

Ho effettuato una scannerizzazione delle vulnerabilità sull'host metasploitable utilizzando il programma Nessus su kali, specificando le porte più comuni cioè dalla prima fino alla 1024. Dopo aver effettuato la scannerizzazione Nessus ci da tutte le vulnerabilità dal livello più critico.

Analizziamo due vulnerabilità critiche e una media.

1.

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.

Questa descrizione indica che il servizio remoto accetta connessioni criptate utilizzando SSL 2.0 e 3.0 che però hanno diverse vulnerabilità crittografiche che sono:

uno schema di padding insicuro e schemi di rinegoziazione e ripresa di sessione insicuri.

Quindi un attaccante può sfruttare queste vulnerabilità per fare attacchi tipo man-in-the-middle o per decrittografare le comunicazioni tra il servizio e il client.

Infatti il NIST ha stabilito che SSL 3.0 non è più accettabile per stabilire connessioni sicure.

La soluzione per questo problema è disabilitare SSL 2.0 e 3.0 ed invece usare TLS 1.2.

2.

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.

Questa descrizione indica che la remote SSH host key è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della libreria OpenSSL. Questo bug è dovuto da un pacchetto di Debian che ha rimosso buona parte delle fonti di entropia. Con questo un hacker può aver un accesso facile della chiave privata così da poter decifrare una sessione remota o attuare un attacco man-in-the-middle.

La soluzione è considerare tutto quello che è crittografato generato dal remote host facilmente prevedibile. In particolare tutto il materiale delle chiavi SSH, SSL e OpenVPN che dovrebbe essere rigenerato.

3.

MEDIUM Unencrypted Telnet Server

Description
The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution
Disable the Telnet service and use SSH instead.

Questa descrizione indica che l'host remoto sta utilizzando un server Telnet su un canale non criptato. Per questo motivo tutti i dati di login e i comandi sono visibili permettendo un attacco man-in-the-middle facendo intercettare una sessione Telnet ottenendo tutti i dati sensibili. SSH è preferibile a Telnet dato che protegge le credenziali dall'essere intercettate.

La soluzione è di sostituire il servizio di Telnet ed usare invece SSH.