**Esercizio di vulnerabilità**

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.

**Risultato:**

L’indirizzo target presenta un totale di 106 vulnerabilità di cui: 8 critiche, 4 ad alto rischio, 16 medie, 6 a basso rischio e 72 da controllare.

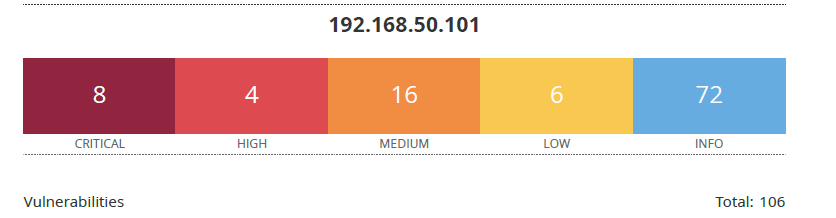


Figura 1 Per maggiori informazioni guardare il file pdf PraticaS5L4\_2

Criticità risolte:

* VNC Server 'password' Password: Il server VNC sulla porta 5900 in esecuzione da un host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di 'password'. Un attaccante remoto non autenticato potrebbe sfruttare ciò per prendere il controllo del sistema.

Soluzione: Aumentare la sicurezza del server VNC mettendo una password più difficile e complessa

* Unix Operating System Unsupported Version Detection: Secondo il numero di versione il sistema operativo Unix in esecuzione sull'host non è più supportato.

La mancanza di supporto implica che non verranno rilasciate nuove patch di sicurezza per il prodotto dal fornitore. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza e che debba essere aggiornato.

Soluzione: aggiornare la versione di UNIX ad una versione più recente supportata.

* HTTP TRACE / TRACK Methods Allowed: Il server web sulla porta 80 remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP utilizzati per eseguire il debug delle connessioni del server web e può essere usato come vulnerabilità.

Soluzione: Disabilitare i servizi Trace and Track per il server http se non vengono utilizzati