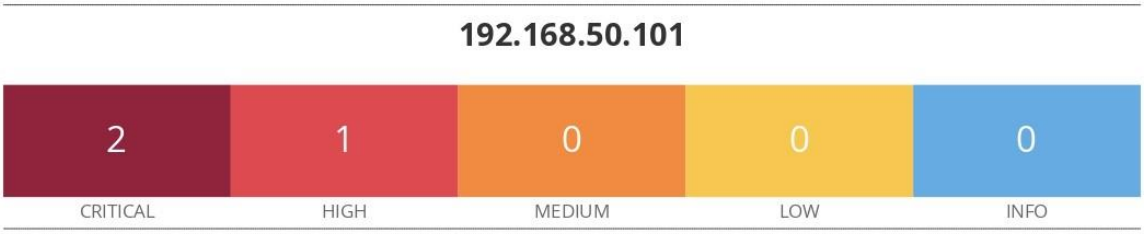
Effettuare un Vulnerability Assessment con **Nessus** sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.
Gli obiettivi dell'esercizio sono:

- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.



Vulnerabilities Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
HIGH	7.5	-	42256	NFS Shares World Readable

* indicates the v3.0 score was not available; the v2.0 score is shown

Vulnerabilità: Unix Operating System Unsupported Version Detection
La versione del sistema Unix non è più supportata e, pertanto non verranno rilasciate future patch di sicurezza.

Soluzione: Aggiornare il sistema ad una versione supportata.

Vulnerabilità: SSL Version 2 and 3 Protocol Detection
Il servizio SSL, essendo una tecnologia standard per la sicurezza delle connessioni internet mediante crittografia dei dati inviati tra web e browser, a causa dei difetti basati sui cifrari CBC e schemi di rinegoziazione e ripresa della sessione non sicuri, è stato stabilito che non è più sicuro dal NIST.

Soluzione: disabilitare il servizio SSL e utilizzare TLS 1.2 o versioni aggiornate

Vulnerabilità: NFS Shares World Readable
Il server NFS sta molte condivisione senza limitarne gli accessi.

Soluzione: Impostare le restrizioni su tutte le condivisioni FNS.