Impartido por:
Joshua Aviles y Brian Guzman

TALLE DE INTRODUCCION AL

ETHICAL HACKING

Este curso tiene como objetivo proporcionar las bases esenciales para iniciar en el mundo del hacking y fomentar el deseo de aprendizaje continuo en este enorme campo.

¿Qué es el hacking ético?

El hacking ético es la práctica de buscar y resolver vulnerabilidades en sistemas informáticos, redes y aplicaciones, siempre con el permiso explícito del propietario

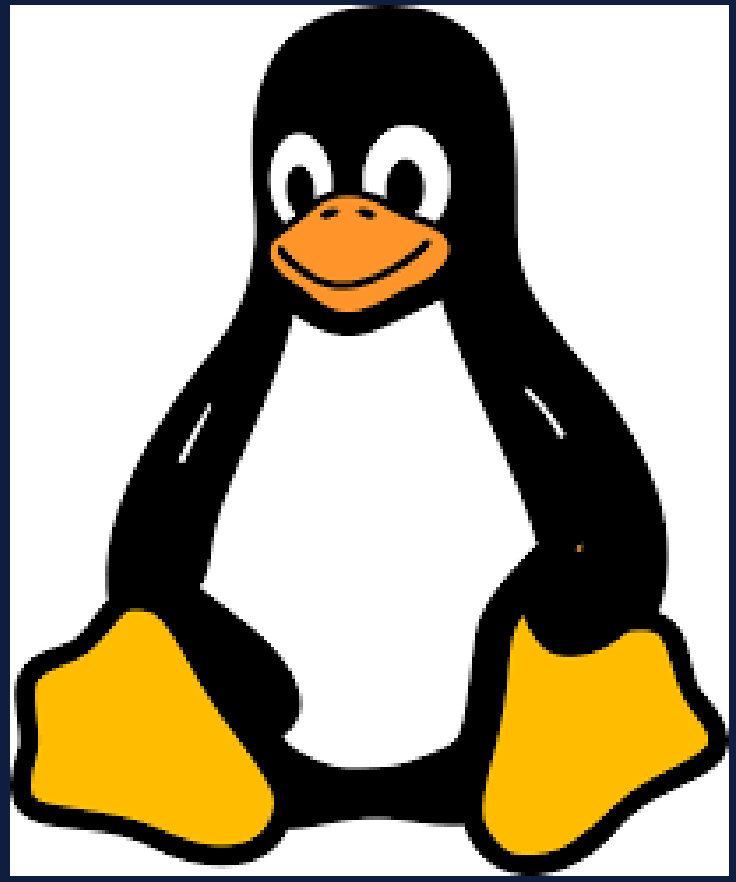
Instalación de nuestro laboratorio

Ahora procederemos a instalar nuestro laboratorio, para eso les dejo el siguiente codigo QR para entrar a mi servidor de discord y que puedan descargar los materiales

Si no pudiste hacer la instalación no te preocupes, puedes seguir este pequeño video y completarla en casa.

COMANDOS BASICOS DE LINUX

Aprender estos comandos será esencial para lo que se viene



whoami

```
❯ whoami
briancgx
```

sudo

```
❯ sudo su
[sudo] password for briancgx:
❯ whoami
root
```

pwd

```
❯ pwd
/home/briancgx/Documents/cursoHacking
```

ls / ls -l / ls -la

```
❯ ls
carpetaVisible  archivo.txt
❯ ls -l
drwxr-xr-x root root 0 B Sun Oct 15 15:05:58 2023 carpetaVisible
.rw-r--r-- root root 0 B Sun Oct 15 15:06:07 2023 archivo.txt
❯ ls -la
drwxr-xr-x root     root      78 B Sun Oct 15 15:06:07 2023 .
drwxr-xr-x briancgx briancgx 144 B Sun Oct 15 15:04:54 2023 ..
drwxr-xr-x root     root       0 B Sun Oct 15 15:05:47 2023 .carpetaOculta
drwxr-xr-x root     root       0 B Sun Oct 15 15:05:58 2023 carpetaVisible
.rw-r--r-- root     root       0 B Sun Oct 15 15:06:07 2023 archivo.txt
```

cd

```
❯ cd carpetaVisible
❯ pwd
/home/briancgx/Documents/cursoHacking/carpetaVisible
```

cat

```
❯ cat test.txt
   File: test.txt
1  Este es un archivo de prueba para el curso de Hacking Ético
```

cp

```
❯ cp test.txt /home/briancgx/Desktop/prueba
```

```
❯ pwd
/home/briancgx/Desktop/prueba
❯ ls -l
.rw-r--r-- root root 61 B Sun Oct 15 15:28:26 2023 test.txt
```

mv

```
❯ mv test.txt nuevoNombre.txt
❯ ls
nuevoNombre.txt
❯ mv nuevoNombre.txt /home/briancgx/Desktop/prueba
```

```
❯ pwd
/home/briancgx/Desktop/prueba
❯ ls
nuevoNombre.txt  test.txt
```

mkdir

```
❯ mkdir Carpeta
❯ ls
Carpeta
```

touch

```
❯ touch Archivo.txt
❯ ls
Archivo.txt
```

rm / rm -r

```
❯ ls
Carpeta  Archivo.txt
❯ rm Archivo.txt
❯ ls
Carpeta
❯ rm -r Carpeta
❯ ls
```

chmod

```
❯ chmod 777 archivo.txt
❯ ls -l
.rwxrwxrwx root root 0 B Sun Oct 15 15:06:07 2023 archivo.txt
```

chown

```
❯ ls -l
.rwxr-xr-x root root 5 B Sun Oct 15 16:54:09 2023 archivo.txt
❯ chown briancgx:briancgx archivo.txt
❯ ls -l
.rwxr-xr-x briancgx briancgx 5 B Sun Oct 15 16:54:09 2023 archivo.txt
```

ping

```
❯ ping google.com
PING google.com (142.250.177.14) 56(84) bytes of data.
64 bytes from atl14s08-in-f14.1e100.net (142.250.177.14): icmp_seq=1 ttl=117 time=73.2 ms
64 bytes from atl14s08-in-f14.1e100.net (142.250.177.14): icmp_seq=2 ttl=117 time=44.4 ms
64 bytes from atl14s08-in-f14.1e100.net (142.250.177.14): icmp_seq=3 ttl=117 time=67.3 ms
```

wget

```
❯ wget https://ceur-ws.org/Vol-2993/paper-07.pdf
--2023-10-15 17:44:24--  https://ceur-ws.org/Vol-2993/paper-07.pdf
Resolving ceur-ws.org (ceur-ws.org)... 137.226.34.231
Connecting to ceur-ws.org (ceur-ws.org)|137.226.34.231|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 967099 (944K) [application/pdf]
Saving to: ‘paper-07.pdf’

paper-07.pdf          100%[=====================>] 944.43K   972KB/s    in 1.0s

2023-10-15 17:44:26 (972 KB/s) - ‘paper-07.pdf’ saved [967099/967099]

❯ ls
archivo.txt  paper-07.pdf
```

apt install

```
~/Documents/cursoHacking took 40s ✔ sudo apt install nano
package
```

apt [upgrade / update]

```
~/Documents/cursoHacking took 40s ✔ sudo apt update
action
```

```
~/Documents/cursoHacking took 40s ✔ sudo apt upgrade
action
```

ip addr show

```
❯ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:64:4f:4e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.80/24 brd 192.168.1.255 scope global dynamic noprefixroute ens33
       valid_lft 86350sec preferred_lft 86350sec
    inet6 fe80::7778:5d3d:98e2:44dc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

nano

```
~/Documents/cursoHacking ✔ nano test.txt
```

echo

```
❯ echo 'Hola, esto es una prueba'
Hola, esto es una prueba
```

man

```
~/Documents/cursoHacking took 3s ✔ man nmap
```

```
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against
       single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are
       offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is
       commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules,
       and monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports
       table".  That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered.  Open means that an application
       on the target machine is listening for connections/packets on that port.  Filtered means that a firewall, filter, or other network obstacle is blocking the port so that
       Nmap cannot tell whether it is open or closed.  Closed ports have no application listening on them, though they could open up at any time. Ports are classified as
       unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and
       closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been
       requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC
       addresses.

       A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for
       faster execution; and then the hostname.

       Example 1. A representative Nmap scan

           # nmap -A -T4 scanme.nmap.org

           Nmap scan report for scanme.nmap.org (74.207.244.221)
           Host is up (0.029s latency).
           rDNS record for 74.207.244.221: li86-221.members.linode.com
           Not shown: 995 closed ports
           PORT     STATE    SERVICE     VERSION
           22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
           | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
           |_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
           80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
           |_http-title: Go ahead and ScanMe!
           646/tcp  filtered ldp
           1720/tcp filtered H.323/Q.931
           9929/tcp open     nping-echo  Nping echo
           Device type: general purpose
           Running: Linux 2.6.X
           OS CPE: cpe:/o:linux:linux_kernel:2.6.39
Manual page nmap(1) line 1 (press h for help or q to quit)
```

nano

```
~/Documents/cursoHacking ✔ nano test.txt
```

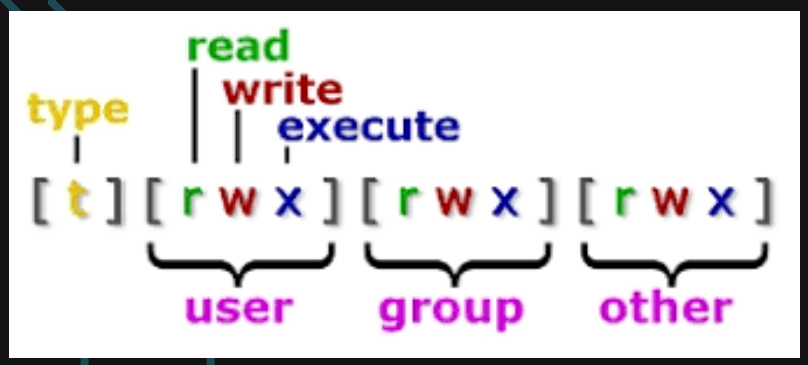
echo

```
❯ echo 'Hola, esto es una prueba'
Hola, esto es una prueba
```

man

```
~/Documents/cursoHacking took 3s ✔ man nmap
```

Permisos en archivos



Tradicional

```
❯ chmod a+rwx archivo.txt
❯ ls -l
.rwxrwxrwx root root 5 B Sun Oct 15 16:54:09 2023 archivo.txt
```

```
❯ chmod a-rwx archivo.txt
❯ ls -l
.--------- root root 5 B Sun Oct 15 16:54:09 2023 archivo.txt
```

```
❯ chmod u+rwx archivo.txt
❯ ls -l
.rwx------ root root 5 B Sun Oct 15 16:54:09 2023 archivo.txt
```

```
❯ chmod go+rx archivo.txt
❯ ls -l
.rwxr-xr-x root root 5 B Sun Oct 15 16:54:09 2023 archivo.txt
```

Notación Octal

Owner	Group	Other
rwx	r-x	r-x
4+2+1	4+0+1	4+0+1
7	5	5

```
❯ chmod 777 archivo.txt
❯ ls -l
.rwxrwxrwx root root 0 B Sun Oct 15 15:06:07 2023 archivo.txt
```

```
❯ chmod 000 archivo.txt
❯ ls -l
.--------- root root 5 B Sun Oct 15 16:54:09 2023 archivo.txt
```

```
❯ chmod 760 archivo.txt
❯ ls -l
.rwxrw---- root root 0 B Sun Oct 15 15:06:07 2023 archivo.txt
```

```
❯ chmod 774 archivo.txt
❯ ls -l
.rwxrwxr-- root root 0 B Sun Oct 15 15:06:07 2023 archivo.txt
```