REPORT TECNICO

FACCILONGO DOMENICO

# NESSUS: VULNERABILITY ASSESSMENT METASPOITABLE

METASPOITABLE IP: 192.168.50.101

VULNERABILITIES TROVATE:

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 9 | 5 | 24 | 5 | 122 |

SCAN INFORMATION:

| | |
|---|---|
| Start Time: | 24/11/2022 h.14:50 |
| End Time: | 24/11/2022 h.15:17 |

HOST INFORMATION:

| | |
|---|---|
| Netbios Name: | METASPOITABLE |
| IP: | 192.168.50.101 |
| MAC Address: | 08:00:27:7B:21:1D |
| OS: | Linux Kernel 2.6 on Ubuntu 8.04 (hardy) |

# VULNERABILITIES CRITICAL

## 51988 - Bind Shell Backdoor Detection

*Synopsis:*

L'host remoto potrebbe essere stato compromesso.

*Description:*

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato potrebbe utilizzarlo collegandosi alla porta e inviando comandi diretti.

*Soluzione:*

Verifica se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

## 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

*Synopsis:*

Le chiavi dell'host SSH remoto sono deboli.

*Description:*

La chiave dell'host SSH remoto è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sui libreria OpenSSL.

*Soluzione:*

Considerare criptografato tutto il materiale generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

## 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Port tcp/25/smtp

*Synopsis:*

Il certificato SSL remoto utilizza una chiave debole.

*Description:*

Il certificato x509 (formato standard per certificati a chiave pubblica) sul server SSL remoto è stato generato su un sistema Debian o Ubuntuche contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato potrebbe facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o organizzare un attacco man in the middle.

*Soluzione:*

Considerare criptografato tutto il materiale generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

## 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Port tcp/5432/postgresql

*Synopsis:*

Il certificato SSL remoto utilizza una chiave debole.

*Description:*

Il certificato x509 (formato standard per certificati a chiave pubblica) sul server SSL remoto è stato generato su un sistema Debian o Ubuntuche contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato potrebbe facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o organizzare un attacco man in the middle.

*Soluzione:*

Considerare criptografato tutto il materiale generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

## 11356 - NFS Exported Share Information Disclosure

*Synopsis:*

E’ possibile accedere alle condivisioni NFS sull’host remoto.

*Description:*

Almeno una delle condivisoni NFS esportate dal server remoto potrebbe essere montata dall’host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

*Soluzione:*

Configura NFS sull’host remoto in modo che solo gli host autorizzati possano montare le sue condivisone remote.

## 20007 - SSL Version 2 and 3 Protocol Detection

Port tcp/25/smtp

*Synopsis:*

Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.

*Description:*

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

- Uno schema di riempimento non sicuro con cifrari CBC.

- Schemi di rinegoziazione e ripresa delle sessioni non sicure.

Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato ei client. Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supporta nulla di meglio), molti browser web lo implementano in un modo non sicuro che consente a un utente malintenzionato di eseguire il downgrade di una connessione (come in POODLE). Pertanto, si consiglia di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di entrata in vigore trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia avanzata" di PCI SSC.

*Soluzione:*

Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.

Utilizzare invece TLS 1.2 (con pacchetti di crittografia approvati) o versioni successive.

## 20007 - SSL Version 2 and 3 Protocol Detection

Port tcp/5432/postgresql

*Synopsis:*

Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.

*Description:*

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

- Uno schema di riempimento non sicuro con cifrari CBC.

- Schemi di rinegoziazione e ripresa delle sessioni non sicure.

Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato ei client. Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supporta nulla di meglio), molti browser web lo implementano in un modo non sicuro che consente a un utente malintenzionato di eseguire il downgrade di una connessione (come in POODLE). Pertanto, si consiglia di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di entrata in vigore trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia avanzata" di PCI SSC.

*Soluzione:*

Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.

Utilizzare invece TLS 1.2 (con pacchetti di crittografia approvati) o versioni successive.

## 33850 - Unix Operating System Unsupported Version Detection

*Synopsis:*

Il sistema operativo in esecuzione sull'host remoto non è più supportato.

*Description:*

In base al numero di versione auto-riportato, 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.

*Soluzione:*

Aggiorna a una versione del sistema operativo Unix attualmente supportata.

## 61708 - VNC Server 'password' Password

*Synopsis:*

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

*Description:*

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

*Soluzione:*

Proteggi il servizio VNC con una password sicura.

## 61708 - VNC Server 'password' Password

*Synopsis:*

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

*Description:*

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

*Soluzione:*

Proteggi il servizio VNC con una password sicura.

# VULNERABILITIES HIGH

## 136769 - ISC BIND Service Downgrade / Reflected DoS

*Synopsis:*

Il server dei nomi remoto è interessato da vulnerabilità di downgrade del servizio/DoS riflesse.

*Description:*

Secondo la sua versione auto-segnalata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

*Soluzione:*

Aggiornamento alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore.

## 42256 - NFS Shares World Readable

*Synopsis:*

Il server NFS remoto esporta condivisioni leggibili da tutti.

*Description:*

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (basato su nome host, IP o intervallo IP).

*Soluzione:*

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

## 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Port tcp/25/smtp

*Synopsis:*

Il servizio remoto supporta l'uso di crittografie SSL di livello medio.

*Description:*

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio. Nessus considera la forza media come qualsiasi crittografia che utilizzi lunghezze di chiave di almeno 64 bit e inferiori a 112 bit, oppure che utilizzi la suite di crittografia 3DES.

Si noti che è notevolmente più semplice aggirare la crittografia di media potenza se l'attaccante si trova sulla stessa rete fisica.

*Soluzione:*

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature di livello medio.

## 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Port tcp/5432/postgresql

*Synopsis:*

Il servizio remoto supporta l'uso di crittografie SSL di livello medio.

*Description:*

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio. Nessus considera la forza media come qualsiasi crittografia che utilizzi lunghezze di chiave di almeno 64 bit e inferiori a 112 bit, oppure che utilizzi la suite di crittografia 3DES.

Si noti che è notevolmente più semplice aggirare la crittografia di media potenza se l'attaccante si trova sulla stessa rete fisica.

*Soluzione:*

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature di livello medio.

## 90509 - Samba Badlock Vulnerability

*Synopsis:*

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

*Description:*

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD ) a causa di una negoziazione errata del livello di autenticazione sui canali RPC (Remote Procedure Call). Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati sensibili sulla sicurezza nel database di Active Directory (AD) o la disabilitazione di servizi critici.

*Soluzione:*

Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

# VULNERABILITIES MEDIUM

## 11213 - HTTP TRACE / TRACK Methods Allowed

*Synopsis:*

Le funzioni di debug sono abilitate sul server Web remoto.

*Description:*

Il server Web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP utilizzati per eseguire il debug delle connessioni del server Web.

*Soluzione:*

Disattiva questi metodi HTTP. Fare riferimento all'output del plug-in per ulteriori informazioni.

## 139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

*Synopsis:*

Il server dei nomi remoto è affetto da una vulnerabilità Denial of Service.

*Description:*

In base al numero di versione auto-riportato, l'installazione di ISC BIND in esecuzione sul server dei nomi remoto è la versione 9.x precedente alla 9.11.22, 9.12.x precedente alla 9.16.6 o 9.17.x precedente alla 9.17.4. Pertanto, è affetto da una vulnerabilità di negazione del servizio (DoS) a causa di un errore di asserzione durante il tentativo di verificare una risposta troncata a una richiesta firmata da TSIG. Un utente malintenzionato remoto autenticato può sfruttare questo problema inviando una risposta troncata a una richiesta firmata TSIG per attivare un errore di asserzione, causando la chiusura del server.

Si noti che Nessus non ha testato questo problema, ma si è invece basato solo sul numero di versione auto-riportato dell'applicazione.

*Soluzione:*

Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

## 136808 - ISC BIND Denial of Service

*Synopsis:*

Il server dei nomi remoto è interessato da una vulnerabilità di errore di asserzione.

*Description:*

Esiste una vulnerabilità Denial of Service (DoS) nelle versioni ISC BIND 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 e precedenti. Un utente malintenzionato remoto non autenticato può sfruttare questo problema, tramite un messaggio appositamente predisposto, per impedire al servizio di rispondere.

Si noti che Nessus non ha testato questo problema, ma si è invece basato solo sul numero di versione auto-riportato dell'applicazione.

*Soluzione:*

Aggiorna alla versione con patch più strettamente correlata alla tua attuale versione di BIND.

## 57608 - SMB Signing not required

*Synopsis:*

La firma non è richiesta sul server SMB remoto.

*Description:*

La firma non è richiesta sul server SMB remoto. Un utente malintenzionato remoto non autenticato può sfruttarlo per condurre attacchi man-in-the-middle contro il server SMB.

*Soluzione:*

Imponi la firma dei messaggi nella configurazione dell'host. Su Windows, questo si trova nell'impostazione del criterio "Server di rete Microsoft: aggiungi firma digitale alle comunicazioni (sempre)". Su Samba, l'impostazione si chiama "firma del server". Vedere i collegamenti "vedi anche" per ulteriori dettagli.

## 52611 - SMTP Service STARTTLS Plaintext Command Injection

*Synopsis:*

Il servizio di posta remota consente l'inserimento di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato.

*Description:*

Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire a un utente malintenzionato remoto e non autenticato di inserire comandi durante la fase del protocollo di testo in chiaro che verranno eseguiti durante la fase del protocollo di testo cifrato.

Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

*Soluzione:*

Contattare il fornitore per vedere se è disponibile un aggiornamento.

## 90317 - SSH Weak Algorithms Supported

*Synopsis:*

Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo.

*Description:*

Nessus ha rilevato che il server SSH remoto è configurato per utilizzare la cifratura a flusso Arcfour o nessuna cifratura. RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con chiavi deboli.

*Soluzione:*

Contattare il fornitore o consultare la documentazione del prodotto per rimuovere le cifrature deboli.

## 31705 - SSL Anonymous Cipher Suites Supported

*Synopsis:*

Il servizio remoto supporta l'uso di cifrari SSL anonimi.

*Description:*

L'host remoto supporta l'uso di cifrari SSL anonimi. Sebbene ciò consenta a un amministratore di configurare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle.

Nota: questo è molto più facile da sfruttare se l'attaccante si trova sulla stessa rete fisica.

*Soluzione:*

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature deboli.

## 51192 - SSL Certificate Cannot Be Trusted

*Synopsis:*

Il certificato SSL per questo servizio non può essere attendibile.

*Description:*

Il certificato X.509 del server non può essere attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena di fiducia può essere interrotta, come indicato di seguito:

- In primo luogo, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica nota. Ciò può verificarsi quando la parte superiore della catena è un certificato autofirmato non riconosciuto o quando mancano certificati intermedi che collegherebbero la parte superiore della catena di certificati a un'autorità di certificazione pubblica nota. - In secondo luogo, la catena di certificati potrebbe contenere un certificato non valido al momento della scansione. Ciò può verificarsi quando la scansione avviene prima di una delle date "notBefore" del certificato o dopo una delle date "notAfter" del certificato

- In terzo luogo, la catena di certificati potrebbe contenere una firma che non corrispondeva alle informazioni del certificato o che non poteva essere verificata. Le firme errate possono essere corrette facendo firmare nuovamente il certificato con la firma errata dall'emittente. Le firme che non è stato possibile verificare sono il risultato dell'utilizzo da parte dell'emittente del certificato di un algoritmo di firma che Nessus non supporta o non riconosce.

Se l'host remoto è un host pubblico in produzione, qualsiasi interruzione nella catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server web. Ciò potrebbe semplificare l'esecuzione di attacchi man-in-the-middle contro l'host remoto.

*Soluzione:*

Acquista o genera un certificato SSL appropriato per questo servizio.