Vulnerability Scanning

Obbiettivo :

Trovare eventuali vulnerabilità su un target Metasploitable di sole porte comuni analizzando però solo le porte “comuni”.

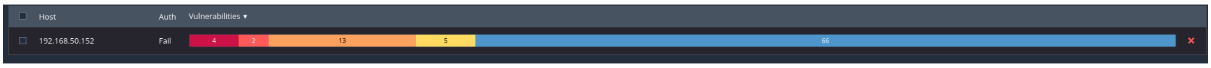
Overview :

- Vulnerability Scanning su un target Metasploitable di sole porte comuni.
- **Porte scansionate** : 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389
- **Tipo scansione** : Basic Network Scan

Si è deciso di effettuare un vulnerability scanning su un target Metasploitable *(Ip 192.168.50.152/24)* delle porte comuni.
Per porte comuni si intendono tutte quelle **porte comunemente usate per servizi** come SSH, HTTP, HTTPS.

Per effettuare il Vulnerability Scanning si utilizza il software **Nessus** che permette lo scansione di un target e la catalogazione delle minacce trovate con eventuali risoluzioni.

Results :



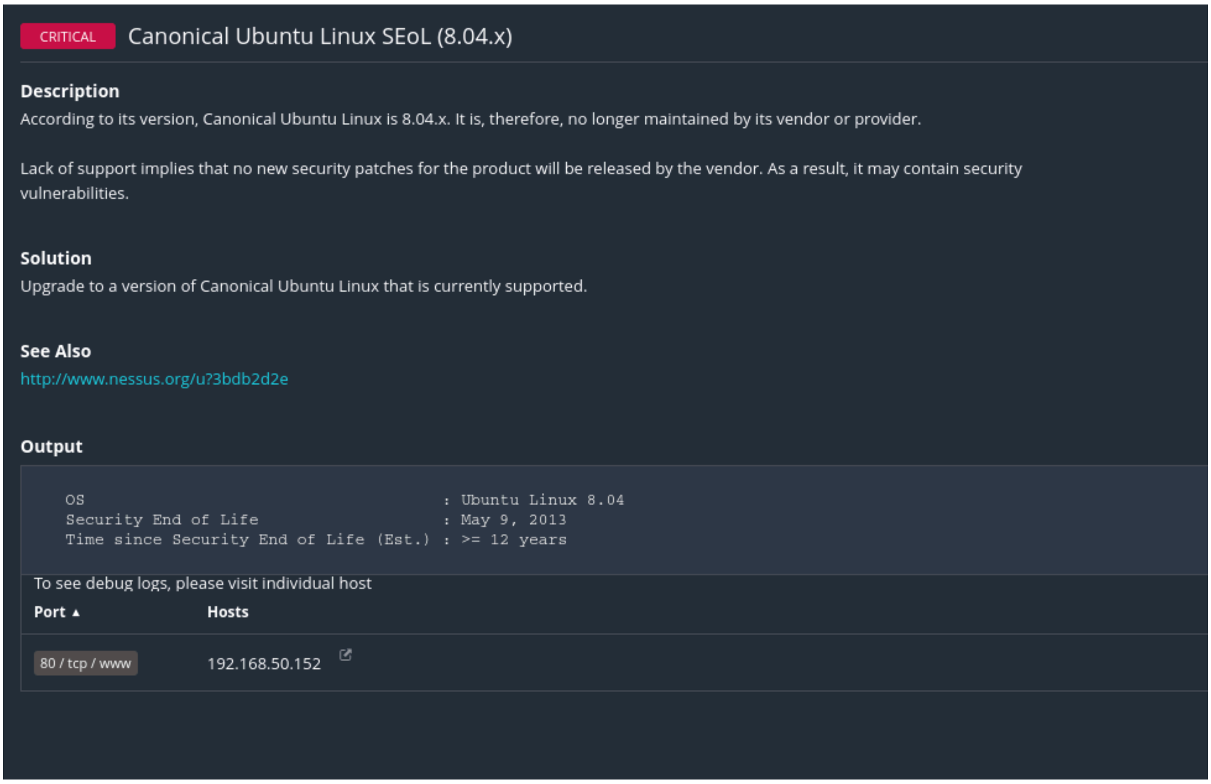
□	Host	Auth	Vulnerabilities ▾					
□	192.168.50.152	Fail	4	2	13	5	66	✕

Figura 1 : ScreenShot del risultato della Vulnerability Scanning su Nessus

- 4 Vulnerabilità critiche
- 2 vulnerabilità alte
- 13 vulnerabilità medie
- 5 vulnerabilità basse
- 66 informazioni

Analisi di alcune vulnerabilità critiche :

Canonical Ubuntu Linux SEoL (8.04.x)



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According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.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

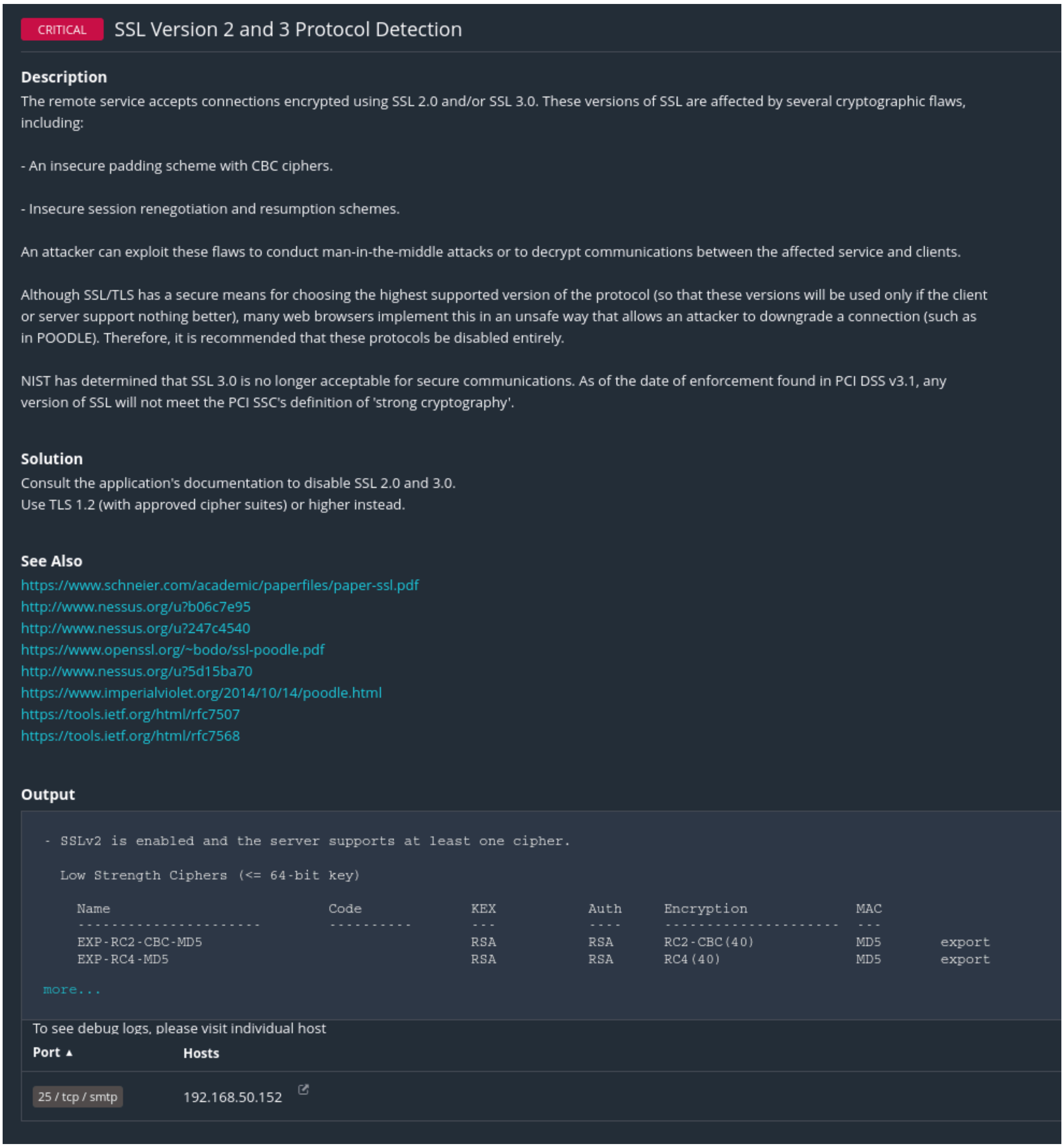
```
  OS                                      : Ubuntu Linux 8.04
  Security End of Life                    : May 9, 2013
  Time since Security End of Life (Est.)  : >= 12 years
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	192.168.50.152

Figure 2 : Versione Obsoleta e non più aggiornata
Soluzione : Aggiornare ad una versione supportata e aggiornata

SSL Version 2 and 3 Protocol Detection



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/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Output

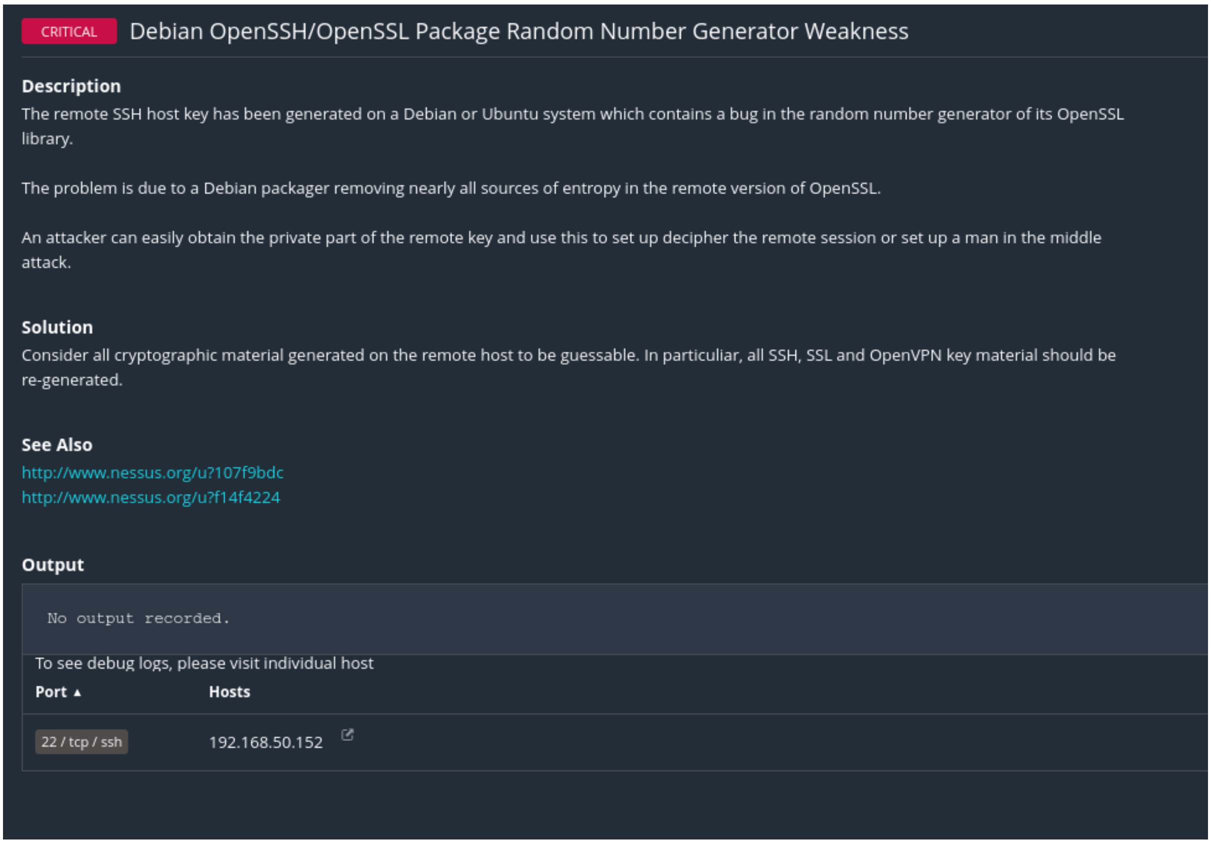
```
- SSLv2 is enabled and the server supports at least one cipher.

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5                                RSA           RSA      RC2-CBC(40)            MD5        export
    EXP-RC4-MD5                                    RSA           RSA      RC4(40)                MD5        export

more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
25 / tcp / smtp	192.168.50.152

Figure 3 : Protocolli SSL obsoleti ciò crea possibilità di attacchi Man-in-the-Middle e cifrature deboli.
Soluzione : Aggiornare o disabilitare protocolli, disabilitare cifrature deboli

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness



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 particuliar, 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

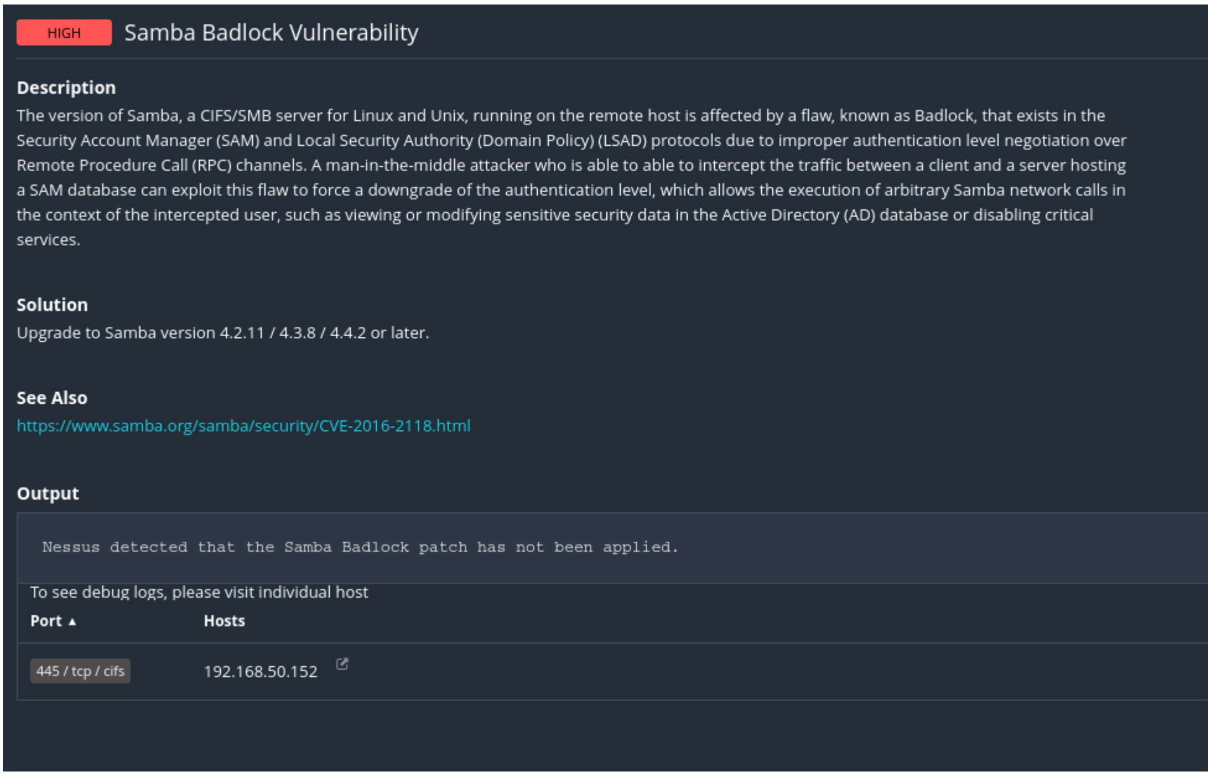
```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
22 / tcp / ssh	192.168.50.152

Figure 4 : La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Un aggressore può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare la decifrazione della sessione remota o per impostare un attacco man in the middle.
Soluzione : Aggiornare sistema, generare chiavi Host e controllare le chiavi generate.

Samba Badlock Vulnerability



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 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

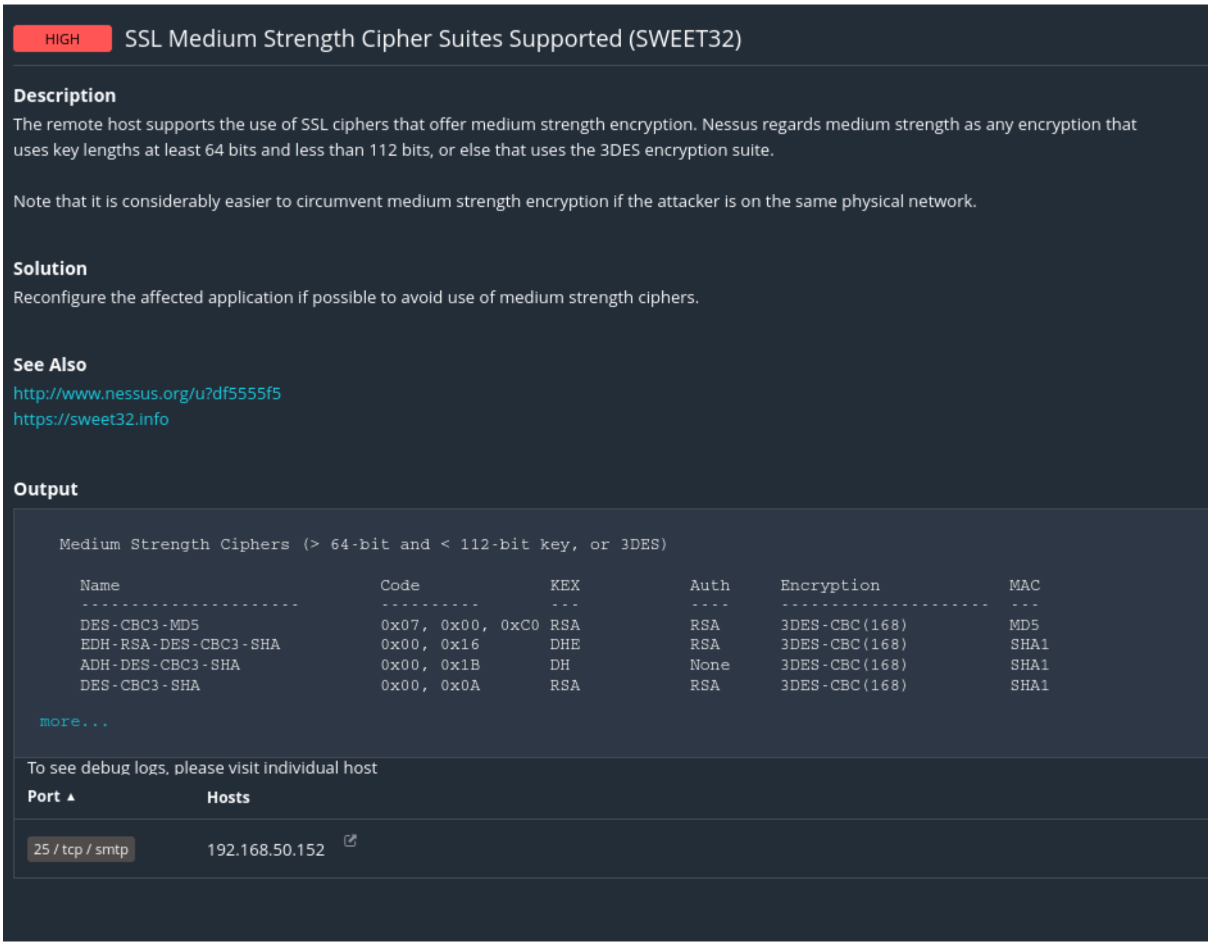
```
Nessus detected that the Samba Badlock patch has not been applied.
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.50.152

Figura 5 : La versione di Samba in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione non corretta del livello di autenticazione sui canali Remote Procedure Call (RPC).
Soluzione : Aggiornare a Samba a versione successiva.

SSL Medium Strength Cipher Suites Supported (SWEET32)



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

Figura 6 : L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia di media potenza.
Soluzione : Configurare l’app correttamente

Conclusion :

L'analisi di vulnerabilità su Metasploitable (limitata alle porte comuni) ha rivelato **4 criticità** e **2 alti rischi**, confermando l'estrema vulnerabilità del sistema. Le falle includono sistema operativo obsoleto (Canonical Ubuntu SEoL), protocolli crittografici deboli (SSL v2/v3, cifrature medie), e difetti specifici in servizi chiave come Samba (Badlock) e la generazione di chiavi SSH/OpenSSL.

Queste debolezze offrono molteplici vie di accesso agli attaccanti.

Raccomandazioni Urgenti:

1. **Aggiornare il S.O.** a una versione supportata.
2. **Disabilitare SSL v2/v3** e cifrature deboli, utilizzando **solo TLS 1.2+**.
3. **Aggiornare OpenSSL/OpenSSH** e **rigenerare immediatamente tutte le chiavi SSH host** a causa del difetto del generatore di numeri casuali.
4. **Aggiornare Samba** per risolvere Badlock.