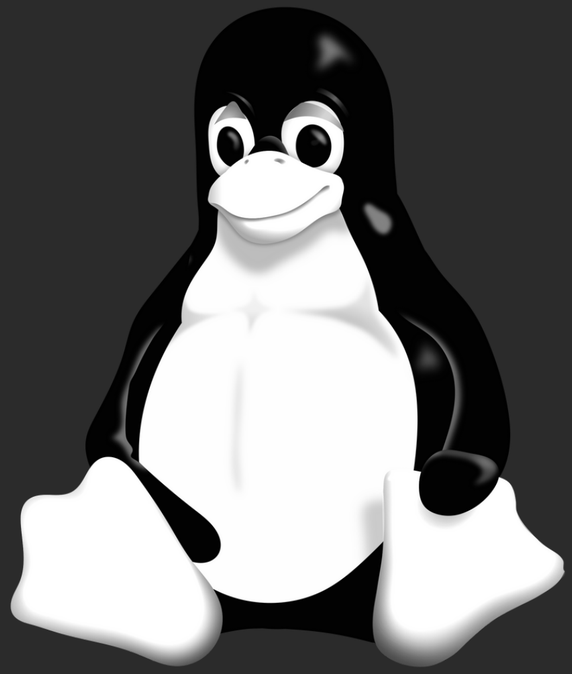
COMANDOS BASICOS DE LINUX



COMANDOS BASICOS DE LINUX

#1

ls:
Se utiliza para listar los contenidos de un directorio

#2

***cd**: Se utiliza para cambiar de directorio. Por ejemplo, "cd Documents" te llevará al directorio llamado "Documents" dentro del directorio actual.*

#3

***pwd**: Muestra el directorio actual en el que te encuentras trabajando.*

#4

***mkdir**: Crea un nuevo directorio. Por ejemplo, "mkdir new_directory" creará un directorio llamado "new_directory" dentro del directorio actual.*

#5

rm: Elimina archivos o directorios. Por ejemplo, "rm file.txt" eliminará el archivo llamado "fil

#6

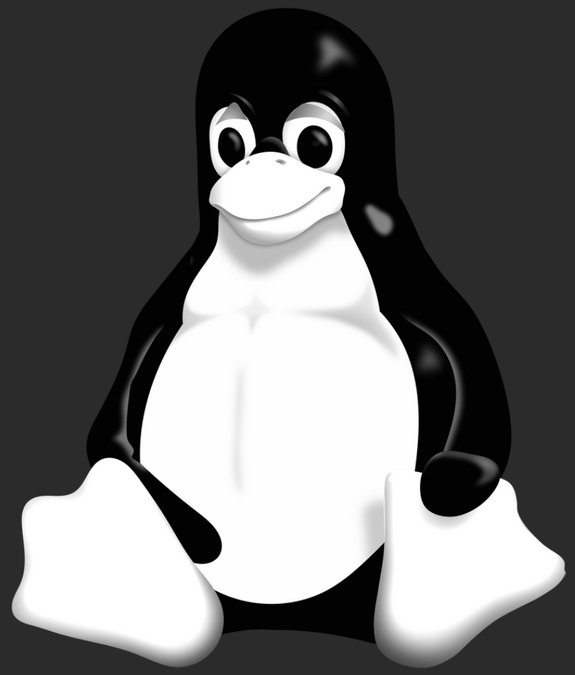
***cp**: Copia archivos o directorios. Por ejemplo, "cp file1.txt file2.txt" copiará "file1.txt" y lo nombrará como "file2.txt".*

#7

***mv**: Mueve o renombra archivos o directorios. Por ejemplo, "mv file.txt new_location/" moverá el archivo "file.txt" al directorio "new_location/".*

#8

***cat**: Muestra el contenido de un archivo en la salida estándar. Por ejemplo, "cat file.txt" mostrará el contenido del archivo "file.txt" en la terminal.*



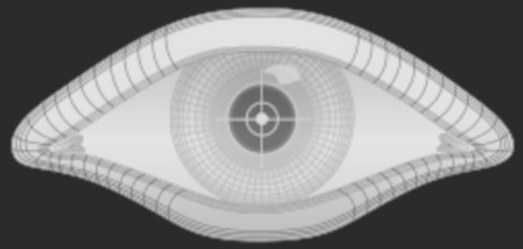
CONCEPTOS DE REDES

***Dirección IP**: Es un identificador numérico único asignado a cada dispositivo conectado a una red que utiliza el protocolo de Internet para la comunicación. Pueden ser direcciones IPv4 (por ejemplo, 192.168.1.1) o direcciones IPv6 (por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).*

***Puerto**: Es un número de 16 bits utilizado para identificar una aplicación específica en un dispositivo de red. Los puertos se utilizan para dirigir el tráfico entrante a una aplicación específica en un dispositivo.*

***Firewall**: Es una barrera de seguridad que controla y monitorea el tráfico de red entrante y saliente en función de un conjunto de reglas. Puede ser utilizado para proteger una red y sus dispositivos de intrusiones maliciosas.*

***La dirección MAC (Media Access Control)** es un identificador único asignado a cada dispositivo de red. Se compone de 48 bits y se utiliza para identificar de manera única un dispositivo en una red local. Es independiente de la dirección IP y se utiliza en la capa de enlace de datos para dirigir el tráfico de red en una red local.*



COMANDOS BÁSICOS DE NMAP

NMAP

#6

Escaneo de Red Completa (-sn)

- Comando: **nmap -sn <objetivo/rango de red>**
- Propósito: Este escaneo realiza una exploración de hosts activos en una red sin realizar un escaneo de puertos. Es útil para identificar qué dispositivos están presentes y responden en la red.

#1

Escaneo de Puertos TCP (-sS)

- *Comando: **nmap -sS <objetivo>***
- *Propósito: Este es uno de los escaneos más comunes. Utiliza un escaneo de tipo SYN para determinar qué puertos están abiertos en el objetivo. Es rápido y menos intrusivo, ya que no establece completamente una conexión.*

#5

Escaneo Agresivo (-A)

- Comando: **nmap -A <objetivo>**
- Propósito: Este escaneo combina varias técnicas, incluyendo detección de sistema operativo, detección de versiones de servicios, detección de scripts y más. Proporciona una visión integral del objetivo.

#2

Escaneo de Puertos UDP (-sU)

- *Comando: **nmap -sU <objetivo>***
- *Propósito: Mientras que el escaneo TCP se centra en los puertos TCP, el escaneo UDP se utiliza para descubrir servicios que utilizan el protocolo UDP. Algunos servicios importantes, como el DNS y el DHCP, utilizan UDP.*

#4

Escaneo de Sistema Operativo (-O)

- Comando: **nmap -O <objetivo>**
- Propósito: Intenta identificar el sistema operativo del objetivo basándose en patrones de respuesta a través de las sondas enviadas. Proporciona información sobre la infraestructura de la red.

#3

Escaneo de Enumeración de Versiones (-sV)

- *Comando: **nmap -sV <objetivo>***
- *Propósito: Este escaneo busca determinar las versiones y los detalles de los servicios que se están ejecutando en los puertos abiertos. Proporciona información valiosa sobre posibles vulnerabilidades asociadas con versiones específicas de software.*

NMAP

#7

Escaneo de Puertos Específicos (-p)

- *Comando:* ***nmap -p puerto,<objetivo>***
- *Propósito: Este comando escanea únicamente los puertos específicos 80 y 443 en el host con la dirección IP 192.168.1.1.*

#8

Escaneo de Intensidad Moderada (-T3)

- *Comando:* ***nmap -T3 192.168.1.1***
- *Propósito: Este comando realiza un escaneo de intensidad moderada en el host con la dirección IP 192.168.1.1. La opción -T3 ajusta la velocidad de escaneo para equilibrar la velocidad con la intrusión.*

#9

Escaneo de Intensidad Agresiva (-T4)

- *Comando:* ***nmap -T4 192.168.1.1***
- *Propósito: Este comando realiza un escaneo de intensidad agresiva en el host con la dirección IP 192.168.1.1. La opción -T4 aumenta la velocidad de escaneo y la intrusión.*

#10

Escaneo de Intensidad Insana (-T5)

- *Comando:* ***nmap -T5 192.168.1.1***
- *Propósito: Este comando realiza un escaneo de intensidad máxima (insana) en el host con la dirección IP 192.168.1.1. La opción -T5 aumenta la velocidad al máximo, pero puede ser más intrusiva y llamar la atención.*

ESCANEO DE VULNERABILIDADES CON NMAP

Escaneo de Vulnerabilidades Básico (-sV --script vuln)

- *Comando:* ***nmap -sV --script vuln <objetivo>***
- *Propósito: Este comando realiza un escaneo de vulnerabilidades básico utilizando scripts de detección de vulnerabilidades disponibles en la base de datos de scripts de Nmap. Identifica posibles vulnerabilidades en los servicios en ejecución en el objetivo.*


```
root@kali:~# nmap --script  vuln -p139,445 192.168.0.18
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-25 20:58 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.18
Host is up (0.0017s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 39.49 seconds
root@kali:~#
```

COMANDOS BASICOS DE NMAP GITHUB