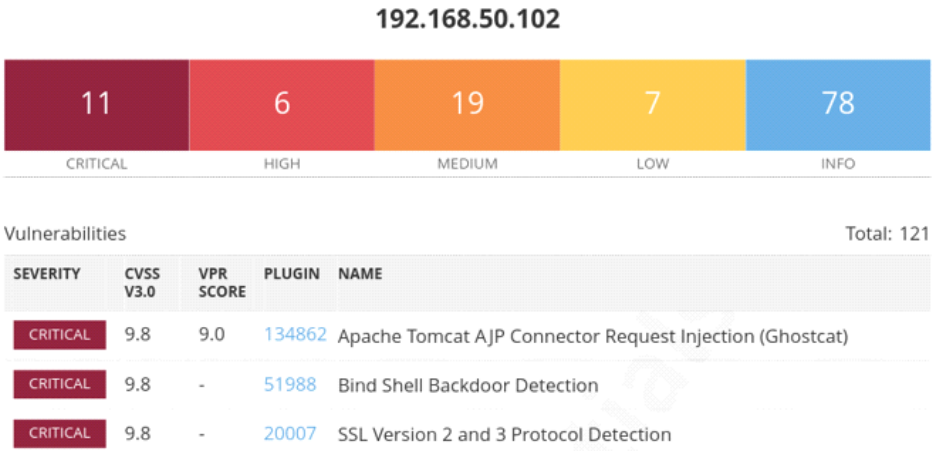

Per l'esercizio di oggi ho utilizzato Nessus per scansionare la rete e le porte di Metasploitable, ciò mi ha consentito di scoprire varie vulnerabilità tra cui 11 critiche, 6 alte, 19 medie e 7 basse, che possono essere risolte utilizzando le soluzioni dateci da nessus stesso.

Ad esempio, per quanto riguarda le 3 vulnerabilità presenti nella foto nessus consiglia delle soluzioni.

Prima vulnerabilita --> Il software consiglia di aggiornare la configurazione del protocollo AJP(Apache Jservlet Protocol) per fare in modo che richieda l'autorizzazione, e aggiornare il server Tomcat a 7.0.100, 8.5.51 o 9.0.31.

Seconda vulnerabilità --> Per quanto riguarda questa vulnerabilità Nessus consiglia di verficare se l'host è stato compromesso e di reinstallare il sistema se necessario.

Terza Vulnerabilità --> Qui il software ci propone di disabilitare SSL 2.0 e SSL 3.0, consultando la documentazione di Metasploitable, e inserire al loro posto il successore del protoccolo SSL ovvero TLS 1.2 o superiore.