Universidad De Granada

Grado ingeniería informática (2017 – 2018)

Fundamentos De Redes

NMAP

Trabajo realizado por Javier Galera Garrido y Antonio Miguel Morillo Chica

---

1. ¿Que es nmap?

Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.

Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

2. ¿Cómo funciona?

Nmap toma como entrada una serie de argumentos que explicaremos más adelante, tipo de sondeo, opciones y la expecificación del objetivo a analiar.

Como salida nmap da un listado objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la "tabla de puertos interesantes". Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El estado puede ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtradoindica que un cortafuegos, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap, pero para los que que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las combinaciones de estado open|filtered y closed|filtered cuando no puede

determinar en cual de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (-sO).

Además de la tabla de puertos interesantes, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC.

3 Uso de nmap.

Nmap se puede usar con apariencia grafica, más conocido como zenmap o por terminal. El uso por terminal de nmap se resume en una sentiencia:

nmap [Tipo(s) de Análisis] [Opciones] {especificación de objetivos}

Ahora le listaremos las opciones más importantes y tipo de analisis existentes para este servicio.

- ESPECIFICACIÓN DE OBJETIVO:

  Se pueden indicar nombres de sistema, direcciones IP, redes, etc. Ej: scanm e.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

  - -iL <archivo_entrada>: Lee una lista de sistemas/redes del archivo.
  - -iR <número de sistemas>: Selecciona objetivos al azar
  - --exclude <sist1[,sist2][,sist3],...>: Excluye ciertos sistemas o redes
  - --excludefile <fichero_exclusión>: Excluye los sistemas indicados en el fichero

- DESCUBRIMIENTO DE HOSTS:
  - -sL: Sondeo de lista - Simplemente lista los objetivos a analizar
  - -sP: Sondeo Ping - Sólo determina si el objetivo está vivo

- -P0: Asume que todos los objetivos están vivos
- -PS/PA/PU [puertos]: Análisis TCP SYN, ACK o UDP de los puertos.
- -PE/PP/PM: Solicita un análisis ICMP del tipo echo, marca de fecha y máscara de red
- -n/-R: No hacer resolución DNS / Siempre resolver
- --dns-servers <serv1[serv2],...>: Especificar servidores DNS específicos
  --system-dns: Utilizar la resolución del sistema operativo

- TÉCNICAS DE ANÁLISIS:
  - -sS/sT/sA/sW/sM: Análisis TCP SYN/Connect()/ACK/Window/Mai mon
  - -sN/sF/sX: Análisis TCP Null, FIN, y Xmas
  - --scanflags <indicador>: Personalizar los indicadores TCP a utilizar
  - -sI <sistema zombi[:puerto_sonda]>: Análisis pasivo («Idle», N. del T.
  - -sO: Análisis de protocolo IP
  - -b <servidor ftp rebote>: Análisis por rebote FTP

- ESPECIFICACIÓN DE PUERTOS Y ORDEN DE ANÁLISIS:
  - -p <rango de puertos>: Sólo sondear los puertos indicados Ej: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  - -F: Rápido - Analizar sólo los puertos listados en el archivo nmap-services
  - -r: Analizar los puertos secuencialmente, no al azar.

- DETECCIÓN DE SERVICIO/VERSIÓN:
  - -sV: Sondear puertos abiertos, para obtener información de servicio/ver sión

- --version-intensity <nivel>: Fijar de 0 (ligero) a 9 (probar todas las son das)
- --version-light: Limitar a las sondas más probables (intensidad 2)
- --version-all: Utilizar todas las sondas (intensidad 9)
- --version-trace: Presentar actividad detallada del análisis (para depurar)

- DETECCIÓN DE SISTEMA OPERATIVO
  - -O: Activar la detección de sistema operativo (SO)
  - --osscan-limit: Limitar la detección de SO a objetivos prometedores
  - --osscan-guess: Adivinar el SO de la forma más agresiva

- TEMPORIZADO Y RENDIMIENTO:
  - -T[0-5]: Seleccionar plantilla de temporizado (los números altos son más rápidos)
  - --min-hostgroup/max-hostgroup <tamaño>: Paralelizar los sondeos
  - --min-parallelism/max-parallelism <msegs>: Paralelización de sondeos
  - --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <msegs>: Indica el tiempo de ida y vuelta de la sonda
  - --max-retries <reintentos>: Limita el número máximo de retransmision es de las sondas de análisis de puertos
  - --host-timeout <msegs>: Abandonar un objetivo pasado este tiempo
  - --scan-delay/--max-scan-delay <msegs>: Ajusta el retraso entre sondas

- EVASIÓN Y FALSIFICACIÓN PARA CORTAFUEGOS/IDS:
  - -f; --mtu <valor>: fragmentar paquetes (opc. con el MTU indicado)
  - -D <señuelo1,señuelo2[,ME],...>: Disimular el análisis con señuelos
    N. del T.: «ME» es «YO» mismo.

- -S <Dirección_IP>: Falsificar la dirección IP origen
- -e <interfaz>: Utilizar la interfaz indicada
- -g/--source-port <numpuerto>: Utilizar el número de puerto dado
- --data-length <num>: Agregar datos al azar a los paquetes enviados
- --ttl <val>: Fijar el valor del campo time-to-live (TTL) de IP
- --spoof-mac <dirección mac/prefijo/nombre de fabricante>: Falsificar la dirección MAC
- --badsum: Enviar paquetes con una suma de comprobación TCP/UDP falsa

- SALIDA:
  - -oN/-oX/-oS/-oG <file>: Guardar el sondeo en formato normal, XML, s|<rIpt kIddi3 (n3n3b4n4n4), y Grepeable (para usar con grep(1), N. d el T.), respectivamente, al archivo indicado.
  - -oA <nombre_base>: Guardar en los tres formatos principales al mism o tiempo
  - -v: Aumentar el nivel de mensajes detallados (-vv para aumentar el efec to)
  - -d[nivel]: Fijar o incrementar el nivel de depuración (Tiene sentido hast a 9)
  - --packet-trace: Mostrar todos los paquetes enviados y recibidos
  - --iflist: Mostrar interfaces y rutas (para depurar)
  - --append-output: Agregar, en vez de sobreescribir, a los archivos indica dos con -o.
  - --resume <archivo>: Retomar un análisis abortado/detenido
  - --stylesheet <ruta/URL>: Convertir la salida XML a HTML según la hoja de estilo XSL indicada

- --webxml: Referenciar a la hoja de estilo de Insecure.Org para tener un XML más portable
- --no_stylesheet: No asociar la salida XML con ninguna hoja de estilos XSL

- MISCELÁNEO:
  - 6: Habilitar análisis IPv6
  - -A: Habilita la detección de SO y de versión
  - --datadir <nombreDir>: Indicar la ubicación de los archivos de datos N map personalizados.
  - --send-eth/--send-ip: Enviar paquetes utilizando tramas Ethernet o paquetes IP "crudos"
  - --privileged: Asumir que el usuario tiene todos los privilegios
  - -V: Muestra el número de versión
  - -h: Muestra esta página resumen de la ayuda.