Brenda San Germán

Lab Nmap

Necesitarán: Kali Linux

ICMP Scanning 🡪 nmap –sn 192.168.168.5

Nmap –P cert.org/24 152.148.0.0/16

Debido a que ICMP no tiene una abstracción de puerto, esto no es lo mismo que escanear puertos. Sin embargo, es útil determinar qué hosts en una red se ejecutan haciendo ping a todos ellos (Nmap utiliza la opción -P para escanear ICMP en paralelo, lo cual puede suceder rápidamente). El usuario también puede aumentar el número de pings en paralelo mediante la opción -L. También puede ser útil ajustar el tiempo de espera de ping utilizando la opción -T.Nmap –sT –T3 –A 10.0.0.8

Ping (ICMP) Sweep 🡪 nmap –sn –PE –PA21,23,80,3389 192.168.168.1-3

Ping sweep se utiliza para determinar los hosts vivos de un rango de direcciones IP enviando peticiones ICMP ECHO a varios hosts. Si un host está vivo, devolverá una respuesta ICMP ECHO. Cuando un sistema hace un ping, envía un solo paquete a través de la red a una dirección IP específica. Este paquete contiene 64 bytes (56 bytes de datos y 8 bytes de información de encabezado de protocolo). El emisor entonces espera o escucha un paquete de devolución del sistema de destino.

TCP scan en modo agresivo con timing normal (-T3) 🡪 nmap –sT –T3 –A 10.0.0.8

Xmas Scan con timing agresivo T4🡪 nmap –sX –T4 [IP Address of Windows Server 2008]

ACK Flag Probe Scan 🡪 nmap –sA –v –T4 [IP Address of Windows Server 2008]

UDO scan con time scan T5 🡪nmap –Su –T5 [IP Address of Windows Server 2008]

IDLE/IPID Header Scan 🡪 nmap –Pn –p- -sI [www.miscursos.tec.mx](http://www.miscursos.tec.mx) [www.nmap.org](http://www.nmap.org)

UDP Scan 🡪 nmap –sU –v 192.168.0.97

Bibliografía

EC-Council. (2015, December 31). CEH v9 Module 03 Scanning Networks [PDF]. EC-Council.