Esercitazione S5-L3

Analisi di alcune vulnerabilità individuate

- **rsh Unauthenticated Access**

Tale problema si riferisce ad un problema con il servizio remote-shell (rsh), un protocollo di rete che permette di eseguire comandi su un computer remoto senza necessità di autenticarsi interattivamente.
In questo caso Nessus ci segnala che sono stati utilizzati degli usernames troppo comuni, che hanno permesso a Nessus stesso di accedere. Inoltre gli account potrebbero non avere password facilitando l'accesso o i file presenti in .rhosts potrebbero essere non adeguatamente configurati.
Tale problema sembrerebbe essere tipico dei dispositivi Cisco Prime LAN Management Solution.
Se si tratta di uno di questi dispositivi, il suggerimento per la risoluzione è qullo di applicare una patch correttiva, altrimenti bisogna impostare delle password o eliminare i file .rhosts

- **VNC server "password" Password**

VNC sta per Virtual Network Computing ed è un sistema di controllo remoto che utilizza un protocollo di rete per trasmettere l'interfaccia grafica del computer remoto a quello locale.
In questo caso il problema risiede in una password poco sicura, infatti la password è "password".
Nessus ci consiglia di modificarla una password più "forte".

- **SSL Version 2 and 3 Protocol Detection**

SSL sta per Secure Socket Layer ed è un protocollo di sicurezza che permette di stabilire una connessione criptata tra due macchine.
Nessus ci avvisa che il sistema target utilizza la versione 2.0 o 3.0 di SSL, la quale è affetta da alcune vulnerabilità come:

- un poco sicuro sistema di "cifratura" basato su CBC;
- una sessione di "negoziazione" che segue schemi poco sicuri;

Questi problemi espongono il sistema a facili attacchi Man-In-The-Middle.
Il suggerimento è di aggiornare a TLS 1.2 o superiore.

- **Bind Shell Backdoor Detection**

La shell risulta in ascolto su una porta senza che sia richiesta alcuna autorizzazione per accedervi. un attaccante, potrebbe collegarsi a questa porta ed inserire comandi in maniera diretta.
In questo caso è importante verificare che l'host non sia stato compromesso e successivamente, se necessario, reinstallare il sistema.

- **vsftpd Smiley Face Backdoor**

vsftpd sta per Very Secure FTP Daemon ed è un software che implementa il protocollo FTP per il trasferimento di file tra computer.
Nessus segnala che la versione di vsftpd presente sul sistema target ha all'interno una backdoor. Infatti, inserendo uno smile :) all'interno della sezione "username" è possibile mettere in ascolto il sistema sulla porta TCP 6200.
La shell termina di ascoltare una volta che un client si è connesso e disconnesso. Ovviamente, questo permette ad un attaccante di entrare nella shell ed eseguire comandi come amministratore.
Nessus ci suggerisce di convalidare e ricompilare una copia legittima del codice sorgente.

- **rlogin Service Detection**

rlogin (Remote Login) è un altro protocollo di rete che permette di connettersi a un altro computer su una rete attraverso una sessione di terminale.
Tale servizio è poco sicuro in quanto permette il passaggio di informazioni da Client a Server in chiaro. Questo espone il sistema allo sniffing, permettendo a persone con intenzioni malevole di leggere informazioni sensibili, come username o password.
Una delle possibili soluzioni è chiudere tal servizio ed utilizzare SSH, molto più sicuro.

- **rsh Service Detection**

Nessus vede che sul sistema viene utilizzato rsh (Remote Shell). Si tratta di un sistema poco sicuro che, come rlogin, permette la trasmissione di informazioni in chiaro, prestando il fianco ad attacchi Man-In-The-Middle.
Anche in questo caso, il consiglio è di sostituire tale servizio con SSH (Secure Shell).

- **Samba Badlock Vulnerability**

Nessus ci segnala che la versione di Samba presente sul sistema target ha una vulnerabilità nota come Badlock. Si tratta di un problema nel "locking" dei file che può essere sfruttata per intercettare e manipolare le comunicazioni permettendo attacchi Man-In-The-Middle.
Nessus consiglia di aggiornare Samba a versioni più recenti.