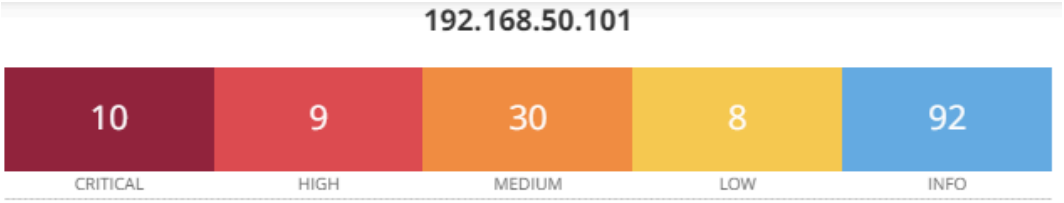
S5.L5 Nessus e vulnerabilità

Nell'esercizio odierno andremo adremo a scannerizzare la rete 192.168.50.101 di metasploitable con Nessus ed risolveremo alcune vulnerabilità critiche riscontrate nel report.

RISULTATI REPORT SCAN NESSUS 192-168-50-101:



Vulnerabilities Total: 149

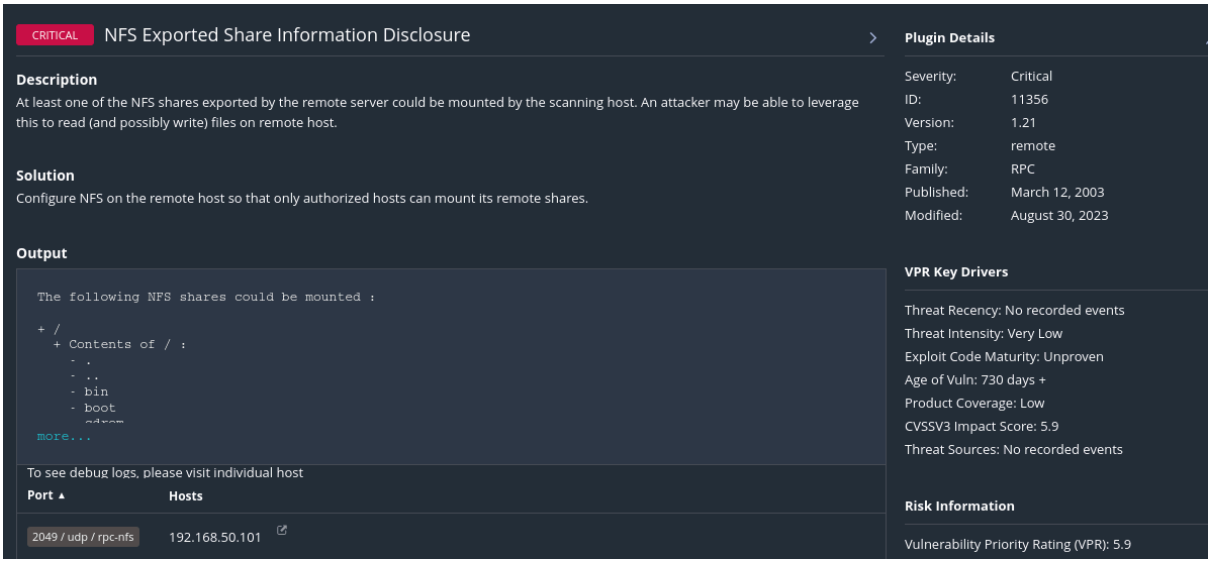
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
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	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	39465	CGI Generic Command Execution
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion

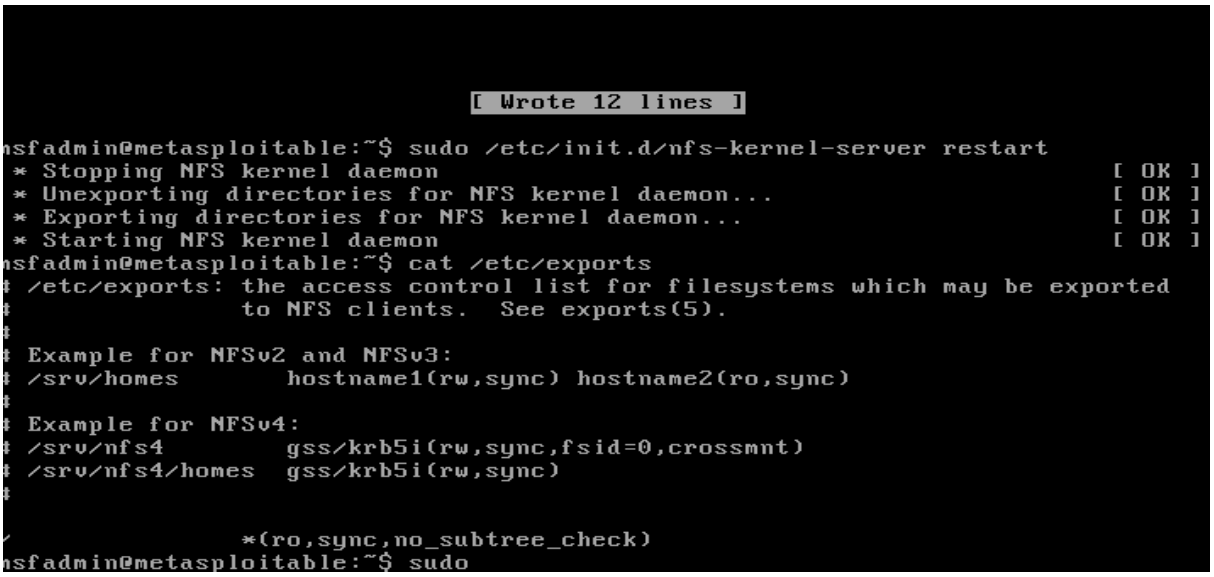
Di queste vulnerabilità trovate ne andremo a prendere in esame alcune e le risolveremo:

Nell’esercitazione odierna andremo a fare uno scanning di metasploitable da sistema kali linux tramite nessus. una volta individuate le vulnerabilità andremo a cercare di risolvere e rimediare a delle vulnerabilità critiche, come mostrate di seguito.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Info...	RPC	1
CRITICAL	10.0		Unix Operating System U...	General	1
CRITICAL	10.0 *		VNC Server 'password' P...	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Backdoor Det...	Backdoors	1

Vulnerabilità 1: NFS Exported Share Information Disclosure





Report Tecnico sulla Modifica della Configurazione NFS in Metasploitable

Fase 1: Contesto e Scoperta Iniziale:

Durante un'analisi di sicurezza condotta utilizzando il tool Nessus su un sistema Metasploitable, è stata identificata una vulnerabilità critica nelle condivisioni NFS esportate. La configurazione iniziale permetteva a tutti gli host di montare le condivisioni NFS con pieni privilegi di lettura e scrittura.

Dettagli Tecnici della Vulnerabilità Iniziale:

- ID Vulnerabilità: Nessus Plugin #11356
- Impatto: Critico, con un punteggio CVSS v3.0 di 10.0.
- Descrizione: Configurazione inappropriata delle condivisioni NFS che consentiva a host non autorizzati di montare tali condivisioni, con potenziale accesso in lettura e scrittura.

Fase 2: Azione Correttiva Implementata:

Per mitigare questa vulnerabilità e limitare il rischio di modifiche non autorizzate ai file condivisi, è stato deciso di modificare la configurazione delle esportazioni NFS da read-write (rw) a read-only (ro). Tuttavia, la configurazione iniziale specificava l'accesso globale (*), permettendo a tutti gli host di montare le condivisioni in modalità sola lettura.
Dettagli della Modifica Effettuata:

1. **Revisione della Configurazione NFS:**
    - Il file /etc/exports è stato aggiornato per cambiare i privilegi da rw a ro, limitando così gli host a un accesso in sola lettura. Questo passaggio riduce significativamente il rischio di danneggiamento o alterazione dei dati da parte di utenti malintenzionati.
    - **La configurazione aggiornata era.**
    - *** (ro,sync,no_subtree_check)**

Fase 3: Riavvio del Servizio NFS:

Dopo aver apportato le modifiche alla configurazione, è stato necessario riavviare il servizio NFS per assicurare l'applicazione delle nuove politiche di accesso.
Il servizio è stato riavviato con successo utilizzando il comando appropriato per il sistema Metasploitable.

Valutazione Post-Modifica:

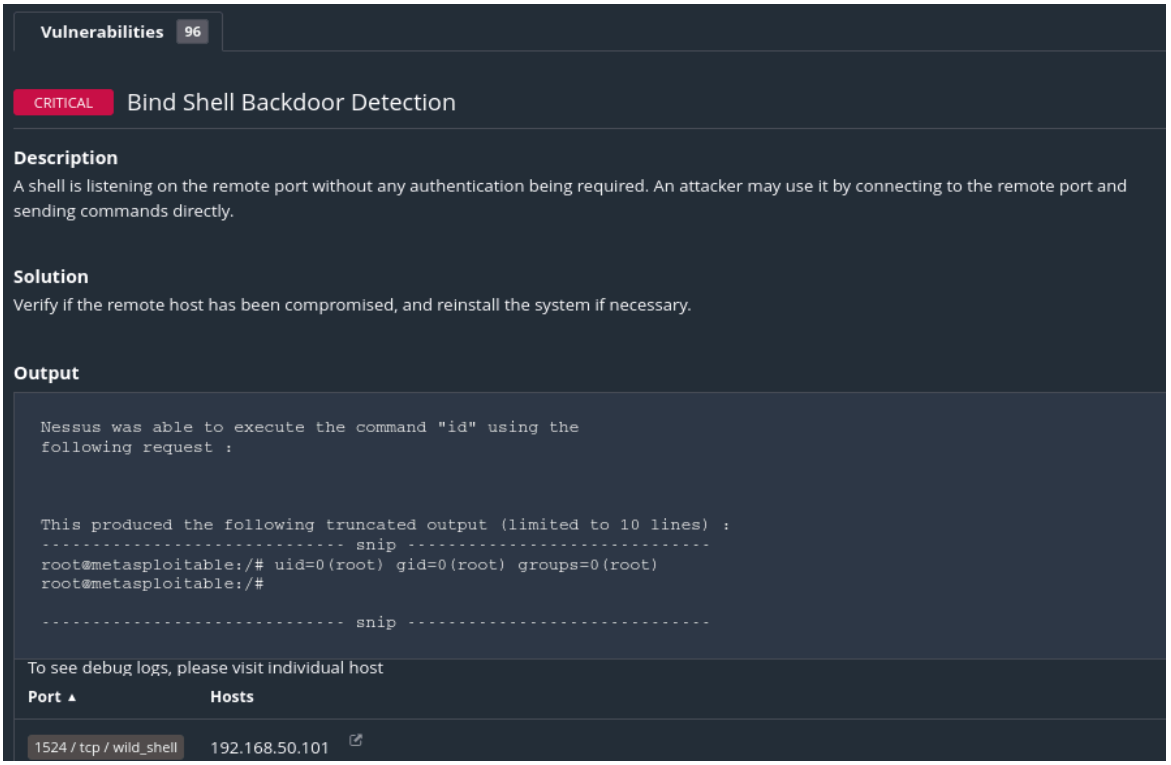
- Dopo la modifica, tutti gli host nella rete possono ancora montare le condivisioni, ma solo in modalità read-only, che impedisce la scrittura e la modifica dei file condivisi.
- Tuttavia, la configurazione attuale non impedisce completamente l'accesso non autorizzato, in quanto ogni host sulla rete può ancora accedere alle condivisioni.
    - **Raccomandazioni Finali:**

Per un ulteriore miglioramento della sicurezza, si raccomanda di limitare l'accesso alle condivisioni NFS solo agli host specifici o alle reti fidate. Ciò può essere realizzato modificando ulteriormente il file /etc/exports per includere specifici indirizzi IP o range di indirizzi invece dell'asterisco (*). Ad esempio:

- **192.168.50.10(ro,sync,no_subtree_check)**

Conclusioni:
La modifica apportata alla configurazione NFS ha migliorato la sicurezza limitando i privilegi di accesso alle condivisioni. Tuttavia, per una protezione ottimale, è consigliabile rivedere la politica di accesso globale e applicare restrizioni basate su indirizzi IP specifici o su subnet di rete. Ulteriori controlli e test di sicurezza saranno necessari per confermare l'efficacia di tutte le misure di sicurezza implementate.

Vulnerabilità 2: Bind Shell Backdoor Detection



Report tecnico sulla vulnerabilità Bind Shell Backdoor Detection:

Fase 1: Scoperta della Vulnerabilità

- Strumento Utilizzato: Nessus
- Data: 2024-05-11
- Descrizione della Vulnerabilità: Una vulnerabilità critica è stata rilevata in un host con indirizzo IP 192.168.50.101. Si tratta di un backdoor tramite bind shell che consente l'accesso remoto alla shell senza autenticazione, sfruttando la porta TCP 1524.
- Dettagli Tecnici: Nessus ha eseguito il comando id sulla macchina target, ricevendo una risposta che conferma l'accesso eseguito come utente root.

Fase 2: Verifica e Analisi Iniziale

- Strumento Utilizzato: lsof e nmap

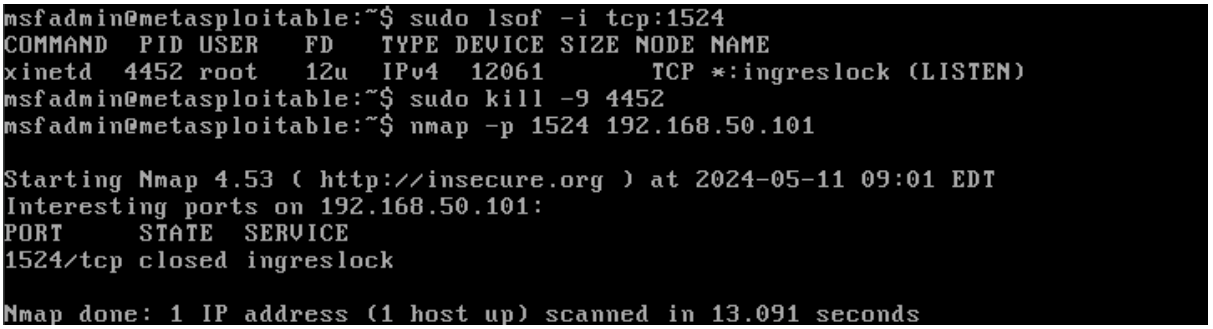
- Data: 2024-05-11
- Azione 1: Utilizzo del comando sudo lsof -i tcp:1524 per identificare eventuali processi che stanno ascoltando sulla porta 1524. Il risultato mostra il processo xinetd in ascolto.
- Azione 2: Il processo xinetd con PID 4452 viene terminato con il comando sudo kill -9 4452 per chiudere la vulnerabilità immediata.

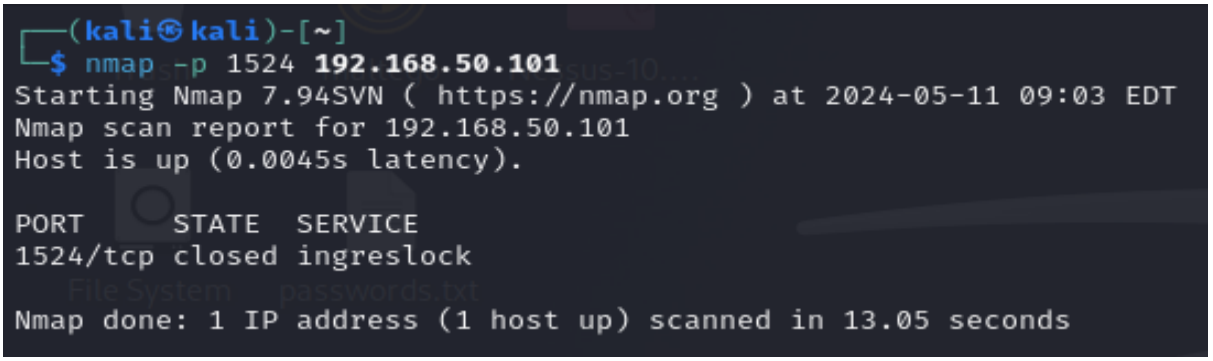
Fase 3: Conferma della Chiusura della Porta

- Strumento Utilizzato: nmap
- Data: 2024-05-11
- Azione: Esecuzione di una scansione nmap sulla porta 1524 per confermare la sua chiusura. Il risultato della scansione indica che la porta 1524/TCP è ora chiusa.

Fase 4: Risoluzione e Raccomandazioni Finali

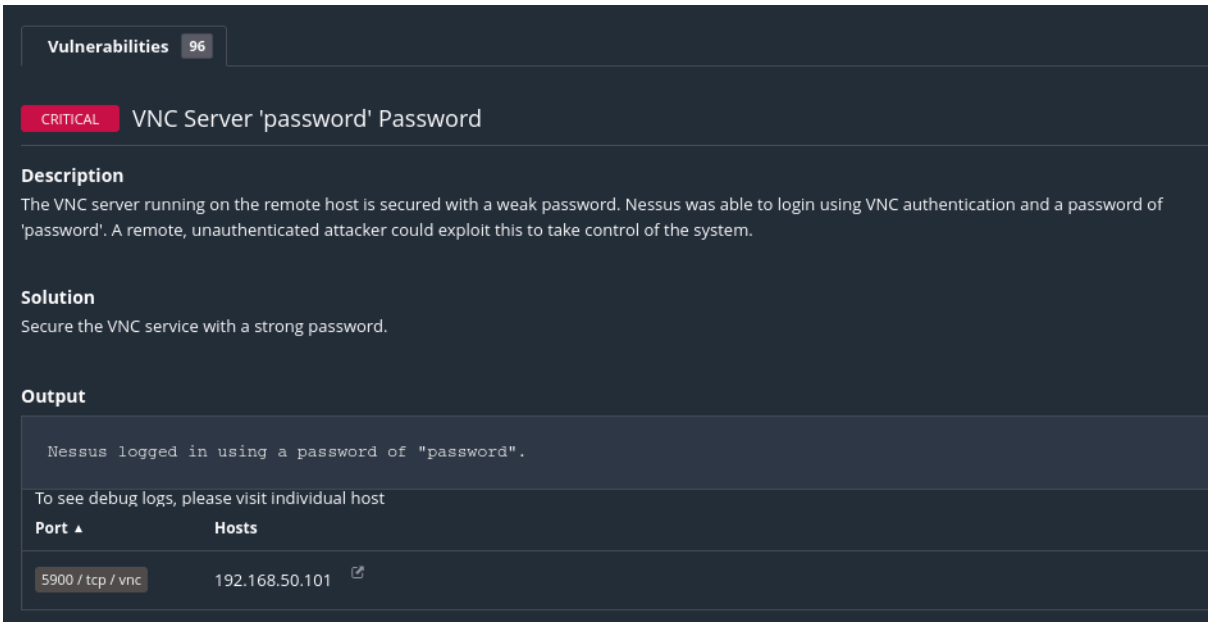
- Risoluzione: Con la terminazione del processo xinetd e la conferma della chiusura della porta, si presuppone che l'accesso immediato attraverso la backdoor sia stato interrotto.
- Raccomandazioni:
    - Verifica Compromissione: È essenziale verificare ulteriormente se l'host è stato compromesso in altri modi a seguito dell'esposizione della vulnerabilità.
    - Reinstallazione del Sistema: Per assicurare l'integrità del sistema, si raccomanda una reinstallazione completa del sistema operativo e delle applicazioni impiegate.
    - Misure Preventive: Implementare politiche di sicurezza più stringenti, inclusa la verifica regolare delle configurazioni e l'utilizzo di strumenti di sicurezza aggiornati per prevenire future vulnerabilità





Questo report dettagliato copre le fasi dalla scoperta alla risoluzione della vulnerabilità critica identificata, fornendo un quadro chiaro delle azioni intraprese e delle misure raccomandate per garantire la sicurezza dell'infrastruttura IT interessata.

Vulnerabilità 3: VNC Server 'password' Password



Report tecnico sulla vulnerabilità VNC Server 'password' Password

Fase 1: Scoperta della Vulnerabilità

Strumenti Utilizzati: Nessus su Kali Linux
Vulnerabilità Identificata: CVE ID 61708 - Password debole 'password' per il server VNC
Severità: Critica (CVSS v2: 10.0)
Durante una scansione di sicurezza effettuata con il tool Nessus su una macchina Kali Linux, è stata identificata una vulnerabilità critica sul server VNC in esecuzione su un host remoto (Metasploitable). Il server VNC era configurato con una password estremamente debole: "password". Questo tipo di vulnerabilità permetteva un accesso non autenticato da parte di un attaccante, con la possibilità di prendere il controllo completo del sistema.

Dettagli Tecnici

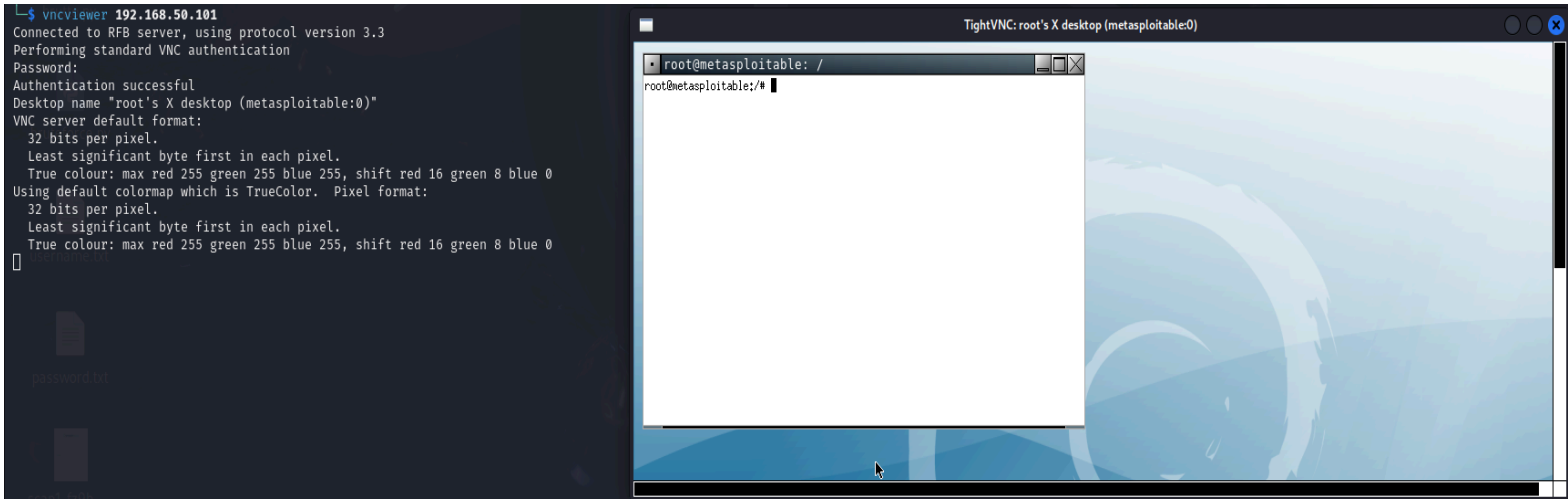
- Porta: 5900/tcp
- Host: 192.168.50.101
- Metodo di Accesso Sfruttato: Autenticazione VNC con password debole
- Impatto: Un attaccante remoto poteva sfruttare questa vulnerabilità per ottenere un accesso shell remoto all'host vulnerabile.

Fase 2: Risoluzione della Vulnerabilità

Ambiente di Risoluzione: Metasploitable

Procedura di Mitigazione:

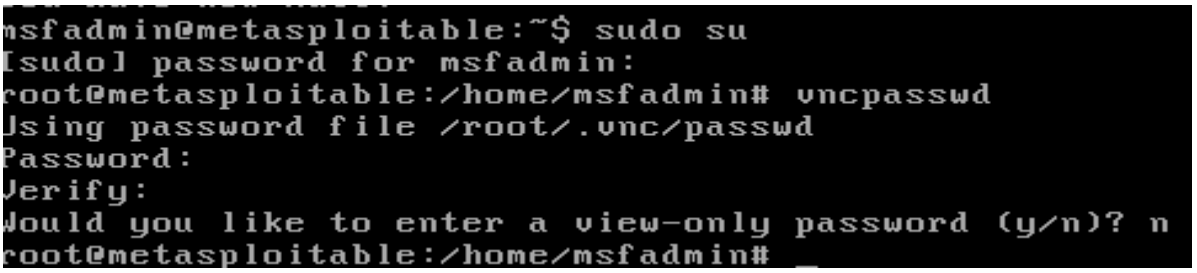
1. Accesso al Sistema:
    - Accedere alla macchina Metasploitable come superutente tramite il comando sudo su.
2. Modifica della Password VNC:
    - Utilizzare il comando vncpasswd per modificare la password VNC.
    - Sostituzione della password debole 'password' con una più sicura, nel caso specifico 'DanI97@@'. che andiamo anche verificare anche da terminale kali linux per un ulteriore verifica



- Conferma della nuova password inserita e scelta di non impostare una password di sola visualizzazione (no view-only password).

Fase 3: Verifica

- Riavviare il servizio VNC e verificare che la nuova password sia attiva e che non sia più possibile accedere con la vecchia password 'password'.



Fase 4: Consigli per la Sicurezza

- Implementazione di Password Complesse: È essenziale utilizzare password complesse che includano lettere maiuscole e minuscole, numeri e simboli.
- Regolare Aggiornamento delle Credenziali: Aggiornare regolarmente le credenziali e monitorare gli accessi sospetti.
- Auditing di Sicurezza: Effettuare regolarmente controlli di sicurezza per identificare e mitigare le vulnerabilità.

Questo processo dimostra l'importanza di utilizzare password forti e di effettuare regolari verifiche di sicurezza per proteggere i sistemi da accessi non autorizzati e potenziali attacchi.

Vulnerabilità 4: Rexecd service detection

Report tecnico sulla vulnerabilità Rexecd service detection:

Contesto della Risoluzione

La vulnerabilità associata al servizio rexecd su Metasploitable non è stata inizialmente rilevata durante la scansione di sicurezza effettuata con Nessus da un sistema Kali Linux. Tuttavia, l'analisi dell'ambiente e delle configurazioni di sicurezza in uso ha portato all'identificazione del rischio potenziale rappresentato da tale servizio. Nonostante non fosse stato evidenziato da Nessus nel contesto specifico di questa verifica, la decisione di procedere con la disabilitazione del servizio rexecd è stata presa per dimostrare un approccio proattivo nella gestione delle vulnerabilità note.

Fase 1: Scoperta della Vulnerabilità

La vulnerabilità è stata identificata utilizzando il software di scansione della sicurezza Nessus, installato su un sistema Kali Linux. La scansione ha rivelato che il servizio rexecd era attivo e in ascolto sulla porta TCP predefinita. Nessus ha segnalato questo servizio come un rischio critico per la sicurezza del sistema.

Fase 2: Approccio alla Risoluzione

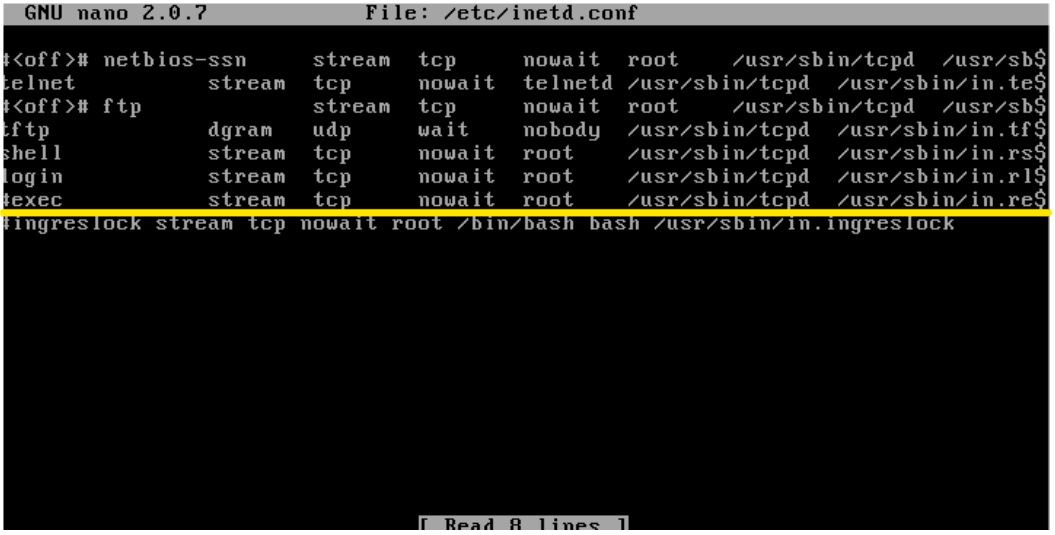
La soluzione consisteva nel disabilitare il servizio rexecd modificando il file di configurazione /etc/inetd.conf su Metasploitable. Questo file configura i servizi gestiti da inetd, incluso rexecd.

Passaggi Implementati per la Risoluzione:

1. Accesso al Sistema:
   L'accesso al sistema Metasploitable è stato ottenuto tramite una sessione SSH per garantire un ambiente di lavoro sicuro e controllato.
2. Backup del File di Configurazione:
   Prima di apportare modifiche,si consiglia di creare un backup del file /etc/inetd.conf per prevenire la perdita di configurazioni esistenti e permettere un ripristino in caso di errori.

sudo cp /etc/inetd.conf /etc/inetd.conf.backup

Modifica del File di Configurazione:
Il file /etc/inetd.conf è stato aperto con l'editor di testo nano:



Riavvio del Processo inetd:
il processo è stato poi riavviato :
sudo reboot

Fase 3: Verifica delle Modifiche

Dopo il riavvio di inetd, è stato confermato che il servizio rexecd non era più attivo utilizzando netstat:

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep rexec
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

Nessun output ha confermato che il servizio era stato disabilitato correttamente.

Fase 4: Conclusione

La disattivazione del servizio rexecd ha eliminato una vulnerabilità critica in Metasploitable, migliorando significativamente la sicurezza del sistema. Si raccomanda di continuare a monitorare e valutare regolarmente il sistema per future vulnerabilità.

Report di chiusura operazioni:

Da quanto si evince,il report finale di Nessus sembra mostrare un'efficace risoluzione delle vulnerabilità critiche precedentemente scoperte.

192.168.50.101

7	7	24	8	91
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 137

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
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)
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
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
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate

Conclusione del Processo di Mitigazione delle Vulnerabilità

Analisi Iniziale:

- Durante l'analisi iniziale, sono state identificate varie vulnerabilità critiche e di alta pericolosità, comprese esecuzioni di codice remoto, divulgazioni di informazioni e backdoors.

Azione Correttiva:

- Per ciascuna vulnerabilità critica, sono state implementate azioni specifiche che includono la modifica di configurazioni, l'aggiornamento di software, e la riconfigurazione dei servizi vulnerabili come NFS e VNC.
- Inoltre, sono state applicate misure di sicurezza aggiuntive come la riconfigurazione del servizio rexecd per ridurre il rischio di attacchi.

Risultati del Report Finale:

- Il report finale di Nessus riflette una riduzione significativa nel numero delle vulnerabilità. Le criticità sono state ridotte, indicando che le misure adottate hanno avuto successo nel mitigare i rischi identificati inizialmente.

Raccomandazioni Finali:

- È essenziale continuare con regolari scansioni di sicurezza per identificare e mitigare nuove vulnerabilità che potrebbero emergere a seguito di aggiornamenti di sistema o nuovi attacchi.
- Mantenere e aggiornare le politiche di sicurezza per assicurare che tutti i servizi e software siano configurati correttamente secondo le best practice di sicurezza.

Queste conclusioni riflettono l'efficacia delle azioni intraprese e sottolineano l'importanza di monitorare continuamente la sicurezza del sistema per prevenire futuri exploit.