Listado de comandos Nmap

Seleccionar objetivos

Direcciones o rangos IP, nombres de sistemas, redes, etc.

Ejemplo: scanme.nmap.org, microsoft.com/24, 192.168.0.1, 10.0.0-255.1-254

- iL fichero lista en fichero -iR n elegir objetivos aleatoriamente, 0 nunca acaba
- –exclude –excludefile fichero excluir sistemas desde fichero

Descubrir sistemas

- PS n tcp syn ping
- PA n ping TCP ACK
- PU n ping UDP
- PM Netmask Req
- PP Timestamp Req
- PE Echo Req
- sL análisis de listado
- PO ping por protocolo
- PN No hacer ping
- n no hacer DNS
- R Resolver DNS en todos los sistemas objetivo
- traceroute: trazar ruta al sistema (para topologías de red)
- sP realizar ping, igual que con –PP –PM –PS443 –PA80

Técnicas de análisis de puertos

- sS análisis utilizando TCP SYN
- sT análisis utilizando TCP CONNECT
- sU análisis utilizando UDP
- sY análisis utilizando SCTP INIT
- sZ utilizando COOKIE ECHO de SCTP
- sO protocolo IP
- sW ventana TCP -sN
- sF -sX NULL, FIN, XMAS
- sA TCP ACK

Puertos a analizar y orden de análisis

- p n-mrango
- p– todos los puertos
- p n,m,z especificados
- p U:n-m,z T:n,m U para UDP, T para TCP
- F rápido, los 100 comunes

- top-ports n analizar los puertos más utilizados
- r no aleatorio

Duración y ejecución:

- T0 paranoico
- T1 sigiloso
- T2 sofisticado
- T3 normal
- T4 agresivo
- T5 locura
- min-hostgroup
- max-hostgroup
- min-rate
- max-rate
- min-parallelism
- max-parallelism
- min-rtt-timeout
- max-rtt-timeout
- initial-rtt-timeout
- max-retries
- host-timeout –scan-delay

Detección de servicios y versiones

- sV: detección de la versión de servicios
- all-ports no excluir puertos
- version-all probar cada exploración
- version-trace rastrear la actividad del análisis de versión
- O activar detección del S. Operativo
- fuzzy adivinar detección del SO
- max-os-tries establecer número máximo de intentos contra el sistema objetivo

Evasión de Firewalls/IDS

- f fragmentar paquetes
- D d1,d2 encubrir análisis con señuelos
- S ip falsear dirección origen
- g source falsear puerto origen
- randomize-hosts orden
- spoof-mac mac cambiar MAC de origen

Parámetros de nivel de detalle y depuración

- v Incrementar el nivel de detalle
- reason motivos por sistema y puerto
- d (1-9) establecer nivel de depuración
- packet-trace ruta de paquetes

Otras opciones

- resume file continuar análisis abortado (tomando formatos de salida con -oN o -oG)
- 6 activar análisis IPV6
- A agresivo, igual que con -O -sV -sC –traceroute

Opciones interactivas

- v/V aumentar/disminuir nivel de detalle del análisis
- d/D aumentar/disminuir nivel de depuración
- p/P activar/desactivar traza de paquetes

Scripts

- sC realizar análisis con los scripts por defecto
- script file ejecutar script (o todos)
- script-args n=v proporcionar argumentos
- script-trace mostrar comunicación entrante y saliente

Formatos de salida

- oN guardar en formato normal
- oX guardar en formato XML
- oG guardar en formato para posteriormente usar Grep
- oA guardar en todos los formatos anteriores