Scansioniamo il sistema Metasploitable con **Nessus**.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Risolviamo le vulnerabilità più **gravi**.

**Bind Shell Backdoor Detection**

Immagine che contiene testo, schermata, software

Descrizione generata automaticamente

Troviamo il processo relativo alla **porta**.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Potremmo fermare il processo o disabilitare il servizio associato, ma comunque potrebbe ripartire al riavvio; è necessario quindi **eliminare** completamente la backdoor dal sistema.

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

Lo facciamo andando nel file di configurazione di **inetd** e cancellando l’ultima riga, responsabile dell’apertura della backdoor tramite la quale si potevano inviare comandi direttamente nella shell di metasploitable da remoto senza autenticazione.

**VNC Server ‘password’ Password**

Immagine che contiene testo, schermata, software, Carattere

Descrizione generata automaticamente

La soluzione qui è molto semplice; basta modificare la password del servizio **vnc** con il comando da terminale **vncpasswd**, impostando una password sicura.

**NFS Exported Share Information Disclosure e NFS Shares World Readable**

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamenteImmagine che contiene testo, schermata, software

Descrizione generata automaticamente

Analizziamo il file di configurazione di **nfs**.

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

Eliminiamo la riga che permetteva l’accesso a **qualunque client da remoto** in scrittura e lettura con permessi di root; inoltre i cambiamenti effettuati sui file condivisi venivano scritti sincronamente sul disco fisico (sopra l’immagine del file di configurazione correttamente modificato). L’accesso andrà consentito soltanto a host specifici e con i permessi minimi necessari.

**SSL Version 2 and 3 Protocol Detection**

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Questo problema è presente sia sulla porta 25 dove è attivo il servizio smtp **postfix** e sulla porta 5432 dove è attivo il servizio **postgresql**.

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

Modificando il file di configurazione sopra e rilanciando la scansione vediamo che il problema per postgresql è risolto, mentre per postfix, trattandosi di una versione molto vecchia che probabilmente non accetta direttive sulla versione ssl, il onsiglio è di aggiornare.

Rieffetuiamo la scansione con Nessus.

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Abbiamo risolto una buona parte dei problemi più gravi; si noti infine come per risolvere i rimanenti basterebbe semplicemente aggiornare i rispettivi software a versioni più recenti.