Vulnerability Scanning

1. Obiettivo e Panoramica

Scopo dell'analisi L'obiettivo è individuare eventuali vulnerabilità su un target Metasploitable analizzando specificamente le porte "comuni".

Metodologia di Scansione

- **Target:** Metasploitable *(IP: 192.168.50.152/24)* .
- **Software utilizzato:** Nessus (per scansione, catalogazione minacce e risoluzioni).
- **Tipologia di scansione:** Basic Network Scan.
- **Porte scansionate:** Sono state analizzate le porte comunemente usate per servizi come SSH, HTTP e HTTPS. Nello specifico:
    - 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389.

2. Riepilogo dei Risultati

L'analisi ha prodotto i seguenti risultati quantitativi riguardo le minacce rilevate:

- **4 Vulnerabilità Critiche**
- **2 Vulnerabilità Alte**
- **13 Vulnerabilità Medie**
- **5 Vulnerabilità Basse**
- **66 Informazioni generali**

---

3. Analisi Dettagliata delle Vulnerabilità

3.1 Vulnerabilità Critiche (Critical)

A. Canonical Ubuntu Linux SEoL (8.04.x)

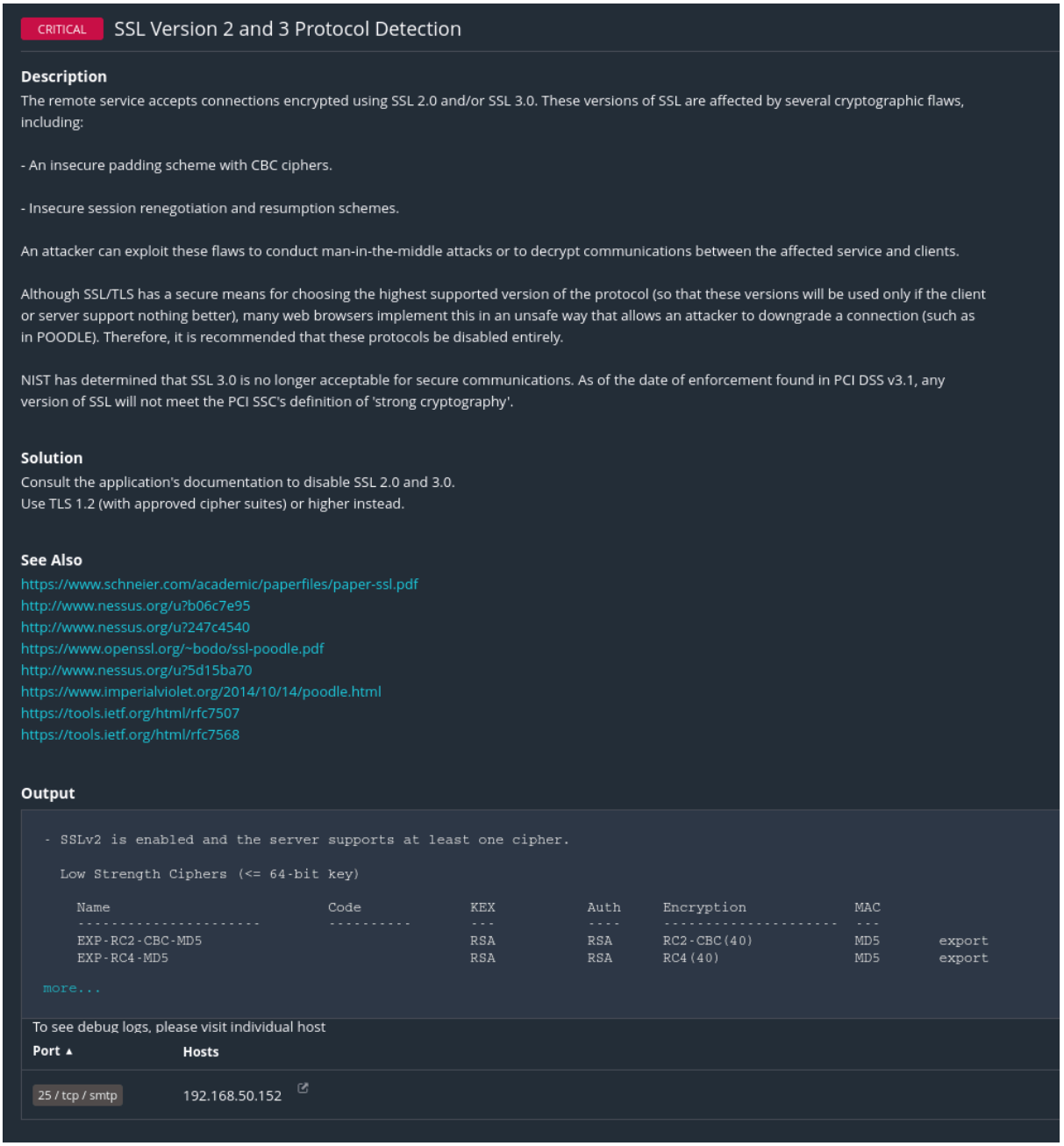
- **Descrizione:** Il sistema operativo rilevato è Ubuntu Linux 8.04.x, una versione non più mantenuta dal fornitore (End of Life). La mancanza di supporto implica che non vengono rilasciate nuove patch di sicurezza, rendendo il sistema esposto a vulnerabilità note.

- **Soluzione:** Aggiornare a una versione di Canonical Ubuntu Linux attualmente supportata.

B. SSL Version 2 and 3 Protocol Detection

- **Descrizione:** Il servizio remoto accetta connessioni crittografate utilizzando i protocolli obsoleti SSL 2.0 e/o SSL 3.0.Queste versioni soffrono di difetti crittografici. Un attaccante può sfruttare questi difetti per condurre attacchi Man-in-the-Middle (MITM) o decriptare le comunicazioni. Il NIST considera SSL 3.0 non più accettabile.

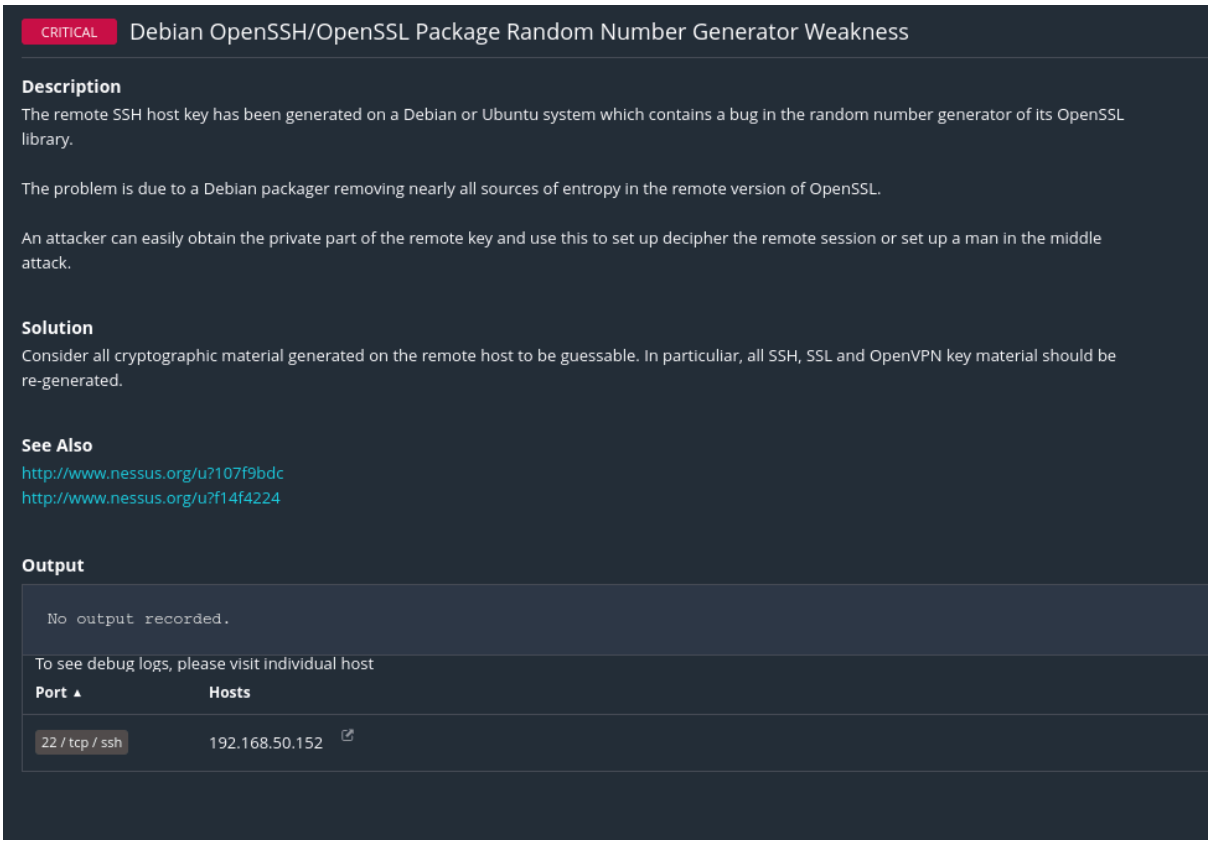
- **Soluzione:** Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizzare TLS 1.2 o superiore.



C. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- **Descrizione:** La chiave host SSH remota è stata generata su un sistema Debian/Ubuntu contenente un bug nel generatore di numeri casuali della libreria OpenSSL.

- **Soluzione:** Considerare compromesso tutto il materiale crittografico generato sull'host. Rigenerare tutte le chiavi SSH, SSL e OpenVPN e aggiornare il sistema.

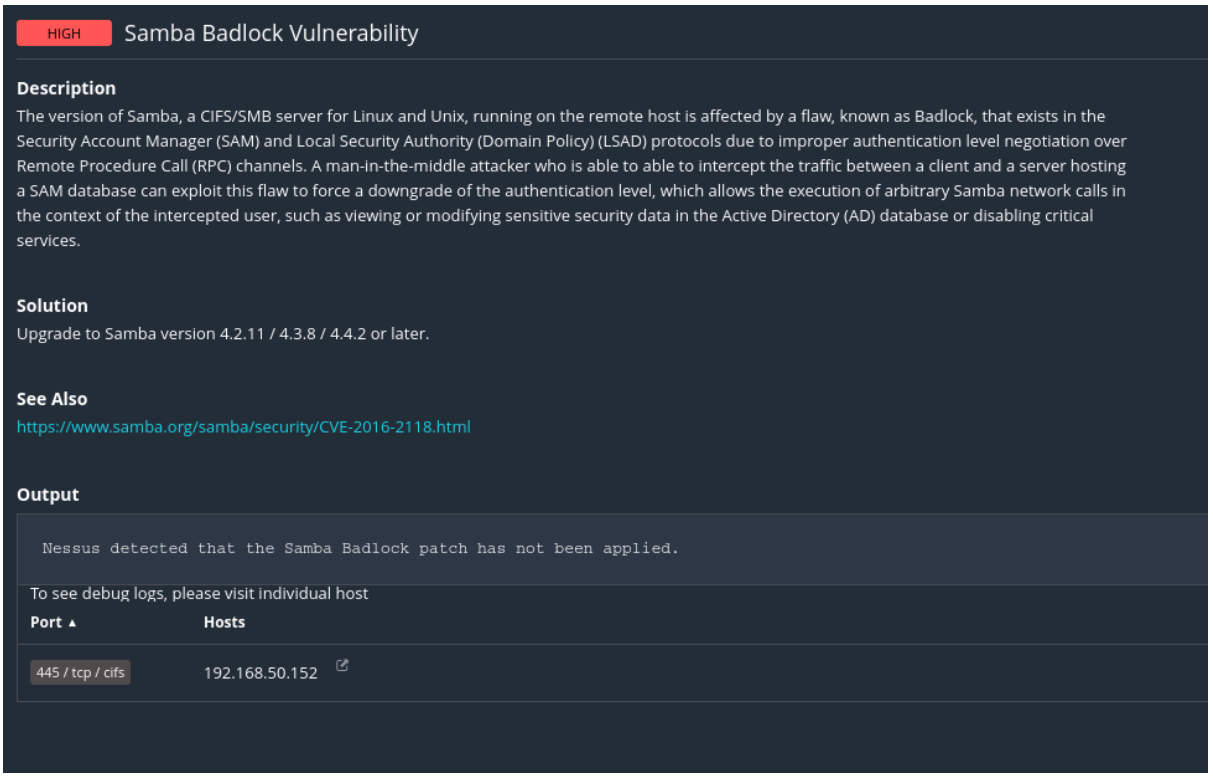


3.2 Vulnerabilità Alte (High)

A. Samba Badlock Vulnerability

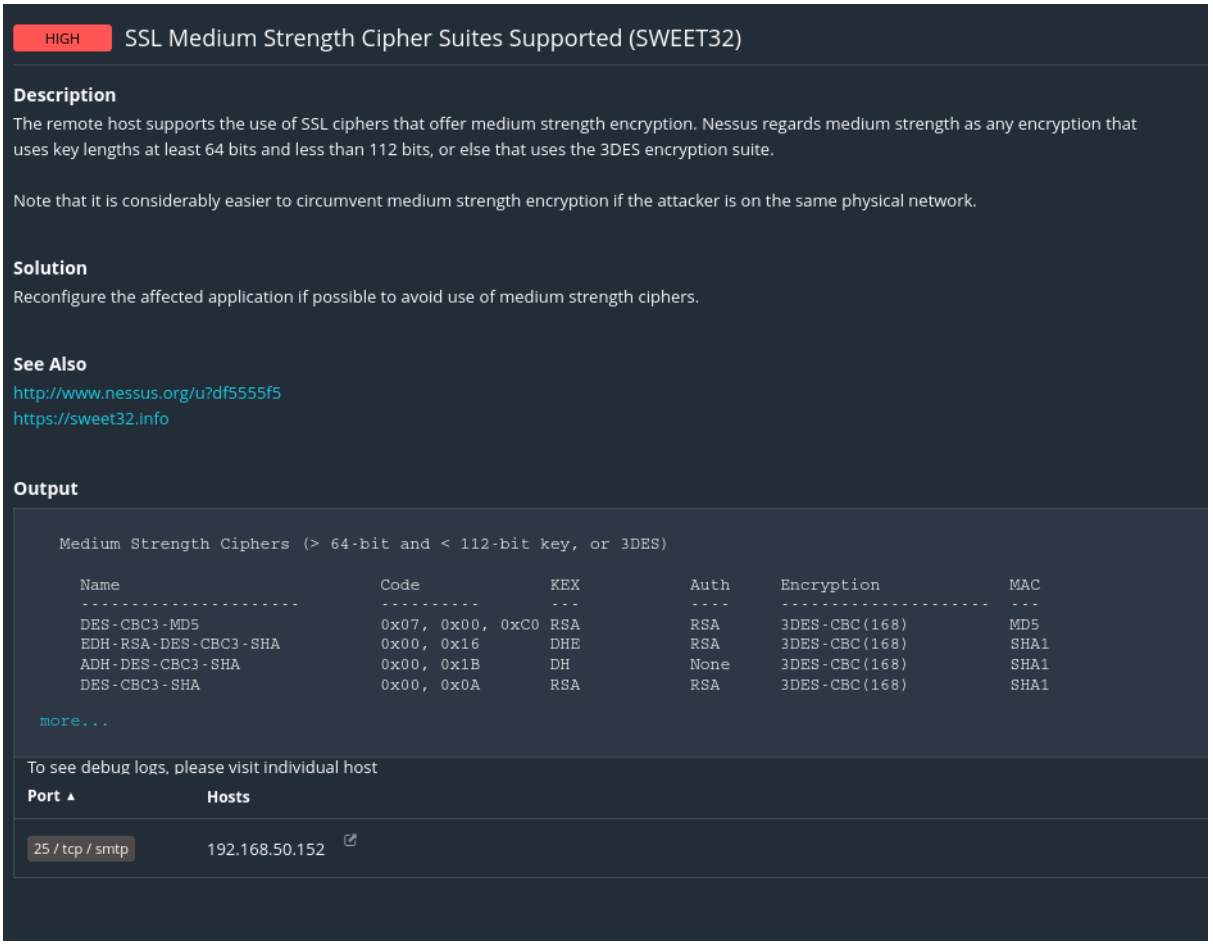
- **Descrizione:** La versione di Samba in esecuzione è affetta dalla vulnerabilità "Badlock" nei protocolli SAM (Security Account Manager) e LSAD.

- **Soluzione:** Aggiornare Samba alla versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.



B. SSL Medium Strength Cipher Suites Supported (SWEET32)

- **Descrizione:** L'host supporta cifrari SSL con crittografia di media potenza. È considerevolmente più facile aggirare la crittografia di media potenza se l'attaccante si trova sulla stessa rete fisica.
- **Soluzione:** Riconfigurare l'applicazione per evitare l'uso di cifrari di media potenza.



4. Conclusioni e Raccomandazioni Urgenti

L'analisi limitata alle sole porte comuni ha rivelato 4 criticità e 2 rischi alti, confermando l'estrema vulnerabilità del sistema target. Le debolezze riscontrate offrono molteplici vettori di attacco.

Piano d'azione raccomandato:

1. **Aggiornamento OS:** Aggiornare immediatamente il Sistema Operativo (Canonical Ubuntu) a una versione supportata.
2. **Hardening Protocolli:** Disabilitare SSL v2/v3 e le cifrature deboli/medie, forzando l'utilizzo di TLS 1.2 o superiore.
3. **Rigenerazione Chiavi:** Aggiornare OpenSSL/OpenSSH e rigenerare immediatamente tutte le chiavi SSH host a causa della prevedibilità del generatore di numeri casuali.
4. **Patching Servizi:** Aggiornare Samba per risolvere la vulnerabilità Badlock.