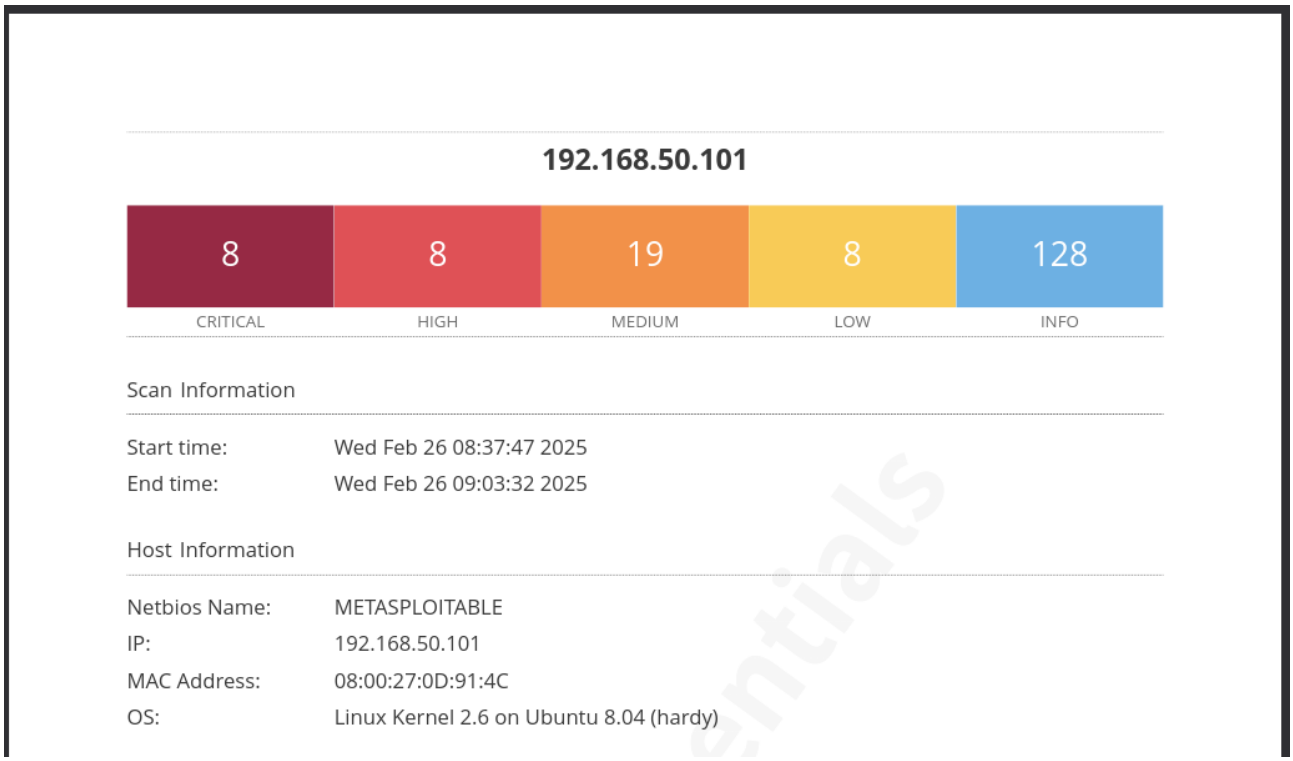
L'esercizio prevede la Vulnerability Scanning sulla macchina Metasploitable (a cui è stato assegnato IP 192.168.50.100) utilizzando Nessus da Kali Linux.



In particolare sono state riscontrate 8 Vulnerabilità critiche, 8 ad Alto Rischio, 19 con rischio medio.

Durante l'analisi il tool da subito possibilità di consultare la vulnerabilità scoperta, in particolare vengono date descrizione della vulnerabilità, soluzione per sistemare ed altra documentazione disponibile per approfondire e studiare la vulnerabilità.

Analysis of the SSL 3.0 protocol

David Wagner
University of California, Berkeley
daw@cs.berkeley.edu

Bruce Schneier
Counterpane Systems
schneier@counterpane.com

Abstract

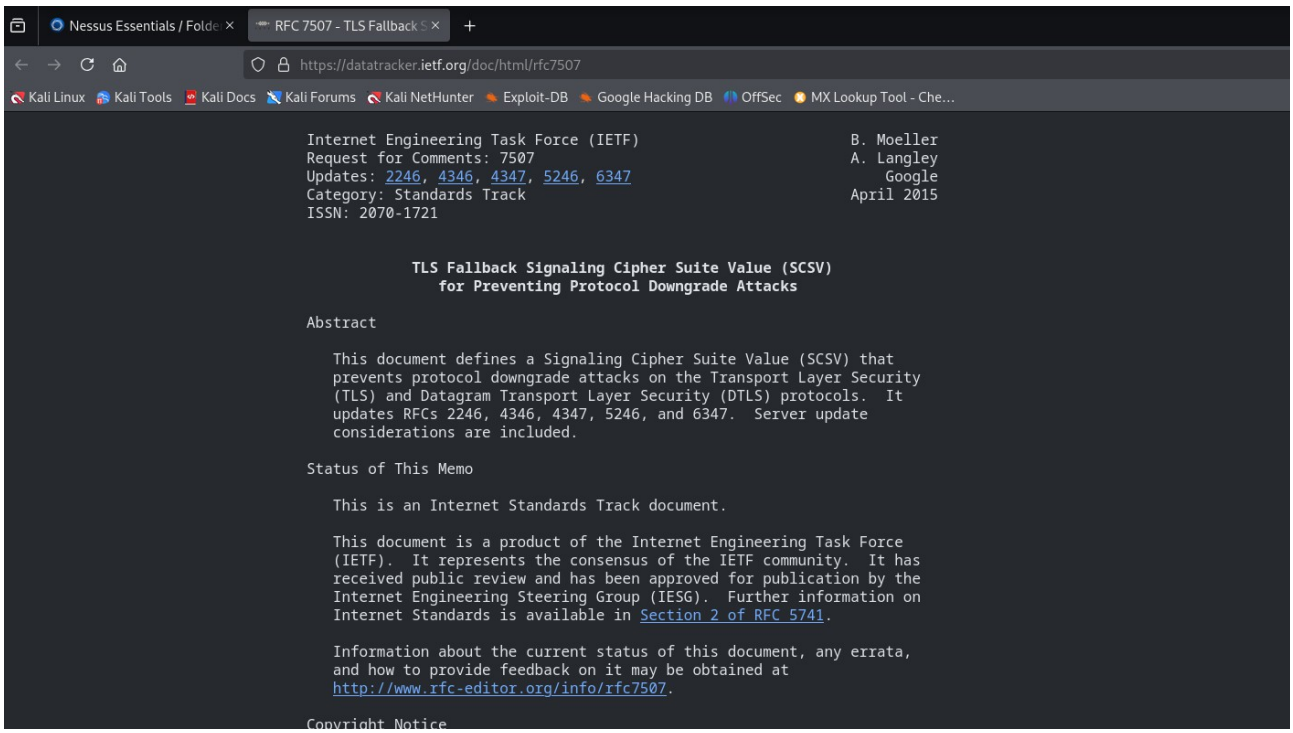
The SSL protocol is intended to provide a practical, application-layer, widely applicable connection-oriented mechanism for Internet client/server communications security. This note gives a detailed technical analysis of the cryptographic strength of the SSL 3.0 protocol. A number of minor flaws in the protocol and several new active attacks on SSL are presented; however, these can be easily corrected without overhauling the basic structure of the protocol. We conclude that, while there are still a few technical wrinkles to iron out, on the whole SSL 3.0 is a valuable contribution towards practical communications security.

1 Introduction

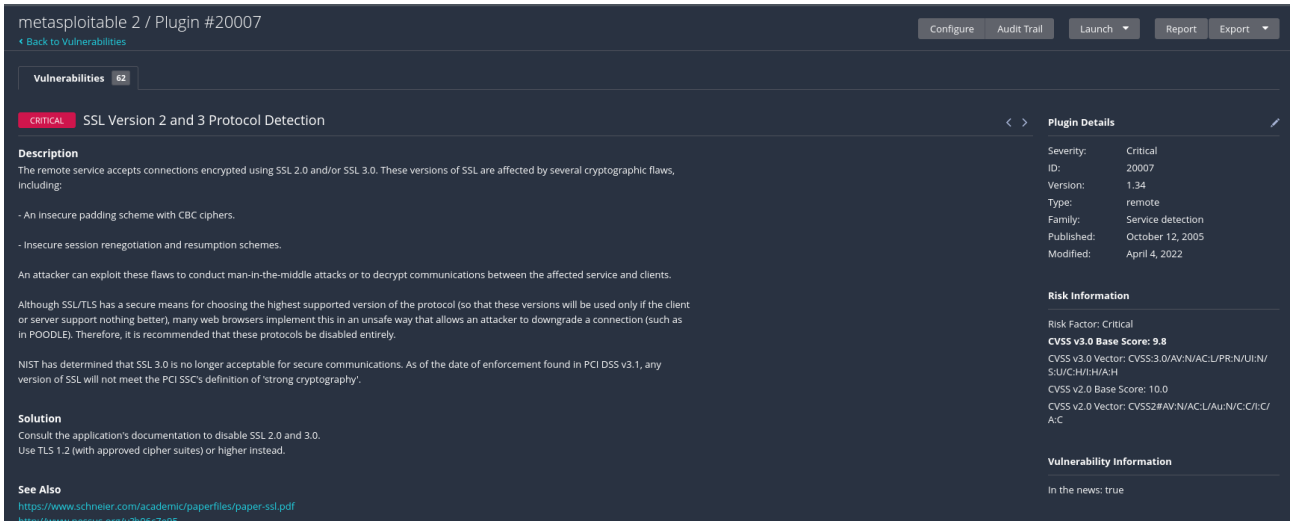
gives some background on SSL 3.0 and its predecessor SSL 2.0. Sections 3 and 4 explore several possible attacks on the SSL protocol and offer some technical discussion on the cryptographic protection afforded by SSL 3.0; this material is divided into two parts, with the SSL record layer analyzed in Section 3 and the SSL key-exchange protocol considered in Section 4. Finally, Section 5 concludes with a high-level view of the SSL protocol's strengths and weaknesses.

2 Background

SSL is divided into two layers, with each layer using services provided by a lower layer and providing functionality to higher layers. The SSL record layer provides confidentiality, authenticity, and replay protection over a connection-oriented reliable transport protocol such as TCP. Layered above the



Nell'immagine sotto riportata quella riguardante la SSL Version 2 and 3 Protocol Detection.



Andando ad analizzare nello specifico questa vulnerabilità, il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0, che sono affette da diversi difetti crittografici che potrebbero essere utili per condurre un attacco man-in-the-middle
La soluzione proposta è quella di disattivare SSL 2.0 e 3.0 e di utilizzare invece TLS 1.2, protocollo più sicuro.