

Masscan

Esta práctica tiene como objetivo detectar cuantas máquinas existen a día de hoy en España que todavía son vulnerables al exploit que utiliza WannaCry. Para llevar a cabo esta práctica vamos a emplear varias herramientas como son masscan y nmap. nmap ya ha sido utilizada en las prácticas anteriores para detectar si alguna de las máquinas virtuales con las que trabajamos eran vulnerables a MS17-010.

Como podéis comprobar en páginas como Nirsoft <http://www.nirsoft.net/countryip/es.html>, los rangos de IPs asignados a ISPs españoles son más de 28,3 millones de IPs. Para poder escanear tal cantidad de IPs utilizando nmap tardaríamos muchos días, es por ello que existen otras herramientas como es masscan que permite escanear un gran número de IPs en un corto espacio de tiempo.

Masscan es una herramienta que sólo está disponible en sistemas operativos Linux ya que utiliza una característica de los mismos como son los sockets asíncronos que permite obtener grandes rendimientos en procesos que hacen un uso intensivo de la red. Para poder hacer la práctica deberéis disponer de un portátil con sistema operativo Linux de forma nativa. Si no os fuera posible disponer de una máquina en la que instalar un sistema operativo Linux, poneros en contacto con el profesor que os asignará una máquina a la que acceder a través de VPN a un servidor con Linux.

La práctica tiene **dos partes claramente diferenciadas**.

La **primera** se realizará con un sistema operativo Linux nativo, a ser posible Ubuntu 16.04 que permite instalar masscan mediante apt-get. El objetivo de esta primera parte consiste en escanear todos los rangos de IPs asignados a ISPs Españoles. Para ello habrá que utilizar masscan. Es recomendable ver en la ayuda de masscan qué parámetros permiten:

- Establecer un rango de IPs de escaneo,
- Limitar los puertos a escanear. Téngase en cuenta que sólo nos interesa el puerto 445.
- Establecen un rating en el número de peticiones por segundo que se van a generar. No se recomienda pasar de 10000.
- Guardar los resultados en un fichero.
- Se recomienda utilizar awk u otra herramienta que permita generar un script de forma que se puedan lanzar todos los escaneos de una vez y volver pasado un tiempo a por los resultados generados en el fichero.

Los resultados que se deben obtener de esta prueba son la fecha y hora en la que se inició el escaneo y las máquinas que tienen el puerto 445 abierto.

La **segunda** parte de la práctica se hará desde la máquina Kali Linux.

Una vez se tenga un listado de todas las IPs con el puerto 445, en la segunda parte se debe utilizar nmap con el script que permite detectar la vulnerabilidad MS17-010. Y obtener el listado de IPs vulnerables.

Esta segunda parte se recomienda lanzar nmap desde una conexión que no se encuentre filtrada, para evitar falsos negativos. Es recomendable leer la ayuda de nmap para conocer qué parámetros se deben utilizar para guardar los resultados en un fichero y poder consultarlo y operar con los resultados a posteriori. Como resultado de esta segunda parte se debe obtener la fecha y la hora en la que se ejecutó el escaneo y las direcciones IPs vulnerables a WannaCry.

Análisis del rango de IPs asignadas a ISPs Españoles.

Usando la herramienta msscan se escanea el rango de ISPs Españoles (mas de 28 millones de IPs) para detectar aquellas que tengan abierta el puerto 445

```
iker@iker-Classic ~/Documentos/Ciberseguridad/masscan $ sudo masscan -c myscan.conf
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2021-10-24 05:44:53 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 2891777 hosts [1 port/host]
Rate: 2.95-kpps, 3.31% done, 0:15:40 remaining, found=10
```

Masscan -c myscan.conf

Se ha configurado un fichero para realizar todo el escaneo y guardar la salida en un xml

```
# My scan
rate = 3000
output-format = xml
output-status = open
output-filename = scan.xml
ports = 445
range = 2.136.0.0-2.143.255.255,2.1!
5.45.175.255,5.83.64.0-5.83.95.255,!
5.205.255.255,5.224.0.0-5.225.255.2!
31.44.159.255,31.214.176.031.214.19:
```

En el fichero de salida obtenemos la información de los **238 host** que tienen el puerto 445 abierto.

```
<host endtime="1635054295"><address addr="46.6.1.130" addr
<host endtime="1635054297"><address addr="2.136.103.221" a
<host endtime="1635054298"><address addr="37.158.57.2" add
<host endtime="1635054299"><address addr="37.10.179.69" ad
<host endtime="1635054311"><address addr="46.6.8.14" addrt
<host endtime="1635054312"><address addr="2.137.212.202" a
<host endtime="1635054313"><address addr="37.12.152.48" ad
<host endtime="1635054313"><address addr="2.137.39.64" add
```

Análisis de los 238 host mediante NMAP:

Una vez obtenida la información de los hosts, se extraen las IPs a un fichero para pasárselas a la herramienta NMAP y hacer el escaneo de los 238 hosts deseados.

El escaneo con NMAP nos detecta 8 máquinas vulnerables a WannaCry.

Hora de escaneo: Domingo 24/10/2021 08:37:08

Hosts vulnerables:

2.136.103.221

37.158.57.2

37.10.179.69

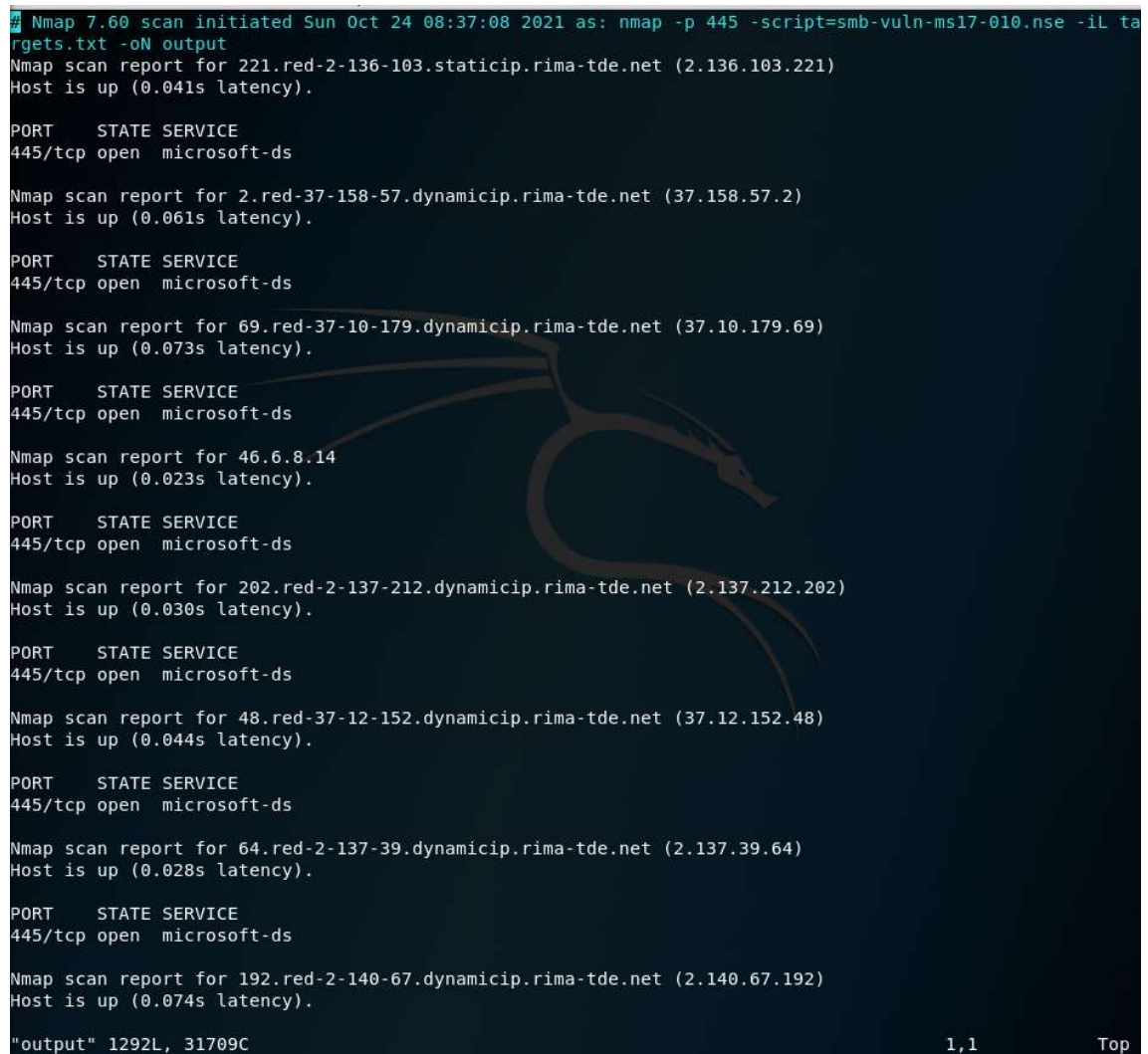
46.6.8.14

2.137.212.202

37.12.152.48

2.137.39.64

2.140.67.192



```
Nmap 7.60 scan initiated Sun Oct 24 08:37:08 2021 as: nmap -p 445 -script=smb-vuln-ms17-010.nse -iL targets.txt -oN output
Nmap scan report for 221.red-2-136-103.staticip.rima-tde.net (2.136.103.221)
Host is up (0.041s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap scan report for 2.red-37-158-57.dynamicip.rima-tde.net (37.158.57.2)
Host is up (0.061s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap scan report for 69.red-37-10-179.dynamicip.rima-tde.net (37.10.179.69)
Host is up (0.073s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap scan report for 46.6.8.14
Host is up (0.023s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap scan report for 202.red-2-137-212.dynamicip.rima-tde.net (2.137.212.202)
Host is up (0.030s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap scan report for 48.red-37-12-152.dynamicip.rima-tde.net (37.12.152.48)
Host is up (0.044s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap scan report for 64.red-2-137-39.dynamicip.rima-tde.net (2.137.39.64)
Host is up (0.028s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap scan report for 192.red-2-140-67.dynamicip.rima-tde.net (2.140.67.192)
Host is up (0.074s latency).

"output" 1292L, 31709C                                     1,1                               Top
```