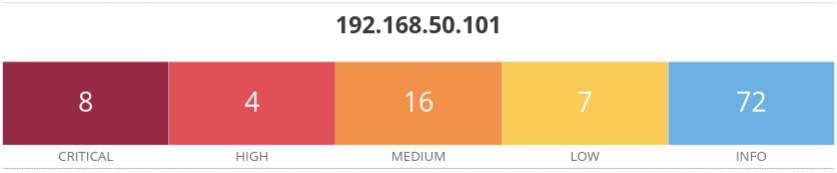
Report vulnerabilità Metasploitable Zanini Riccardo

La presente presentazione riassume i risultati di una scansione delle vulnerabilità effettuata sulla macchina "Metasploitable" utilizzando lo strumento Nessus. Lo scopo di questa scansione è identificare e mitigare potenziali minacce alla sicurezza del sistema.

In questa analisi, le vulnerabilità individuate, i relativi miglioramenti e i potenziali danni sono stati valutati sulla base di ricerche condotte sul web. Ciò è dovuto alla mancanza di competenze specifiche non ancora specifiche per una valutazione autonoma. <3

Il totale delle vulnerabilità riscontrate è di seguito riportate:

- 8 vulnerabilità critiche
- 4 vulnerabilità alte
- 16 vulnerabilità medie
- 7 vulnerabilità balle



Di seguito ci focalizzeremo sulla risoluzione di 2 vulnerabilità per ciacun gruppo.

Analisi Vulnerabilità critiche:

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Vulnerabilità 1 (plugin 61708)

Descrizione: VCN Server “password” Password

Impatto:

- Accesso non autorizzato: Se il server VNC non è configurato correttamente, malintenzionati potrebbero accedervi e controllare il computer da remoto.

- Intercettazione dei dati: Le informazioni trasmesse tra il server e il client VNC potrebbero essere intercettate e violate se non viene utilizzata una connessione crittografata.

- Malware: I server VNC vulnerabili possono essere utilizzati per diffondere malware sul computer remoto.
- Attacchi Denial-of-Service (DoS): Un server VNC potrebbe essere sovraccaricato da richieste, rendendolo inaccessibile agli utenti legittimi.

Rimedi:

- Utilizzare password forti e autenticazione a due fattori.

- Crittografare le connessioni VNC con SSL/TLS.
- Mantenere aggiornato il software VNC.

Vulnerabilità 2 (plugin 33850)

Descrizione: Unix Operation System Unsupported Version Detection

Impatto:

- Mancanza di aggiornamenti di sicurezza: Il rischio più significativo è la mancanza di aggiornamenti di sicurezza. Una volta che un sistema operativo raggiunge la fine del suo ciclo di vita, il fornitore non rilascia più patch per le vulnerabilità di sicurezza. Questo significa che i sistemi obsoleti sono molto più vulnerabili a malware, attacchi informatici e altre minacce online.

- Problemi di compatibilità: Con il progredire della tecnologia, software e hardware nuovi potrebbero non essere compatibili con i sistemi operativi obsoleti. Questo può causare problemi di funzionalità e impedire l'utilizzo di software e hardware moderni.

- Riduzione del supporto da parte dei fornitori: Una volta che un sistema operativo non è più supportato, diventa difficile ottenere assistenza dal fornitore. Questo può rendere più difficile la risoluzione di problemi e la gestione del sistema.

Rimedi:

- Aggiornare a un sistema operativo supportato: L'opzione migliore è quella di aggiornare a un sistema operativo supportato. Questo eliminerà tutti i rischi associati all'utilizzo di un sistema obsoleto.

- Eseguire la scansione del sistema per le vulnerabilità: Se non è possibile aggiornare immediatamente, è importante eseguire regolarmente la scansione del sistema per le vulnerabilità e applicare tutte le patch disponibili.

- Segmentare la rete: È possibile ridurre il rischio di attacchi isolando il sistema operativo non supportato dal resto della rete.

Analisi Vulnerabilità alte:

HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability

Vulnerabilità 1 (plugin 42256)

Descrizione: NFS Shares World Readable

Impatto:

- Accesso non autorizzato: Se le condivisioni NFS sono accessibili in lettura a tutti, chiunque sulla rete può accedere ai file e alle cartelle memorizzati su di esse. Questo può portare a furti di dati, perdita di informazioni sensibili e persino danni al sistema.
- Malware: Gli utenti malintenzionati possono caricare malware sulle condivisioni NFS accessibili in lettura a tutti. Questo malware può quindi diffondersi ad altri sistemi sulla rete, causando seri danni.
- Attacchi di denial-of-service: Le condivisioni NFS accessibili in lettura a tutti possono essere utilizzate per lanciare attacchi denial-of-service (DoS). Questi attacchi possono sovraccaricare il server NFS, rendendolo inaccessibile agli utenti legittimi.

Rimedi:

- Limitare l'accesso: Concedere l'accesso alle condivisioni NFS solo agli utenti e ai gruppi che ne hanno bisogno. Evitare di rendere le condivisioni accessibili in lettura a tutti.
- Utilizzare autenticazione e autorizzazione: Utilizzare un meccanismo di autenticazione e autorizzazione per controllare chi può accedere alle condivisioni NFS e quali azioni può eseguire.
- Crittografare i dati: Crittografare i dati in transito e a riposo per proteggerli da accessi non autorizzati.

Vulnerabilità 2 (plugin 136769)

Descrizione: ISC BIND Service downgrade

Impatto:

- Vulnerabilità note: Le versioni precedenti di BIND potrebbero contenere vulnerabilità note che sono state corrette nelle versioni più recenti. L'esecuzione del downgrade a una versione precedente significa esporre il sistema a queste vulnerabilità, che potrebbero essere sfruttate da malintenzionati per compromettere il sistema.
- Instabilità e malfunzionamenti: Le versioni precedenti di BIND potrebbero essere instabili o presentare malfunzionamenti che non sono presenti nelle versioni più recenti. Ciò può causare interruzioni del servizio DNS e altri problemi.
- Mancanza di supporto: Il fornitore potrebbe non fornire più supporto per le versioni precedenti di BIND. Ciò significa che potrebbe essere difficile ottenere assistenza per risolvere problemi o per ottenere patch per le vulnerabilità.

Rimedi:

- Aggiornare a una versione recente: L'opzione migliore è quella di aggiornare a una versione recente e supportata di BIND. Ciò garantirà che il sistema sia protetto dalle ultime vulnerabilità e che funzioni correttamente con software moderno.
- Valutare attentamente la necessità di un downgrade: Prima di eseguire il downgrade di BIND, è importante valutare attentamente la necessità di farlo. In molti casi, non è necessario eseguire il downgrade e i rischi associati al downgrade potrebbero superare i benefici.
- Se necessario eseguire il downgrade, utilizzare la versione più recente possibile: Se è assolutamente necessario eseguire il downgrade di BIND, utilizzare la versione più recente possibile. Ciò ridurrà il rischio di esporre il sistema a vulnerabilità note.

Analisi Vulnerabilità medie:

MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Vulnerabilità 1 (plugin 57582)

Descrizione: SSL Certificate Cannot Be Trusted

Impatto:

- Certificato scaduto: Un certificato SSL ha una data di scadenza. Se il certificato è scaduto, il browser non lo considererà più valido.

- Certificato non valido: Il certificato SSL potrebbe non essere valido per il nome di dominio del sito web.

- Certificato non firmato da un'autorità di certificazione (CA) affidabile: Il certificato SSL deve essere firmato da una CA fidata affinché il browser lo consideri valido.

Rimedi:

- Aggiornare il certificato SSL: Se il certificato è scaduto, è necessario aggiornarlo con un nuovo certificato valido.
- Assicurarsi che il certificato SSL sia valido per il nome di dominio del sito web: Il certificato SSL deve essere

valido per il nome di dominio del sito web a cui si sta accedendo.

Vulnerabilità 2 (plugin 104743)

Descrizione: TSL Version 1.0 Protocol detenction

Impatto:

Attacco di downgrade: Un malintenzionato potrebbe forzare il browser a utilizzare TSL 1.0 anziché una versione più recente e sicura del protocollo. Ciò potrebbe consentire all'attaccante di intercettare e decifrare le comunicazioni tra il browser e il server.

Attacco di downgrade di TLS 1.2: Un malintenzionato potrebbe utilizzare una tecnica nota come "downgrade di TLS 1.2" per forzare il browser a utilizzare TSL 1.0 anziché TLS 1.2. Ciò potrebbe consentire all'attaccante di sfruttare le vulnerabilità note di TSL 1.0.

Attacco BEAST: L'attacco BEAST (Browser Exploit Against SSL/TLS) sfrutta una vulnerabilità di TSL 1.0 per rubare i cookie di sessione utente. I cookie di sessione possono essere utilizzati per accedere agli account utente senza la loro conoscenza o autorizzazione.

Rimedi:

Aggiornare il software del server web e del client: Assicurarsi che il software del server web e del client sia aggiornato all'ultima versione. Le versioni più recenti del software supportano TSL 1.2 e TSL 1.3 e disabilitano per impostazione predefinita TSL 1.0.

Disabilitare TSL 1.0 sul server web: È possibile disabilitare TSL 1.0 sul server web configurando il server web per accettare solo connessioni TSL 1.2 o versioni successive.

Utilizzare un firewall per bloccare le connessioni TSL 1.0: È possibile utilizzare un firewall per bloccare le connessioni TSL 1.0 in ingresso e in uscita.

Analisi Vulnerabilità basse:

LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection

Vulnerabilità 1 (plugin 70658)

Descrizione: SSH Server CBC Mode Chiper Enabled

Impatto:

- Attacco Oracle di padding: Questo attacco sfrutta un'implementazione non corretta del padding CBC per decifrare il testo cifrato. L'attaccante può inviare blocchi di testo cifrato manipolati al server e osservare le risposte per recuperare informazioni sui dati sottostanti.

- Attacco di rolling IV: Questo attacco sfrutta un valore di vettore di inizializzazione (IV) prevedibile o riutilizzato per decifrare più blocchi di testo cifrato. L'attaccante può utilizzare l'IV per collegare i blocchi di testo cifrato e recuperare informazioni sui dati sottostanti.

- Attacco di troncamento: Questo attacco sfrutta un testo cifrato troncato per decifrare i dati rimanenti. L'attaccante può intercettare una trasmissione cifrata e rimuovere alcuni blocchi di testo cifrato prima di inviarlo al server. Il server tenterà di decifrare il testo cifrato troncato, rivelando all'attaccante i dati rimanenti.

Rimedi:

- Utilizzare un metodo di autenticazione aggiuntivo: Oltre alla cifratura, è consigliabile utilizzare un metodo di autenticazione aggiuntivo, come la firma digitale, per garantire l'integrità e l'autenticità dei dati.

- Mantenere il software aggiornato: Assicurarsi che il software SH Server e il software client siano aggiornati all'ultima versione. Le versioni più recenti del software potrebbero includere patch per le vulnerabilità note.