I documenti caricati sono report base e dettagliati di due scansioni di sicurezza eseguite utilizzando Nessus su un host con l'indirizzo IP 192.168.50.101, identificato come "METASPLOITABLE".
Questi report includono una lista di vulnerabilità suddivise per severità (CRITICAL, HIGH, MEDIUM, LOW, INFO) e forniscono dettagli su ciascuna vulnerabilità rilevata. Ecco un riassunto delle sezioni principali:

VULNERABILITÀ CRITICHE E ALTE:
Apache Tomcat AJP Connector Request Injection (Ghostcat): Vulnerabilità che permette la lettura/inclusione di file e potenzialmente l'esecuzione di codice remoto.
VNC Server 'password' Password: Il server VNC utilizza una password debole ("password"), permettendo a un attaccante remoto non autenticato di prendere il controllo del sistema.
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness: Le chiavi generate sono deboli e facilmente indovinabili a causa di un difetto nel generatore di numeri casuali.
VULNERABILITÀ MEDIE:
ISC BIND Service Downgrade / Reflected DoS: Vulnerabilità che consente a un attaccante non autenticato di degradare il servizio del server DNS o utilizzarlo per attacchi di riflessione.
NFS Shares World Readable: Il server NFS esporta condivisioni leggibili da qualsiasi utente senza restrizioni.
VULNERABILITÀ BASSE E INFORMATIVE:
FTP Server Detection: Identifica un server FTP in esecuzione su vsftpd versione 2.3.4.
HTTP Server Type and Version: Identifica il tipo e la versione del server web Apache/2.2.8 (Ubuntu).
SSH Server Type and Version: Identifica il tipo e la versione del server SSH come OpenSSH_4.7p1 Debian-8ubuntu1.
RACCOMANDAZIONI:
Ogni vulnerabilità elencata è accompagnata da una descrizione dettagliata, link a ulteriori informazioni, e soluzioni raccomandate per mitigare o risolvere la vulnerabilità.
Il rapporto è un'analisi approfondita delle potenziali debolezze di sicurezza presenti sull'host esaminato, fornendo un'ampia gamma di informazioni utili per migliorare la sicurezza del sistema target.

SUGGERIMENTI PER MIGLIORARE LE VULNERABILITÀ

Apache Tomcat AJP Connector Request Injection (Ghostcat)
Vulnerabilità che permette la lettura/inclusione di file e potenzialmente l'esecuzione di codice remoto.
Soluzione: Aggiornare la configurazione AJP per richiedere autorizzazione e/o aggiornare il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successive.

VNC Server 'password' Password
Il server VNC utilizza una password debole ("password"), permettendo a un attaccante remoto non autenticato di prendere il controllo del sistema.
Soluzione: Configurare il servizio VNC con una password robusta e complessa.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Le chiavi SSH generate sono deboli a causa di un difetto nel generatore di numeri casuali di OpenSSL.
Soluzione: Rigenerare tutte le chiavi crittografiche SSH, SSL e OpenVPN utilizzando una versione aggiornata di OpenSSL.

ISC BIND Service Downgrade / Reflected DoS
Vulnerabilità che consente a un attaccante di degradare il servizio del server DNS o utilizzarlo per attacchi di riflessione.
Soluzione: Aggiornare ISC BIND alla versione specificata nel vendor advisory.

NFS Shares World Readable
Il server NFS esporta condivisioni leggibili da qualsiasi utente senza restrizioni.
Soluzione: Configurare il server NFS per limitare l'accesso alle condivisioni solo agli host autorizzati.

SSL Version 2 and 3 Protocol Detection
Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0, che hanno notevoli vulnerabilità.

Soluzione: Disabilitare SSL 2.0 e 3.0, e utilizzare TLS 1.2 o superiore.

SMB Signing not required
La firma dei messaggi non è richiesta sul server SMB, permettendo potenzialmente attacchi man-in-the-middle.
Soluzione: Abilitare e forzare la firma dei messaggi nelle configurazioni del server SMB.

SSH Weak Algorithms Supported
Il server SSH è configurato per utilizzare algoritmi di cifratura deboli.
Soluzione: Rimuovere gli algoritmi deboli come Arcfour dalla configurazione del server SSH.

SSL Certificate Cannot Be Trusted
Il certificato SSL del server non può essere considerato attendibile.
Soluzione: Acquisire o generare un certificato SSL valido e correttamente firmato da una autorità di certificazione riconosciuta.

SSL Certificate Expiry
Il certificato SSL del server è scaduto.
Soluzione: Acquisire o generare un nuovo certificato SSL per sostituire quello esistente.

SSL DROWN Attack Vulnerability
Il server supporta SSLv2, rendendolo vulnerabile all'attacco DROWN.
Soluzione: Disabilitare SSLv2 e i cipher di crittografia di livello export.