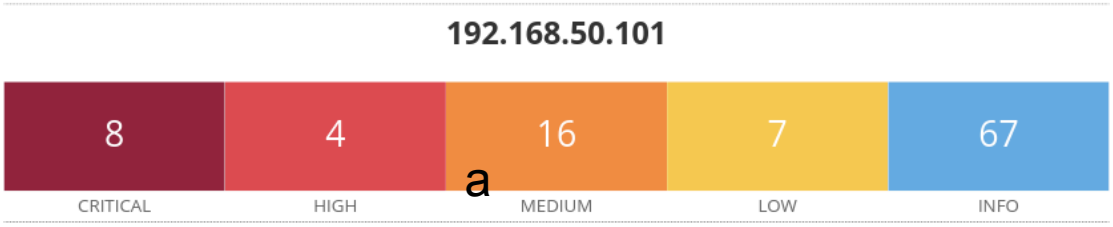
S5L4



Vulnerabilities Total: 102

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

Scannerizzando l'indirizzo IP di Metasploitable tramite Nessus, possiamo notare come ci restituisce come risultato che sono presenti 8 errori di livello critico il che lo rendono vulnerabile e poco sicuro. Qua di seguito andrò a **descrivere** il tipo di **vulnerabilità** come può essere **sfruttata** da un attaccante e una soluzione per migliorare la situazione.

Apache Tomcat AJP:
Vulnerabilità: La vulnerabilità riguarda un'AJP connector che consente a un attaccante remoto non autenticato di leggere file dell'applicazione web o, se consentito, di caricare codice malevolo per ottenere l'esecuzione remota di codice (RCE).
Sfruttamento: Un attaccante potrebbe leggere file sensibili dell'applicazione o caricare codice malevolo tramite file JSP per assumere il controllo del server, compromettendo la sicurezza e l'integrità del sistema.
Soluzione: Per risolvere questa vulnerabilità, è consigliabile aggiornare il software, disabilitare o proteggere l'AJP connector, filtrare e validare l'input, implementare monitoraggio per rilevare attività sospette, utilizzare firewall e altre misure di sicurezza, e condurre test regolari di penetrazione e revisioni della sicurezza.

Bind shell backdoor detection:
Vulnerabilità: L' host remoto potrebbe essere stato compromesso e presenta una shell in ascolto su una porta remota senza richiedere alcuna autenticazione.
Sfruttamento: Un attaccante potrebbe connettersi alla porta remota e inviare comandi direttamente alla shell, ottenendo così un accesso non autorizzato al sistema compromesso.
Soluzione: Per risolvere questa vulnerabilità, è necessario identificare e rimuovere la shell compromessa, implementare controlli di accesso e autenticazione appropriati, aggiornare e configurare correttamente il software per prevenire future intrusioni, e condurre un'indagine approfondita per determinare la portata del compromesso e adottare le misure di mitigazione appropriate.

SSL version 2 and protocol 3 Detection solution
Vulnerabilità: Il servizio remoto utilizza un protocollo di crittografia con vulnerabilità conosciute.
Sfruttamento: Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0, entrambi affetti da difetti crittografici, come un regime di padding insicuro con cifrari CBC e schemi insicuri di rinegoziazione e ripresa della sessione. Un attaccante può sfruttare queste vulnerabilità per condurre attacchi di tipo man-in-the-middle o decriptare comunicazioni tra il servizio e i client.
Soluzione: È consigliabile disabilitare completamente SSL 2.0 e SSL 3.0 poiché sono considerati insicuri. È necessario utilizzare versioni più recenti e sicure di TLS per garantire una comunicazione crittograficamente robusta. Inoltre, è importante verificare che i browser web implementino correttamente la scelta della versione più sicura del protocollo per evitare attacchi di degradazione della connessione come POODLE.

Unix Operating System Unsupported Version
Vulnerabilità: Il sistema operativo Unix in esecuzione sul host remoto non è più supportato.
Sfruttamento: Poiché il sistema operativo non è più supportato, non verranno rilasciati nuovi aggiornamenti di sicurezza dal venditore. Ciò significa che il sistema è probabile che contenga vulnerabilità di sicurezza non corrette.
Soluzione: Per affrontare questa vulnerabilità, è consigliabile migrare verso un sistema operativo supportato per garantire l'accesso a patch di sicurezza aggiornate e proteggere il sistema da potenziali minacce.

Debian openssh/openssl package random number generator
Vulnerabilità: Le chiavi host SSH remote sono deboli a causa di un bug nella generazione delle chiavi su sistemi Debian o Ubuntu, che coinvolge il generatore di numeri casuali della libreria OpenSSL.
Sfruttamento: Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man-in-the-middle.
Soluzione: Per risolvere questa vulnerabilità, è necessario rigenerare le chiavi host SSH utilizzando un sistema con un generatore di numeri casuali affidabile e poi aggiornare le chiavi sui sistemi client. Inoltre, è consigliabile aggiornare l'OpenSSL alla versione corretta che risolve questo problema di generazione delle chiavi.

Debian openssh/openssl package random number generator(SSL CHECK)
Vulnerabilità: Il certificato SSL remoto utilizza una chiave debole a causa di un bug nella generazione delle chiavi su sistemi Debian o Ubuntu, che coinvolge il generatore di numeri casuali della libreria OpenSSL.
Sfruttamento: Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man-in-the-middle.
Soluzione: Per risolvere questa vulnerabilità, è necessario rigenerare il certificato SSL utilizzando un sistema con un generatore di numeri casuali affidabile e quindi aggiornare il certificato sul server SSL. Inoltre, è consigliabile aggiornare l'OpenSSL alla versione corretta che risolve questo problema di generazione delle chiavi.

NFS Exported Share Information Disclosure
Vulnerabilità: È possibile accedere alle condivisioni NFS sul host remoto.
Sfruttamento: Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare ciò per leggere (e eventualmente scrivere) file sul host remoto.
Soluzione: Per mitigare questa vulnerabilità, è consigliabile configurare correttamente le autorizzazioni di accesso alle condivisioni NFS, limitando l'accesso solo agli utenti autorizzati e implementando le misure di sicurezza appropriate, come l'utilizzo di autenticazione e crittografia per proteggere le comunicazioni NFS. Inoltre, è consigliabile utilizzare strumenti di monitoraggio per rilevare e rispondere prontamente a eventuali attività sospette sulle condivisioni NFS.

VNC Server 'password' Password
Vulnerabilità: Il server VNC in esecuzione sul host remoto è protetto da una password debole.
Sfruttamento: L'attaccante potrebbe sfruttare questa debolezza della password per accedere al server VNC senza autenticazione e ottenere il controllo del sistema.
Soluzione: Per risolvere questa vulnerabilità, è necessario cambiare la password del server VNC utilizzando una password forte e complessa. È importante utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali per creare una password robusta e difficilmente indovinabile. Inoltre, è consigliabile utilizzare le funzionalità di autenticazione e crittografia offerte dal server VNC per proteggere ulteriormente l'accesso al sistema.