Vulnerabilità Host

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.32.101
MAC Address:	08:00:27:F4:08:97
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

A seguito della scansione effettuata tramite software Nessus sull'host in questione, sono state rilevate: 44 minacce suddivise in:

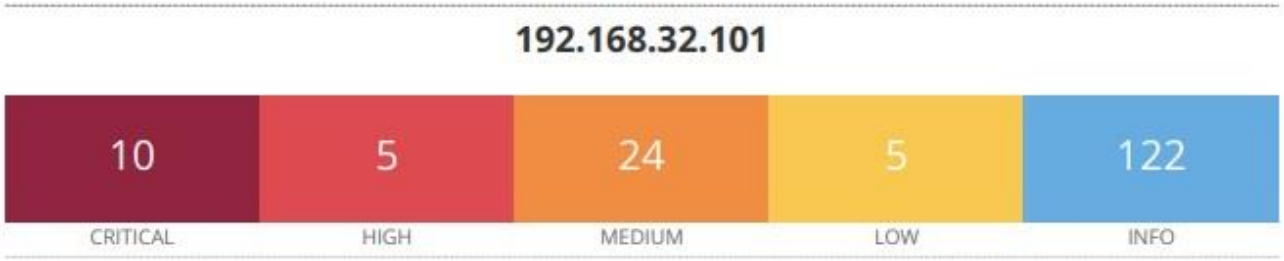
Critica

Alta

Media

Bassa

e 122 Informazioni su applicazioni e servizi.



Orlando Tangari

Minacce di livello critico:

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Sinossi: è presente 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 parametro server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione: Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o versione successiva.

51988 – Bind Shell Backdoor Detection

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 da connessione alla porta remota e invio diretto dei 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

Sinossi: Le chiavi host SSH remote sono deboli.

Descrizione: La chiave host SSH remota 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 al fatto che un pacchetto Debian 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 decifratura della sessione o impostare un uomo nel mezzo attacco.

Soluzione: Considerare decifrabile tutto il materiale crittografico generato sull'host remoto.
In particolare, tutti gli SSH, Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

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

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 al fatto che un pacchetto Debian 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 impostare un uomo nel mezzo attacco.

Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH, il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

11356 - NFS Exported Share Information Disclosure

Sinossi: È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione: Almeno una delle condivisioni NFS esportate dal server remoto può 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.

Soluzioni: Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le proprie condivisioni remote.

20007 - Rilevamento del protocollo SSL versione 2 e 3

Sintassi: 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 affetto da diversi difetti crittografici, tra cui: uno schema di padding insicuro con cifrari CBC, schemi di rinegoziazione e ripresa delle sessioni insicuri. Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client. Sebbene SSL / TLS abbia un mezzo sicuro per scegliere la versione più supportata del protocollo (quindi che queste versioni verranno utilizzate solo se il client o il server non supportano nulla di meglio), molti browser web implementare questa operazione in modo non sicuro che consenta a un utente malintenzionato di eseguire il downgrade di una connessione, ad esempio in POODLE. Pertanto, si consiglia di disabilitare completamente questi protocolli. Soluzione: Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0. Utilizzare invece TLS 1.2 (con suite di crittografia approvate) o superiore.

Minacce di livello alto:

136769 – Servizio ISC BIND Downgrade / Ripercussioni DoS

Sinossi: Il server dei nomi remoto è interessato dalle vulnerabilità di Service Downgrade/Reflected DoS.

Descrizione: Secondo la versione segnalata, l'istanza di ISC BIND 9, in esecuzione sul server remoto è in downgrade di prestazioni e di vulnerabilità DoS. Ciò è dovuto al fatto che BIND DNS non limita un sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Soluzione: Eseguire l'aggiornamento alla versione ISC BIND a cui si fa riferimento nell'advisory del fornitore.

42256 – Condivisioni NFS leggibili in tutto il mondo

Sinossi: Il server remoto NFS è esposto in tutto il mondo

Descrizione: Il server NFS remoto esporta una o più condivisioni senza limitare l'accesso (in base a nome host, IP, o intervallo IP).

Soluzione: Applicare le restrizioni appropriate a tutte le condivisioni NFS.

42873 - Suite di crittografia SSL con supporto a media potenza (SWEET32)

Sintassi: Il servizio remoto supporta l'uso di SSL cifrate di media potenza.

Descrizione: L'host remoto supporta l'uso di crittografie SSL a media potenza. Si consigliano chiave crittografate comprese tra 64 bit e 112 bit, oppure che si utilizzi la suite di crittografia 3DES.

Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di crittografie di media intensità.

Minacce di livello medio:

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 al server Web.

Soluzione: Disattivare questi metodi HTTP.
Fare riferimento all'output del plugin per ulteriori informazioni.

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 interessato da una vulnerabilità ad attacchi di tipo Denial of Service.

Descrizione: In base al numero di versione riportato, l'installazione di ISC BIND in esecuzione sul Server 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. È, quindi, influenzato da una vulnerabilità ad attacchi di tipo DoS, dovuta a un errore di asserzione durante il tentativo di verificare un file troncato in risposta a una richiesta firmata 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.

Soluzione: Aggiornamento BIND 9.11.22, 9.16.6, 9.17.4 o versione successiva.

Minacce di livello basso:

70658 - Crittografia in modalità CBC server SSH abilitata

Sinossi: Il server SSH è configurato per utilizzare il Cipher Block Chaining.

Descrizione: Il server SSH è configurato per supportare la crittografia CBC (Cipher Block Chaining). Ciò potrebbe consentire a un utente malintenzionato di recuperare il messaggio di testo normale dal testo cifrato. Si noti che questo plugin controlla solo le opzioni del server SSH e non controlla le vulnerabilità versioni software.

Soluzione: Consultare la documentazione del prodotto per disabilitare la crittografia dei cifratori in modalità CBC e abilitare la crittografia della modalità di cifratura CTR o GCM.