**NMAP**

Nmap è un tool di port scanner che permette di effettuare scansioni molto invasive o meno invasive a seconda delle necessità di chi lo usa.

**REPORT NMAP METASPLOITABLE**

**Immagine che contiene testo

Descrizione generata automaticamente**

Con il comando nmap target –script smb-os-discovery possiamo scansionare le porte aperte con i rispettivi servizi e, inoltre, possiamo sapere qual è il tipo di sistema operativo del target che in questo caso è Metasploitable. É un comando di script.

Immagine che contiene testo

Descrizione generata automaticamente

Con il comando nmap -sS target possiamo effettuare una scansione chiamata stealth scan che non completa il 3WH ed effettua un collegamento solo con il SYN e poi chiude la richiesta senza rispondere. Questo tipo di scansione è poco invasiva, per questo chiamata stealth.

Immagine che contiene testo

Descrizione generata automaticamente

Con il comando nmap -sT target effettuiamo una scansione delle porte e dei servizi che va a completare la connessione 3WH e quindi effettua una connessione completa TCP e di conseguenza è più rumorosa come scansione.

Immagine che contiene testo

Descrizione generata automaticamente

Con il comando nmap -sV target andiamo ad effettuare una scansione molto invasiva che mostra, oltre alle porte e i servizi attivi, anche la versione di ogni servizio. Come già detto, questa scansione è la più aggressiva e rallenta molto la rete bersaglio.

**REPORT NMAP WINDOWS**

Immagine che contiene testo

Descrizione generata automaticamente

Con il comando nmap target –script smb-os-discovery possiamo sapere il tipo di sistema operativo del target. In questo caso il comando non ha funzionato perché è stata disabilitata una regola sul Firewall che ne permetta la scansione. Il problema può essere risolto con la creazione di una regola (in questo caso andando ad abilitare la regola che è stata disabilitata), oppure con l’inserimento dello switch -T che definisce la velocità di scansione. Questa switch può andare da -T0 a -T5 dove 0 è lentissimo e 5 è velocissimo. Con la switch -T0 e -T1 si possono eludere sistemi di sicurezza come IDS.

Nella foto successiva possiamo notare la stessa scansione ma con la regola del Firewall abilitata.

Immagine che contiene testo

Descrizione generata automaticamente