Report: Analisi delle Vulnerabilità con Nessus

Introduzione e Scopo dell'Analisi

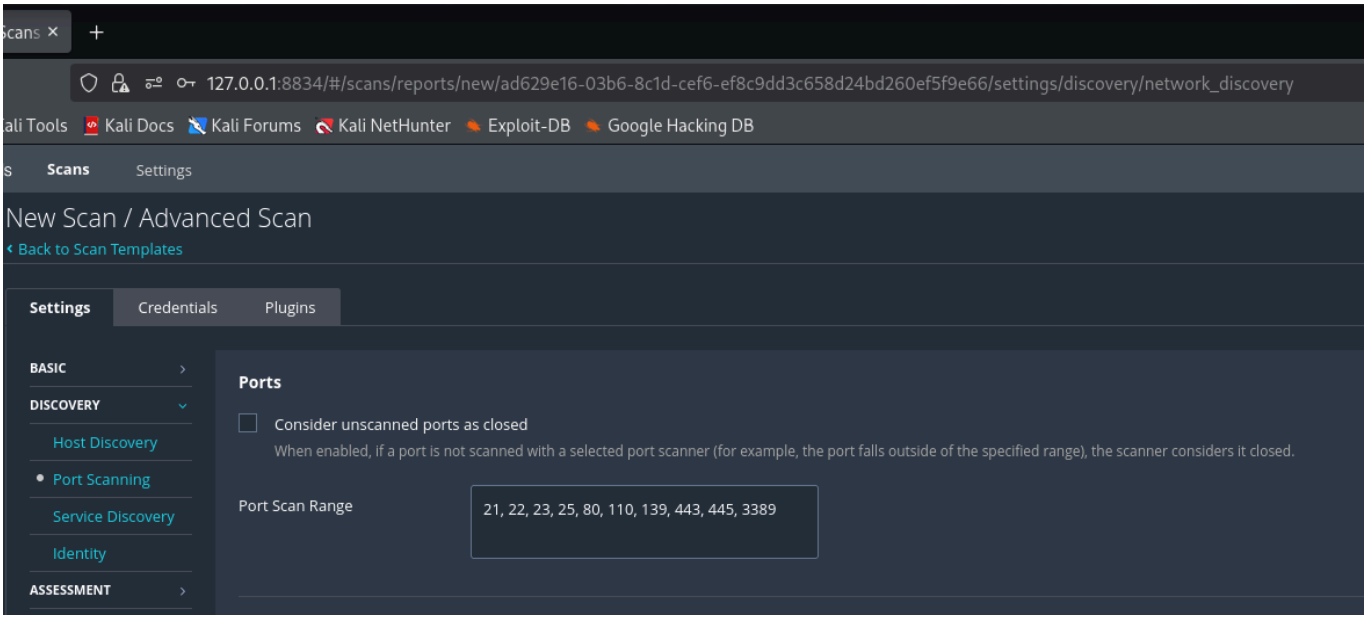
In questo report sono presenti i risultati di un'analisi di vulnerabilità eseguita sul sistema target "**Metasploitable**". L'analisi è stata condotta utilizzando lo scanner di rete **Tenable Nessus Essentials**, con l'obiettivo primario di identificare, classificare e analizzare le lacune di sicurezza presenti. Il documento mira a fornire un'analisi dettagliata e pratica delle vulnerabilità rilevate, in particolare quelle classificate come critiche e alte, al fine di supportare le azioni necessarie per sistemare i problemi rilevati.

Dettagli della Scansione

Obiettivo: **Metasploitable** (192.168.50.11)

Strumento Utilizzato: **Tenable Nessus Essentials**

Range porte scansionate: **21-23, 25, 80, 110, 139, 443, 445, 3389**



Preparazione e Configurazione della Scansione

Una configurazione precisa è la chiave per ottenere risultati utili. Invece di una scansione generica, diremo a Nessus esattamente cosa e come cercare.

Impostare il Bersaglio

Il nostro "**Target**" è la macchina virtuale **Metasploitable**. La macchina avrà come indirizzo IP 192.168.50.11 che inseriremo in Nessus per poterlo analizzare.

Ecco le porte che analizzeremo e i servizi che solitamente ospitano:

- **Porta 21: FTP** (File Transfer Protocol) - Utilizzato per il trasferimento di file tra client e server.
- **Porta 22: SSH** (Secure Shell) - Consente l'accesso remoto sicuro (cifrato) a riga di comando.
- **Porta 23: Telnet** - Protocollo di accesso remoto non cifrato e obsoleto (insicuro).
- **Porta 25: SMTP** (Simple Mail Transfer Protocol) - Utilizzato dai server di posta per l'invio e l'inoltro di email.
- **Porta 80: HTTP** (Hypertext Transfer Protocol) - Standard per la navigazione Web (non cifrato).
- **Porta 110: POP3** (Post Office Protocol 3) - Consente ai client di scaricare le email da un server.
- **Porta 139: NetBIOS** - Protocollo storico per la condivisione di risorse in reti Windows (Legacy).
- **Porta 443: HTTPS** (HTTP Secure) - Versione sicura (cifrata) di HTTP, essenziale per il Web moderno.
- **Porta 445: SMB** (Server Message Block) - Il protocollo moderno per la condivisione di file e stampanti in ambienti Windows e Linux.
- **Porta 3389: RDP** (Remote Desktop Protocol) - Permette l'accesso e il controllo dell'interfaccia grafica di un computer remoto.

Tipo di Scansione

Nessus offre diverse opzioni. Le principali sono:

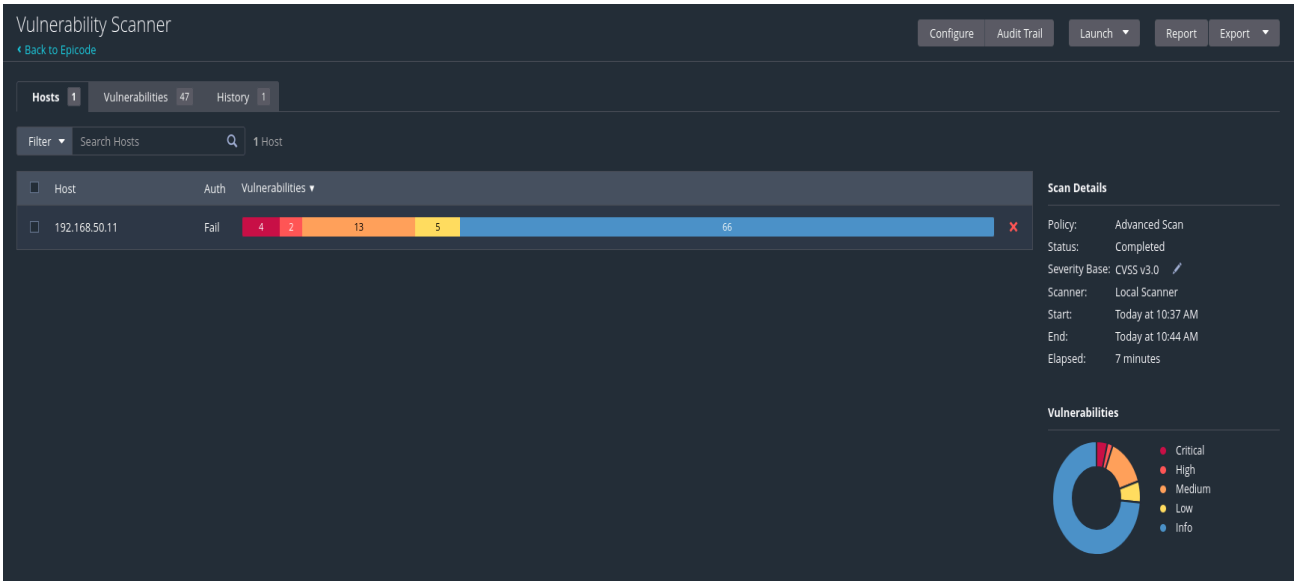
• **Basic Network Scan**: Utilizza una configurazione predefinita, ottima per un'analisi rapida e generale.

• **Advanced Scan**: Permette una personalizzazione completa, inclusa la possibilità di specificare un intervallo di porte preciso, come abbiamo scelto di fare in questo esercizio.

Riepilogo dei Risultati

La classificazione delle vulnerabilità in base al loro livello di severità, valutato tramite il **Common Vulnerability Scoring System (CVSS)**, è un passaggio fondamentale per una gestione efficace della sicurezza. Questo approccio consente di prioritizzare gli interventi, concentrando le risorse prima sulle minacce che presentano il rischio più elevato per l'integrità, la riservatezza e la disponibilità del sistema. La scansione ha identificato un numero significativo di vulnerabilità, distribuite su vari livelli di gravità.

Vulnerabilità riscontrate:



Riepilogo delle Vulnerabilità per Severità

CRITICO - - - - - - > 4 vulnerabilità trovate

ALTO - - - - - - - - - > 2 vulnerabilità trovate

MEDIO - - - - - - - - > 13 vulnerabilità trovate

BASSO - - - - - - - - > 5 vulnerabilità trovate

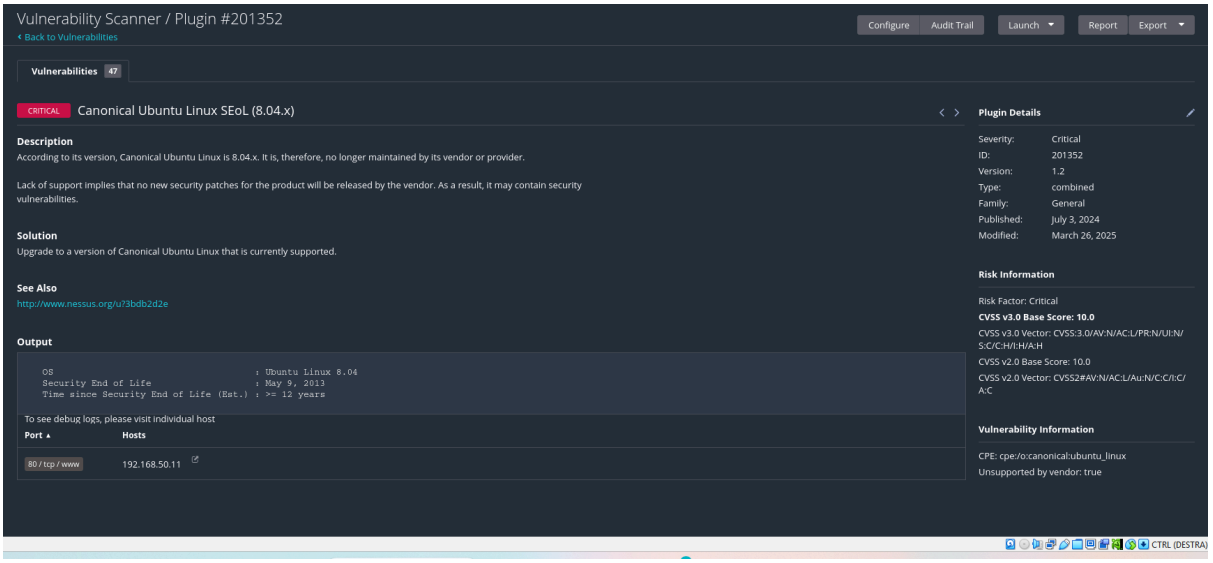
INFO - - - - > 66

Data l'elevata concentrazione di vulnerabilità critiche e alte, andremo ad analizzare con un'analisi dettagliata ciascuna di esse.

Analisi Dettagliata delle Vulnerabilità critiche

1) CRITICAL: CANONICAL UBUNTU LINUX SEoL

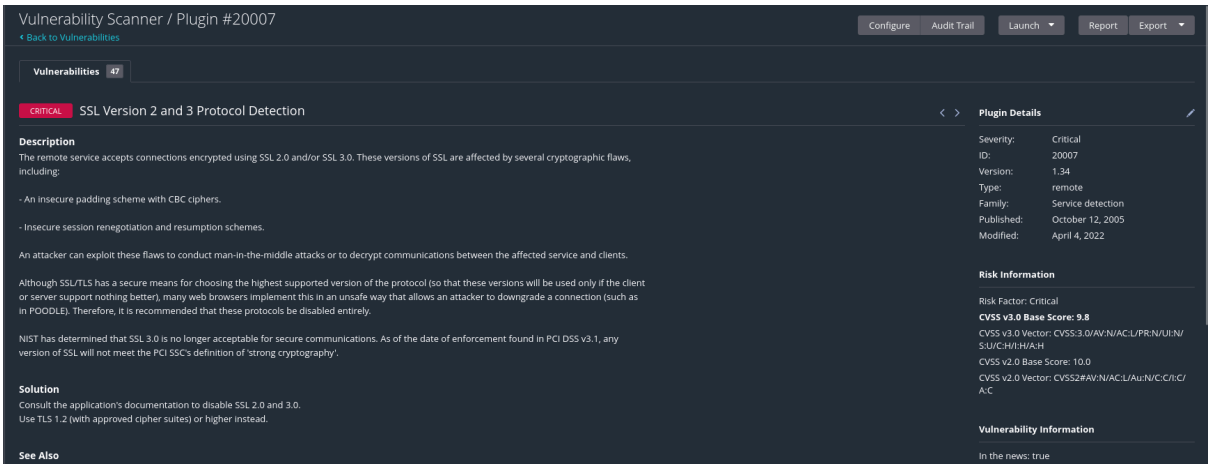
Descrizione del Rischio: Il sistema operativo rilevato, Ubuntu 8.04.x, non è più supportato dal produttore. Ciò significa che non riceve più aggiornamenti di sicurezza, incluse le patch per vulnerabilità scoperte di recente. Un sistema operativo obsoleto è un bersaglio primario per gli aggressori, poiché le sue debolezze sono spesso pubbliche e gli exploit facilmente disponibili, esponendo il sistema a un rischio di compromissione quasi certo.



Possibile soluzione: Questo sistema non riceve aggiornamenti di sicurezza da oltre 12 anni. Non esistono "patch" da scaricare per chiudere questa falla perché il problema è l'intero sistema operativo. **Soluzione Unica: Aggiornamento del Sistema Operativo.** Non esiste un modo per rendere sicuro Ubuntu 8.04 oggi. L'unico rimedio efficace è **sostituire il sistema operativo** con una versione supportata.

2) Critical : SSL Version 2 and 3 Protocol Detection

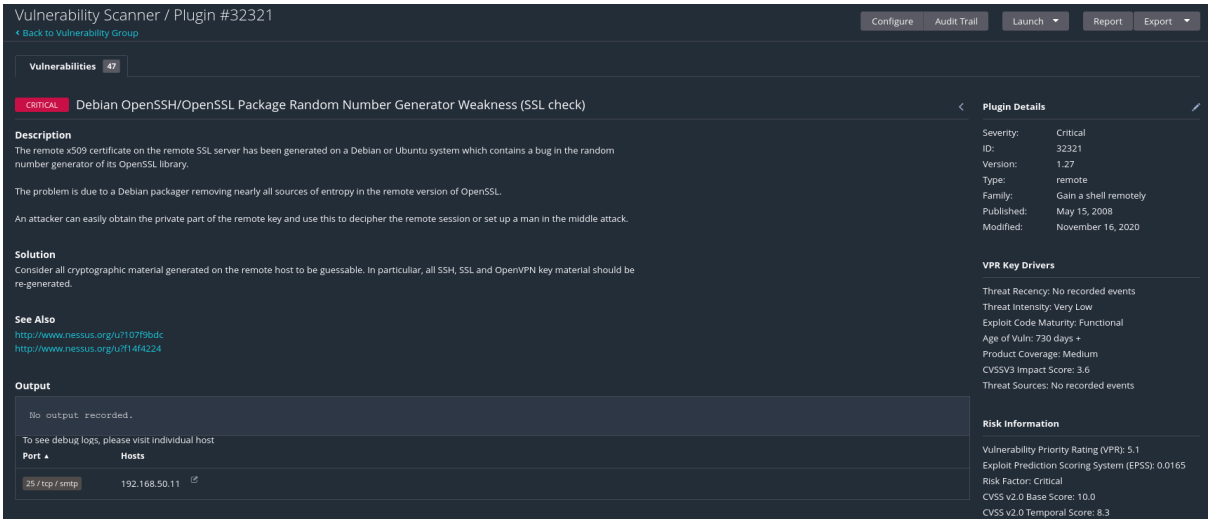
Descrizione del Rischio: La scansione ha rilevato il supporto per i protocolli crittografici SSL versione 2 (SSLv2) e versione 3 (SSLv3). Entrambi i protocolli sono considerati obsoleti e insicuri, presentando gravi vulnerabilità di progettazione (come POODLE per SSLv3) che permettono a un aggressore di intercettare e decifrare il traffico di rete, compromettendo la confidenzialità dei dati trasmessi.



Possibile soluzione: Disabilitare SSLv2/v3 e usare TLS 1.2.

3) Critical: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Descrizione del Rischio: Nessus ha rilevato che il certificato X.509 utilizzato dal servizio SMTP (posta elettronica) sulla porta 25 è stato generato su una versione di Debian/Ubuntu affetta da un grave bug nella libreria OpenSSL.
Il problema tecnico: Il generatore di numeri pseudo-casuali (PRNG) di OpenSSL su queste versioni datate non utilizzava sufficiente entropia. A causa di un errore umano (un manutentore del pacchetto rimosse delle righe di codice per evitare avvisi di debug), lo spazio delle chiavi possibili si è ridotto drasticamente. Invece di miliardi di combinazioni, esistono solo poche migliaia di chiavi possibili per ogni architettura (circa 32.767).



Possibile soluzione:

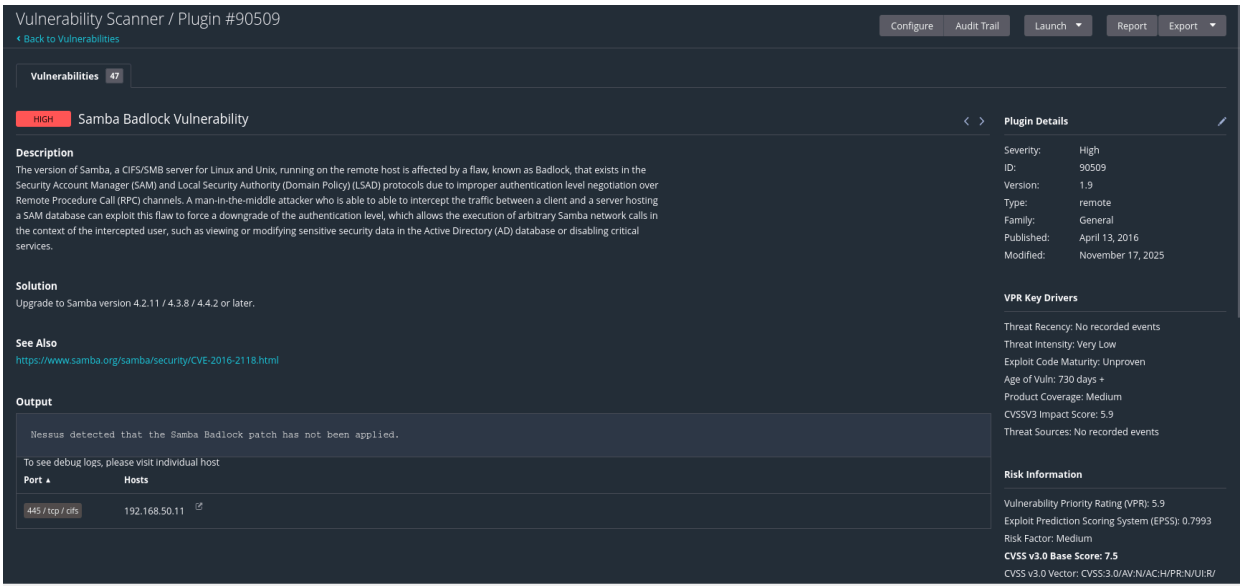
1. **Patching del Sistema:** Aggiornare immediatamente il pacchetto `openssl` e le relative librerie (`libssl`) a una versione non vulnerabile tramite il gestore pacchetti del sistema operativo.
2. **Rigenerazione delle Chiavi :** Eliminare e rigenerare da zero tutti i certificati SSL/TLS, le chiavi host SSH e le chiavi utente SSH che sono state create sulla macchina vulnerabile. Le vecchie chiavi sono da considerarsi compromesse per sempre.

3. **Revoca:** Revocare i vecchi certificati presso la Certification Authority e rimuovere le vecchie chiavi pubbliche dai file `authorized_keys` degli altri server.

Analisi Dettagliata delle Vulnerabilità alte

1) High: Samba Badlock Vulnerability

Descrizione del Rischio: La versione di Samba in esecuzione è affetta dalla vulnerabilità nota come "Badlock" (CVE-2016-2118). Questa falla di sicurezza può essere sfruttata per eseguire attacchi man-in-the-middle (MITM) contro le connessioni di autenticazione SAMR e LSA, consentendo a un aggressore di impersonare utenti e ottenere un'escalation dei privilegi all'interno del dominio o del sistema.



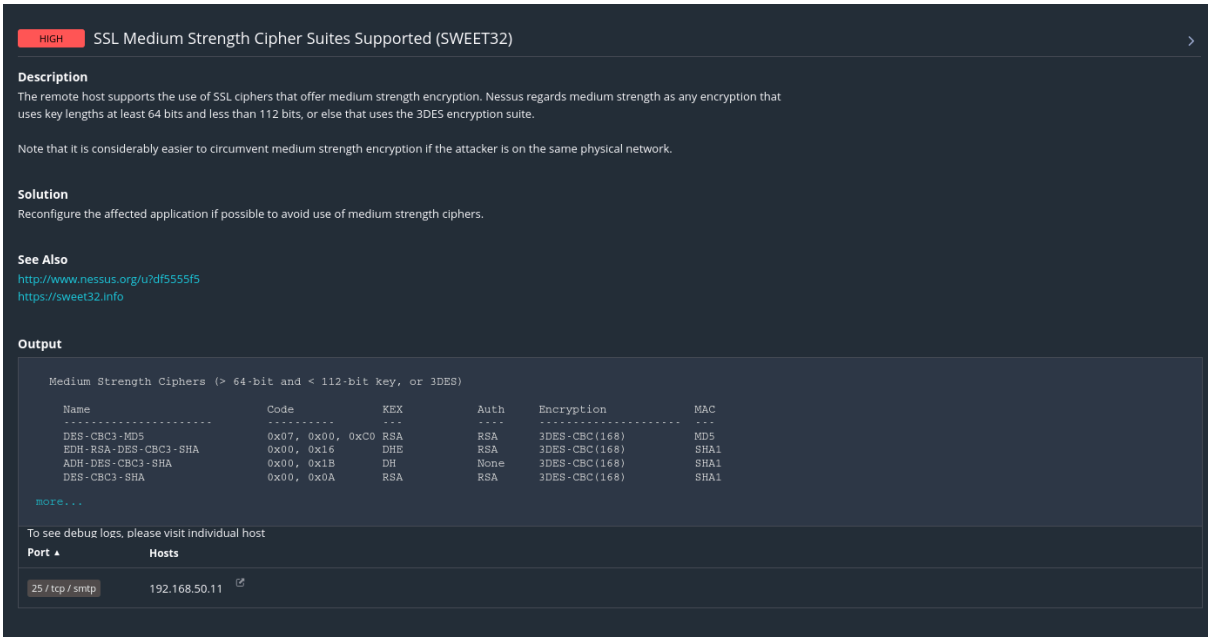
Possibile soluzione: aggiornamento del software server.

1. **Aggiornamento Software:** Aggiornare Samba a una versione che contenga la patch per **Badlock.** Secondo il report di Nessus, le versioni sicure partono dalla 4.2.11, 4.3.8, 4.4.2 o superiori.
2. **Configurazione:** Dopo l'aggiornamento, verificare nel file `smb.conf` che le opzioni di firma del server (`server signing`)

siano impostate su "mandatory" o "required" per prevenire ulteriori tentativi di MitM, sebbene questo possa impattare le prestazioni.

2) SSL Medium Strength Cipher Suites Supported (SWEET32)

Descrizione del rischio: i server SMTP accetta connessioni cifrate utilizzando suite di cifratura di "media forza" (chiavi tra 64 e 112 bit) o che utilizzano l'algoritmo 3DES. L'output di Nessus mostra esplicitamente l'uso di **3DES-CBC.** Questa configurazione espone il server all'attacco **SWEET32** (CVE-2016-2183). L'algoritmo 3DES è un cifrario a blocchi di 64 bit; se un attaccante riesce a catturare una grande quantità di traffico cifrato (circa 32 GB), può sfruttare le collisioni nei blocchi per recuperare parti del testo in chiaro (come i cookie di sessione o le credenziali), specialmente se si trova sulla stessa rete fisica.



Possibile soluzione:

1) **Re-configurazione: M**odificare la configurazione del servizio (in questo caso Postfix o il servizio che gestisce l'SMTP) per disabilitare il supporto ai cifrari obsoleti.
2) **Hardening:** Permettere solo cifrari "High Strength" (es. AES-128, AES-256) e disabilitare esplicitamente SSLv3, TLS 1.0 e qualsiasi suite che includa DES, 3DES o RC4.

Conclusioni e Valutazione del Rischio

L'attività di Vulnerability Assessment condotta sulla macchina target (IP: 192.168.50.11) ha evidenziato uno stato di sicurezza **estremamente critico**.

L'analisi tecnica porta alle seguenti considerazioni finali:

1. Causa Radice: Obsolescenza del Sistema Operativo

La quasi totalità dei rischi di sicurezza deriva dall'utilizzo di **Canonical Ubuntu 8.04**, un sistema operativo in stato di *End-of-Life* (SEoL). Non ricevendo aggiornamenti di sicurezza da oltre dieci anni, il sistema è strutturalmente vulnerabile e non è possibile applicare patch standard contro exploit noti e pubblici.

2. Compromissione Totale della Riservatezza dei Dati

La crittografia è inefficace. La combinazione di protocolli obsoleti (**SSLv2/v3**), cifrari deboli (**SWEET32**) e il difetto critico nel generatore di numeri casuali (**OpenSSL PRNG**) consente a un attaccante di intercettare e decifrare con estrema facilità tutto il traffico cifrato (incluso HTTPS e SSH).

3. Esposizione a Rischi di Movimento Laterale nella Rete

Vulnerabilità specifiche, come **Samba Badlock**, non rappresentano un rischio solo per la macchina isolata, ma espongono la rete locale a potenziali attacchi ***Man-in-the-Middle*** (MitM). Questo facilita agli aggressori il movimento e l'accesso ad altri sistemi connessi (movimenti laterali).