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.

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, menu

Descrizione generata automaticamente

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Metasploitable (IP: 10.0.2.6):

OS Fingerprint:

Risultati: Linux 2.6.9 - 2.6.33

Commento: L'OS fingerprint suggerisce che il sistema operativo su Metasploitable è basato su Linux.

Syn Scan:

Risultati: Molti servizi aperti, tra cui SSH, FTP, Telnet, SMTP, HTTP, e altri.

Commento: La scansione SYN ha identificato numerosi servizi aperti su Metasploitable.

TCP Connect Scan:

Risultati: Simili alla scansione SYN, con l'identificazione di molti servizi.

Commento: La scansione TCP Connect conferma i risultati della scansione SYN.

Version Detection:

Risultati: Identificati vari servizi con versioni specifiche, tra cui vsftpd, OpenSSH, Apache, Samba, ecc.

Commento: La version detection fornisce informazioni più dettagliate sui servizi in esecuzione su Metasploitable.

Windows 7 (IP: 10.0.2.5):

OS Fingerprint:

Risultati: Indicazioni di possibili sistemi operativi Windows, tra cui Windows 8.1, Windows Phone 7.5 o 8.0, ecc.

Commento: Gli esiti dell'OS fingerprint suggeriscono un sistema operativo Windows, ma non è possibile una corrispondenza esatta.

Syn Scan:

Risultati: Porte aperte, inclusi servizi come MSRPC, NetBIOS, Microsoft-DS, ecc.

Commento: La scansione SYN ha identificato servizi tipici di un sistema Windows.

TCP Connect Scan:

Risultati: Simili alla scansione SYN, con l'identificazione di servizi tipici di Windows.

Commento: La scansione TCP Connect conferma i risultati della scansione SYN.

Version Detection:

Risultati: Identificati servizi specifici con versioni, come Microsoft Windows RPC, Microsoft Windows 7, ecc.

Commento: La version detection fornisce dettagli specifici sulla versione dei servizi Windows in esecuzione.

Commenti Generali:

Entrambi i sistemi hanno numerose porte aperte, ma Metasploitable è configurato per essere vulnerabile e usato come piattaforma di test.