Nella scansione dell'host richiesto sono stare individuate 12 vulnerabilità critiche che necessitano un'azione immediata per evitare eventuali attacchi ed altre 5 vulnerabilità a rischio alto che vanno anch'esse eliminate successivamente.

192.168.1.103

12	5	23	9	136
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sat Aug 26 11:58:49 2023
End time:	Sat Aug 26 12:23:46 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.1.103
MAC Address:	08:00:27:5C:EF:24
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

Total: 108

SEVERITY	CVSS V3.0	VPR SCORE	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	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
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

- La prima vulnerabilità di lettura/inclusione nel connettore AJP, dove un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare il codice JavaServer Pages (JSP) e ottenere l'esecuzione di codice remoto (RCE). La soluzione consigliata sarebbe quella di aggiornare la configurazione di APJ e aggiornare il server Tomcat a una versione 9.0.31 o successiva.

- La seconda vulnerabilità riguarda la possibile compromissione dell'host remoto tramite una shell in ascolto su una porta remota senza alcuna autorizzazione, la soluzione richiede di verificare un eventuale compromissione e reinstallare il sistema se necessario.

- Abbiamo poi tre vulnerabilità critiche riguardanti le chiavi dell'host SSH remoto deboli. 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 packager Debian ha rimosso 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 attacco man in the middle. Quindi dobbiamo considerare tutto il materiale crittografico generato sull'host remoto facilmente accessibile da un eventuale malintenzionato, in particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

- La sesta vulnerabilità riguarda il remote name resolver (o il server che utilizza a monte) è interessato da una vulnerabilità di avvelenamento della cache DNS. Il remote DNS resolver non utilizza porte casuali quando esegue una richiesta su server DNS di terze parti. Un utente malintenzionato remoto non autenticato può sfruttare questa situazione per avvelenare il server DNS remoto, consentendogli di deviare il traffico legittimo verso siti arbitrari, bisogna quindi contattare il fornitore del server DNS per un aggiornamento di sicurezza che risolva il bug.

- La settima vulnerabilità è dovuta al fatto che è possibile accedere alle condivisioni NFS sull'host remoto. Almeno una delle condivisioni NFS esportate dal server potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) un file sull'host remoto. Per risolvere questa vulnerabilità bisogna configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

- Abbiamo poi due vulnerabilità causate dalla crittografia usata su una risorsa remota che utilizza un protocollo con punti deboli noti. 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 sicuri.
  Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i clienti.
  Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più alta supportata del protocollo (queste versioni verranno utilizzate solo se il client o il server non supportano niente 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 disattivare completamente questi protocolli.
  Il NIST "National Institute of Standards and Technology" ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. La soluzione è quella di consultare la documentazione del

servizio per disattivare SSL 2.0 e 3.0 ed utilizzare invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

- La decima vulnerabilità con rischio 10 è causata dal sistema operativo in esecuzione sull'host remoto che non è più supportato. Il numero di versione del sistema operativo Unix in esecuzione sull'host remoto non è più supportato; la mancanza di supporto implica che il fornitore non rilascerà alcuna nuova patch di sicurezza per il prodotto e di conseguenza, è probabile che contenga vulnerabilità di sicurezza. Bisogna quindi eseguire l'upgrade a una versione del sistema operativo Unix attualmente supportata.

- L'undicesima vulnerabilità con rischio 10 è causata da un server VNC in esecuzione sull'host remoto protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema. La soluzione è quindi proteggere il servizio VNC con una password complessa.

Abbiamo poi 5 vulnerabilità a rischio alto che necessitano un intervento dopo aver risolto quelle critiche.

- La prima vulenrabilità ad alto 8,6 rischio riguarda il server dei nomi remoto DNS che è interessato da vulnerabilità di downgrade del servizio/DoS riflesso. Secondo la versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesso. 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 può sfruttare questa situazione per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione. La soluzione è aggiornare alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore

- La seconda e terza vulnerabilità a rischio alto 7,5 riguardano il servizio remoto che supporta l'uso di crittografie SSL di media potenza, l'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio (utilizza chiavi di lunghezza compresa tra almeno 64 bit e meno di 112 bit, oppure che utilizza la suite di crittografia 3DES). Bisogna considerare che è molto più semplice eludere la crittografia di livello medio se l'aggressore si trova sulla stessa rete; per questo bisogna ,se possibile, riconfigurare l'applicazione interessata per evitare l'uso di crittografie di media complessità.

- La quarta vulnerabilità ad alto rischio 7,5 è causata da un server SMB in esecuzione sull'host remoto che è interessato dalla vulnerabilità Badlock. 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 impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato 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 visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici. È quindi necessario aggiornare Samba ad una versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

- La quinta è dovuta al server NFS remoto che esporta condivisioni leggibili da tutto il mondo; questo sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP, o intervallo IP). Si devono posizionare le opportune restrizioni su tutte le condivisioni NFS per risolvere la vulnerabilità.

Ci sono poi le vulnerabilità a rischio medio che richiedono un intervento dopo aver risolto prima le altre vulnerabilità.

- Il server DNS remoto è vulnerabile agli attacchi di snooping della cache. Il server DNS remoto risponde alle query per domini di terze parti su cui non è impostato il bit di ricorsione. Ciò potrebbe consentire a un utente malintenzionato remoto di determinare quali domini sono stati risolti di recente tramite questo server dei nomi e quindi quali host sono stati visitati di recente. Nota: se si tratta di un server DNS interno non accessibile alle reti esterne, gli attacchi sarebbero limitati alla rete interna. Ciò può includere dipendenti, consulenti e potenzialmente utenti su una rete ospite o connessione WiFi, se supportata. Contattare il fornitore del software DNS per una correzione.

  Le funzioni di debug sono abilitate sul server Web remoto.
- 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. Disabilita questi metodi HTTP. Fare riferimento all'output del plugin per ulteriori informazioni. Il server dei nomi remoto è interessato da una vulnerabilità di tipo Denial of Service. Secondo il numero di versione 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. È pertanto affetto da una vulnerabilità di tipo Denial of Service (DoS) dovuta a un errore di asserzione durante il tentativo di verificare una risposta troncata 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 l'uscita del server. Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.
- Il server dei nomi remoto è interessato da una vulnerabilità legata all'errore di asserzione. Esiste una vulnerabilità Denial of Service (DoS) nelle versioni ISC BIND 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 - 9.17.1 e precedenti. Un utente malintenzionato remoto non autenticato può sfruttare questo problema, tramite un messaggio appositamente predisposto, per impedire al servizio di rispondere. Esegui l'upgrade alla versione con patch più strettamente correlata alla versione corrente di BIND.
- La firma non è richiesta sul server SMB remoto. Un utente malintenzionato remoto non autenticato può sfruttare questa situazione per condurre attacchi man-in-the-middle contro il server SMB. Applica la firma dei messaggi nella configurazione dell'host. Su Windows, questo si trova nell'impostazione del criterio "Server di rete Microsoft: firma digitale alle comunicazioni (sempre)". Su Samba l'impostazione si chiama "firma del server".
- Il servizio di posta remoto consente l'inserimento di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato. 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 in chiaro che verrà eseguito durante la fase del protocollo del 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. Contattare il fornitore per verificare se è disponibile un aggiornamento.
- Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo. Abbiamo rilevato che il server SSH remoto è configurato per utilizzare la crittografia a flusso Arcfour o nessuna crittografia. RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con le chiavi deboli. Contattare il fornitore o consultare la documentazione del prodotto per rimuovere le cifre deboli.

- Il servizio remoto supporta l'uso di crittografie SSL anonime. L'host remoto supporta l'uso di crittografie SSL anonime. Mentre ciò consente a un amministratore di configurare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per farlo verificare l'identità dell'host remoto e rendere il servizio vulnerabile a un attacco man-in-the-middle. Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di codici deboli.
- Il certificato SSL per questo servizio non può essere considerato attendibile. Il certificato X.509 del server non può essere considerato 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 una pubblica autorità di certificazione. Ciò può verificarsi quando il vertice della catena è un utente non riconosciuto e autofirmato certificato 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 corrisponde alle informazioni del certificato o che non può essere verificata. Le firme errate possono essere risolte facendo sì che il certificato con la firma errata venga firmato nuovamente dall'emittente. 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 rendere più semplice l’esecuzione di attacchi man-in-the-middle contro l’host remoto. Acquista o genera un certificato SSL adeguato per questo servizio.

- Il certificato SSL del server remoto è già scaduto. Questo plugin controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sulla destinazione e segnala se qualcuno è già scaduto. Acquista o genera un nuovo certificato SSL per sostituire quello esistente.
- Il certificato SSL per questo servizio è per un host diverso. L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per una macchina diversa. Acquista o genera un certificato SSL adeguato per questo servizio.
- L'host remoto potrebbe essere interessato da una vulnerabilità che consente a un utente malintenzionato remoto di decrittografare potenzialmente il traffico TLS catturato. L'host remoto supporta SSLv2 e pertanto potrebbe essere interessato da una vulnerabilità che consente un attacco Oracle di riempimento di Bleichenbacher tra protocolli noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione Secure Sockets Layer Versione 2 (SSLv2) e consente di decrittografare il traffico TLS catturato. Un utente malintenzionato può sfruttare questa situazione per decrittografare la connessione TLS utilizzando il traffico precedentemente catturato e la crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata. Disabilita SSLv2 e le suite di crittografia di livello di esportazione. Assicurati che le chiavi private non vengano utilizzate da nessuna parte con software server che supporti le connessioni SSLv2.
- Il servizio remoto supporta l'utilizzo della cifratura RC4. L'host remoto supporta l'utilizzo di RC4 in uno o più pacchetti di crittografia. Il codice RC4 è difettoso nella generazione di un flusso di byte pseudo-casuale, per cui nel flusso viene introdotta un'ampia varietà di piccoli errori, diminuendone la casualità. Se il testo in chiaro viene crittografato ripetutamente (ad esempio, cookie HTTP) e un utente malintenzionato è in grado di ottenere molti testi cifrati (ad esempio decine di milioni), l'utente malintenzionato potrebbe essere in grado di derivare il testo in chiaro. Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso delle crittografie RC4. Prendi in

considerazione l'utilizzo di TLS 1.2 con le suite AES-GCM soggette al supporto di browser e server Web.

- La catena di certificati SSL per questo servizio termina con un certificato autofirmato non riconosciuto. 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 plugin non controlla le catene di certificati che terminano con un certificato non autofirmato, ma firmato da un'autorità di certificazione non riconosciuta. Acquista o genera un certificato SSL adeguato per questo servizio.

- Il servizio remoto supporta l'uso di crittografie SSL deboli.L'host remoto supporta l'uso di codici SSL che offrono una crittografia debole. Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di codici deboli. L'host remoto supporta una serie di codici deboli. L'host remoto supporta i pacchetti di crittografia EXPORT_RSA con chiavi inferiori o uguali a 512 bit. Un utente malintenzionato può prendere in considerazione 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 crittografia deboli. Riconfigurare il servizio per rimuovere il supporto per i pacchetti di crittografia EXPORT_RSA.
- Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.0. TLS 1.0 presenta numerosi 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 che non sono 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 completamente disabilitato entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti terminali SSL/TLS a cui si connettono) che possono essere verificati come non suscettibili ad eventuali exploit noti. Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.