NESSUS

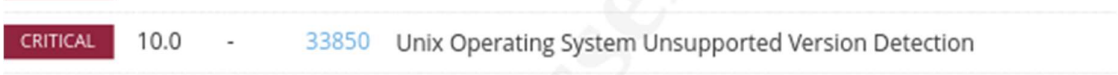
VULNERABILITY SCANNER

Nessus è uno strumento molto potente in fase di Penetration Testing, esso è un Vulnerability Scanner cioè un software che esegue una scansione di un sistema o di una rete alla ricerca delle vulnerabilità conosciute.

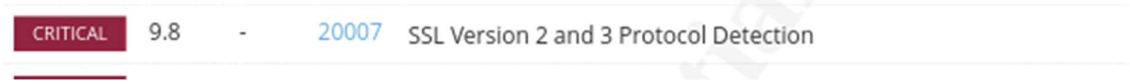
Per fare pratica con questo strumento sono andata a scansionare la macchina virtuale Metasploitable con IP: 192.168.50.101. Sono venute fuori 70 vulnerabilità; quelle che andrò ad analizzare sono le prime quattro.

- "NFS Exported Share Information Disclousure": riguarda la condivisione di file e risorse su una rete tramite il protocollo NFS. La vulnerabilità che è venuta fuori è che qualcuno è in ascolto sulla porta remota senza che abbia fatto l'autenticazione, e questo potrebbe essere sfruttato da un malintenzionato per connettersi e prendere il comando.
  La soluzione che propongo è di configurare in modo adeguato le autorizzazioni e limitarne l'accesso.

- "Unix Operating System Unsupported Version Detection": questa ci dice che il sistema Unix sta eseguendo una versione del sistema operativo non supportata, quindi il fornitore non rilascerà aggiornamenti per quella versione. La soluzione che propongo è quella di installare un'aggiornamento che sia supportato dal sistema operativo Unix.



- “SSL Version 2 and 3 Protocol Detection”: il servizio remoto accetta queste due versioni di SSL, i quali hanno dei difetti crittografici quindi un malintenzionato potrebbe fare degli attacchi man-in-the-middle. Quindi una soluzione potrebbe essere quella di disattivare queste due versioni e utilizzare TLS 1.2.



- “Apache Tomcat A JP Connector Request Injection (Ghostcat)” quest’ultimo è un protocollo utilizzato per consentire la comunicazione tra un server web Apache e un server Tomcat. La vulnerabilità è chiamata “Ghostcat” che consente un inclusione remota di file. Questa cosa può essere sfruttata da un attaccante che può leggere e accedere ai file all’interno del server. Una soluzione potrebbe essere quella di aggiornare il server Tomcat.