EPICODE

Esercizio S5 – L3

TRACCIA:

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:  
● OS fingerprint.  
● Syn Scan.  
● TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?  
● Version detection.

E la seguente sul target Windows 7:  
● OS fingerprint.

SVOLGIMENTO:

● OS fingerprint

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

segue

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Tramite “nmap -O” su ip di Metasploitable si sono ricevute informazioni sul sistema operativo di Metasploitable.

● TCP connect

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

segue

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Tramite “nmap -sT” si ottengono informazioni sulle porte aperte stabilendo una connessione completa.

● Syn Scan

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

segue

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Tramite “nmap -sS” si ottengono sempre informazioni sulle porte aperte ma lo si fa in modo più furtivo.  
  
La differenza, oltre alla già menzionata maggior furtività, è nella velocità di scansione (1,44 secondi contro 0,35 secondi) e nell’affidabilità delle informazioni (minore rispetto alla connessione completa).

● Version detection

Immagine che contiene testo, schermata, Carattere, menu

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Tramite “nmap -sV” si ottengono informazioni maggiori sui servizi delle porte.

Windows 7: ● OS fingerprint

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Utilizzando “nmap -Pn -O” su ip di Windows 7 si è cercato, eliminando la richiesta “ping” di ottenere informazioni sul sistema operativo nonostante il firewall di Windows. Si è provato ad utilizzare anche “nmap -Pn –osscan-limit” e “nmap -Pn –osscan-guess” per ottenere informazioni ma senza risultato.