**Laboratorio #3: NMAP**

|  |
| --- |
| **Tiempo estimado de duración: 1.5 hora (90 minutos)**  **Nota importante**: Atienda las instrucciones del profesor para el desarrollo del laboratorio, luego realice las actividades de acuerdo a sus instrucciones.  **Instrucciones del laboratorio #1**: Ud. es un administrador de red que desea conocer el uso de “nmap” para la de búsqueda de los componentes de la red interna y los cuales pueden ser posibles objetivos para los APT’s.  **Recursos necesarios**: Uso de la máquina virtual Kali Linux 2016. |

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

**Ejercicio 1: Realice un escaneo a un único host y a una dirección IP (IPv4)**

|  |
| --- |
| Instrucción: Escanear una única dirección IP  nmap 192.168.1.6 |
|  |

|  |
| --- |
| Instrucción: Escanear un nombre de host  nmap scanme.nmap.org |
|  |

|  |
| --- |
| Instrucción: Escanear un nombre de host con más información  nmap -v scanme.nmap.org |
|  |

**Ejercicio 2: Escanear varias direcciones IP o subred (IPv4)**

|  |
| --- |
| Instrucción: Escanear la red utilizando la secuencia de tipo: IP1,IP2,IP3 y con comas  nmap 192.168.1.1,2,3 |
|  |

|  |
| --- |
| Instrucción: Escanear un rango de direcciones  nmap 192.168.1.1-20, nmap 192.168.1.\*, nmap 192.168.1.0/24 |
|  |

**Ejercicio 3: Lea la lista de hosts / redes desde un archivo (IPv4)**

|  |
| --- |
| Instrucción: Crear un archivo de texto con el nombre y extensión “su\_apellido.txt” (ruta: cat > /tmp/apellido.txt) para analizar el rango de direcciones (192.168.1.0/24, 192.168.1.1/24, 192.168.2.1/24, 192.168.3.1/24), ejecute el comando siguiente:  nmap -iL /root/Desktop/su\_apellido.txt |
|  |

**Ejercicio 4: Exclusión de hosts / redes (IPv4)**

|  |
| --- |
| Instrucción: Escanear un gran número de hosts / redes se pueden excluir los hosts de una exploración, ejecutar lo siguiente:  nmap 192.168.1.0/24 --exclude 192.168.1.1  nmap 192.168.1.0/24 --exclude 192.168.1.1,192.168.1.254  nmap 192.168.1.\* --exclude 192.168.1.3  O excluir lista desde un archivo llamado “exclude.txt” en la ruta: /tmp/exclude.txt  Ejecutar:  nmap -iL/tmp/scanlist.txt --excludefile /tmp/exclude.txt |
|  |

**Ejercicio 5: Utilice un script para detectar el sistema operativo (IPv4)**

|  |
| --- |
| Instrucción: Se puede detectar que sistema operativo y versión se está ejecutando en el host remoto. Para habilitar la detección de sistema operativo y versión, la exploración de la escritura y la Ruta de seguimiento, podemos usar la opción "-A". nmap -A 192.168.1.254 nmap –v -A 192.168.1.1 nmap –A –iL /tmp/scanlist.txt |
|  |

**Ejercicio 6: Para saber si un host / red están protegidos por un firewall**

|  |
| --- |
| Instrucción: Ejecutar las sentencias descritas e indique los resultados  nmap -sA 192.168.1.6  nmap -sA server1.cyberciti.biz |
|  |

**Ejercicio 7: Escanear un host si está protegido por el firewall**

|  |
| --- |
| Instrucción: Para escanear un host si está protegido por ningún software de filtrado de paquetes o cortafuegos. Realizar la siguiente consulta nmap -PN 192.168.1.6 nmap -PN server1.cyberciti.biz |
|  |

**Ejercicio 8: Escanear una red y averiguar qué servidores y dispositivos están en marcha**

|  |
| --- |
| Instrucción: Con la ayuda de la opción "-sP" podemos comprobar que hosts están vivos y en red, con esta opción se salta nmap la detección de puertos y otras acciones. nmap -sP 192.168.1.0/24 |
|  |

**Ejercicio 9: Realizar un análisis rápido**

|  |
| --- |
| Instrucción: Se puede realizar un análisis rápido con la opción "-F" para las exploraciones para los puertos que figuran en los archivos de nmap-services y deja todos los demás puertos.  nmap -F 192.168.1.1 |
|  |

**Ejercicio 10: Mostrar la razón (reason), un puerto está en un estado particular**

|  |
| --- |
| Instrucción: Realizar la siguiente instrucción:  nmap -reason 192.168.1.6  nmap –reason server1.cyberciti.biz |
|  |

**Ejercicio 11: Mostrar únicamente los puertos abiertos (o posiblemente abiertos)**

|  |
| --- |
| Instrucción: Ejecutar las siguientes instrucciones para mostrar los puertos abiertos de las direcciones  nmap --open 192.168.1.1  nmap --open server1.cyberciti.biz |
|  |

**Ejercicio 12: Muestra todos los paquetes enviados y recibidos**

|  |
| --- |
| Instrucción: Ejecutar las siguientes instrucciones:  nmap --packet-trace 192.168.1.1  nmap --packet-trace server1.cyberciti.biz |
|  |

**Ejercicio 13: show interfaces de host y rutas**

|  |
| --- |
| Instrucción: Ejecutar las siguientes instrucciones:  nmap --iflist |
|  |

**Ejercicio 14: Escanear puertos específicos**

|  |
| --- |
| Instrucción: Ejecutar las siguientes instrucciones (**nmap-p [puerto] hostName**).  Escanear el puerto 21, 23, 80 y 443.  nmap -p [puerto] 192.168.1.1 |
|  |

|  |
| --- |
| Instrucción: Escanear el puerto **TCP** 443 (especificando el puerto)  nmap -p T:443 192.168.1.2 |
|  |

|  |
| --- |
| Instrucción: Escanear el puerto UDP 53 (especificando el puerto).  nmap -sU -p 53,3478 192.168.1.6 |
|  |

|  |
| --- |
| Instrucción: Escanear dos puertos – múltiples puertos 80, 443  nmap -p 80,443 192.168.1.3 |
|  |

|  |
| --- |
| Instrucción: Escanea rangos de puertos siguiente:  nmap -p 80-200 192.168.1.2 |
|  |

|  |
| --- |
| Instrucción: Combinar todas las opciones  nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.6  nmap -p U:53,111,137,T:21-25,80,139,8080 server1.cyberciti.biz  nmap -v -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.1.6 |
|  |

|  |
| --- |
| Instrucción: Analizar todos los puertos con comodín “ **\*** “  nmap -p "\*" 192.168.1.6 |
|  |

|  |
| --- |
| Instrucción: Escanear puertos principales, es decir $ escanear puertos numéricos más comunes  nmap --top-ports 5 192.168.1.1  nmap --top-ports 10 192.168.1.1 |
|  |

**Ejercicio 15: La forma más rápida para escanear todos los dispositivos / equipos para puertos abiertos a la vez**

|  |
| --- |
| Instrucción: Ejecutar la siguiente instrucción:  nmap -T5 192.168.1.0/24 |
|  |

**Ejercicio 16: Detectar el sistema operativo remoto**

|  |
| --- |
| Instrucción: Utilice la opción "-O" y "-osscan-guess" también ayuda a descubrir la información del sistema operativo.  nmap -O 192.168.1.6  nmap -O --osscan-guess 192.168.1.6  nmap -v -O --osscan-guess 192.168.1.6 |
|  |

**Ejercicio 17: Detectar servicios remotos (servidor / daemon) números de versión**

|  |
| --- |
| Instrucción: Ejecutar la siguiente instrucción:  nmap -sV 192.168.1.1 |
|  |

**Ejercicio 18: Escanear un host que utiliza TCP ACK (PA) y TCP Syn (PS) de ping**

|  |
| --- |
| Instrucción: A veces, los cortafuegos de filtrado de paquetes bloquea las solicitudes de ping ICMP estándar, en ese caso, podemos utilizar métodos TCP ACK y TCP Syn para escanear hosts remotos. Ejecutar la siguiente instrucción:  nmap -PS 192.168.1.6 |
|  |

**Ejercicio 18a - Analizar Host remoto para puertos específicos con TCP Syn**

|  |
| --- |
| Instrucción: Realizar las siguientes instrucción:  nmap -PS 80,21,443 192.168.1.1 |
|  |

**Ejercicio 18b - Analizar Host remoto para puertos específicos con TCP ACK**

|  |
| --- |
| Instrucción: Realizar las siguientes instrucciones:  nmap -PA -p 22,80 192.168.1.3  nmap -PA 192.168.1.1  nmap -PA 80,21,200-512 192.168.1.1 |
|  |

**Ejercicio 19: Escanear un host utilizando el protocolo IP**

|  |
| --- |
| Instrucción: Ejecutar la siguiente instrucción:  nmap -PO 192.168.1.1 |
|  |

**Ejercicio 20: Escanear un host con el protocolo UDP**

|  |
| --- |
| Instrucción: Este análisis no pasa por firewalls y filtros de pantalla que sólo TCP:  nmap -PU 192.168.1.1  nmap -PU 2000.2001 192.168.1.1 |
|  |

**Ejercicio 21: Descubre los más utilizados los puertos TCP que utilizan TCP SYN Scan**

|  |
| --- |
| Instrucción: Para realizar un escaneo sigiloso realizar:  nmap -sS 192.168.1.6   * Conoce las más comunes que utilizan los puertos TCP usando “TCP connect scan” (aviso: no hay exploración sigilosa) * Conocer el sistema operativo - Compruebe más puertos utilizando TCP Syn# # #nmap -sT 192.168.1.6 * Conoce las más comunes que utilizan los puertos TCP usando TCP ACK scan   nmap -sA 192.168.1.6   * Conoce las más comunes que utilizan los puertos TCP usando TCP Window scan   nmap -sW 192.168.1.6   * Conoce las más comunes que utilizan los puertos TCP usando TCP Maimon scan   nmap -sM 192.168.1.6 |
|  |

**Ejercicio 22: Escanear un host para servicios UDP (UDP scan)**

|  |
| --- |
| Instrucción: La mayoría de los servicios populares de internet se extienden sobre el protocolo TCP. No obstante, DNS, SNMP y DHCP; estos son tres de los servicios UDP más comunes. Utilice la sintaxis siguiente para averiguar los servicios UDP:  nmap -sU nas03  nmap -sU 192.168.1.6 |
|  |

**Ejercicio 23: Analizar en busca de protocolo IP**

|  |
| --- |
| Instrucción: Este tipo de análisis permite determinar qué protocolos IP (TCP, ICMP, IGMP, etc) son compatibles con los equipos de destino. Ejecutar la siguiente instrucción: nmap -sO 192.168.1.6 |
|  |

**Ejercicio 24: Escanear debilidades de seguridad en un firewall**

|  |
| --- |
| Instrucción: Los siguientes tipos de exploración explotar una escapatoria sutil en el TCP y bueno para probar la seguridad de los ataques más comunes:   * TCP Null Scan para engañar a un servidor de seguridad para generar una respuesta * No establece ningún bit (encabezado TCP bandera es 0).   nmap -sN 192.168.1.6   * TCP Fin scan para comprobar el firewall * Establece sólo el bit TCP FIN   nmap -sF 192.168.1.6   * TCP Xmas escaneado para comprobar firewall * Establece el FIN, PSH, URG y banderas, encendiendo el paquete como un árbol de Navidad   nmap -sX 192.168.1.6 |
|  |

**Ejercicio 25: Digitalizar un servidor de seguridad de los fragmentos de paquetes**

|  |
| --- |
| Instrucción: La opción-f hace que la exploración solicitada (incluyendo las exploraciones ping) a utilizar pequeños paquetes IP fragmentados. La idea es dividir la cabecera TCP a través de varios paquetes para que sea más difícil para los filtros de paquetes, sistemas de detección de intrusos y otras molestias para detectar lo que está haciendo.  nmap -f 192.168.1.1  nmap -f fw2.nixcraft.net.in  nmap -f 15 fw2.nixcraft.net.in   * Establece el tamaño de su propia compensación con la opción --mtu   nmap --mtu 32 192.168.1.1 |
|  |

**Ejercicio 26: Capa de un análisis con señuelos**

|  |
| --- |
| Instrucción: La opción-D que aparece al host remoto que el host (s) se especifica como señuelos a escanear la red de destino también. Así, sus IDS puede informar escaneos de puertos 5-10 de direcciones IP únicas, pero no sabrán qué IP se escanearlos y que eran señuelos inocentes:  nmap -n -Ddecoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip  nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5 |
|  |

**Ejercicio 27: Digitalizar un firewall para la falsificación de direcciones MAC**

|  |
| --- |
| Instrucción: Realice un “Spoof” (disfrazar) de su dirección MAC  nmap --spoof-mac MAC-ADDRESS-HERE 192.168.1.6  Añadir otra opción  nmap -v -sT -PN --spoof-mac MAC-ADDRESS-HERE 192.168.1.6  Usar una dirección MAC aleatoria:  El número 0, significa nmap elige una dirección MAC al azar  nmap -v -sT -PN --spoof-mac 0 192.168.1.1 |
|  |

**Ejercicio 28: Guardar la salida en un archivo de texto**

|  |
| --- |
| Instrucción: Ejecute la siguientes instrucciones para guardar en un archivo de texto.  nmap 192.168.1.1 > output.txt  nmap -oN /path/to/filename 192.168.1.1  nmap -oN output.txt 192.168.1.1 |
|  |

**Ejercicio 29: Versión de NMAP instalado**

|  |
| --- |
| Instrucción: Ejecutar la siguiente instrucción para conocer la versión de nmap instalado.  nmap –V |
|  |

**Ejercicio 30: Escaneo de puertos de forma consecutiva**

|  |
| --- |
| Instrucción: Ejecutar la siguiente instrucción:  nmap -r 192.168.0.101 |
|  |

**Ejercicio 31: Interfaces de impresión de Host y rutas**

|  |
| --- |
| Instrucción: Usted puede encontrar la interfaz y ruta de información de host con nmap con la opción "-iflist". Ejecutar lo siguiente:  nmap --iflist |
|  |

**Laboratorio 1: Uso de Zenmap**

|  |
| --- |
| Explicación: Esta opción sondea todos los puertos TCP reservados en el servidor scanme.nmap.org. La opción -v activa el modo detallado (también llamado verboso). nmap -v scanme.nmap.org |
| Indique los resultados: |

|  |
| --- |
| Explicación: Lanza un sondeo de tipo SYN sigiloso contra cada una de las 255 máquinas en la “clase C” de la red donde está el sistema "analizame". También intenta determinar cuál es el sistema operativo que se ejecuta en cada máquina que esté encendida. Esto requiere permisos de root por la opción de sondeo SYN y por la de detección de sistema operativo. nmap -sS -O scanme.nmap.org/24 |
| Indique los resultados: |

|  |
| --- |
| Explicación: Lanza una enumeración de equipos y un sondeo TCP a cada uno de la primera mitad de las 255 posibles subredes de 8 bit en la red de clase B 198.116. Esto probará si los sistemas están ejecutando sshd, DNS, pop3d, imapd o tienen un servidor en el puerto 4564. Para cualquier puerto que se encuentre abierto, se realizará una detección de versión para determinar qué aplicación se está ejecutando.  Ejecutar:nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127 |
| Indique los resultados: |

|  |
| --- |
| Ejecutar: nmap -v -iR 100000 -P0 -p 80  Explicación: Solicita a Nmap que elija 100.000 sistemas aleatoriamente y los sondee buscando servidores web (puerto 80). La enumeración de sistemas se deshabilita con -P0 ya que es un desperdicio enviar un par de pruebas para determinar si el sistema debe ser analizado cuando de todas maneras sólo se va a analizar un puerto. |
| Indique los resultados: |

|  |
| --- |
| Explicación: Esto sondea 4096 IP’s para buscar cualquier servidor web (sin enviar sondas ICMP) y guarda la salida en formato para grep y en XML. nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20 |
| Indique los resultados: |

**Fuente**: https://nmap.org/man/es/man-examples.html