


Laboratorio Hacking – Clase gratuita



❖ **Descargue la imagen de metasploitable**

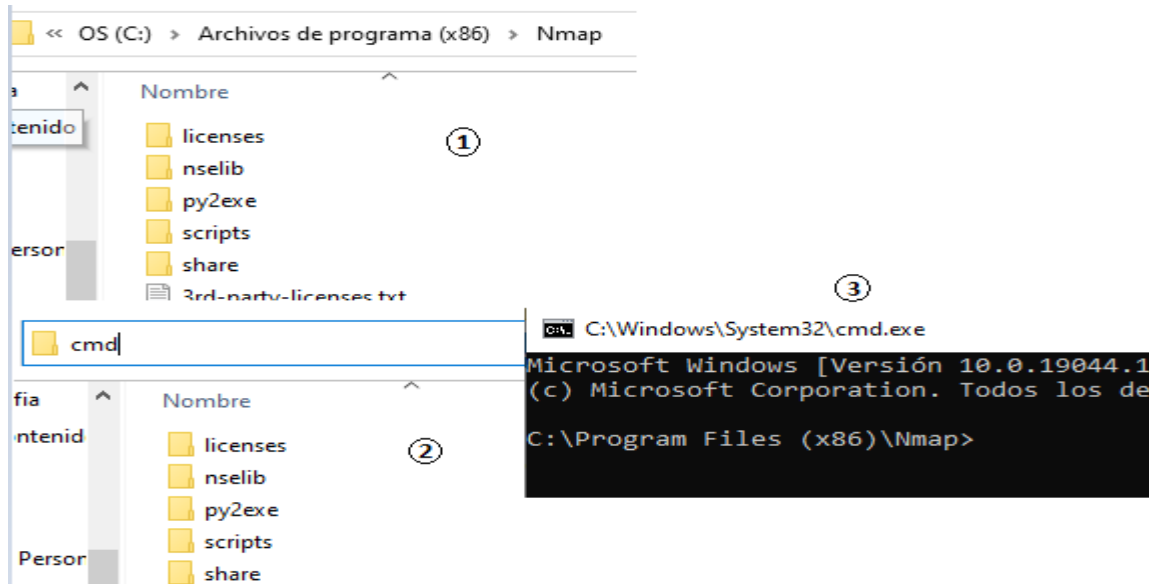
<https://sourceforge.net/projects/metasploitable/>

Se descargará un archivo .zip

 metasploitable-linux-2.0.0.zip

Descomprímalo y a continuación seleccione y ejecute el archivo llamado **Metasplotaible.vmx**, este es el archivo de configuración de la maquina virtual y le permitirá importarla en una herramienta como vmware o virtualbox.

Nombre	Tamaño	Comprimido	Tipo
..			Carpeta de archivos
Metasploitable.vmx	269	184	VMware Team Member
Metasploitable.vmx	2.804	1.072	VMware virtual machine configuration
Metasploitable.vmsd	0	0	VMware snapshot metadata
Metasploitable.vmdk	1.925.644.288	865.080.549	Virtual Machine Disk Format
Metasploitable.nvram	8.684	1.847	VMware Virtual Machine nonvolatile RAM



Otra opción es abrir la consola de comandos cmd y luego ingresar el siguiente comando para ir al directorio de instalación de Nmap:

cd C:\Program Files (x86)\Nmap

```
C:\Program Files (x86)>cd C:\Program Files (x86)\Nmap\
C:\Program Files (x86)\Nmap>
```

❖ Para descargar Wireshark visite el siguiente sitio (seleccione su sistema operativo)

<https://www.wireshark.org/download.html>

❖ Sitio web Exploit DB

<https://www.exploit-db.com/>

❖ Algunos comandos de interés para el uso de Metasploit en Kali Linux

msfconfig → Abrir la consola

usr/share/metasploit-framework/modules/exploits → Ruta ubicación de exploits

search exploit → Buscar un exploit por palabra clave

use exploit/ruta_exploit → seleccionar un exploit a utilizar

show options → Desplegar las opciones de configuración del exploit y payload

set RHOSTS → Configurar la dirección IP del host de destino (víctima)

set RPORT → Configurar el puerto de destino de la comunicación hacia la víctima

exploit → ejecutar el exploit