EPICODE

Progetto S5 – L5

TRACCIA:

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.  
N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.  
Per dimostrare l’efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

SOLUZIONE:

Si riporta screenshot della scansione Nessus sul target Metasploitable.  
  
Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Vulnerabilità critiche scelte:

* UnrealIRCd Backdoor Detection
* VNC Server 'password' Password
* Bind Shell Backdoor Detection
* Risoluzione prima vulnerabilità critica (UnrealIRCd Backdoor Detection):

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Tramite Metasploit si è entrati in Metasploitable per poter risolvere il problema. Nonostante si sia capito come risolvere, non si è riusciti a riscaricare il software e risolvere la vulnerabilità.

* Risoluzione seconda vulnerabilità critica (VNC Server 'password' Password):

Immagine che contiene testo, Carattere, schermata

Descrizione generata automaticamente

L’immagine sopra mostra le modifiche apportate alla password debole, sostituita con una più forte.

* Risoluzione terza vulnerabilità critica: (Bind Shell Backdoor Detection)

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Tramite Netcat ci si è connessi da remoto a Metasploitable sulla porta indicata dalla vulnerabilità Nessus.  
Successivamente si è cercato il PID del processo e si è proceduto ad eliminare la backdoor.

A causa delle lunghe tempistiche di scansione di Nessus non si è fatto in tempo a terminarla per verificare le nuove condizioni delle vulnerabilità.