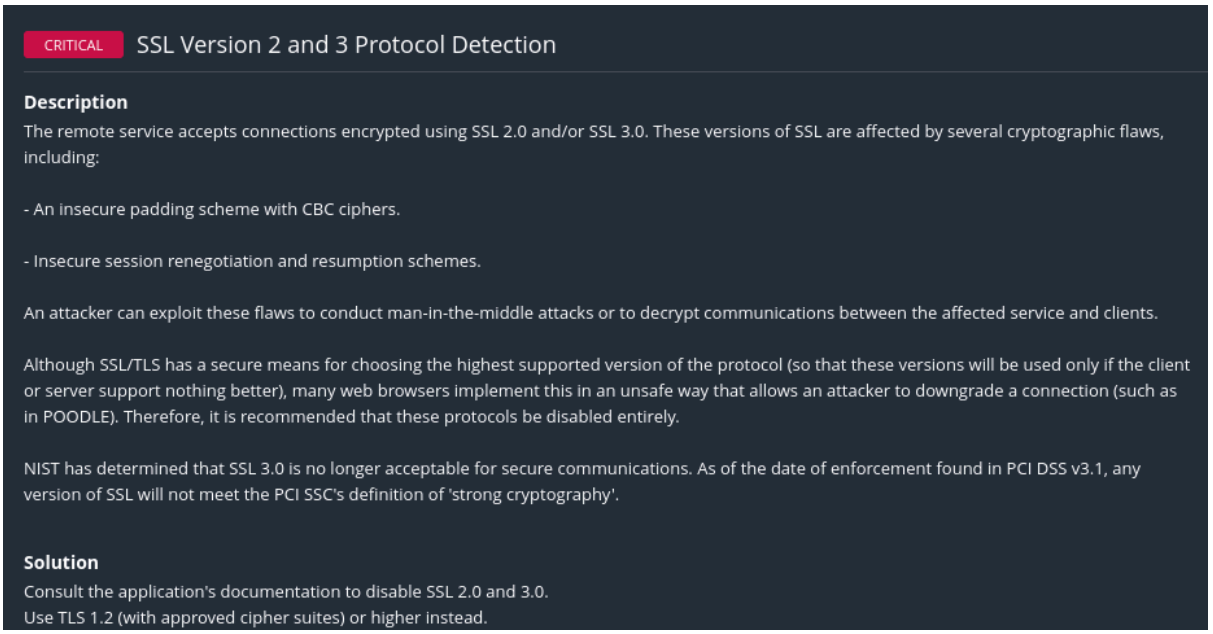
Ho effettuato una scannerizzazione delle vulnerabilità sull'host metasploitable utilizzando il programma Nessus su kali, specificando le porte più comuni cioè dalla prima fino alla 1024.
Dopo aver effettuato la scannerizzazione Nessus ci da tutte le vulnerabilità dal livello più critico.
Analizziamo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

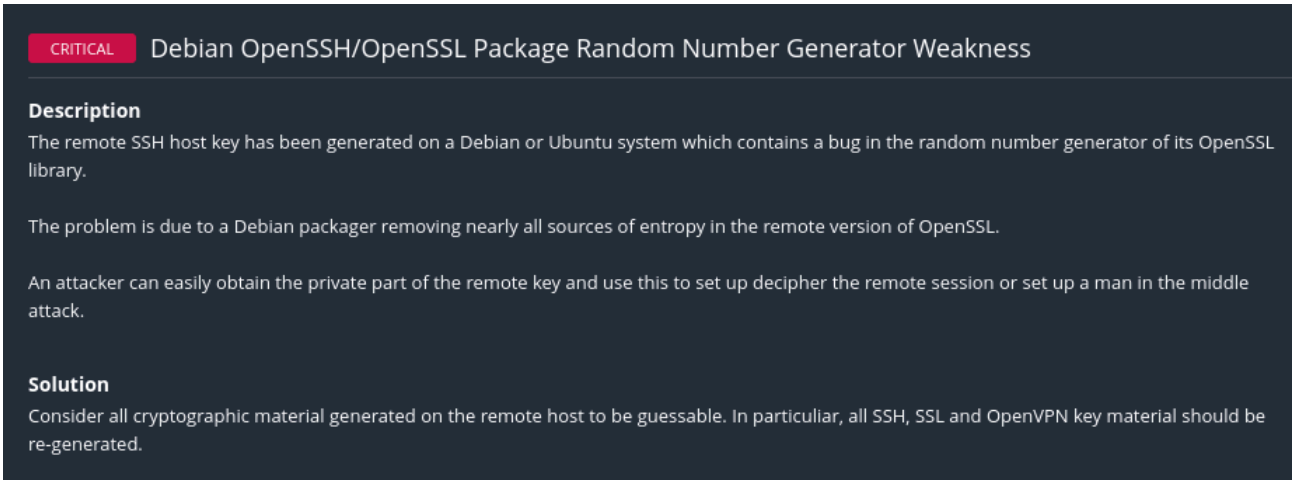
1.



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.

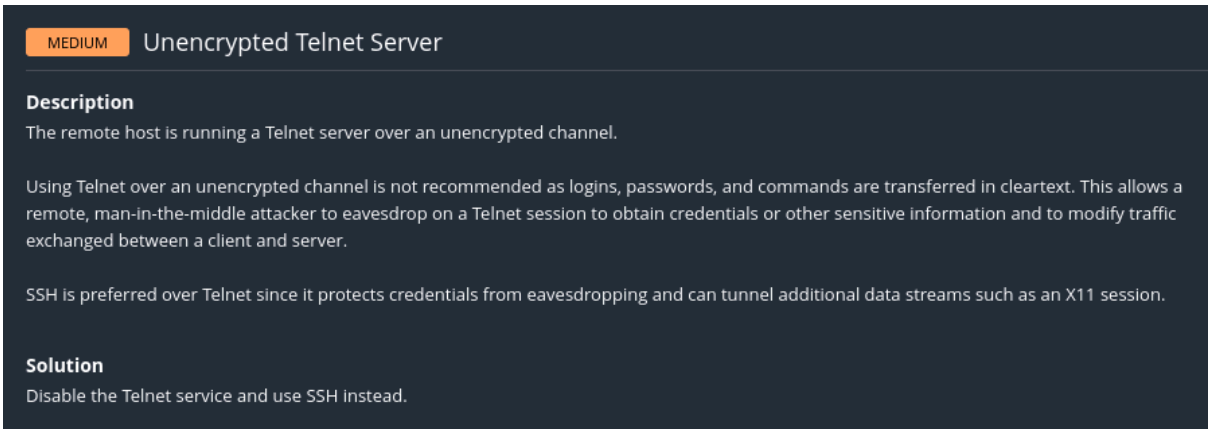
2.



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.



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.