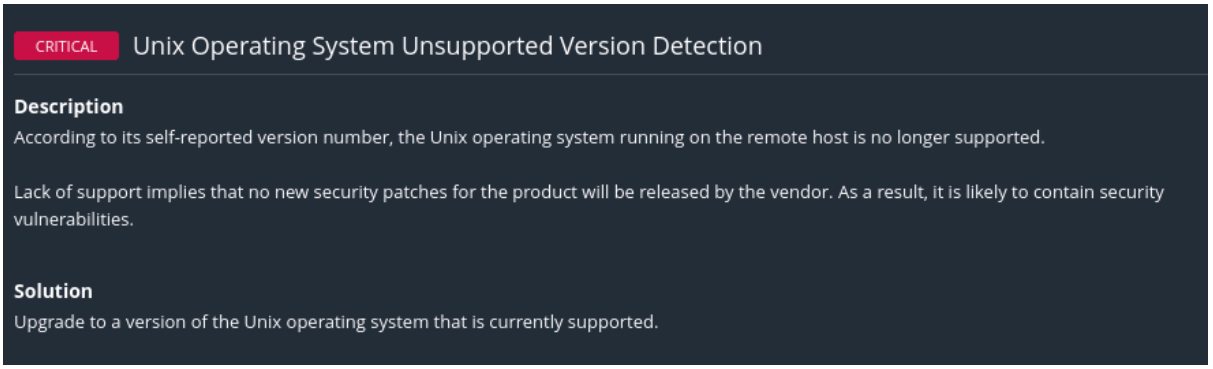
Nell’esercizio di oggi vedremo il funzionamento di Nessus, uno scanner di vulnerabilità. Esso funziona in modo simile a quello di un antivirus, cioè ha un database nel quale cercherà le vulnerabilità conosciute per le versioni rilevate sull’host. Può generare falsi positivi e/o falsi negativi.
Per l’esercizio scannerizzeremo metasploitable.

Terminata la scansione ci verrà mostrato il risultato con la lista delle vulnerabilità e sulla destra sotto forma di grafico. Le vulnerabilità vengono ordinate dalla più grave alla meno grave usando un punteggio da 1 a 10.



Selezionando una vulnerabilità è possibile vederne i dettagli, come informazioni e anche come mitigarla. Nella figura sopra lo scanner ci avvisa che la versione del sistema operativo ha raggiunto la fine del suo ciclo di vita, detta end of life, cioè uno stato in cui il software non viene più supportato dal produttore. Un aggiornamento del sistema non è quindi possibile in questo caso, di conseguenza nessus ci consiglia di passare ad un sistema che sia supportato.

La vulnerabilità che vediamo nella figura sopra è un’altra vulnerabilità critica con un punteggio di 10 su 10. Essa ci indica che un server è protetto da una

password debole e facilmente aggirabile da un attaccante. Il rimedio a questa situazione è usare una password complessa.

La vulnerabilità qui sopra è una vulnerabilità media che indica la presenza di un servizio poco sicuro. Telnet è un protocollo di accesso remoto che trasmette dati in chiaro e può essere sfruttato molto facilmente da un attaccante per ottenere accesso ad un sistema. Il rimedio è quello di disabilitare telnet e usare SSH al suo posto.