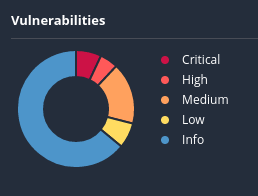
PRATICA 30 OTTOBRE 2024

Obiettivo: Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

NESSUS

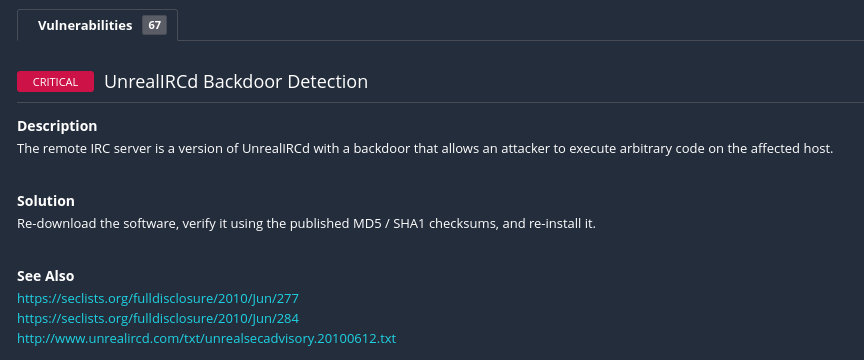
Il programma che andremo ad utilizzare oggi si chiama Nessus. Grazie ad esso saremo in grado di identificare i punti deboli e potenziale falle di sicurezza nei sistemi IT che verranno controllati.

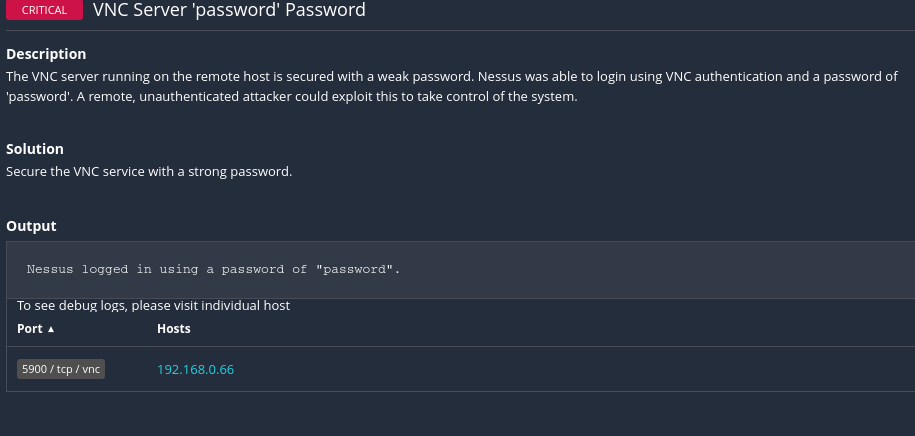
Utilizzando come target la VM Metasploitable andremo a controllare le vulnerabilità e spiegheremo come risolverle in maniera tale da poter rispettare il compromesso accessibilità/sicurezza.  
  
SCANSIONE. Una volta effettuata la scansione, questi sono i risultati:



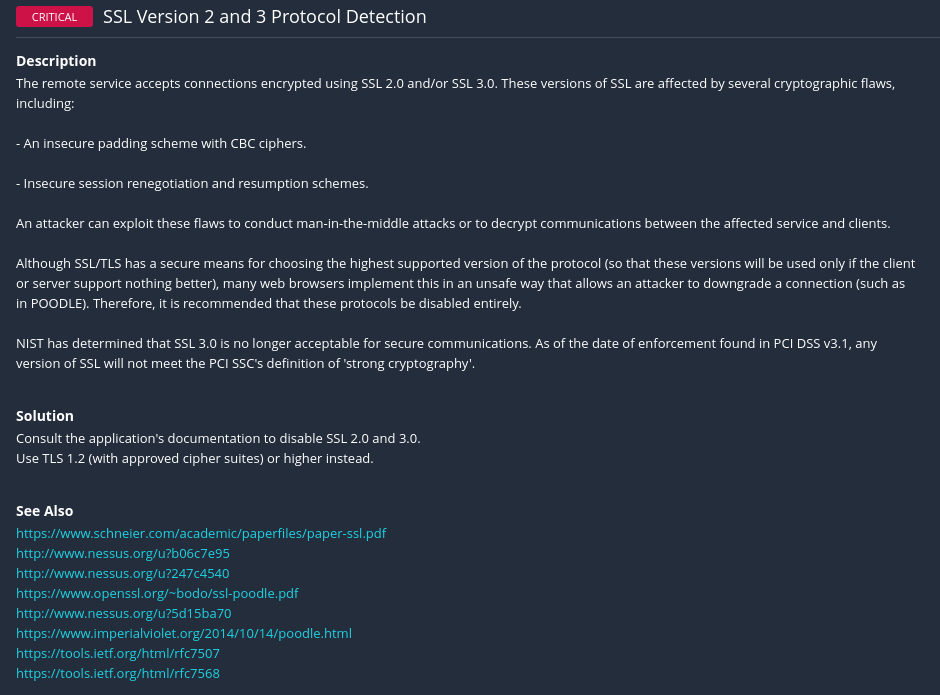
Come visibile nel grafico, possiamo vedere la presenza di varie vulnerabilità di livello critico. Il consiglio sarebbe quello di risolvere queste criticità nel minor tempo possibile.  
Di seguito un report:

Prima vulnerabilità critica



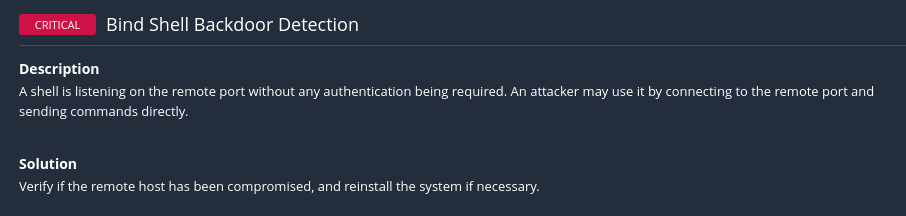
In base al report di Nessus, e alla soluzione che ci suggerisce, il modo migliore per risolvere questa vulnerabilità è disinstallare il software UnrealIRCd e reinstallarlo usando l’ultima versione disponibile. In questo modo il rischio backdoor verrebbe risolto completamente.  
  
Seconda vulnerabilità critica

Problema semplice da risolvere, ma assolutamente non trascurabile. La password attualmente attiva è molto debole. Si consiglia di cambiarla, utilizzandone una più forte e difficile da indovinare.  
  
Terza vulnerabilità critica

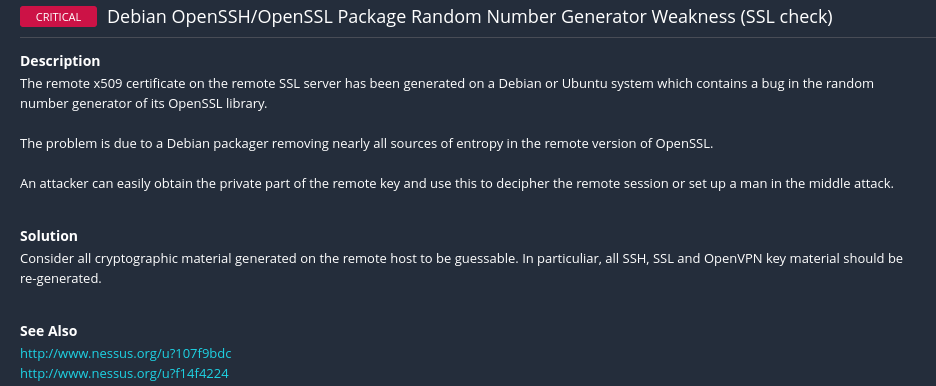


In questo caso il protocollo di criptazione SSL/TLS è obsoleto. Questo permetterebbe ad eventuali attacchi man-in-the-middle di rubare dati non criptati, lasciando in chiaro informazioni sensibili. Si consiglia di effettuare un upgrade a TLS 1.2

Quarta vulnerabilità critica



Un’altra potenziale backdoor presente sulla macchina host. Si consiglia di controllare la presenza di eventuali presenze indesiderate e re-installare il sistema tramite un’installazione pulita.  
  
Quinta vulnerabilità critica



A causa di un bug presente del generatore di numeri casuale della libreia OpenSSL, tutto il materiale crittografato non è al sicuro perché potrebbe essere decifrato con facilità. Si consiglia di rigenerare le key SSH, SSL e OpenVPN per rimettere in sicurezza il sistema.

In allegato troverete anche un report completo su tutte le vulnerabilità, critiche o meno, effettuato da Nessus.