

16.05.2025



VULNERABILITY ASSESSMENT

SCANSIONE INIZIALE METASPLOITABLE 2
FABIO MUNGIOVÌ

SCANSIONE INIZIALE

METASPLOITABLE 2

INDICE

SOMMARIO.....	2
RISULTATI E VALUTAZIONE	2
ANALISI VULNERABILTA'	3
CRITICAL	3
HIGH	6
MEDIUM	8
LOW	13
INFO	15
SCREENSHOT	15
CONCLUSIONI	15

SOMMARIO

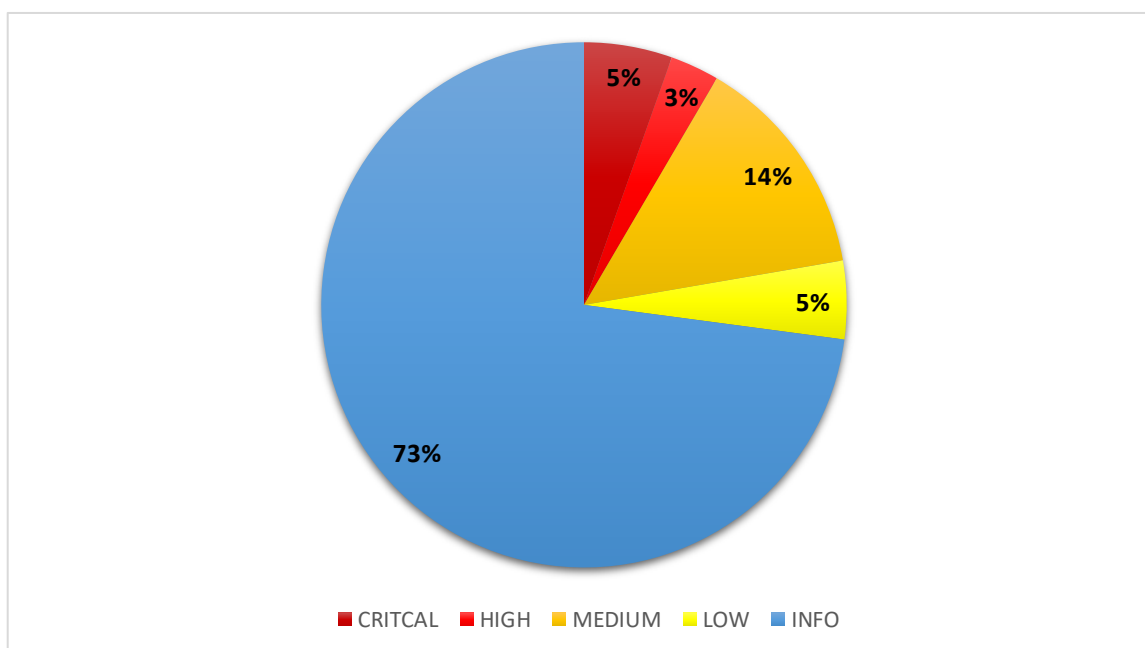
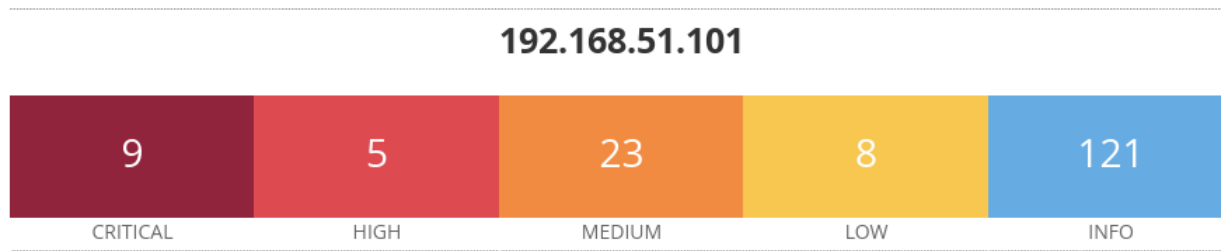
L'obiettivo di questo Vulnerability Scan è analizzare le vulnerabilità del sistema Metasploitable. La scansione è stata effettuata tramite il tool Nessus, con la macchina target locata in una subnet differente dalla macchina di test, con IP 192.168.51.101. Verrà mostrato il grafico con il numero delle vulnerabilità riscontrate, in seguito verranno analizzate nel dettaglio.

RISULTATI E VALUTAZIONE

I Risultati dello scan vengono suddivisi in base al loro impatto e al tipo di rischio a cui espongono.

Nessus utilizza un sistema di classificazione delle vulnerabilità basato sulla gravità. Questa classificazione è determinata principalmente dal **CVSS** (Common Vulnerability Scoring System), un framework standardizzato per valutare il rischio associato a una vulnerabilità.

Di seguito i risultati generali della scansione.



ANALISI VULNERABILTA'

Di seguito le informazioni sulla scansione e la lista delle vulnerabilità riscontrate in ordine di criticità, con una breve descrizione e le azioni di mitigazione consigliate dal tool Nessus.

Scan Information

Start time: Thu May 15 21:59:11 2025

End time: Thu May 15 22:24:52 2025

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.51.101

OS: Linux Kernel 2.6 on Ubuntu

CRITICAL

NOME	CVSS
Canonical Ubuntu Linux SEoL	CRIT 10
<p>Port tcp/80/www</p> <p>Synopsis Una versione non supportata di Canonical Ubuntu Linux è installata nell'host remoto.</p> <p>Descrizione Secondo la sua versione, Canonical Ubuntu Linux è 8.04.x. non è più gestito dal suo venditore o fornitore. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.</p> <p>Soluzione Esegui l'aggiornamento a una versione di Canonical Ubuntu Linux attualmente supportata.</p>	

NOME	CVSS
VNC Server 'password' Password	CRIT 10
<p>Port tcp/5900/vnc</p> <p>Synopsis Un server VNC in esecuzione sull'host remoto è protetto da una password debole.</p> <p>Descrizione Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo problema per assumere il controllo del sistema.</p> <p>Soluzione Proteggi il servizio VNC con una password complessa.</p>	

NOME	CVSS
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	CRIT 10
<p>Port tcp/22/ssh tcp/25/smtp tcp/5432/postgresql</p> <p>Synopsis Le chiavi host SSH remote sono deboli.</p> <p>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. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare, decifrare la sessione remota o impostare un attacco man in the middle.</p> <p>Soluzione Si consideri tutto il materiale crittografico generato nell'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN deve essere rigenerato</p>	

NOME	CVSS
Apache Tomcat AJP Connector Request Injection (Ghostcat)	CRIT 9.8
<p>Port tcp/8009/ajp13</p> <p>Synopsis È presente un connettore AJP vulnerabile in ascolto sull'host remoto.</p> <p>Descrizione È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato può sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile.</p> <p>Soluzione Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.</p>	

NOME	CVSS
Bind Shell Backdoor Detection	CRIT 9.8
<p>Port tcp/1524/wild_shell</p> <p>Synopsis È possibile che l'host remoto sia stato compromesso.</p> <p>Descrizione Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo connettendosi alla porta remota e inviando direttamente comandi.</p> <p>Soluzione Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.</p>	

NOME	CVSS
SSL Version 2 and 3 Protocol Detection	CRIT 9.8
<p>Port tcp/5432/postgresql tcp/25/smtp</p> <p>Synopsis Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.</p> <p>Descrizione Il servizio remoto accetta connessioni crittografate con SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici. 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.</p> <p>Soluzione Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizzare invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.</p>	

HIGH

NOME	CVSS
ISC BIND Service Downgrade / Reflected DoS	HIGH 8.6
<p>Port udp/53/dns</p> <p>Synopsis Il server dei nomi remoto è interessato da vulnerabilità di downgrade del servizio/DoS riflesso.</p> <p>Descrizione Secondo la sua versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata da downgrade delle prestazioni e vulnerabilità DoS riflesse. Un utente malintenzionato remoto non autenticato può sfruttare questo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.</p> <p>Soluzione Eseguire l'aggiornamento alla versione ISC BIND a cui si fa riferimento nell'advisory del fornitore.</p>	

NOME	CVSS
NFS Shares World Readable	HIGH 7.5
<p>Port tcp/2049/rpc-nfs</p> <p>Synopsis Il server NFS remoto esporta condivisioni leggibili da tutti.</p> <p>Descrizione Il server NFS remoto esporta una o più condivisioni senza limitare l'accesso (in base al nome host, all'IP o all'intervallo IP).</p> <p>Soluzione Porre le opportune restrizioni su tutte le condivisioni NFS.</p>	

NOME	CVSS
SSL Medium Strength Cipher Suites Supported (SWEET32)	HIGH 7.5
<p>Port tcp/25/smtp tcp/5432/postgresql tcp /22/ ssh</p> <p>Synopsis Il servizio remoto supporta l'uso di cifrari SSL di media intensità.</p> <p>Descrizione L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia di media intensità. Nessus considera la forza media come qualsiasi crittografia che utilizza lunghezze di chiave di almeno 64 bit e inferiori a 112 bit, oppure che utilizza la suite di crittografia 3DES.</p> <p>Soluzione Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari di media intensità.</p>	

NOME	CVSS
Samba Badlock Vulnerability	HIGH 7.5
<p>Port tcp/445/cifs</p> <p>Synopsis Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.</p> <p>Descrizione 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, che esiste nei protocolli Security Account Manager (SAM) e LSAD (Local Security Authority) (LSAD) a causa di una negoziazione errata 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.</p> <p>Soluzione Aggiorna a Samba versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.</p>	

MEDIUM

NOME	CVSS
TLS Version 1.0 Protocol Detection	MED 6.5
<p>Port tcp/25/smtp tcp/5432/postgresql</p> <p>Synopsis Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS.</p> <p>Descrizione Il servizio remoto accetta connessioni crittografate con TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. versioni più recenti di TLS come 1.2 e 1.3 sono progettate per questi difetti e dovrebbero essere utilizzate quando possibile.</p> <p>Soluzione Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.</p>	

NOME	CVSS
SSL Anonymous Cipher Suites Supported	MED 5.9
<p>Port tcp/25/smtp</p> <p>Synopsis Il servizio remoto supporta l'utilizzo di crittografie SSL anonime.</p> <p>Descrizione L'host remoto supporta l'uso di cifrature SSL anonime. Sebbene ciò consenta a un amministratore di configurare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle.</p> <p>Soluzione Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature deboli.</p>	

NOME	CVSS
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	MED 5.9
<p>Port tcp/25/smtp</p> <p>Synopsis L'host remoto può essere interessato da una vulnerabilità che consente a un utente malintenzionato remoto di decrittografare potenzialmente il traffico TLS acquisito.</p> <p>Descrizione L'host remoto supporta SSLv2 e pertanto potrebbe essere affetto da una vulnerabilità che consente un attacco crossprotocol Bleichenbacher padding oracle noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione di Secure Sockets Layer versione 2 (SSLv2) e consente di decrittografare il traffico TLS acquisito. Un utente malintenzionato man-in-the-middle può sfruttare questo problema per decrittografare la connessione TLS utilizzando il traffico precedentemente acquisito e la crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.</p> <p>Soluzione Disabilita SSLv2 e le suite di crittografia di livello di esportazione.</p>	

NOME	CVSS
SSL Anonymous Cipher Suites Supported	MED 5.9
<p>Port tcp/25/smtp</p> <p>Synopsis Il servizio remoto supporta l'utilizzo di crittografie SSL anonime.</p> <p>Descrizione L'host remoto supporta l'uso di cifrature SSL anonime. Sebbene ciò consenta a un amministratore di configurare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle.</p> <p>Soluzione Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature deboli.</p>	

NOME	CVSS
HTTP TRACE / TRACK Methods Allowed	MED 5.3
<p>Port tcp/80/www</p> <p>Synopsis Le funzioni di debug sono abilitate sul server Web remoto.</p> <p>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.</p> <p>Soluzione Disabilitare questi metodi HTTP.</p>	

NOME	CVSS
SMB Signing not required	MED 5.3
<p>Port tcp/445/cifs</p> <p>Synopsis La firma non è richiesta nel server SMB remoto.</p> <p>Descrizione La firma non è richiesta nel server SMB remoto. Un utente malintenzionato remoto non autenticato può sfruttare questo problema per condurre attacchi man-in-the-middle contro il server SMB.</p> <p>Soluzione Applica la firma dei messaggi nella configurazione dell'host. Su Samba, l'impostazione si chiama "firma del server".</p>	

NOME	CVSS
DNS Server Zone Transfer Information Disclosure (AXFR)	MED 5.0
<p>Port tcp/80/www</p> <p>Synopsis Il server dei nomi remoto consente i trasferimenti di zona</p> <p>Descrizione Il server dei nomi remoto consente l'esecuzione di trasferimenti di zona DNS. Un trasferimento di zona consente a un utente malintenzionato remoto di popolare istantaneamente un elenco di potenziali obiettivi.</p> <p>Soluzione Limita i trasferimenti di zona DNS solo ai server che necessitano delle informazioni.</p>	

NOME	CVSS
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	MED 4.3
<p>Port tcp/25/smtp</p> <p>Synopsis L'host remoto supporta un set di crittografie deboli.</p> <p>Descrizione L'host remoto supporta EXPORT_RSA suite di crittografia con chiavi inferiori o uguali a 512 bit. Un utente malintenzionato può fattorizzare un modulo RSA a 512 bit in un breve lasso di tempo.</p> <p>Soluzione Riconfigurare il servizio per rimuovere il supporto per i pacchetti di crittografia EXPORT_RSA.</p>	

NOME	CVSS
SSH Weak Algorithms Supported	MED 4.3
<p>Port tcp/22/ssh</p> <p>Synopsis Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo.</p> <p>Descrizione Nessus ha rilevato che il server SSH remoto è configurato per utilizzare la crittografia del flusso Arcfour o per non crittografare affatto. La RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con le chiavi deboli.</p> <p>Soluzione Contattare il fornitore o consultare la documentazione del prodotto per rimuovere le crittografie deboli.</p>	

NOME	CVSS
SSH Weak Algorithms Supported	MED 4.0
<p>Port tcp/25/smtp</p> <p>Synopsis Il servizio di posta remota consente l'iniezione di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato.</p> <p>Descrizione Il servizio SMTP remoto contiene un difetto software nell'implementazione STARTTLS che potrebbe consentire a un utente malintenzionato remoto e non autenticato di inserire comandi durante la fase di protocollo in chiaro che verranno eseguiti durante la fase di protocollo in testo cifrato.</p> <p>Soluzione Contatta il fornitore per verificare se è disponibile un aggiornamento.</p>	

NOME	CVSS
SSL (Multiple Issues)	MED -
<p>Port tcp/25/smtp tcp/5432/postgresql</p> <p>Descrizione Sono state rilevate diverse vulnerabilità relative alla gestione dei certificati SSL/TLS e al supporto di cifrature deboli sui servizi analizzati. Nello specifico:</p> <ul style="list-style-type: none">• Utilizzo di certificati SSL auto firmati o non emessi da una CA affidabile• Certificati SSL scaduti o prossimi alla scadenza• Certificati SSL con hostname non corrispondente al server• Supporto di suite di cifratura deboli (ad esempio RC4, EXPORT, 3DES)• Supporto di certificati che non possono essere considerati affidabili dai client <p>Impatto Queste vulnerabilità possono consentire ad un attaccante di intercettare, alterare o decifrare il traffico cifrato, esponendo dati sensibili e credenziali. Inoltre, i client potrebbero ricevere avvisi di sicurezza e rifiutare la connessione ai servizi esposti.</p> <p>Soluzione Acquista o genera un certificato SSL adeguato a questo servizio.</p>	

NOME	CVSS
ISC Bind (Multiple Issues)	MED -
<p>Port udp/53/dns</p> <p>Descrizione Sono state riscontrate vulnerabilità relative al software DNS ISC BIND, in particolare:</p> <ul style="list-style-type: none">• Utilizzo di versioni di ISC BIND affette da vulnerabilità note (versioni precedenti a 9.11.22, 9.16.6, 9.17.x)• Possibilità di Denial of Service (DoS) tramite sfruttamento di bug noti nel servizio DNS <p>Impatto Queste vulnerabilità possono essere sfruttate da un attaccante per causare l'arresto del servizio DNS (Denial of Service), con conseguente interruzione della risoluzione dei nomi e potenziale impatto sulla disponibilità dei servizi di rete.</p> <p>Soluzione Si raccomanda di aggiornare ISC BIND all'ultima versione stabile disponibile, superiore a quelle vulnerabili, così da correggere tutte le falle di sicurezza note e prevenire possibili attacchi DoS.</p>	

LOW

NOME	CVSS
SSH (Multiple Issues)	LOW -
<p>Port tcp/22/ssh</p> <p>Sono state riscontrate alcune vulnerabilità legate alla configurazione del servizio SSH, in particolare:</p> <ul style="list-style-type: none">• Abilitazione di cifrature CBC mode, considerate deboli• Abilitazione di algoritmi di key exchange deboli• Abilitazione di algoritmi MAC deboli <p>Impatto Queste configurazioni possono, in determinate condizioni, facilitare attacchi di tipo crittografico (ad esempio attacchi di tipo plaintext recovery o downgrade attack), riducendo la sicurezza complessiva delle connessioni SSH. Tuttavia, il rischio è considerato basso, soprattutto in ambienti controllati.</p> <p>Soluzione Si raccomanda di disabilitare le cifrature CBC mode, gli algoritmi di key exchange e i MAC deboli nella configurazione SSH.</p>	

NOME	CVSS
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	LOW 3.7
<p>Port tcp/25/smtp</p> <p>Synopsis L'host remoto supporta un set di crittografie deboli.</p> <p>Descrizione L'host remoto supporta EXPORT_DHE suite di cifratura con chiavi inferiori o uguali a 512 bit. Attraverso la crittoanalisi, una terza parte può trovare il segreto condiviso in un breve lasso di tempo.</p> <p>Soluzione Riconfigurare il servizio per rimuovere il supporto per i pacchetti di crittografia EXPORT_DHE.</p>	

NOME	CVSS
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	LOW 3.4
<p>Port tcp/25/smtp tcp/5432/postgresql</p> <p>Synopsis È possibile ottenere informazioni sensibili dall'host remoto con servizi abilitati SSL/TLS</p> <p>Descrizione L'host remoto è interessato da una vulnerabilità di divulgazione di informazioni man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi crittografati</p> <p>Soluzione Disable SSLv3.</p>	

NOME	CVSS
X Server Detection	LOW 2.6
<p>Port tcp/6000/x11</p> <p>Synopsis Un server X11 è in ascolto sull'host remoto</p> <p>Descrizione L'host remoto esegue un server X11. X11 è un protocollo client-server che può essere utilizzato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto. Poiché il traffico X11 non è crittografato, è possibile che un utente malintenzionato intercetti la connessione.</p> <p>Soluzione Limitare l'accesso a questa porta. Se la funzione client/server X11 non viene utilizzata, disabilitare completamente il supporto TCP in X11 (nolisten tcp).</p>	

NOME	CVSS
ICMP Timestamp Request Remote Date Disclosure	LOW 1.4
<p>Port icmp/0</p> <p>Synopsis È possibile determinare l'ora esatta impostata sull'host remoto.</p> <p>Descrizione L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un utente malintenzionato di conoscere la data impostata sul computer di destinazione.</p> <p>Soluzione Filtra le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita (14).</p>	

INFO




Durante la scansione sono stati rilevati alcuni finding (121) classificati come "informativi". Queste segnalazioni non rappresentano vulnerabilità o rischi di sicurezza immediati, ma forniscono dettagli aggiuntivi sulla configurazione, sui servizi attivi o su altre caratteristiche dell'ambiente analizzato.

I finding informativi sono utili per la comprensione del contesto, per l'inventario dei sistemi e per identificare potenziali aree di miglioramento, ma non richiedono interventi urgenti.

SCREENSHOT

Questa schermata, acquisita dai risultati del tool Nessus, elenca le vulnerabilità con criticità più alta.

Lo useremo come riferimento con il report della scansione finale, dopo le azioni di mitigazione, per evidenziare le vulnerabilità risolte.

<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲
<input type="checkbox"/> CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General
<input type="checkbox"/> CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/> CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Inje...	Web Servers
<input type="checkbox"/> CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection
<input type="checkbox"/> CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/> CRITICAL	 2 SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/> HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General
<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC
<input type="checkbox"/> MIXED	 15 SSL (Multiple Issues)	General
<input type="checkbox"/> MIXED	 5 ISC Bind (Multiple Issues)	DNS

CONCLUSIONI

La valutazione ha evidenziato la presenza di vulnerabilità ad alto rischio dovute al supporto di cifrature deboli e/o anonime nei protocolli SSL/TLS, che espongono i servizi al rischio di attacchi di tipo Man-in-the-Middle (MITM) e alla possibile decifrabilità del traffico.

Si raccomanda di intervenire tempestivamente disabilitando tutte le cifrature deboli e anonime, adottando esclusivamente TLS 1.2 o superiore e cipher considerati sicuri, per garantire la riservatezza e l'integrità delle comunicazioni.