

# Report: Analisi delle Vulnerabilità con Nessus

## Introduzione e Scopo dell'Analisi

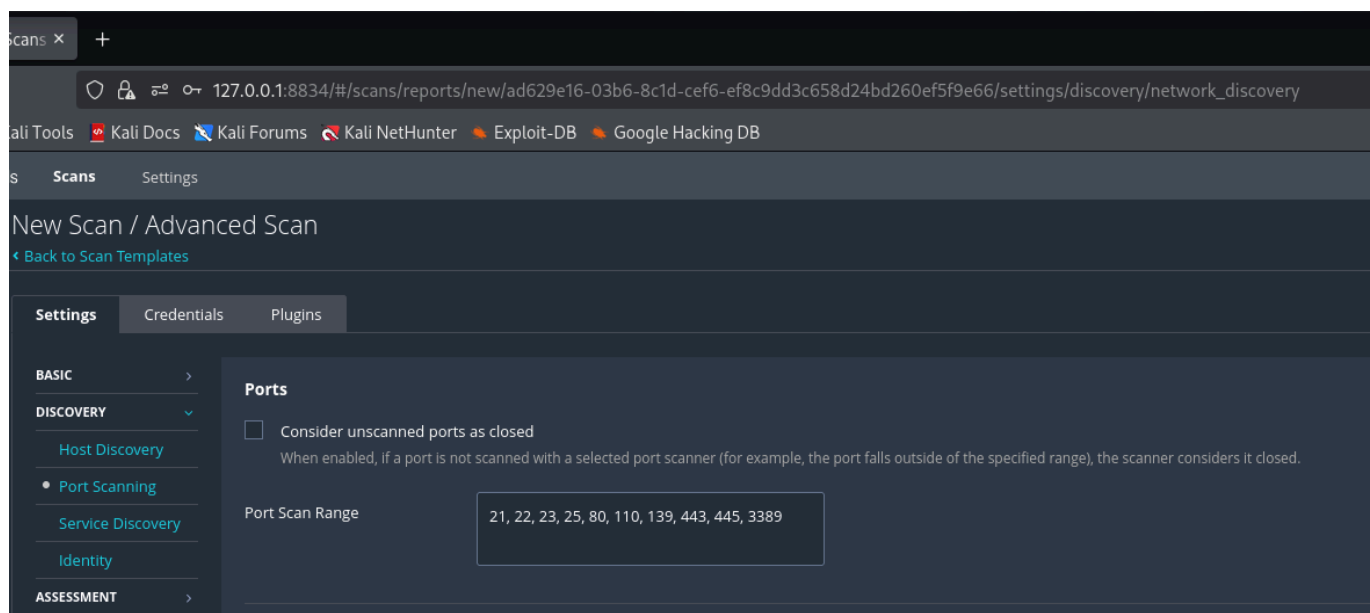
In questo report sono presenti i risultati di un'analisi di vulnerabilità eseguita sul sistema target "**Metasploitable**". L'analisi è stata condotta utilizzando lo scanner di rete **Tenable Nessus Essentials**, con l'obiettivo primario di identificare, classificare e analizzare le lacune di sicurezza 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

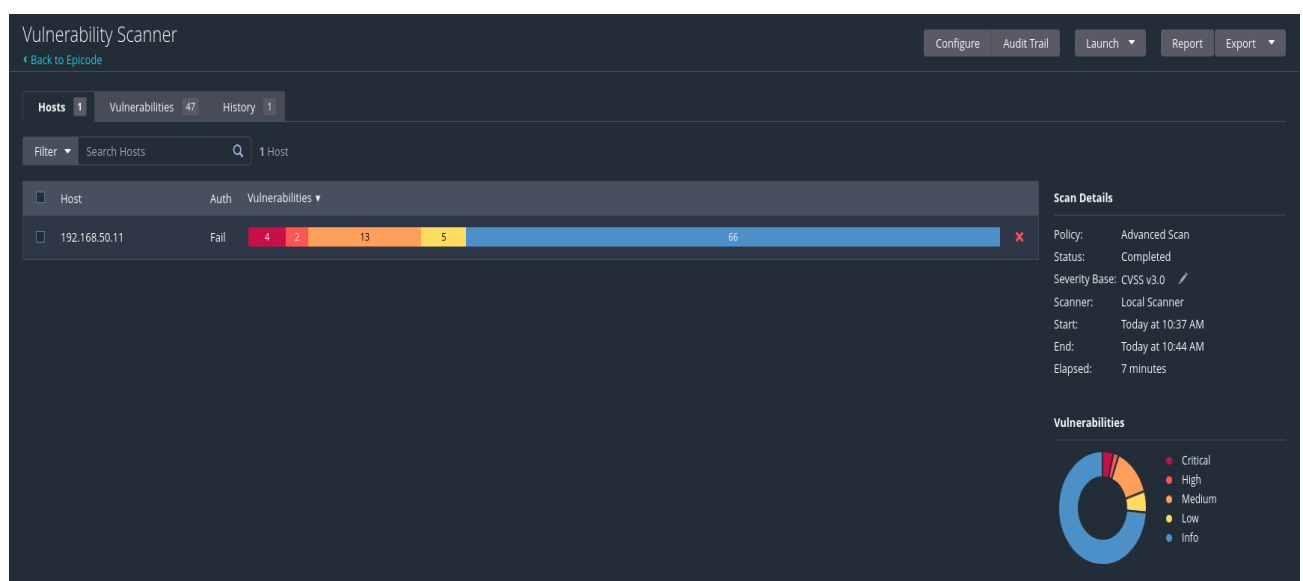
**Nessus** offre diverse opzioni. Le principali sono:

- **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.

The screenshot displays the Nessus Vulnerability Scanner interface for Plugin #201352. The main title is 'Vulnerability Scanner / Plugin #201352'. Below the title, there are tabs for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. The 'Vulnerabilities' section shows 47 items, with the first one being 'CRITICAL: Canonical Ubuntu Linux SEoL (8.04.x)'. The 'Description' section states: 'According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.' The 'Solution' section suggests: 'Upgrade to a version of Canonical Ubuntu Linux that is currently supported.' The 'See Also' section provides a link: 'http://www.nessus.org/u/3bdb2d2e'. The 'Output' section shows a table with columns 'OS', 'Security End of Life', and 'Time since Security End of Life (Est.)'. The table contains one row: 'Ubuntu Linux 8.04', 'May 9, 2013', and '>= 12 years'. The 'Plugin Details' section on the right shows: 'Severity: Critical', 'ID: 201352', 'Version: 1.2', 'Type: combined', 'Family: General', 'Published: July 3, 2024', and 'Modified: March 26, 2025'. The 'Risk Information' section shows: 'Risk Factor: Critical', 'CVSS v3.0 Base Score: 10.0', 'CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H', 'CVSS v2.0 Base Score: 10.0', and 'CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C'. The 'Vulnerability Information' section shows: 'CPE: cpe:/o:canonical:ubuntu\_linux' and 'Unsupported by vendor: true'. The bottom of the interface shows a status bar with icons and the text 'CTRL (DESTRA)'.

OS	Security End of Life	Time since Security End of Life (Est.)
Ubuntu Linux 8.04	May 9, 2013	>= 12 years

**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.

The screenshot shows a web-based vulnerability scanner interface. At the top, it says 'Vulnerability Scanner / Plugin #20007'. Below this, there's a navigation bar with 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. The main content area is titled 'Vulnerabilities 47'. A specific vulnerability is highlighted: 'CRITICAL SSL Version 2 and 3 Protocol Detection'. The description explains that the remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which are affected by several cryptographic flaws, including insecure padding schemes and session renegotiation. It also mentions that an attacker can exploit these flaws for man-in-the-middle attacks. The solution section advises consulting application documentation to disable SSL 2.0 and 3.0, and using TLS 1.2 instead. On the right, a 'Plugin Details' sidebar shows metadata like ID (20007), Version (1.34), Type (remote), and Family (Service detection). It also includes a 'Risk Information' section with a CVSS v3.0 Base Score of 9.8 and a 'Vulnerability Information' section noting it's in the news.

Section	Details
<b>Description</b>	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: <ul style="list-style-type: none"><li>- An insecure padding scheme with CBC ciphers.</li><li>- Insecure session renegotiation and resumption schemes.</li></ul> An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.
<b>Solution</b>	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.
<b>See Also</b>	
<b>Plugin Details</b>	Severity: Critical ID: 20007 Version: 1.34 Type: remote Family: Service detection Published: October 12, 2005 Modified: April 4, 2022
<b>Risk Information</b>	Risk Factor: Critical CVSS v3.0 Base Score: 9.8 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS v2.0 Base Score: 10.0 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
<b>Vulnerability Information</b>	In the news: true

**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).

Vulnerability Scanner / Plugin #32321

Configure Audit Trail Launch Report Export

Vulnerabilities 47

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

**Description**

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

**Solution**

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

**See Also**

<http://www.nessus.org/u/1079bdc>  
<http://www.nessus.org/u/114f4224>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
25 / tcp / smtp	192.168.50.11

**Plugin Details**

Severity: Critical  
ID: 32321  
Version: 1.27  
Type: remote  
Family: Gain a shell remotely  
Published: May 15, 2008  
Modified: November 16, 2020

**VPR Key Drivers**

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Functional  
Age of Vuln: 730 days +  
Product Coverage: Medium  
CVSSV3 Impact Score: 3.6  
Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 5.1  
Exploit Prediction Scoring System (EPSS): 0.0165  
Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Temporal Score: 8.3

### Possibile soluzione:

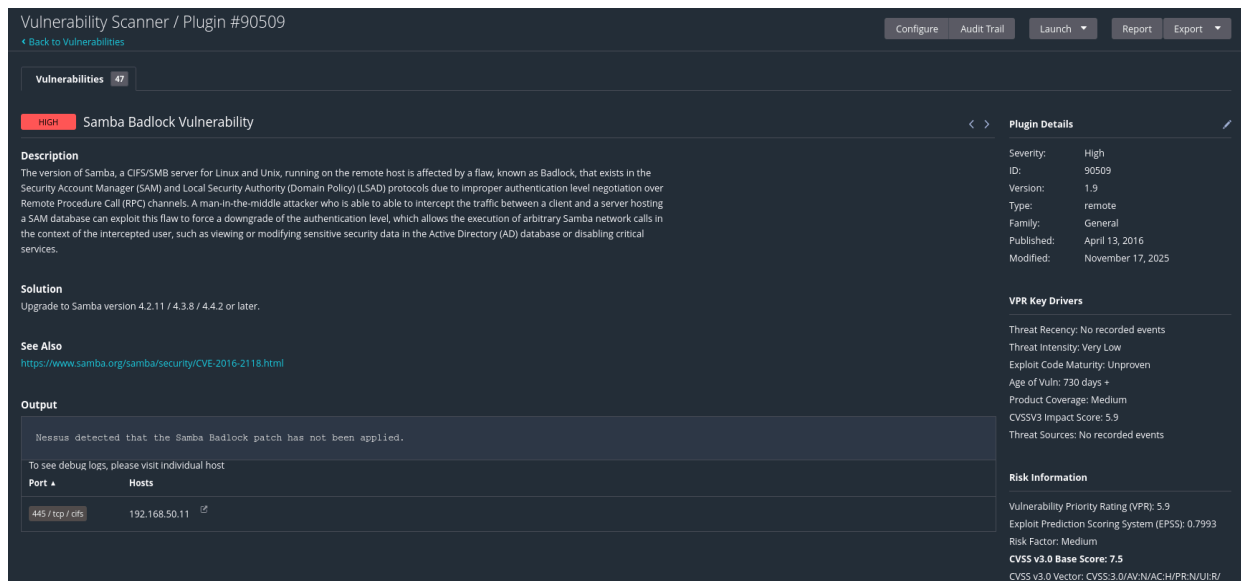
- Patching del Sistema:** Aggiornare immediatamente il pacchetto **openssl** e le relative librerie (**libssl**) a una versione non vulnerabile tramite il gestore pacchetti del sistema operativo.
- Rigenerazione delle Chiavi :** Eliminare e rigenerare da zero tutti i certificati SSL/TLS, le chiavi host 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.



The screenshot displays the Nessus Vulnerability Scanner interface for a specific vulnerability. The top navigation bar includes links for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. The main header shows 'Vulnerability Scanner / Plugin #90509' and a 'Back to Vulnerabilities' link. The vulnerability is identified as 'Samba Badlock Vulnerability' with a severity of 'HIGH'. The description explains that the Samba server is affected by a flaw in the SAMR and LSA protocols, allowing a man-in-the-middle attacker to intercept traffic and force a downgrade of the authentication level. The solution is to upgrade Samba to version 4.2.11 / 4.3.8 / 4.4.2 or later. The 'See Also' section provides a link to the CVE entry. The 'Output' section shows a message from Nessus: 'Nessus detected that the Samba Badlock patch has not been applied.' Below this, a table lists the affected hosts, showing port 445/tcp on host 192.168.50.11. The right sidebar contains 'Plugin Details' (Severity: High, ID: 90509, Version: 1.9, Type: remote, Family: General, Published: April 13, 2016, Modified: November 17, 2025), 'VPR Key Drivers' (Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days +, Product Coverage: Medium, CVSSv3 Impact Score: 5.9, Threat Sources: No recorded events), and 'Risk Information' (Vulnerability Priority Rating (VPR): 5.9, Exploit Prediction Scoring System (EPSS): 0.7993, Risk Factor: Medium, CVSS v3.0 Base Score: 7.5, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/).

**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.

HIGH

SSL Medium Strength Cipher Suites Supported (SWEET32)

>

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.  
  
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

<http://www.nessus.org/u?d555f5>  
<https://sweet32.info>

Output

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)  

Name	Code	Key	Auth	Encryption	MAC
DES-CBC-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC(168)	MD5
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DHE	RSA	3DES-CBC(168)	SHA1
ADH-DES-CBC3-SHA	0x00, 0x1B	DH	None	3DES-CBC(168)	SHA1
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

  
[more...](#)

To see debug logs, please visit individual host

Port

Hosts

25 / tcp / smtp192.168.50.11

### Possibile soluzione:

- 1) **Re-configurazione:** Modificare 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).