Traccia

Effettuare una scansione completa sul target Metasploitable.
Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high 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.
Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Svolgimento

Di seguito l'elenco delle vulnerabilità critiche/alte evidenziate da una prima scansione.

Vulnerabilities Total: 109

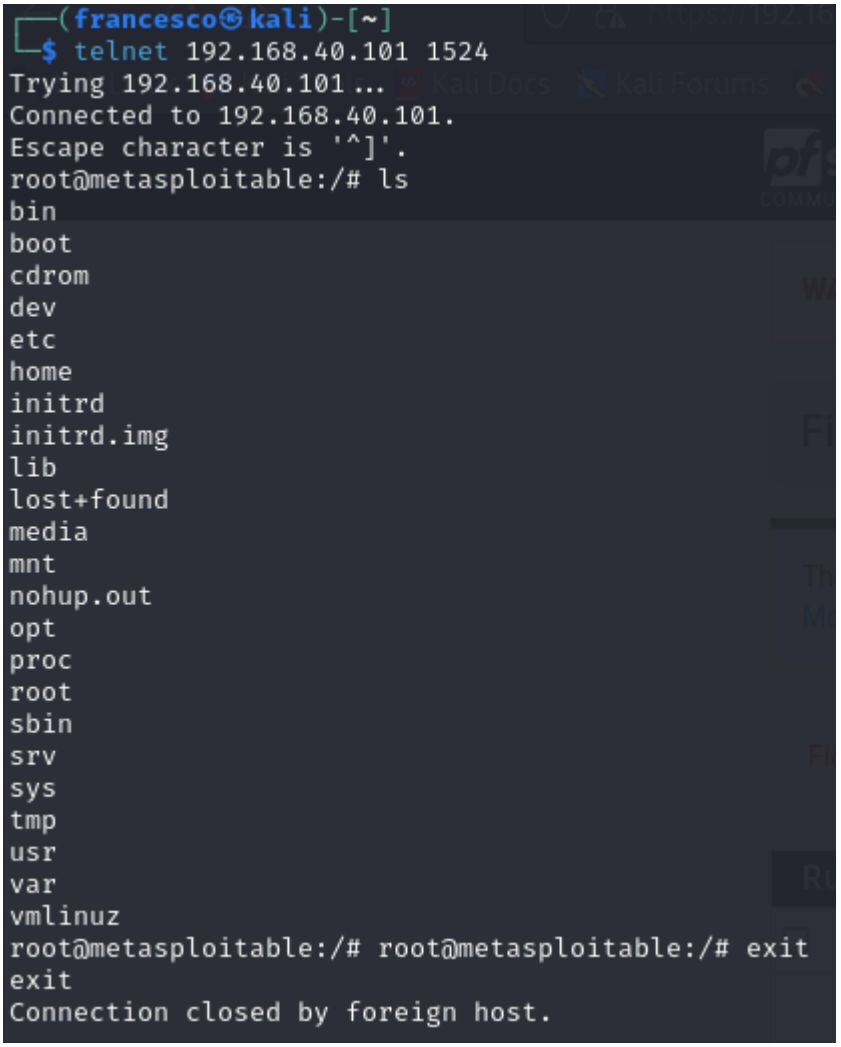
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	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
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection

Vulnerabilità critiche 8, alte 6, totali 109.

Bind Shell Backdoor Detection

Descrizione: una shell è in ascolto sulla porta TCP 1524 e permette la connessione senza autenticazione.

Abbiamo sfruttato questa vulnerabilità per connetterci, tramite il protocollo telnet, su questa porta, la connessione è andata a buon fine, inoltre eravamo connessi come root.

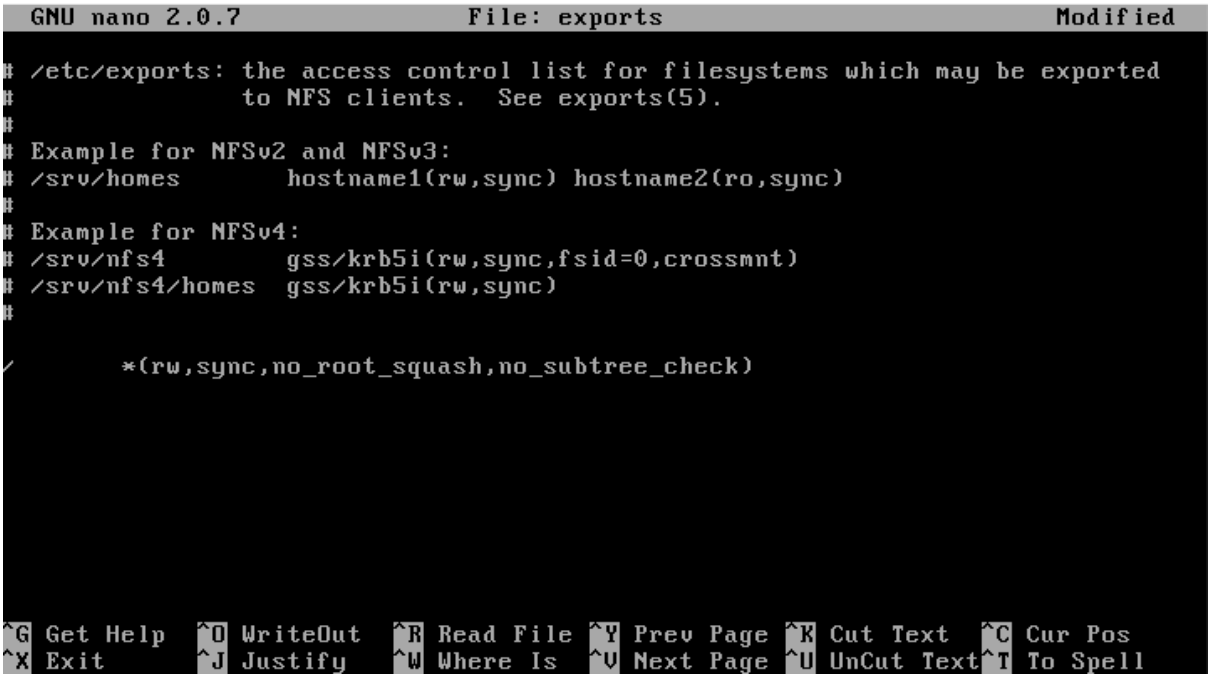


Soluzione: abbiamo creato una policy firewall che blocca le connessioni in entrata, da qualsiasi host, alla porta 1524 TCP dell'IP 192.168.40.101 (Meta).

NFS Exported Share Information Disclosure

Descrizione: una cartella condivisa sul protocollo NFS può essere montata da chiunque.

Facendo delle ricerche, abbiamo scoperto che il file di configurazione del servizio NFS si trova nella cartella *etc* con il nome *exports*.



Per condividere una cartella è sufficiente inserire il percorso della stessa, gli host a cui deve essere accessibile e le eventuali opzioni, con questa struttura *<percorso> <host>(<opzioni>)*.

Come si vede nell'immagine, prima delle parentesi, si trova il carattere *. Questo indica che la cartella in questione può essere montata da qualsiasi host.

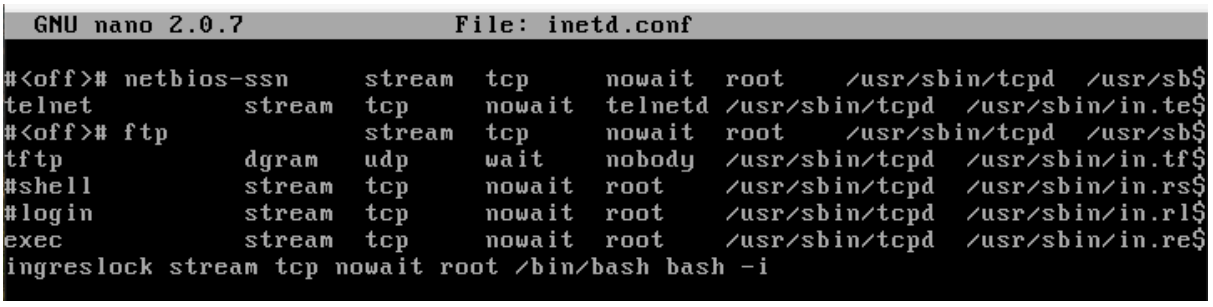
Soluzione: sostituire l'asterisco con l'indirizzo dell'host a cui si vuole dare il permesso di montare la cartella.

VNC Server 'password' Password

Descrizione: il servizio VNC attivo sul server è protetto da una password debole, Nessus è stato in grado di autenticarsi con la password ‘password’.
Il servizio VNC era stato installato, ma non configurato.
Soluzione: con il comando *vncserver* si lancia la configurazione del servizio, viene richiesto di creare una password iniziale, ed eventualmente una password per la sola lettura. Viene creato il file di configurazione, ed una volta riavviato il servizio il problema si risolve.

rlogin Service Detection, rsh Service Detection

Descrizione: ci sono due servizi che danno la possibilità di accedere alla macchina tramite i relativi protocolli.



Soluzione: è sufficiente commentare le righe relative a questi servizi, nel file *inetd.conf* (file in cui sono contenuti i servizi esposti di Meta)

Vulnerabilities Total: 95

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*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	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

Come si può vedere, da una seconda scansione, le vulnerabilità descritte sono state risolte.