S5l3

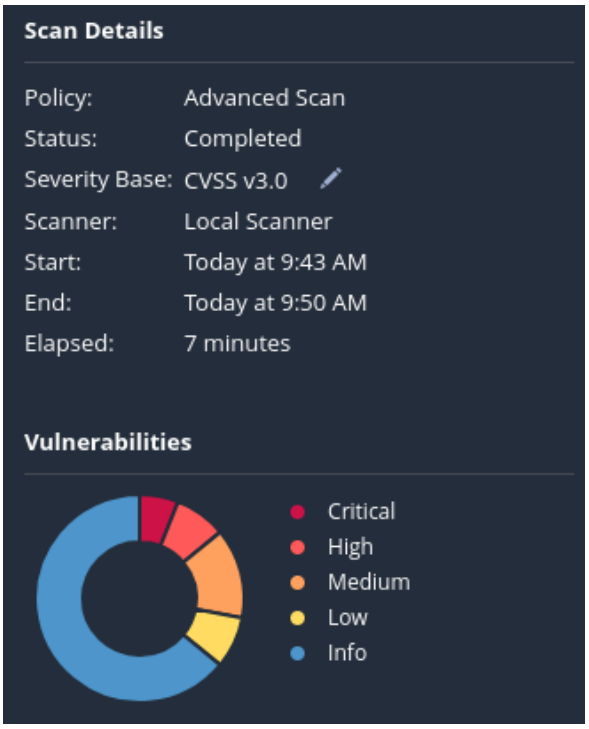
Introduzione

Nel report sono documentati i risultati di un'attività di Vulnerability Scanning eseguita sulla macchina Metasploitable utilizzando lo strumento Nessus.

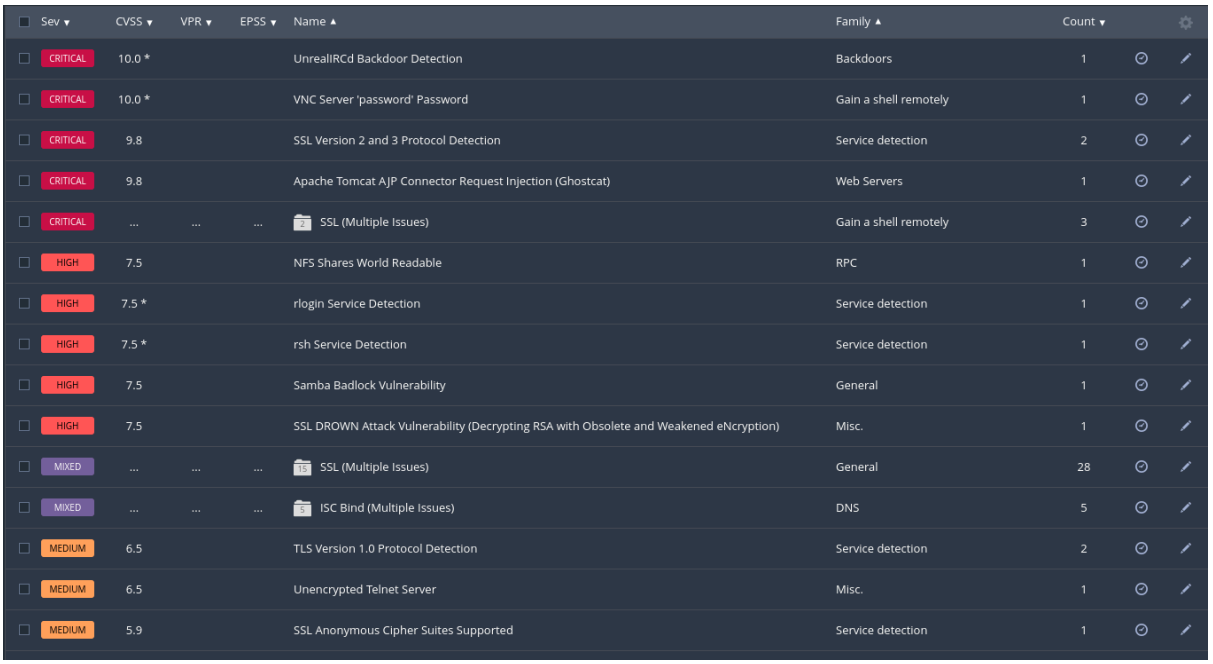
La scansione è stata configurata per analizzare esclusivamente porte comuni, spesso bersaglio di attacchi informatici, tra cui: FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80), POP3 (110), NetBIOS (139), HTTPS (443), SMB (445) e RDP (3389). Il report fornirà una panoramica delle vulnerabilità rilevate, la loro gravità, e una breve analisi dei rischi associati, con riferimenti a possibili misure di mitigazione.

L'analisi delle vulnerabilità è stata condotta basandosi sulle informazioni fornite da Nessus, arricchite da ulteriori ricerche sulle vulnerabilità più critiche, con lo scopo di comprendere meglio le possibili implicazioni per la sicurezza e le strategie di difesa.

Vulnerability Scan:



Vulnerability Scan:



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *			UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5			NFS Shares World Readable	RPC	1
HIGH	7.5 *			rlogin Service Detection	Service detection	1
HIGH	7.5 *			rsh Service Detection	Service detection	1
HIGH	7.5			Samba Badlock Vulnerability	General	1
HIGH	7.5			SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9			SSL Anonymous Cipher Suites Supported	Service detection	1

Analisi delle vulnerabilità:

Ecco l'analisi delle vulnerabilità rilevate divise per pericolosità da cvss 7,5>, con una breve spiegazione e possibili soluzioni:

Vulnerabilità Critiche (CRITICAL)

UnrealIRCd Backdoor Detection (CVSS 10.0)

Descrizione: Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato.
Soluzione: Scaricare nuovamente il software, verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.

VNC Server 'password' Password (CVSS 10.0)

Descrizione: Il server VNC in esecuzione sull'host remoto è 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 situazione per assumere il controllo del sistema.

Soluzione: Proteggi il servizio VNC con una password complessa.

SSL Version 2 and 3 Protocol Detection (CVSS 9.8)

Descrizione: 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 client.

Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più alta supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla 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 ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di entrata in vigore stabilita in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia avanzata" del PCI SSC.

Soluzione: Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVSS 9.8)

Descrizione: È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato 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 codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice in modalità remota (RCE).

Soluzione: Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

SSL (Multiple Issues)

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) (CVSS 10)

Descrizione: Il certificato x509 remoto sul server SSL remoto è stato generato 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.

Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (CVSS 10)

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.

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.

Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Vulnerabilità Alte (HIGH)

NFS Shares World Readable (CVSS 7.5)

Descrizione: Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP o intervallo IP).

Soluzione: Posizionare le opportune restrizioni su tutte le condivisioni NFS.

rlogin Service Detection (CVSS 7.5)

Descrizione: Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono passati tra il client e il server rlogin in chiaro. Un utente malintenzionato man-in-the-middle può sfruttare questa situazione per sniffare login e password. Inoltre, potrebbe consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale), potrebbe essere possibile ignorare l'autenticazione.

Infine, rlogin è un modo semplice per trasformare l'accesso in scrittura su file in accessi completi tramite i file .rhosts o rhosts.equiv.

Soluzione: Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilita questo servizio e utilizza invece SSH.

rsh Service Detection (CVSS 7.5)

Descrizione: Il servizio rsh è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono passati tra il client e il server rsh in chiaro. Un utente malintenzionato man-in-the-middle può sfruttare questa situazione per sniffare login e password. Inoltre, potrebbe consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale), potrebbe essere possibile ignorare l'autenticazione.

Infine, rsh è un modo semplice per trasformare l'accesso in scrittura su file in accessi completi tramite i file .rhosts o rhosts.equiv.

Soluzione: Commentare la riga 'rsh' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilita questo servizio e utilizza invece SSH.

Samba Badlock Vulnerability (CVSS 7.5)

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 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 la visualizzazione o la modifica di dati sensibili di sicurezza nel database di Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione: Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

SSL DROWN Attack Vulnerability (CVSS 7.5)

Descrizione: 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.

Soluzione: 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.