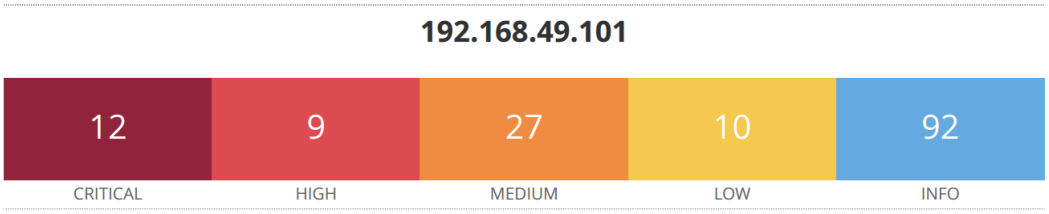
REPORT

Traccia:

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo). A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web. Gli obiettivi dell'esercizio sono:
- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Le vulnerabilità emerse dalla scansione sono numerose ,come si vede nella foto sottostante, e sono classificate per criticità. Per rendere il lavoro più breve verranno elencate solo le vulnerabilità "critical" ovvero quelle più rischiose.



Vulnerabilities Total: 150

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	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	9.8	-	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*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Nell’immagine allegata possiamo vedere quali sono le vulnerabilità “CRITICAL” rilevate da Nessus. Ad ognuna di esse verrà affiancata una descrizione.

Apache PHP-CGI Remote Code Execution

L'installazione di PHP sul server web remoto contiene una falla che potrebbe consentire a un attaccante remoto di passare gli argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Questo potrebbe essere sfruttato per eseguire codice arbitrario, rivelare il codice sorgente PHP, causare un arresto anomalo del sistema, e altro.

Apache Tomcat AJP Connector Request Injection (Ghostcat)

È stata individuata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere file dell'applicazione web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta caricamenti di file, un attaccante potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione remota di codice (RCE).

Bind Shell Backdoor Detection

Uno shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarlo collegandosi alla porta remota e inviando comandi direttamente.

SSL Version 2 and 3 Protocol Detection

Il servizio remoto accetta connessioni criptate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diverse falle crittografiche, tra cui:

- Uno schema di padding non sicuro con cifrari CBC.
- Schemi di rinegoziazione e ripresa di sessione non sicuri.

phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)

Secondo il numero di versione auto-riferito, l'applicazione phpMyAdmin ospitata sul server web remoto è precedente alla versione 4.8.6. Pertanto, è soggetta a una vulnerabilità di SQL injection (SQLi) che si verifica nella funzionalità del designer di phpMyAdmin. Un attaccante remoto non autenticato può sfruttare ciò per iniettare manipolare query SQL nel database di backend, con conseguente divulgazione o manipolazione di dati arbitrari.

Apache Tomcat SEoL (<= 5.5.x)

Secondo la sua versione, Apache Tomcat è inferiore o uguale alla versione 5.5.x. Di conseguenza, non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza ed è consigliabile aggiornare a una versione più recente di Tomcat per garantire la sicurezza del sistema.

Unix Operating System Unsupported Version Detection

Secondo il numero di versione auto-dichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza. È consigliabile aggiornare il sistema operativo a una versione più recente o migrare a un sistema operativo supportato per garantire la sicurezza del sistema.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Il certificato SSH remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.Il problema è causato dalla rimozione da parte di un pacchettizzatore Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL.Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man-in-the-middle.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Il certificato X.509 remoto sul server SSL è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è causato dalla rimozione, da parte di un pacchettizzatore Debian, di quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man-in-the-middle.

NFS Exported Share Information Disclosure

La condivisione NFS esportata dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare ciò per leggere (e eventualmente scrivere) file sull'host remoto.

UnrealIRCd Backdoor Detection

Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un attaccante di eseguire codice arbitrario sull'host interessato.
Come soluzione riscarica il software, verificalo utilizzando i checksum MD5 / SHA1 pubblicati e reinstallalo.

VNC Server 'password' Password

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare l'accesso utilizzando l'autenticazione VNC e una password di 'password'. Un attaccante remoto non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Per proteggere il servizio VNC, è necessario utilizzare una password robusta.