EPICODE

Esercizio S5 – L4

TRACCIA:

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan».

A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo 3 vulnerabilità (2 critiche e 1 media).

Gli obiettivi dell’esercizio sono:  
● Fare pratica con lo strumento, con la configurazione e l’avvio delle scansioni.  
● Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

SOLUZIONE:

[Report Nessus Metasploitable](file:///C:\Users\andre\Desktop\Andrea_yf36zh.pdf)

* Vulnerabilità critica: VNC Server “password” Password  
    
  Criticità:  
  Si tratta di una vulnerabilità critica perché il server VNC (Virtual Network Computing) che permette l’accesso remoto ha una password estremamente debole. Infatti, la password è: “password”, una delle più usate e meno sicure.

Un Black hat potrebbe facilmente prendere il controllo del sistema.  
  
Soluzione:  
Si rende necessaria la modifica della password con una più complessa (possibilmente con almeno un certo numero di caratteri, tra cui lettere, numeri e caratteri speciali).  
Si consiglia anche l’implementazione dell’autenticazione a due fattori (per esempio con un secondo codice di verifica a 6 cifre).

* Vulnerabilità critica: UnrealIRCd Backdoor Detection

Criticità:

Si tratta di una vulnerabilità critica perché la versione presente del software UnrealIRCd (Unreal Internet Relay Chat Daemon) contiene una backdoor che potrebbe sfruttare un attaccante remoto per eseguire comandi sul server IRC (Internet Relay Chat). Nello specifico l’attaccante potrebbe essere in grado di rubare informazioni sensibili e creare un nuovo utente con privilegi elevati.

Soluzione:  
Si rende necessario aggiornare il software alla versione più recente. Si consiglia anche di utilizzare un buon software antivirus.

* Vulnerabilità critica: Unencrypted Telnet Server

Criticità:  
Utilizzare il protocollo Telnet è una pessima idea in quanto i dati trasmessi (tra cui password e login) sono totalmente in chiaro. Ciò consente ad un potenziale attaccante di intercettare i dati in chiaro e modificarli, o comunque di accedere ad informazioni sensibili.

Soluzione:  
La miglior soluzione è quella di disattivare il protocollo Telnet e attivare SSH che crittografa i dati in entrambe le direzioni, permettendo l’accesso remoto con un livello di sicurezza molto maggiore.