M3 D6

ESERCIZIO

GIORNO 5 – SCANSIONE CON NMAP

Date le richieste dell'esercizio, vado a presentare in breve la funzione di ogni comando da me eseguito da terminale Kali verso la macchina Metasploitable.

nmap -sS:
Esegue una scansione SYN sulle prime 1000 porte dell'host specificato.
Questa scansione utilizza il SYN/ACK del 3-way handshake per determinare se una porta è aperta, chiusa o filtrata.

nmap -sV:
Esegue una scansione di versione sulle prime 1000 porte dell'host specificato.
Questa scansione utilizza la risposta del servizio per determinare la versione del software in esecuzione sulla porta.

nmap -sV -oN file.txt:
Esegue una scansione di versione sulle prime 1000 porte dell'host specificato e salva i risultati in un file di testo denominato "file.txt".

nmap -sS -p 8080:
Esegue una scansione SYN solo sulla porta 8080 dell'host specificato.

nmap -sS -p:
Esegue una scansione SYN su tutte le porte dell'host specificato.

nmap -sU -r -v:
Esegue una scansione UDP su tutte le porte dell'host specificato, utilizzando il ritrasmissione dei pacchetti per determinare se una porta è aperta o chiusa.

nmap -O:
Esegue una rilevazione del sistema operativo dell'host specificato, utilizzando la risposta del sistema per determinare il sistema operativo in esecuzione.

nmap -F:
Esegue una scansione rapida sulle porte più comuni dell'host specificato.

nmap -PR:
Esegue una scansione ping sui dispositivi della rete, utilizzando il protocollo ARP per rilevare la presenza di dispositivi attivi sulla rete.

nmap -sP:
Esegue una scansione ping sui dispositivi della rete, utilizzando il protocollo ICMP per rilevare la presenza di dispositivi attivi sulla rete.

nmap -PN:
Esegue una scansione su un host specificato, ignorando il protocollo di risposta alle richieste di ping, che viene spesso utilizzato per nascondere la presenza di un host sulla rete.
Il 3-way handshake viene effettuato solo durante le scansioni SYN, in cui nmap invia un pacchetto SYN al server di destinazione e attende la risposta SYN/ACK per determinare se una porta è aperta. Al contrario, durante le scansioni UDP, utilizza la ritrasmissione dei pacchetti per determinare se una porta è aperta o chiusa, senza effettuare il 3-way handshake.
Le scansioni ICMP e ARP non utilizzano il 3-way handshake.