

# 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.

**CRITICAL** Canonical Ubuntu Linux SEoL (8.04.x)

**Description**

According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.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.

**Solution**

Upgrade to a version of Canonical Ubuntu Linux that is currently supported.


**See Also**

<http://www.nessus.org/u?3bdb2d2e>

**Output**

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

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	192.168.50.152 

## 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.

**CRITICAL** SSL Version 2 and 3 Protocol Detection

**Description**

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:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

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'.

**Solution**

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

**See Also**

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>  
<http://www.nessus.org/u7b06c7e95>  
<http://www.nessus.org/u7247c4540>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.nessus.org/u75d15ba70>  
<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://tools.ietf.org/html/rfc7507>  
<https://tools.ietf.org/html/rfc7568>

**Output**

```
- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

      Name                               Code          KEX          Auth          Encryption          MAC
      -----
      EXP - RC2 - CBC - MD5              -----
      EXP - RC4 - MD5                    -----
      more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
25 / tcp / smtp	192.168.50.152

## 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.

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

**Description**

The remote SSH host key 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 set up 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?107f9bdc>  
<http://www.nessus.org/u?f14f4224>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
22 / tcp / ssh	192.168.50.152 

## 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.

**HIGH** Samba Badlock Vulnerability

**Description**

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

**Solution**

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.


**See Also**

<https://www.samba.org/samba/security/CVE-2016-2118.html>

**Output**

```
Nessus detected that the Samba Badlock patch has not been applied.
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.50.152 

## 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.

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?df5555f5>  
<https://sweet32.info>

### Output

```


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

Name                               Code                KEX          Auth      Encryption          MAC
-----
DES-CBC3-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 / smtp	192.168.50.152 

## 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.