Report e Commento

Tramite il programma Nessus è stata fatta una scansione delle porte comuni (1-1024) della macchina Metasploitable al seguente indirizzo IP.

Sono risultate evidenti problemi per un totale di 70 Vulnerabilità di cui 11 Critiche.

L'analisi delle prime Vulnerabilità riscontrate ha prodotto i seguenti risultati:

- **I° NFS (NetworkFileSystem)**: una criticità in questo protocollo è molto grave poiché esso consente la condivisione di file remoti. Una mancata sicurezza dello stesso può consentire l'accesso a PC remoti verso Host analizzato con la possibilità di leggere e più pericolosamente scrivere interi file. La soluzione consigliata dal rapporto è di creare dei privilegi di accesso alla sezione in condivisione.

- **II° Unix Opereting System Unsupported Version Detection**: questa criticità rilevata indica un mancato aggiornamento del sistema Unix. Questo significa che o serve è necessario un aggiornamento del sistema, se non è possibile farlo è necessario una sostituzione poiché un sistema non più supportato da aggiornamenti è sicuramente più vulnerabile e inoltro potrebbe non rispettare nuove politiche sulla privacy e sul trattamento dei dati personali, che comporterebbe anche la possibilità di ricevere sanzioni.

- **III° VNC (VirtualNetworkComputing) server**: la scansione a rilevato una particolare fragilità della password legata a questo servizio. Chiaramente un servizio che consente la connessione in remoto legato ad una psw così fragile (password=password) diventa un sistema vulnerabile al più semplice degli attacchi di brute force. Cambiare la psw è la soluzione a questo problema.

- **IV°Bind Shell Backdoor Detection**: con questa criticità è sto possibile per Nessun sfruttare una Backdoor shell di tipo Blind. Questa è molto pericolosa perché fornisce un ingresso aperto accessibile da remoto, difatti il programma è riuscito ad accedere al sistema e garantirsi i privilegi di amministratore con due semplici righe di codice. La soluzione in questo caso, se il sistema risulta irrimediabilmente compromesso, è di reinstallare il sistema operativo.