S5E3

Vulnerability Scanning

L'obbiettivo dell'esercizio è effettuare 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.

Cosa è Nessus?

Nessus è un vulnerability scanner.
Vulnerability scanner utilizzano dei database di vulnerabilità note e controlli di sicurezza per rilevare le vulnerabilità di un sistema.
Gli scanner effettuano le verifiche delle vulnerabilità su:

- Servizi in ascolto su porte TCP / UDP.
- Configurazioni di sistemi operativi, software e piattaforme.
- Registri di Windows.

Lo scopo principale del VA è identificare le vulnerabilità e configurazioni errate che potrebbero essere sfruttate da un malintenzionato.

Fase 1 della scansione : configurazione

In questa fase andrò a specificare su Nessus il Target, le porte da scannerizzare, e il tipo di scansione.

- Target = Metasploitable, IP 192.168.1.161/24
- Porte = 0 - 1024 (porte note)
- Tipo di scansione = Basic Network Scan (una scansione basica ma ricca di informazioni)

Fase 2 della scansione : esecuzione

Dopo aver configurato la scansione non ci resta che attendere i risultati. Nessus impiegherà una decina di minuti per scannerizzare l'IP dato, ovviamente questo tempo salirà nel caso dovessimo scannerizzare un'intera rete.

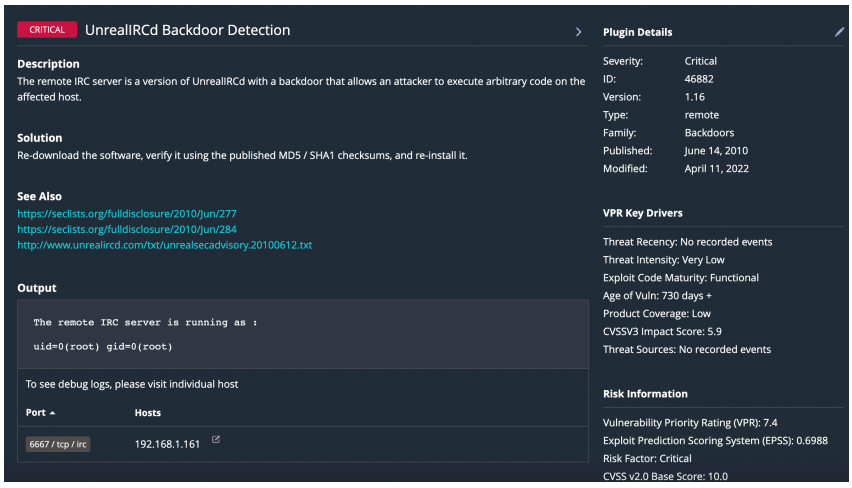
Fase 3 della scansione : Analisi

Ora che la scansione è terminata possiamo chiedere a Nessus di fornirci un report delle vulnerabilità. In questo caso da Pentester il nostro lavoro non finisce qui, una parte importante del lavoro è approfondire le vulnerabilità più critiche.

Fase 4 della scansione : approfondimento

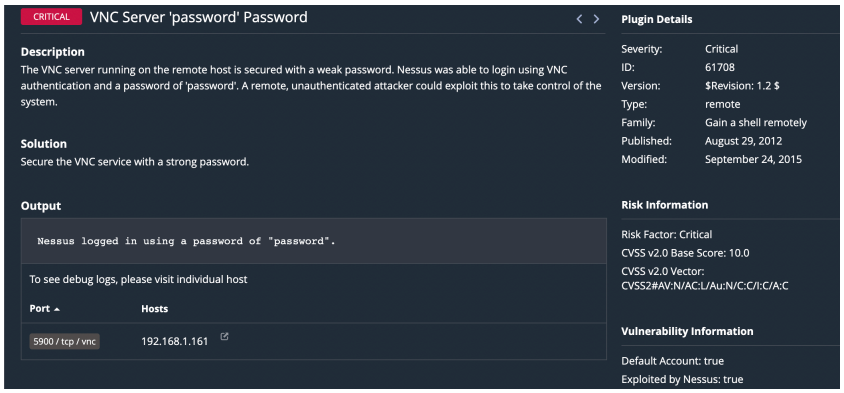
Ora andremo ad approfondire 5 vulnerabilità critiche trovate da Nessus sulla macchina metasploitable.

Vulnerabilità 1 : Backdoor



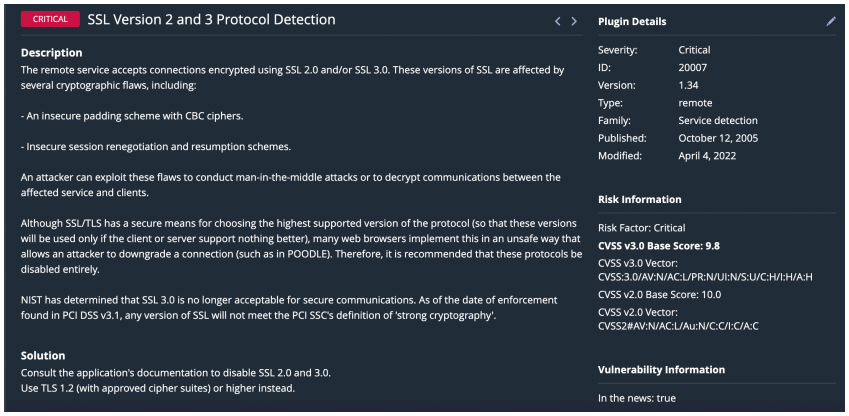
Come si può vedere dall'immagine, Nessus ci fornisce una **descrizione** della vulnerabilità.
In questo caso ci dice che è stata trovata una backdoor che può permettere ad un attaccante di controllare la macchina a suo piacimento.
La **soluzione** consigliata è di scaricare nuovamente la macchina virtuale da un sito certificato, controllando che la macchina in questo caso non sia infetta.

Vulnerabilità 2 : VNC server password



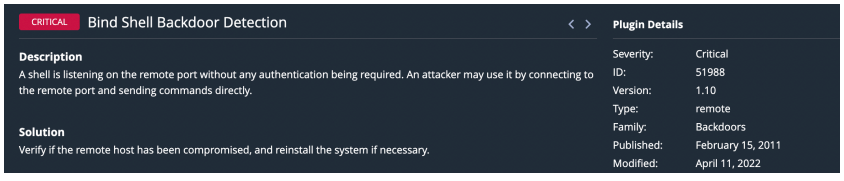
La seconda vulnerabilità trovata da Nessus è che la password del server VNC è la parola ‘password’. Si consiglia di risolvere mettendo a protezione del server VNC una password più potente.

Vulnerabilità 3 : versioni SSL poco sicure



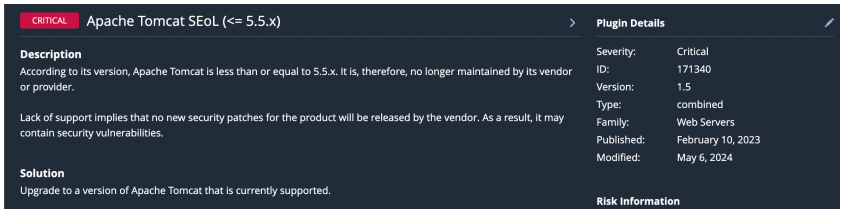
La terza vulnerabilità è un uso di versioni poco affidabili. In questo caso Nessus ha trovato delle vulnerabilità del servizio SSL in versione 2 e 3.
Il consiglio è di risolvere disabilitando le due versioni del servizio SSL e utilizzare il servizio TLS in versione 1.2 o più recente.

Vulnerabilità 4 : Backdoor n2



È stata trovata una seconda backdoor, per risolvere si consiglia di guardare la **vulnerabilità 1**

Vulnerabilità 5 : Versione Apache poco sicura



In questo caso la versione Apache non è aggiornata, non ha a disposizione supporto o patch per contrastare gli attacchi più moderni.