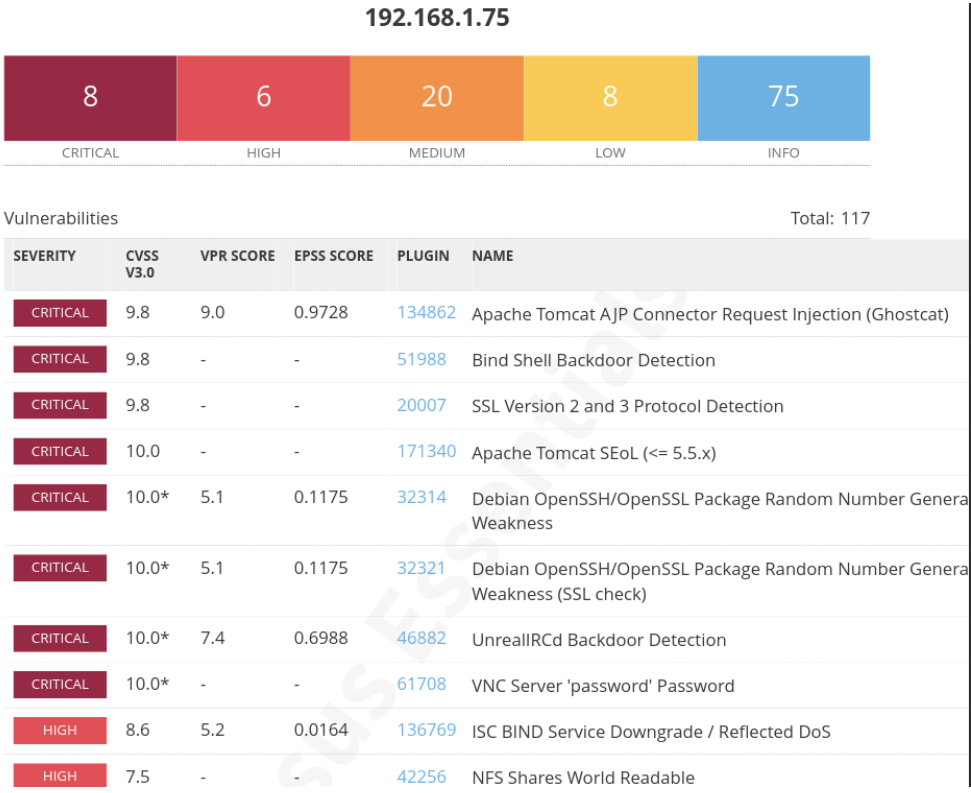
Analisi delle vulnerabilità della macchina Metasploitable2 attraverso macchina Kali Linux e ausilio di Nessus

L’analisi ha prodotto i seguenti risultati

si nota che nel nostro caso la Metasploitable2 presenta numerose criticità che rendono la macchina molto



SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat A JP Connector Request Injection (**Ghostcat**)

La vulnerabilità Ghostcat (CVE-2020-1745) colpisce il connettore AJP di Apache Tomcat.
Questa vulnerabilità consente a un attaccante non autenticato di accedere a file sensibili del server.
Inoltre, in contesti in cui il server consente il caricamento di file, l'attaccante potrebbe caricare file JSP (Java Server Page) malevoli.

Per mitigare questa vulnerabilità aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiorna il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successive, poiché gli aggiornamenti di sicurezza possono risolvere problemi noti.
Può essere utile limitare l'accesso alla porta AJP (solitamente la porta 8009) e configurare adeguatamente le regole del firewall.

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Generat Weakness

In questa vulnerabilità la chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che presenta un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzare queste informazioni per decifrare la sessione o per impostare un attacco man-in-the-middle.

Come soluzione si può provare a considerare tutti i materiali crittografici generati sull'host remoto come indovinabili. In particolare, è necessario rigenerare tutto il materiale chiave SSH, SSL e OpenVPN.

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0*	7.4	0. 6988	46882	UnrealIRCd Backdoor Detection

In questa vulnerabilità il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un attaccante di eseguire codice arbitrario sull'host compromesso.

Per risolvere la problematica bisoca riscaricare il software, fare una verifica utilizzando i checksum MD5/SHA1 pubblicati e reinstallare il software.