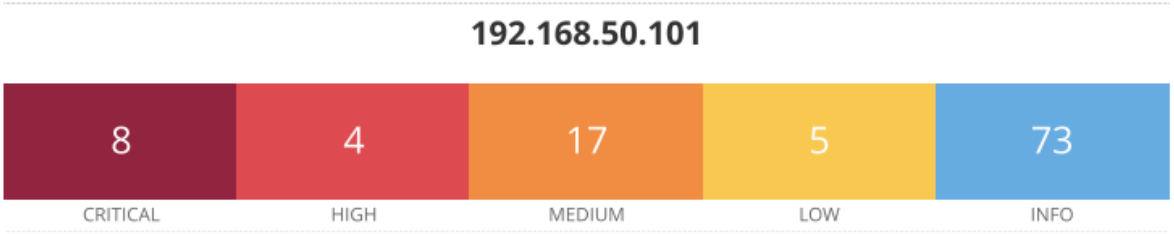
Esercizio 23-02

Traccia: si effettui un Vulnerability scan usando Metasploitable come target. Con i risultati si producano 3 report: 1 per manager, 1 per tecnico informatico e 1 completo per studio personale.

Report Manager

Il Vulnerability Assessment eseguito dallo scanner Nessus ha evidenziato queste vulnerabilità



Vulnerabilities Total: 107

SEVERITY	CVSS V3.0	PLUGIN	NAME
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	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*	61708	VNC Server 'password' Password
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability

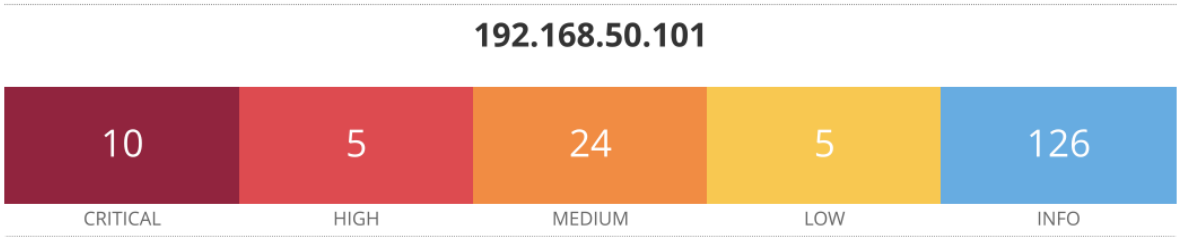
Si consiglia di cominciare a lavorare da subito sulla risoluzione delle vulnerabilità di livello critico, per poi passare a quelle di livello alto e così via. Ripeteremo la scansione quando tutte le vulnerabilità critiche verranno sistemate.

Il Vostro tecnico informatico ha ricevuto un report con specifiche tecniche e soluzioni consigliate per ogni vulnerabilità trovata.

Resto a disposizione per qualsiasi chiarimento. Cordiali saluti

Report per tecnico

Queste sono le vulnerabilità trovate con la scansione di Nessus



Tra le quelle di livello più alto abbiamo:

1. 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)
2. 51988 - Bind Shell Backdoor Detection
3. 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
4. 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
5. 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
6. 11356 - NFS Exported Share Information Disclosure
7. 20007 - SSL Version 2 and 3 Protocol Detection
8. 20007 - SSL Version 2 and 3 Protocol Detection
9. 33850 - Unix Operating System Unsupported Version Detection
10. 61708 - VNC Server 'password' Password
11. 136769 - ISC BIND Service Downgrade / Reflected DoS
12. 42256 - NFS Shares World Readable
13. 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
14. 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
15. 90509 - Samba Badlock Vulnerability

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat) - rischio Critico
Sintesi
C'è un connettore AJP vulnerabile in ascolto sull'host remoto.
Descrizione
Un attaccante potrebbe approfittare di un server vulnerabile per fare upload di file malevoli per ottenere la possibilità di eseguire codice da remoto.
Soluzione
Aggiornare la configurazione di AJP per ottenere autorizzazione e/o aggiornare il Tomcat alla versione 7.0.100, 8.5.51, 9.0.31.

51988 - Bind Shell Backdoor Detection - rischio Critico
Sintesi
L'host remoto potrebbere esser stato compromesso.
Descrizione
Una shell è in ascolto sulla porta remota senza alcuna autorizzazione concessa. Un attaccante potrebbe usarla per connettersi alla porta remota e inviare direttamente comandi.
Soluzione
Verificare se l'host remoto è stato compromesso, e se necessario reinstallare il sistema.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness - rischio Critico
Sintesi
Le chiavi di crittografia dell'host SSH remoto sono deboli:
Descrizione
La chiavi di crittografia dell'host SSH remoto sono state generate da un sistema Debian o Ubuntu con un bug nella generazione randomica di numeri della propria libreria OpenSSL.
Soluzione
Considerare che tutto il materiale crittografato generato dall'host remoto è deducibile. In particolare, tutti i materiali crittografati SSH, SSL e OpenVPN dovrebbero essere rigenerati.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) - rischio Critico
Sintesi
Le chiavi di crittografia dell'host SSH remoto sono deboli:
Descrizione
La chiavi di crittografia dell'host SSH remoto sono state generate da un sistema Debian o Ubuntu con un bug nella generazione randomica di numeri della propria libreria OpenSSL.
Soluzione
Considerare che tutto il materiale crittografato generato dall'host remoto è deducibile. In particolare, tutti i materiali crittografati SSH, SSL e OpenVPN dovrebbero essere rigenerati.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) - rischio Critico
Sintesi
Le chiavi di crittografia dell'host SSH remoto sono deboli:
Descrizione
La chiavi di crittografia dell'host SSH remoto sono state generate da un sistema Debian o Ubuntu con un bug nella generazione randomica di numeri della propria libreria OpenSSL.
Soluzione
Considerare che tutto il materiale crittografato generato dall'host remoto è deducibile. In particolare, tutti i materiali crittografati SSH, SSL e OpenVPN dovrebbero essere rigenerati.

11356 - NFS Exported Share Information Disclosure- rischio Critico
Sintesi
È possibile accedere alle condivisioni NFS dall'host remoto.
Descrizione
Almeno una delle condivisioni NFS esportate dal server remoto potrebbero essere intercettate da uno scanner. Un attaccante potrebbe approfittarne per leggere (e possibilmente scrivere) file da remoto.
Soluzione
Configurare NFS sull'host remoto così che solo gli host autorizzati possano vedere le condivisioni remote..

20007 - SSL Version 2 and 3 Protocol Detection - rischio Critico
Sintesi
Le versione SSL 2.0 /3.0, dalle quali il servizio remoto accetta le connessioni, hanno numerose falle.
Descrizione
Una shell è in ascolto sulla porta remota senza alcuna autorizzazione concessa. Un attaccante potrebbe usarla per connettersi alla porta remota e inviare direttamente comandi.
Soluzione
Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.
Usare invece TLS 1.2 o superiore

20007 - SSL Version 2 and 3 Protocol Detection - rischio Critico
Sintesi
Le versione SSL 2.0 /3.0, dalle quali il servizio remoto accetta le connessioni, hanno numerose falle.
Descrizione
Una shell è in ascolto sulla porta remota senza alcuna autorizzazione concessa. Un attaccante potrebbe usarla per connettersi alla porta remota e inviare direttamente comandi.
Soluzione
Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.
Usare invece TLS 1.2 o superiore

33850 - Unix Operating System Unsupported Version Detection - rischio Critico
Sintesi
Il sistema operativo in esecuzione sull'host remoto non è più supportato.
Descrizione
Il sistema operativo funzionante sull'host remoto non è più supportato. Mancanza di supporto significa che il venditore non provvederà più a rilasciare pacth per la sicurezza del sistema, questo comporterà delle vulnerabilità nel corso del tempo.
Soluzione
Aggiornare il sistema operativo a una versione che è attualmente supportata.

61708 - VNC Server 'password' Password - rischio Critico
Sintesi
Un server VNC in esecuzione sull'host remoto è protetto da una password debole.
Descrizione
Un attaccante remoto potrebbe sfruttare questa debolezza per prendere il controllo del sistema
Soluzione
Mettere in sicurezza il server VNC con una password forte.

136769 - ISC BIND Service Downgrade / Reflected DoS - rischio Alto
Sintesi
Il nome del server remoto è affetto da vulnerabilità Service Downgrade/Reflected DoS.
Descrizione
Un attaccante non autorizzato potrebbe usare questa debolezza per degradare il servizio del server o per usare il server come un riflettore per attacchi riflessi.
Soluzione
Aggiornare ISC BIND alla versione a indicata dal venditore.

42256 - NFS Shares World Readable - rischio Alto
Sintesi
Il server NFS remoto esporta condivisioni mondialmente leggibili.
Descrizione
Il server NFS sta esportando una o più condivisioni senza nessuna restrizione degli accessi (basata su hostname, IP, o range di IP).
Soluzione
Apportare le opportune restrizioni a tutte le condivisioni NFS.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) - rischio Alto
Sintesi
Il servizio remoto supporta l'utilizzo di cifratori SSL di livello medio.
Descrizione
È considerevolmente più semplice raggirare criptazioni di livello medio se l'attaccante si trova nella stessa rete fisica.
Soluzione
Riconfigurare l'applicazione affetta se è possibile evitare l'utilizzo di cifratori di medio livello.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) - rischio Alto
Sintesi
Il servizio remoto supporta l'utilizzo di cifratori SSL di livello medio.
Descrizione
È considerevolmente più semplice raggirare criptazioni di livello medio se l'attaccante si trova nella stessa rete fisica.
Soluzione
Riconfigurare l'applicazione affetta se è possibile evitare l'utilizzo di cifratori di medio livello.

90509 - Samba Badlock Vulnerability - rischio Alto
Sintesi
Il server SMB in esecuzione sull'host remoto è affetta da Badlock vulnerability.
Descrizione
Un man-in-the-middle potrebbe intercettare il traffico tra host e server e downgradare il livello di autenticazione, che gli permetterebbe di vedere e modificare dati della sicurezza sensibili nella Active Directory (AD).
Soluzione
Aggiornare Samba alle versioni 4.2.11 / 4.3.8 / 4.4.2 o superiori.

11213 - HTTP TRACE / TRACK Methods Allowed - rischio Medio
Sintesi
Funzioni di debug sono abilitate sul web server remoto.
Descrizione
Il web server remoto supporta i metodi TRACE e/o TRACK. Questi sono metodi HTTP usati per debug connessioni web server.
Soluzione
Disabilitare questi metodi HTTP.

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS - rischio Medio
Sintesi
Il nome del server remoto è affetto da una vulnerabilità di negazione del servizio.
Descrizione
Un attaccante potrebbe riuscire a triggerare il server e causarne la chiusare.
Soluzione
Aggiornare BIND alle versioni 9.11.22, 9.16.6, 9.17.4 o superiori.

136808 - ISC BIND Denial of Service - rischio Medio
Sintesi
Il nome del server remoto è affetto da una vulnerabilità di fallimento di asserzione.
Descrizione
Un attaccante non autorizzato, utilizzando un messaggio costruito appositamente, potrebbe causare la cessazione di risposta dei servizi.
Soluzione
Aggiornare BIND alla versione più recente

57608 - SMB Signing not required - rischio Medio
Sintesi
Non è richiesta registrazione sul server remoto SMB.
Descrizione
Un attaccante non autorizzato potrebbe condurre un attacco man-in-the-middle contro il server SMB.
Soluzione
Rinforza il messaggio di registrazione nella configurazione dell'host.

52611 - SMTP Service STARTTLS Plaintext Command Injection - rischio Medio
Sintesi
Il servizio remoto di mail permette l'immissione di comandi testuali durante lo stabilimento di un canale di comunicazioni.
Descrizione
Un attaccante non autorizzato potrebbe far partire comandi durante la fase di protocollo che verrà eseguita durante la fase di cifratura testuale
Soluzione
Contattare il venditore per scoprire se è disponibile una versione aggiornata di SMTP.