CICLO FORMATIVO DE GRADO SUPERIOR - TÉCNICO EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN REDES

**Seguridad y Alta Disponibilidad**

NMAP

**Nombre y apellidos:**
**- Diego Pastrana Monzón**

## Análisis de redes con NMAP (Ubuntu)

Nmap es una herramienta de código abierto utilizada para analizar redes y realizar auditorías de seguridad. Gracias a sus capacidades y versatilidad, este software se ha convertido en un elemento básico en ciberseguridad y administración de sistemas. El conjunto de funciones de Nmap va más allá de la exploración básica de redes e incluye:

- Descubrimiento del host: Nmap identifica los hosts activos en una red, sentando las bases para una exploración más profunda.
- Exploración de puertos: Nmap descubre puertos y servicios abiertos, lo que permite a los administradores conocer la superficie de ataque de una red.
- Detección de versiones: Nmap puede identificar versiones de servicios y ayudar a localizar posibles vulnerabilidades asociadas a versiones específicas.
- Interacción programable: el NSE (Nmap Scripting Engine) de Nmap permite a los usuarios crear análisis a medida y automatizar tareas complejas.
- Huella digital del sistema operativo: las capacidades de detección de SO de Nmap permiten a los administradores identificar los sistemas operativos que se ejecutan en los hosts descubiertos, lo que ayuda con el inventario de la red y las evaluaciones de seguridad.

1. Preparar el entorno e instalar Nmap.

Para realizar esta práctica, vamos a necesitar una máquina virtual normal de Ubuntu y otra maquina virtual que provea un servicio por puerto (tu ordenador si usas XAMPP o la máquina virtual de las prácticas de docker, etc). Asegurate que están configuradas en adaptador puente para garantizar la conexión.

En la maquina sin servicios, vamos a instalar nmap con el siguiente comando:

```
root@iso:/home/ubuntu/Desktop# apt install nmap
```

**2.** Mapeo de red básico.

El primer paso en la exploración de la red es el descubrimiento de hosts, que revela los dispositivos activos en la red. Esto se hace mediante el siguiente comando:

```
root@iso:/home/ubuntu/Desktop# nmap <target>
```

En el comand, <target> tiene que sustituirse una dirección IP, un nombre de host o un rango de direcciones IP.

Prueba a mapear la red puente, puedes conseguir la dirección de esta en la configuración de red (ver anexo).

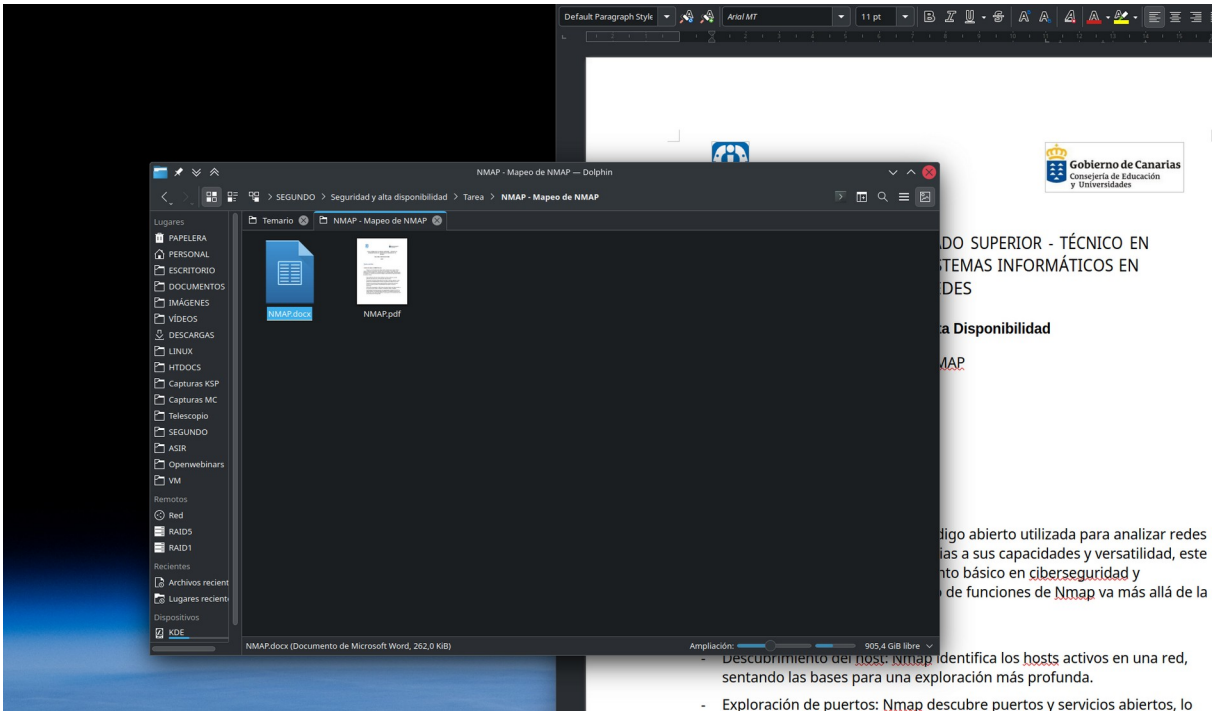
```
root@iso:/home/ubuntu/Desktop# nmap 192.168.1.0/24
```

Como has visto, el mapeo de la red es un proceso algo costoso al comprobar todas la ip's y todos los puertos, por lo que su uso para el seguimiento del estado de la red es relativo.

**3.** Mapeo con ping

Para comprobar que dispositivos se encuentran activos en la red, lo recomendable es usar un mapeo con ping. Básicamente implementa un bucle donde realiza un ping a cada ip, recogiendo la disponibilidad y latencia de los ordenadores conectados. El comando es nmap -sn <target>.

```
root@iso:/home/ubuntu/Desktop# nmap -sn 192.168.1.0/24
```


NMAP - Mapeo de NMAP — Dolphin
SEGUNDO
Seguridad y alta disponibilidad
Tarea
NMAP - Mapeo de NMAP
Temario
NMAP - Mapeo de NMAP
Lugares
PAPELERA
PERSONAL
ESCRITORIO
DOCUMENTOS
IMÁGENES
VÍDEOS
DESCARGAS
LINUX
HTDOCS
Capturas KSP
Capturas MC
Telescopio
SEGUNDO
ASIR
Openwebinars
VM
Remotos
Red
RAID5
RAID1
Recientes
Archivos recient
Lugares recient
Dispositivos
KDE
NMAP.docx
NMAP.pdf
NMAP.docx (Documento de Microsoft Word, 262,0 KiB)
Ampliación:
905,4 GiB libre
Default Paragraph Style
Arial MT
11 pt
Gobierno de Canarias
Consejería de Educación y Universidades
DO SUPERIOR - TÉCNICO EN
TEMAS INFORMÁTICOS EN
DES
a Disponibilidad
MAP
digo abierto utilizada para analizar redes
ias a sus capacidades y versatilidad, este
nto básico en ciberseguridad y
de funciones de Nmap va más allá de la
- Descubrimiento del host: Nmap identifica los hosts activos en una red, sentando las bases para una exploración más profunda.
- Exploración de puertos: Nmap descubre puertos y servicios abiertos, lo

4. Mapeo de puertos concretos.

   Otra opción muy utilizada es el mapeo de puertos, el cual permite limitar el mapeo a puertos concretos en la red. Vamos a probar con los puertos 80 y 443, puertos por defecto para httpd (asegúrate encendido el servicio de apache en otra máquina virtual o en XAMPP). Prueba a ejecutar el siguiente comando sustituyendo la ip:

```
root@iso:/home/ubuntu/Desktop# nmap -p 80,443 192.168.1.0/24
```

5. Detección de versiones

   Para revisar las versiones de los servicios que se encuentran el la red, podemos usar la opción -sV. Tener en cuenta que si no incluimos la opción -p, se aplicará la búsqueda a TODOS los puertos. Aquí hay un ejemplo:

```
root@iso:/home/ubuntu/Desktop# nmap -sV -p 80,443 192.168.1.0/24
PORT   STATE  SERVICE VERSION
80/tcp  open   http    lighttpd 1.4.34
443/tcp closed https
```

6. Huella digital del sistema

   Permite ver las versiones de los Sistemas Operativos que se ejecutan en cada ordenador de la red. Se ejecuta con la opción -O:

```
root@iso:/home/ubuntu/Desktop# nmap -O 192.168.1.37
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-21 14:20 GMT
Nmap scan report for 192.168.1.37
Host is up (0.00081s latency).
Not shown: 991 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1042/tcp open  afrog
1043/tcp open  boinc
3306/tcp open  mysql
7070/tcp open  realserver
MAC Address: 04:42:1A:E9:3C:48 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 (93%), Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 1703
(89%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows 10 1607 (87%), Microsoft Windows 10 1511 (87%), Mic
rosoft Windows Server 2008 R2 or Windows 8.1 (87%), Microsoft Windows Server 2016 (87%), Microsoft Windows Vista SP0 o
r SP1, Windows Server 2008 SP1, or Windows 7 (87%), Microsoft Windows 10 1511 - 1607 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

7. Explorar puertos TCP y UDP.

   También podemos investigar la revisando exclusivamente los puertos que usan un protocolo TCP o UDP.

   Para la exploración por TCP, se ejecuta el siguiente comando:

```
root@iso:/home/ubuntu/Desktop# nmap -sT 192.168.1.0/24
```

IMPORTANTE, cuando realicemos la exploración de puertos UDP, como el protocolo no utiliza una conexión, el proceso de búsqueda se puede demorar hasta 18 horas. Para realizar búsquedas rápidas, debemos usar la opción -F para limitarlo a los 100 principales puertos en vez de los 65635 que existen realmente.

```
root@iso:/home/ubuntu/Desktop# nmap -sU 192.168.1.0/24 -F
```

8. Escaneo SYN.

El escaneo SYN, un escaneo semiabierto o sigiloso, envía paquetes SYN a los puertos objetivo sin completar el protocolo de enlace y evalúa las respuestas para determinar la apertura del puerto sin conectarse completamente. Esta técnica es más rápida que el escaneo de conexión TCP y es menos probable que se detecte. Aquí tienes un ejemplo de un escaneo SYN:

```
root@iso:/home/ubuntu/Desktop# nmap -sS 192.168.1.0/24
```

9. Scripts de auditoría.

Todos estos comandos permiten comenzar con una auditoría de seguridad al listar todos los puertos abiertos, servicios y sistemas operativos en uso en tu red. Esta auditoría de seguridad te indicará los posibles puntos de entrada de agentes maliciosos. Aun así, puedes encontrar aún más información sobre el estado de tu red a través de Nmap Scripting Engine (NSE).

NSE incluye un conjunto de scripts que te ayudarán a encontrar vulnerabilidades en tus sistemas. La lista actual de scripts NSE tiene 604 entradas que puedes consultar https://nmap.org/nsedoc/scripts/. La mayoría de ellos están preinstalados en Nmap.

Para nuestro ejemplo, utilizaremos el script vulners, que utiliza la base de datos de vulnerabilidades Vulners. Este script depende de tener información sobre las versiones de software, por lo que debes utilizar el indicador -sV con él.

```
root@iso:/home/ubuntu/Desktop# nmap -sV --script vulners 192.168.1.37
```

# Anexo:

- Obtener la red en la que nos encontramos (Ubuntu).

  Si desconoces o no te acuerdas de como esta configurada la red, puedes usar el comando ifconfig en la terminal para ver las interfaces de red y contrastarlas con la que te aparece en la configuración.

```
root@iso:/home/ubuntu/Desktop# ifconfig
```