**Report sulle Tecniche di scansione con Nmap**

1)OS Fingerprint: Comando nmap -O 192.168.1.3 da kali a metasploitable

Immagine che contiene testo, schermata, menu

Descrizione generata automaticamente

2)SYN Scan: Comando -sS 192.168.1.3 da kali a metasploitable

Immagine che contiene testo, schermata

Descrizione generata automaticamente

3)TCP Connect: comando nmap -sT 192.168.1.3 da kali a metasploitable

Immagine che contiene testo, schermata

Descrizione generata automaticamente

4)Versione detection: comando nmap -sV 192.168.1.3 da kali a metasploitable

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente

5)OS Fingerprint su Windows 7: comando nmap -O 192.168.1.3 da kali a Windows 7

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Report Dettagliato delle Scansioni con Nmap**

**Target: Metasploitable (IP: 192.168.1.3)**

**1. OS Fingerprint:**

**- Scopo del Comando:** Identifica il sistema operativo della macchina target tramite pacchetti specificamente formati per analizzare le risposte del TCP/IP stack.

**- Risultati:** Rilevamento di un sistema operativo Linux, versione kernel tra 2.6.9 e 2.6.33.

**2. SYN Scan:**

**- Scopo del Comando:** Effettua una scansione rapida utilizzando pacchetti SYN per identificare porte aperte sul target senza completare la connessione TCP.

**- Risultati:** Conferma di diverse porte aperte che indicano servizi attivi come SSH, HTTP e altri.

**3. TCP Connect:**

**- Scopo del Comando:** Completa la connessione TCP per ciascuna porta aperta per verificare la disponibilità dei servizi.

**- Risultati:** Conferma dei risultati della SYN Scan, mostrando una coerenza tra le porte aperte rilevate in entrambi i modi.

**4. Version Detection:**

**- Scopo del Comando:** Determina le versioni dei servizi in esecuzione sulle porte aperte.

**- Risultati:** Rilevamento delle versioni specifiche dei servizi come vsftpd, OpenSSH, e Apache, indicando potenziali vulnerabilità note associate a queste versioni.

**Target: Windows 7 (IP: 192.168.1.4)**

**1. OS Fingerprint:**

**- Scopo del Comando:** Identifica il sistema operativo tramite analisi delle risposte del TCP/IP stack.

**- Risultati:** Non è stato possibile determinare un OS specifico a causa della presenza di molteplici fingerprint possibili, suggerendo l'uso di tecniche di sicurezza avanzate che ostacolano l'identificazione.

**Conclusione e Quesito Extra**

**- Importanza delle Scansioni:** Le scansioni realizzate offrono una visione dettagliata delle configurazioni di rete e dei servizi esposti di Metasploitable, utili per valutazioni di sicurezza e formazione. Al contrario, la scansione di Windows 7 mostra una maggiore resistenza alle tecniche standard di fingerprinting, evidenziando una sicurezza più robusta.

**- Consigli per Migliorare le Scansioni su Windows 7:** Per superare le barriere di sicurezza e ottenere risultati più definiti, si raccomanda l'adozione di tecniche di scansione stealth come il Fragmented Packet Scan o Decoy Scanning, che possono aiutare a evitare la rilevazione da parte di sistemi IDS/IPS, oppure trovare un modo di bypassare il firewall, come ad esempio nel nostro caso, in quanto abbiamo eseguito i test su delle macchine virtuali, quindi disattivando il firewall il comando fingerprint su windows 7 ha funzionato.

**Esempio del comando nmap -O 192.168.1.4 con firewall windows 7 disattivato:**

Immagine che contiene testo, schermata

Descrizione generata automaticamente