Scan Iniziale Metasploitable2

Abbiamo effettuato uno scan su l'host di Metasploitable2(192.168.32.105) col Vulnerability Scanner Nessus Essentials dove abbiamo riscontrato numerose vulnerabilità:

10 vulnerabilità critiche ,5 vulnerabilità alte e 24 vulnerabilità medie.

VULNERABILITA' CRITICHE

134862 - Iniezione richiesta connettore Apache Tomcat AJP (Ghostcat)
-
Sinossi
C'è un connettore AJP vulnerabile in ascolto sull'host remoto.
Descrizione
È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JSP (JavaServer Pages) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

51988 - Rilevamento Backdoor Bind Shell
-
Sinossi
L'host remoto potrebbe essere stato compromesso.
Descrizione
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando comandi direttamente.

32314 – Debolezza del generatore di numeri casuali del pacchetto Debian OpenSSH/OpenSSL
-
Sinossi
Le chiavi dell'host SSH remoto sono deboli.
Descrizione
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 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 può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare la decifrazione della sessione remota o impostare un attacco man in the middle.

32321 – Debolezza del generatore di numeri casuali del pacchetto Debian OpenSSH/OpenSSL (verifica SSL) - (viene ripetuta due volte sia per il plugin tcp/5432/postgresql sia per tcp/25/smtp)
-
Sinossi
Il certificato SSL remoto utilizza una chiave debole.
Descrizione
Il certificato x509 remoto sul server SSL 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 dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o organizzare un attacco man in the middle.

11356 - Divulgazione di informazioni sulla condivisione esportata NFS
-
Sinossi
È possibile accedere alle condivisioni NFS sull'host remoto.
Descrizione
Almeno una delle condivisioni 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.

20007 - Rilevamento del protocollo SSL versione 2 e 3 (viene ripetute due volte sia per il plugin tcp/25/smtp sia per il plugin tcp/5432/postgresql)
-
Sinossi
Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.
Descrizione
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 insicuro 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.

33850 - Rilevamento versione non supportata del sistema operativo Unix
-
Sinossi
Il sistema operativo in esecuzione sull'host remoto non è più supportato.
Descrizione
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.

61708 - Password 'password' del server VNC
-
Sinossi
Un server VNC in esecuzione sull'host remoto è protetto da una password debole.
Descrizione
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.

VULNERABILITA' MEDIE

136769 - Downgrade del servizio ISC BIND / DoS riflesso
-
Sinossi
Il server dei nomi remoto è interessato da vulnerabilità di downgrade del servizio/DoS riflesse.
Descrizione

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.

42256 - Condivisioni NFS leggibili in tutto il mondo
-
Sinossi
Il server NFS remoto esporta condivisioni leggibili da tutti.
Descrizione
Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (basato su nome host, IP o intervallo IP).

42873 - Suite di cifratura a media resistenza SSL supportate (SWEET32) (ripetuto due volte per plugin tcp/5432/postgresql e per il plugin tcp/25/smtp)

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

90509 - Vulnerabilità al blocco di Samba -

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

Descrizione

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.

VULNERABILITA' MEDIE

11213 - Metodi HTTP TRACE/TRACK consentiti

-

Sinossi

Le funzioni di debug sono abilitate sul server Web remoto.

Descrizione

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.

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

-

Sinossi

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

Descrizione

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.

136808 - ISC BIND Denial of Service

-

Sinossi

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

Descrizione

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.

57608 - Firma SMB non richiesta

-

Sinossi

La firma non è richiesta sul server SMB remoto.

Descrizione

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.

52611 - Servizio SMTP STARTTLS Iniezione di comandi in testo normale

-

Sinossi

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

Descrizione

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.

90317 - Algoritmi deboli SSH supportati

-

Sinossi

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

Descrizione

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.

31705 - Suite di cifratura anonime SSL supportate

-

Sinossi

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

Descrizione

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.

51192 - Il certificato SSL non può essere considerato attendibile (ripetuta 2 volte per plugin tcp/25/smtp e tcp/5432/postgresql)

Sinossi
Il certificato SSL per questo servizio non può essere attendibile.
Descrizione
Il certificato X.509 del server non può essere attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena della fiducia può essere spezzata, come indicato di seguito:

- Innanzitutto, 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.

15901 - Scadenza certificato SSL (ripetuta 2 volte per plugin tcp/25/smtp e tcp/5432/postgresql)
-
Sinossi
Il certificato SSL del server remoto è già scaduto.
Descrizione
Questo plug-in controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sulla destinazione e segnala se sono già scaduti.

45411 - Certificato SSL con nome host errato (ripetuta 2 volte per plugin tcp/25/smtp e tcp/5432/postgresql)
-
Sinossi
Il certificato SSL per questo servizio è per un host diverso.
Descrizione
L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per una macchina diversa.

89058 - Vulnerabilità dell'attacco SSL DROWN (decrittografia RSA con crittografia obsoleta e indebolita)
-
Sinossi
L'host remoto potrebbe essere interessato da una vulnerabilità che consente a un utente malintenzionato remoto di decrittografare potenzialmente il traffico TLS acquisito.
Descrizione
L'host remoto supporta SSLv2 e pertanto può essere interessato da una vulnerabilità che consente un attacco Oracle di riempimento Bleichenbacher cross-protocol noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione di Secure Sockets Layer Version 2 (SSLv2) e consente la decrittografia del traffico TLS acquisito. Un utente malintenzionato man-in-the-middle può sfruttarlo per decrittografare la connessione TLS utilizzando traffico acquisito in precedenza e crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.

65821 - Suite di cifratura SSL RC4 supportate (Bar Mitzvah) (ripetuta 2 volte per plugin tcp/25/smtp e tcp/5432/postgresql)
-
Sinossi
Il servizio remoto supporta l'uso della cifratura RC4.
Descrizione
L'host remoto supporta l'uso di RC4 in una o più suite di cifratura.
Il cifrario RC4 è imperfetto nella sua generazione di un flusso di byte pseudo-casuale in modo che un'ampia varietà di piccoli pregiudizi venga introdotta nel flusso, diminuendo la sua casualità.

Se il testo in chiaro viene crittografato ripetutamente (ad esempio, i cookie HTTP) e un utente malintenzionato è in grado di ottenere molti (cioè decine di milioni) di testi cifrati, l'attaccante potrebbe essere in grado di derivare il testo in chiaro.

57582 - Certificato autofirmato SSL (ripetuta 2 volte per plugin tcp/25/smtp e tcp/5432/postgresql)
-
Sinossi
La catena di certificati SSL per questo servizio termina con un certificato autofirmato non riconosciuto.
Descrizione
La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se l'host remoto è un host pubblico in produzione, ciò annulla l'uso di SSL poiché chiunque potrebbe stabilire un attacco man-in-the-middle contro l'host remoto.

Tieni presente che questo plug-in non verifica la presenza di catene di certificati che terminano con un certificato non autofirmato, ma firmato da un autore del certificato non riconosciuto

26928 - Suite di cifratura deboli SSL supportate
-
Sinossi
Il servizio remoto supporta l'uso di cifrari SSL deboli.
Descrizione
L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia debole.
Nota: questo è notevolmente più facile da sfruttare se l'attaccante si trova sulla stessa rete fisica

81606 - SSL/TLS EXPORT_RSA <= suite di cifratura a 512 bit supportate (FREAK)
-
Sinossi
L'host remoto supporta una serie di cifrari deboli.
Descrizione
L'host remoto supporta le suite di cifratura EXPORT_RSA con chiavi inferiori o uguali a 512 bit.
Un utente malintenzionato può fattorizzare un modulo RSA a 512 bit in un breve lasso di tempo.

Un utente malintenzionato man-in-the-middle potrebbe essere in grado di eseguire il downgrade della sessione per utilizzare le suite di crittografia EXPORT_RSA (ad esempio CVE-2015-0204).
Pertanto, si consiglia di rimuovere il supporto per le suite di cifratura deboli.

78479 - SSLv3 Padding Oracle su vulnerabilità di crittografia legacy ridotta (POODLE)
(ripetuta 2 volte per plugin tcp/25/smtp e tcp/5432/postgresql)

Sinossi
È possibile ottenere informazioni riservate dall'host remoto con servizi abilitati per SSL/TLS.

Descrizione
L'host remoto è affetto da una vulnerabilità di divulgazione di informazioni man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi crittografati utilizzando cifrari a blocchi in modalità Cipher Block Chaining (CBC).
Gli aggressori MitM possono decrittografare un byte selezionato di un testo cifrato in appena 256 tentativi se sono in grado di forzare un'applicazione vittima a inviare ripetutamente gli stessi dati su connessioni SSL 3.0 appena create.

Finché un client e un servizio supportano entrambi SSLv3, è possibile eseguire il "rollback" di una connessione a SSLv3, anche se TLSv1 o più recente è supportato dal client e dal servizio.

Il meccanismo TLS Fallback SCSV impedisce gli attacchi di "rollback della versione" senza influire sui client legacy; tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. I siti che non possono disabilitare SSLv3 immediatamente dovrebbero abilitare questo meccanismo.

Questa è una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. La disabilitazione di SSLv3 è l'unico modo per mitigare completamente la vulnerabilità.

104743 - Rilevamento protocollo TLS versione 1.0 (ripetuta 2 volte per plugin tcp/25/smtp e tcp/5432/postgresql)
-
Sinossi
Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS.
Descrizione
Il servizio remoto accetta connessioni crittografate tramite TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS come 1.2 e 1.3 sono progettate contro questi difetti e dovrebbero essere utilizzate quando possibile.

A partire dal 31 marzo 2020, gli endpoint non abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser Web e i principali fornitori.

PCI DSS v3.2 richiede che TLS 1.0 sia disabilitato completamente entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti di terminazione SSL/TLS a cui si connettono) che possono essere verificati come non soggetti a exploit noti.