192.168.50.101

6	4	15	4	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 99

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9737	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*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
MEDIUM	6.5	4.4	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.972	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9434	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet and Weakened eNcryption)

MEDIUM	5.9	4.4	0.0076	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed

Nessus Essentials

Punti principali

1. **Numero totale di vulnerabilità rilevate**: **99**
    - **6 critiche**
    - **4 alte**
    - **15 medie**
    - **4 basse**
    - **70 informative**
2. **Metadati**:
    - **CVSS V3.0**: Sistema di valutazione della gravità della vulnerabilità
    - **VPR Score**: Un punteggio di priorità per indicare la rilevanza (priorità di risposta).
    - **EPSS Score**: Valuta la probabilità di exploit attivo per una vulnerabilità.

Vulnerabilità critiche

1. **Bind Shell Backdoor Detection**:
    - **CVSS**: 9.8.
    - Descrizione: Rilevamento di una backdoor che potrebbe consentire a un attaccante il controllo remoto.
2. **SSL Version 2 and 3 Protocol Detection**:
    - **CVSS**: 9.8.
    - Descrizione: Versioni insicure di SSL sono abilitate, soggette a exploit come POODLE.
    - **Azione richiesta**: Forzare l'uso di protocolli TLS moderni.
3. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**:
    - **CVSS**: 10.0.
    - Problema: Utilizzo di numeri casuali prevedibili per chiavi crittografiche. Esistono due rilevamenti separati ma simili.
    - **Azione richiesta**: Aggiornare OpenSSH e OpenSSL.

Vulnerabilità alte

1. **NFS Shares World Readable**:
    - **CVSS**: 7.5.
    - Rischio: File condivisi tramite NFS accessibili globalmente.
2. **Samba Badlock Vulnerability**:
    - **CVSS**: 7.5.
    - Rischio: Attacchi man-in-the-middle nei server Samba.
3. **SSL Medium Strength Cipher Suites Supported (SWEET32)**:
    - **CVSS**: 7.5.
    - Problema: Cifrari deboli con una chiave di 64 bit che espone a possibili exploit.

Azioni consigliate

1. **Priorità critica**:
    - Risolvere le vulnerabilità con CVSS 10 e 9.8 (Debian OpenSSL, Tomcat Ghostcat, SSL, e VNC).
2. **Alto impatto**:
    - Proteggere i file condivisi (NFS).
    - Aggiornare o configurare correttamente ISC BIND.
3. **Medio impatto**:
    - Aggiornare protocolli di crittografia (TLS 1.2/1.3).
    - Eliminare certificati auto-firmati o non fidati.