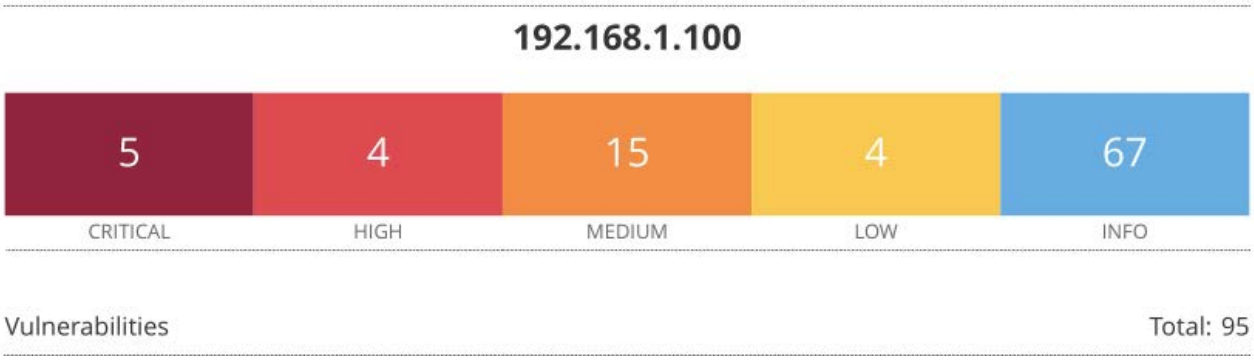
Report vulnerability scan Nessus

Questo report riporta le vulnerabilità critiche rilevate durante la scansione di rete condotta con Nessus. Il report esamina ciascuna vulnerabilità in dettaglio, fornendo informazioni sulla sua natura, il rischio associato e eventuali risorse utili per risolverla.



Sono state rilevate in totale 95 vulnerabilità dalla scansione fatta da Nessus sulla macchina virtuale Metasploitable, di cui 7 sono vulnerabilità critiche.
Tra queste criticità troviamo

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9741	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	0.1994	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1994	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password

La prima vulnerabilità è Apache Tomcat AJP Connector Request Injection (Ghostcat), è molto grave e riguarda Apache Tomcat, un popolare server web open-source.
Questo problema è stato identificato come una potenziale esposizione a attacchi di iniezione di richieste nel connettore AJP (un protocollo usato per la comunicazione tra il server web Apache e il server di applicazioni Tomcat.)
Possono esserci diverse cause e conseguenze, alcune tra le più gravi sono:
1-L'attaccante potrebbe visualizzare, modificare o eliminare file sensibili che si trovano nel filesystem.
2-Possibile accesso ai dati riservati e la possibilità di compromettere ulteriormente altre applicazioni web

Invece per ridurre il rischio ed eliminare questo problema lútente potrebbe:
1-Aggiornare Apache Tomcat: Il problema è stato risolto in versioni successive di Tomcat, quindi aggiornare la piattaforma è essenziale per risolvere il problema.
2-Impostare correttamente le configurazioni di rete e i permessi sui file per evitare l'accesso non autorizzato ai file sensibili.

La seconda vulnerabilità critica riscontrata è la SSL Version 2 and 3 Protocol Detection

Quest'ultima si riferisce all'utilizzo di protocolli obsoleti e insicuri, ed i rischi principali sono:

1- Compromissione dei dati: Gli attacchi possono intercettare o decifrare i dati trasmessi.
2-Attacchi MITM e POODLE: Permettono a un attaccante di alterare le comunicazioni e decriptare informazioni sensibili.
3-Impatto su integrità e riservatezza: I dati possono essere manomessi senza rilevamento.

Per andar e a risolvere questi rischi e quindi aumentare la protezione della macchina potremmo:
Disabilitare SSL 2.0 e 3.0 su server e forzare l'uso di TLS 1.2 o TLS 1.3, perché quest'ultima è una versione aggiornata e migliorata di SSL con una migliore crittografia ed un supporto attivo.

La terza criticità è invece "Debian OpenSSH/OpenSSL Package Random Number Generator Weakness".
Il problema principale di questa vulnerabilità è un errore nella configurazione del generatore di numeri casuali in Debian, che ha impattato la qualità delle chiavi crittografiche generate. Questo problema è emerso quando Debian ha utilizzato un algoritmo debole per la generazione di numeri casuali, utilizzando un seed predeterminato e non sicuro.

I rischi principali dati da questa vulnerabilità sono:
1-Previsibilità delle chiavi crittografiche: La debolezza ha reso le chiavi crittografiche generate predicibili e quindi vulnerabili a attacchi di forza bruta.
2-Compromissione della sicurezza: Gli attaccanti che conoscevano l'algoritmo o il comportamento del generatore di numeri casuali debole potrebbero decifrare le comunicazioni criptate o forzare l'accesso a sistemi protetti da SSH o OpenSSL.
3-Rischio di accesso non autorizzato: Poiché le chiavi erano prevedibili, un attaccante avrebbe potuto intercettare le comunicazioni e ottenere accesso remoto non autorizzato.

Per andare a ridurre i rischi di questa vulnerabilità possiamo:
1-Fare aggiornamenti software, perché la vulnerabilità è stata corretta con gli aggiornamenti a OpenSSL e OpenSSH rilasciati da Debian. È essenziale aggiornare i pacchetti vulnerabili alle versioni più recenti che non utilizzano il generatore di numeri casuali debole.
2-Verifica della sicurezza: Controllare se il sistema è stato compromesso o se le chiavi deboli sono state utilizzate in altre comunicazioni o connessioni.

La quarta vulnerabilità è la VNC Server 'password' Password. riguarda il sistema di autenticazione di VNC, un protocollo per l'accesso remoto a computer grafici. In particolare, è legata al metodo di protezione della password di autenticazione usato dai server VNC.

I rischi principali dati da quest'ultima sono:
1-Intercettazione delle credenziali, perché alcune implementazioni di VNC non cifrano la password o la trasmettono in modo non abbastanza sicuro, un attaccante potrebbe intercettare la password durante la trasmissione nella rete.
2-Brute Force: Se la password è debole o comune, un attaccante potrebbe provare varie combinazioni fino a indovinare la password e ottenere accesso non autorizzato al sistema.
3-Accesso remoto non autorizzato: Un attaccante che riesce a ottenere la password potrebbe accedere e controllare il sistema remoto, compromettendo la sicurezza dell'intero sistema.

Per ridurre i rischi l'utente può:
1-Impostare una password forte, perché è fondamentale usare una password complessa per l'autenticazione VNC, che contenga una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali.
2-imitare l'accesso: Limitare l'accesso al server VNC tramite firewall o configurazioni che permettano solo a determinati indirizzi IP di connettersi, riducendo la superficie di attacco.

3-Limitare l'accesso: Limitare l'accesso al server VNC tramite firewall o configurazioni che permettano solo a determinati indirizzi IP di connettersi, riducendo la superficie di attacco.
4-Disabilitare l'autenticazione di base. Evitare di utilizzare il metodo di autenticazione di base e utilizzare altre soluzioni più sicure offerte dai server VNC.