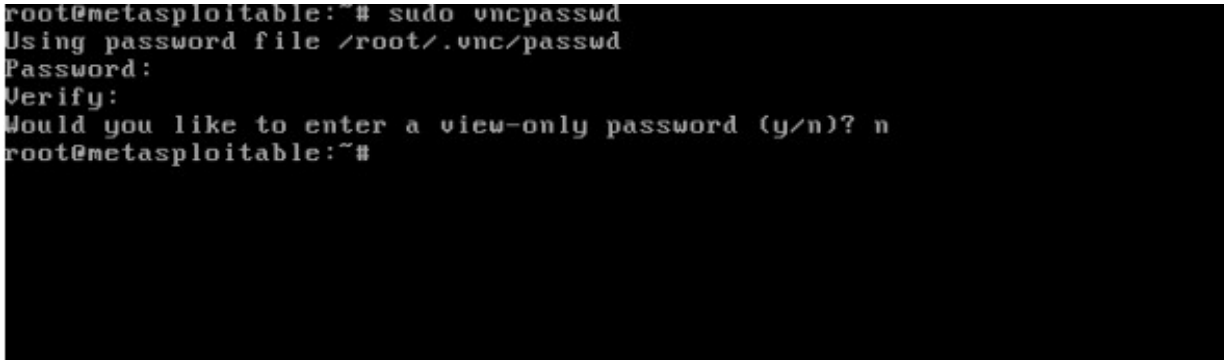
9.8 51988 BIND SHELL BACKDOOR DETECTION

Impostare regola firewall nella directory ETC/INIT.D tramite il seguente comando:
ip tables -A INPUT -p tcp - -dport 1524 -j DROP.
La porta segnalata dalla vulnerabilità è stata così chiusa.
Per forzare la macchina a caricare la regola al boot vado a modificare il file RC.LOCAL



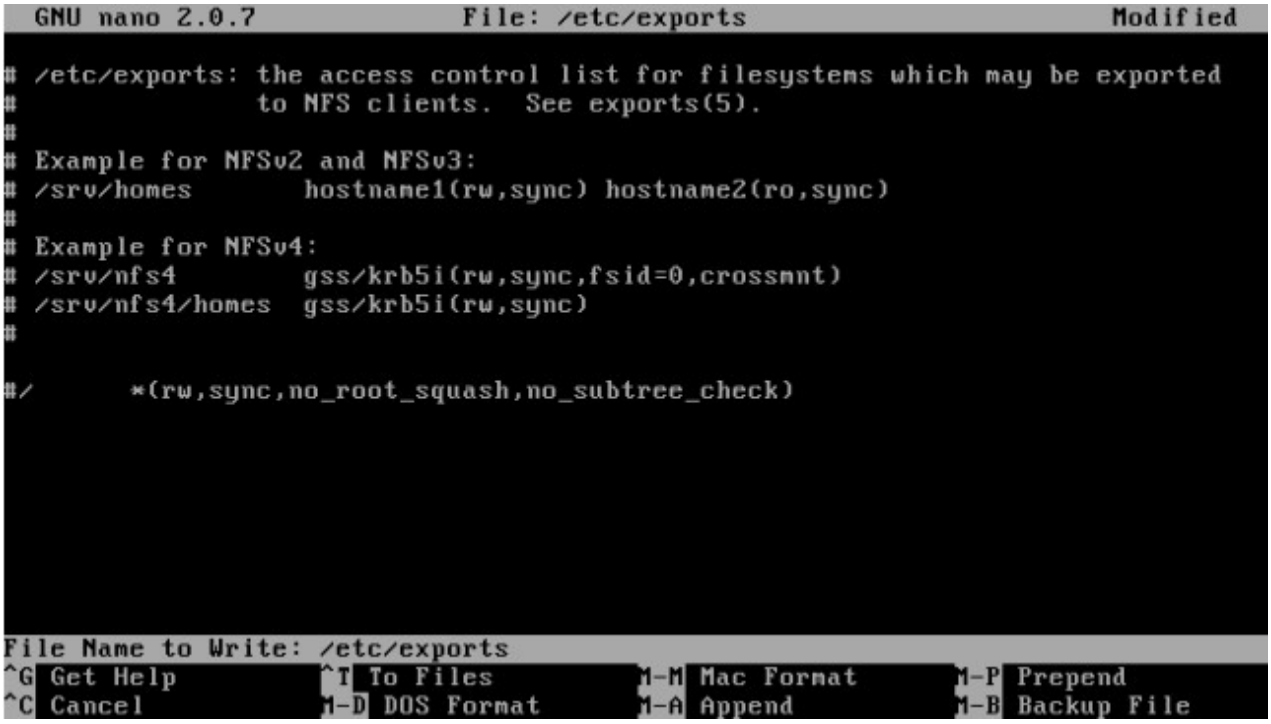
Aggiungere la riga iptables-restore</etc/init.d/fwrules
Per rimediare ad altri eventuali problemi di backdoor presenti nel report disattivare alcuni dei servizi in ascolto modificando il file INETD.CONF come seguente:

10.0* 61708 VNC SERVER 'password' PASSWORD



Per risolvere la vulnerabilità della password, vado a modificare il file PASSWD nella directory /ROOT/.VNC/ e lo applico poi eseguendo il comando: sudo passwd

10.0* 11356 NFS EXPORTED SHARE INFORMATION DISCLOSURE



Rimuovere cartella ROOT dal file EXPORTS per risolvere la vulnerabilità.

PUNTO 3:

Scansione post – remediation actions ci porterà la presenza di un numero minore di vulnerabilità.

Vulnerabilities Total: 102

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	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*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability