

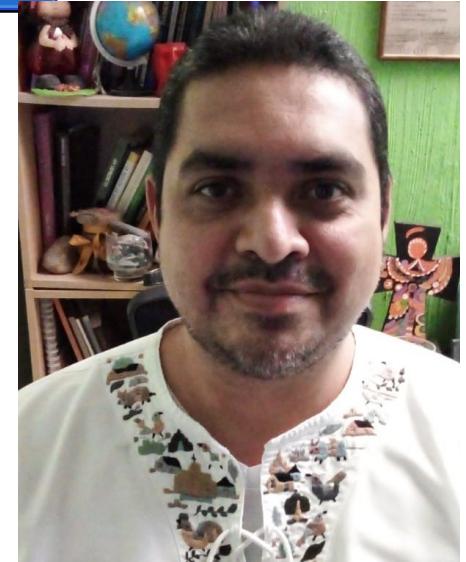
Escalamiento de Privilegios en la maquina virtual Kkoptrix Level 1

**Herbert Fernández Tamayo
El Salvador, Centro America**

Noviembre 2020

whoami

- @heftamayo
- <https://www.linkedin.com/in/herbert-eduardo-fernandez-tamayo-51522968/>
- Ingeniero en Sistemas y Computación
- Desarrollador Web
- Consultor Freelancer en Tecnologías de Información
- Facilitador para distintas universidades en El Salvador
- Becario del nanodegree sobre Machine Learning Engineer con Microsoft Azure (Microsoft - Udacity, 2020)
- Infosec enthusiast



Objetivo del Taller

- Obtener permisos de administración en una máquina intencionalmente vulnerable siguiendo las fases de la metodología de hacking ético

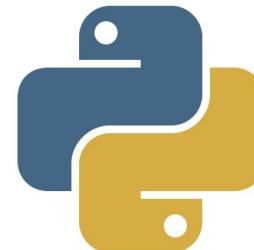
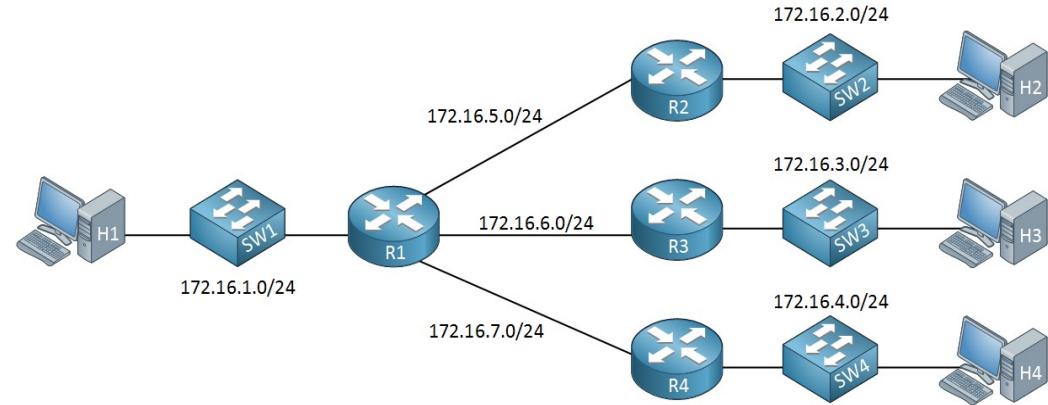
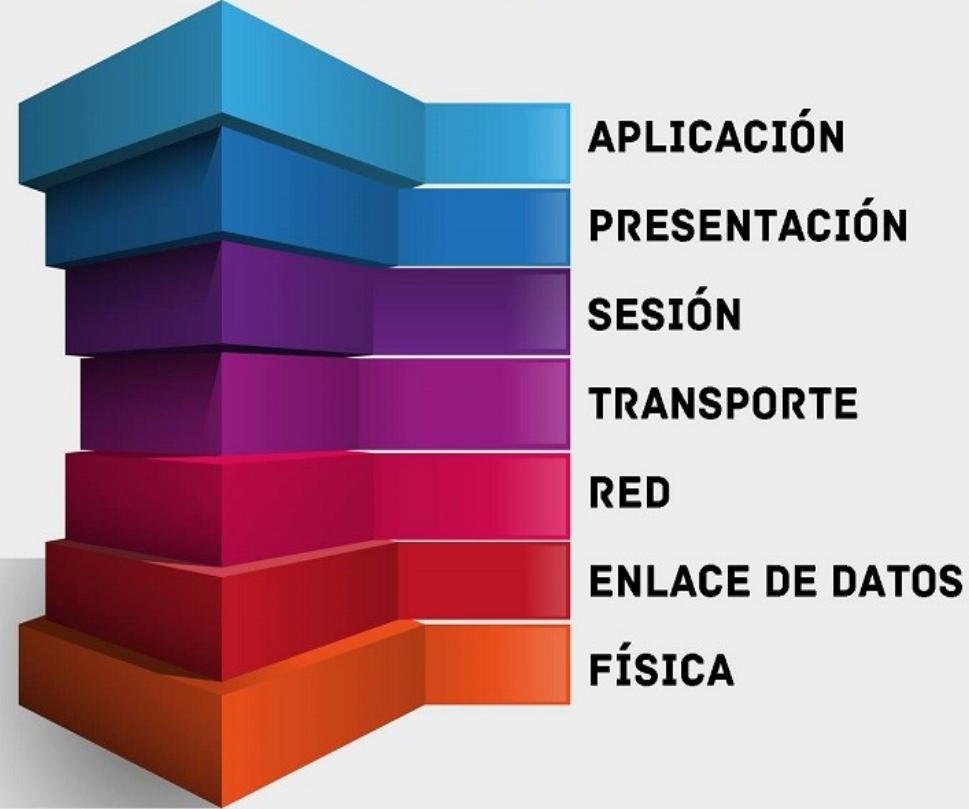
MARCO TEORICO

Marco Teórico?



Conceptos importantes

MODELO OSI



python

Hacking Etico

- “The hacker ethic is a philosophy and set of moral values that is common within hacker culture. Practitioners of the hacker ethic believe that sharing information and data with others is an ethical imperative. The hacker ethic is related to the concept of freedom of information, as well as the political theories of liberalism, anarchism, and libertarianism.”

https://en.wikipedia.org/wiki/Hacker_ethical



Penetration test

- “A penetration test, colloquially known as a pen test, pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.[1][2] Not to be confused with a vulnerability assessment.[3] The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data,[4][5] as well as strengths,[6] enabling a full risk assessment to be completed.”

https://en.wikipedia.org/wiki/Penetration_test



1. ESTABLECIMIENTO DEL ENTORNO DE TRABAJO

Pre-requisitos mínimos para el taller

- Equipo de computo con 4 GB RAM, procesador a 64 bits con una velocidad de 2 Ghz y al menos 50 GB de espacio libre en Disco Duro
- Soporte para virtualización
- Kali Linux versión 2019 en adelante
- Vmware Player versión 13 en adelante
- Kioptix Level 1

A. Kali Linux

- Distribución basada en Ubuntu diseñada para ejecución de pruebas de penetración (pentesting) y hacking ético (ethical hacking)
- www.kali.org/downloads

Cómo seleccionar la descarga de Kali Linux

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.4	4.1G	50492d761e400c2b5e22c8f253dd6f75c27e4bc84e33c2eff272476a0588fb02
Kali Linux 64-Bit (Live)	Torrent	2020.4	3.3G	4d764a2ba67f41495c17247184d24b7f9ac9a7c57415bbbed663402aec78952b
Kali Linux 64-Bit (NetInstaller)	Torrent	2020.4	471M	fbbb3b86567892f91b8298be7c03e9be8c78c6f048e4c6fff539948743465d79
Kali Linux 32-Bit (Installer)	Torrent	2020.4	3.4G	39aa231bc209e19a2fd91c145f23a8dde70a4bc540877a77e56b1c7a733337fd

B. KIOPTRIX

- Maquina virtual basada en Vmware. Es intencionalmente vulnerable para realizar prácticas de pentesting y ethical hacking
- El proyecto esta a cargo de la compañía vulnhub con el objetivo de facilitar una serie de maquinas virtuales para todos los interesados en desarrollar habilidades en tecnologías de información orientadas a infosec

ABOUT VULNHUB

Aim/Goal

To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration.

Descargar Kioptrix L1

- <https://www.vulnhub.com/entry/kioptrix-level-1-1,22/>

Download

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you download!

Kioptrix_Level_1.rar (Size: 186 MB)

Download: http://www.kioptrix.com/dlvm/Kioptrix_Level_1.rar

Download (Mirror): https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar

Download (Torrent): https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar.torrent ( Magnet)

C. Puesta a punto del equipo de computo



- Redimensionar disco duro: <https://youtu.be/OdyITD5i7n0>
- Extender una distro Linux en USB:
<https://youtu.be/LWpJw6bG6go>
- Cambiar parámetros en el UEFI: <https://youtu.be/jkmhpGiSGf4>
- Otros aspectos relacionados a instalación y post-instalación:
https://www.youtube.com/playlist?list=PLsQR_Tmsj29nQoH22uirqcNsAzoIMe19G

D. Instalación de vmware en Kali 2020



Dudas durante el proceso: envíame un DM a [@heftamayo](https://twitter.com/heftamayo)

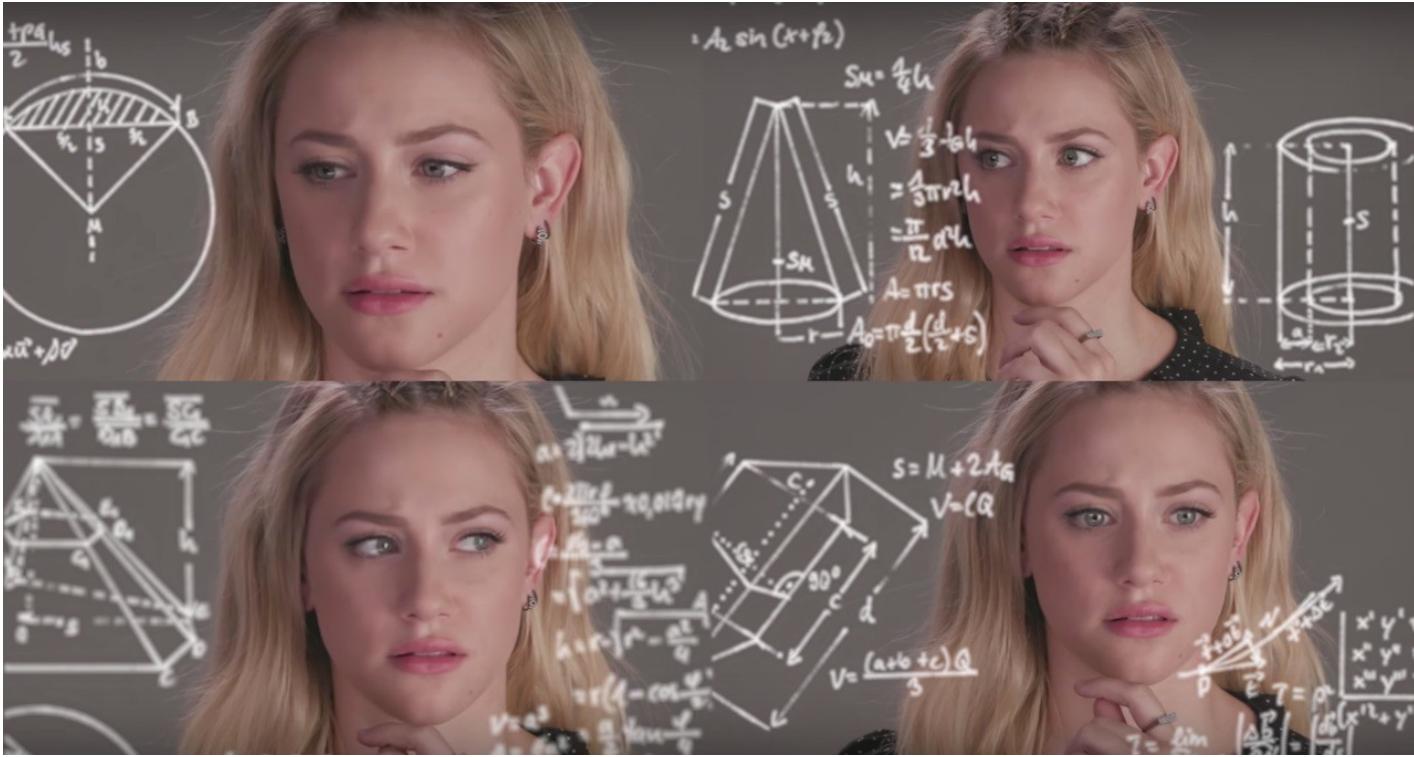
E. Montar una S.O. en Vmware



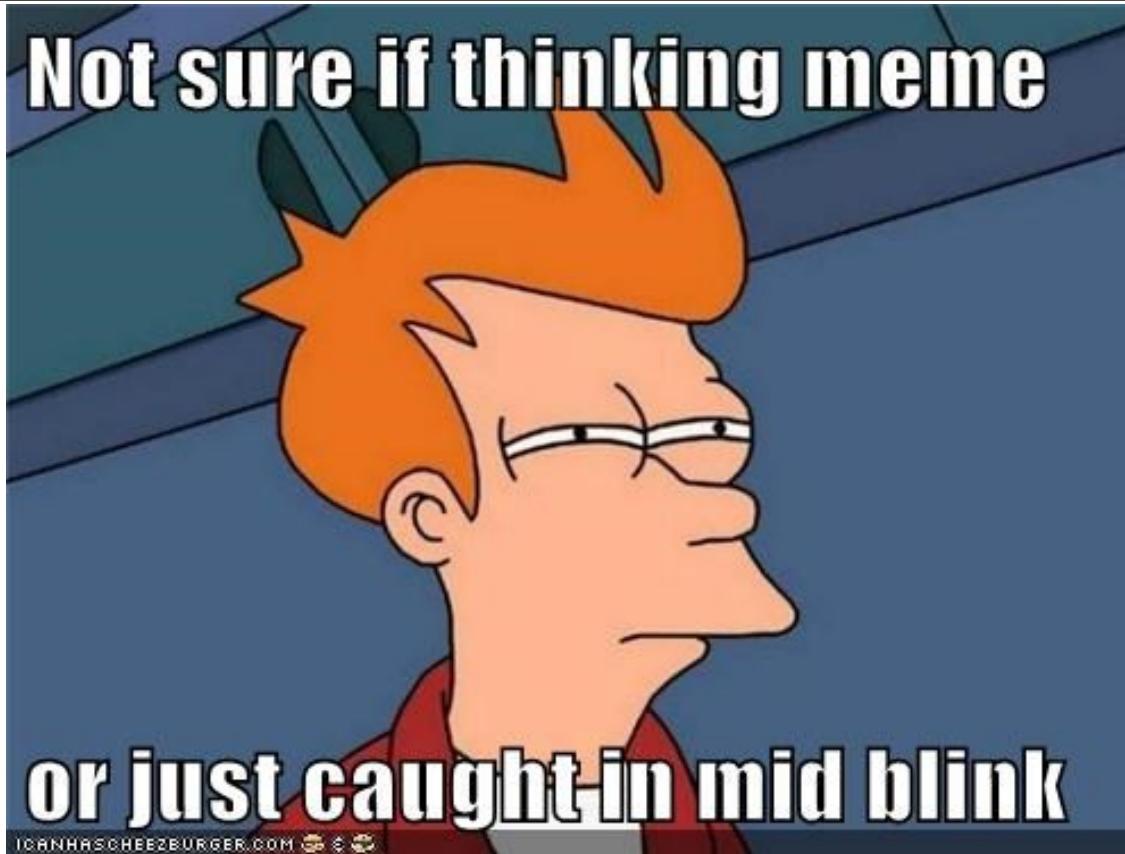
- Montar una imagen de Ubuntu en Vmware:
https://youtu.be/B4Vtj6Y_rfE
- Montar Kali Linux L1 en Vmware:
<https://youtu.be/NxeBxMHJBgl>

F. El resultado esperado

- Demo

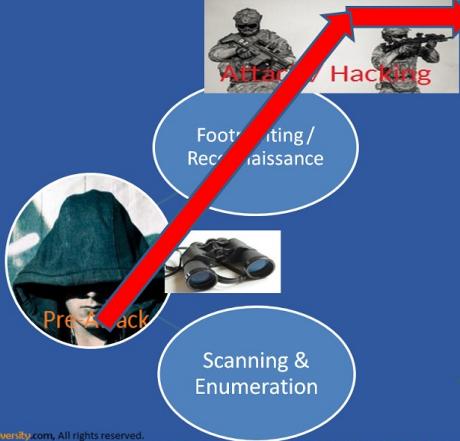


F. El resultado esperado?



2. METODOLOGÍA DE HACKING ETICO

Hacking Methodology



© 2018 CBTUniversity.com, All rights reserved.



How to Conduct Ethical Hacking

Step 1: Talk to your client on the needs of testing



Step 2: Prepare NDA documents and ask the client to sign them



Step 3: Prepare an ethical hacking team and draw up schedule for testing



Step 4: Conduct the test



Step 5: Analyze the results and prepare a report



Step 6: Deliver the report to the client

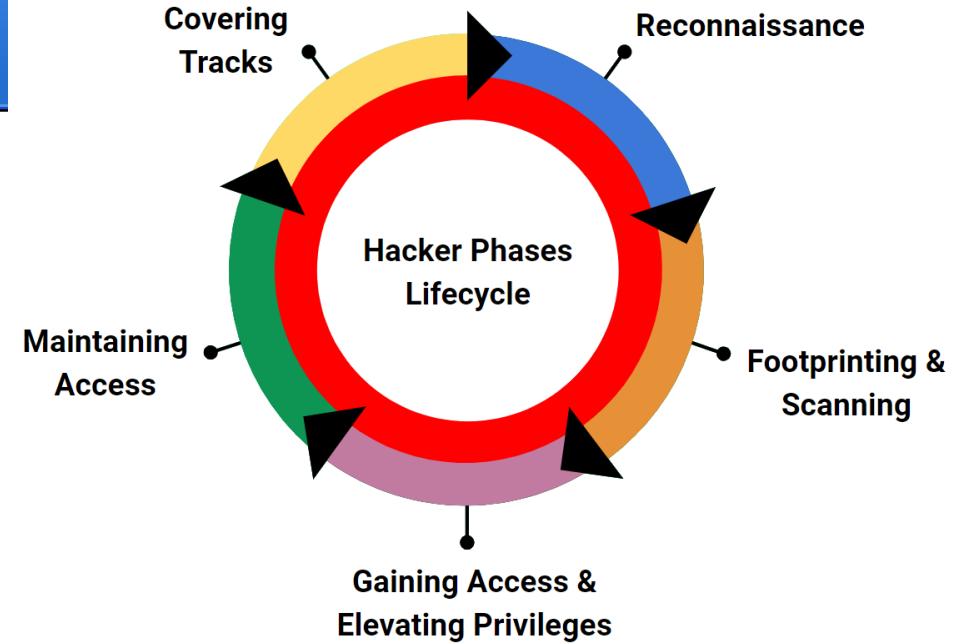


Note: In-depth Penetration Testing methodology is covered in EC-Council's LPT program

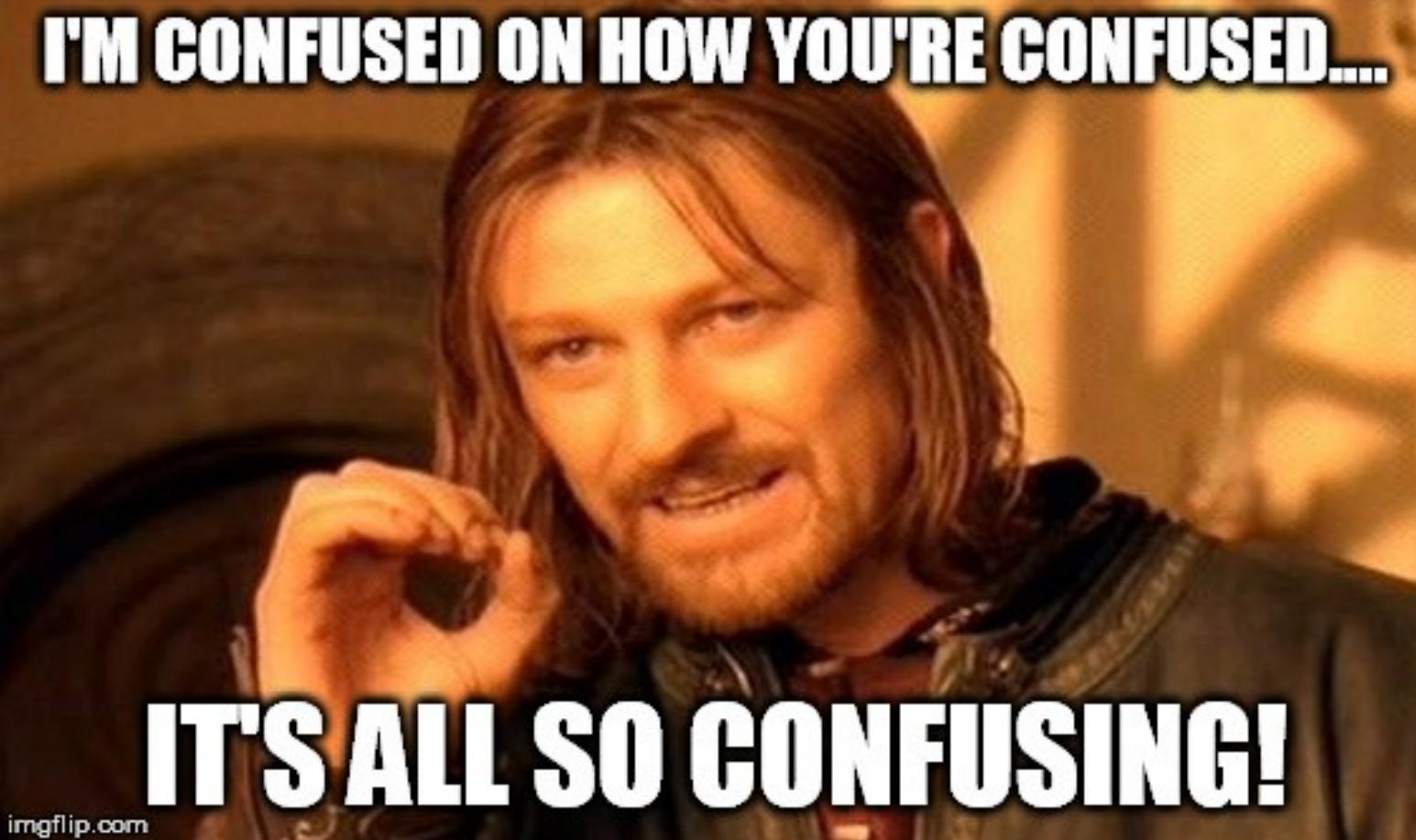
EC-Council

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

SEMANA
GLOBAL
UTH
II EDICIÓN 2020



I'M CONFUSED ON HOW YOU'RE CONFUSED....



IT'S ALL SO CONFUSING!

Metodología genérica



3. METODOLOGÍA DE ETHICAL HACKING: RECONOCIMIENTO (RECON)

Reconocimiento Pasivo

- DEMO
- Información de direcciones de correo electrónico (**hunter.io**)
- Identificación de tecnología utilizada en sitio web (**wappalyzer**)
- Identificación de dominios (**theHarvester**)
- Google Fu
- Redes Sociales

Por hacer

- Fingerprinting: Sublister, crt.sh, breachparser, whatweb
- Hunting subdomain: Amass
- Más ejercicios con Google Fu
- OSINT con redes sociales
- Reconocimiento activo *

4. METODOLOGÍA DE ETHICAL HACKING: Escaneo y enumeración

- DEMO: Escaneo
 - Cargar Kroptrix L1
 - Scanning y ubicación de la IP
 - Escanear puertos y servicios con nmap

```
root@asusmk11:~# nmap -p -A 192.168.1.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 09:55 CDT
Nmap scan report for 192.168.1.104
Host is up (0.00069s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
|_ssl-date: 2020-05-11T14:59:04+00:00; +1m53s from scanner time.
|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2 DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2 DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|_SSL268/tcp open  status      1 (RPC #100024)
```



- DEMO: Enumeración
 - Information disclosure
 - Escaneo de vulnerabilidades con nikto
 - Enumeración de directorios con dirbuster

- DEMO: Enumeración
 - Enumerar servicios con el protocolo SMB
 - Enumerar SSH

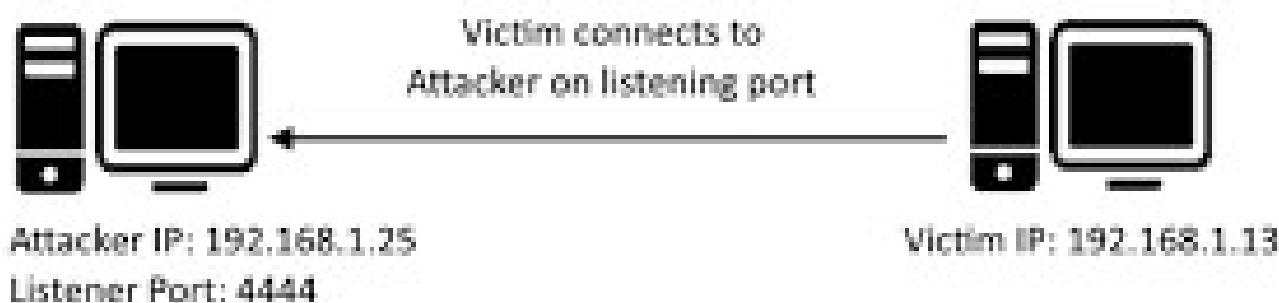
Por hacer

- Enumeración con Burp Suite
- Enumeración con Nessus
- Investigación de vulnerabilidades

5. METODOLOGÍA DE ETHICAL HACKING: Explotación

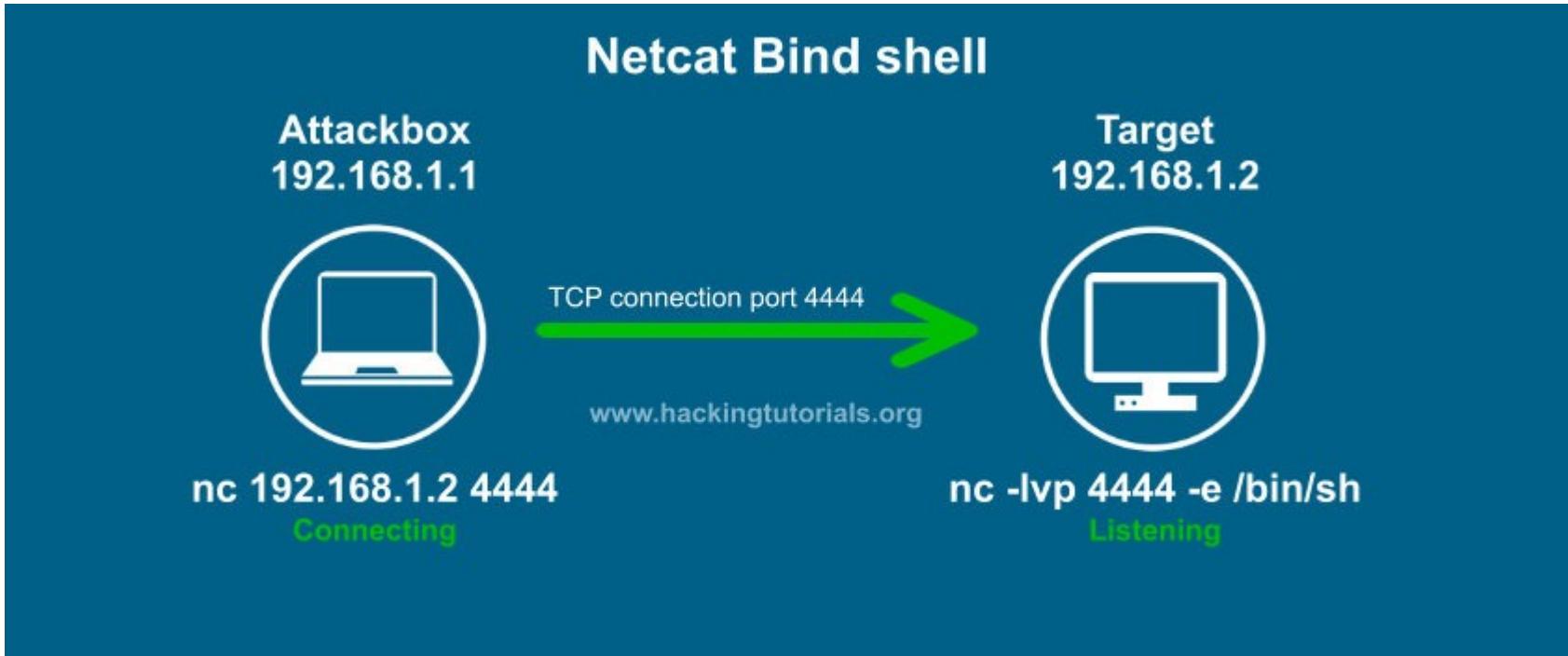
a) shells

- Garantizar el acceso a un equipo, idealmente, de manera permanente
- Reverse shell: el equipo comprometido abre una conexión hacia el equipo del especialista en seguridad



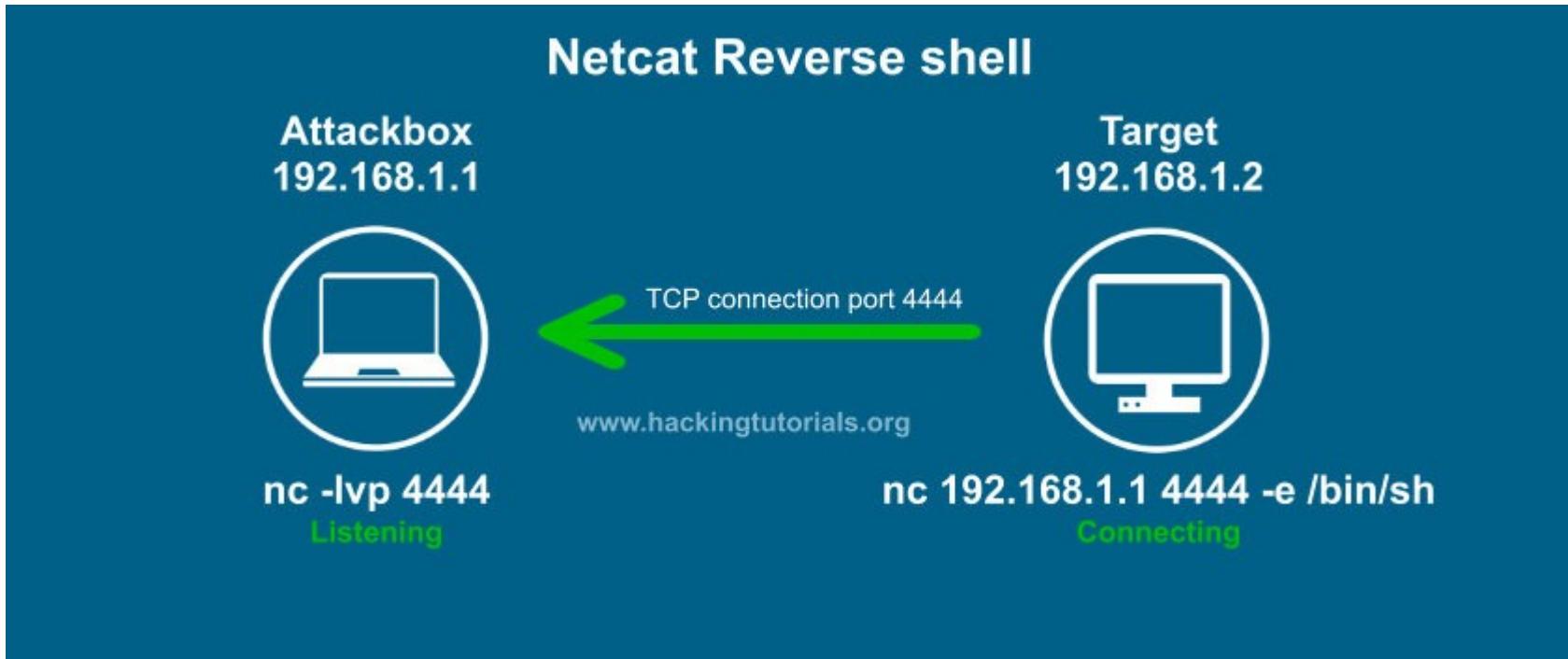
netcat

- Utilería para leer conexiones TCP y UDP entrantes o salientes



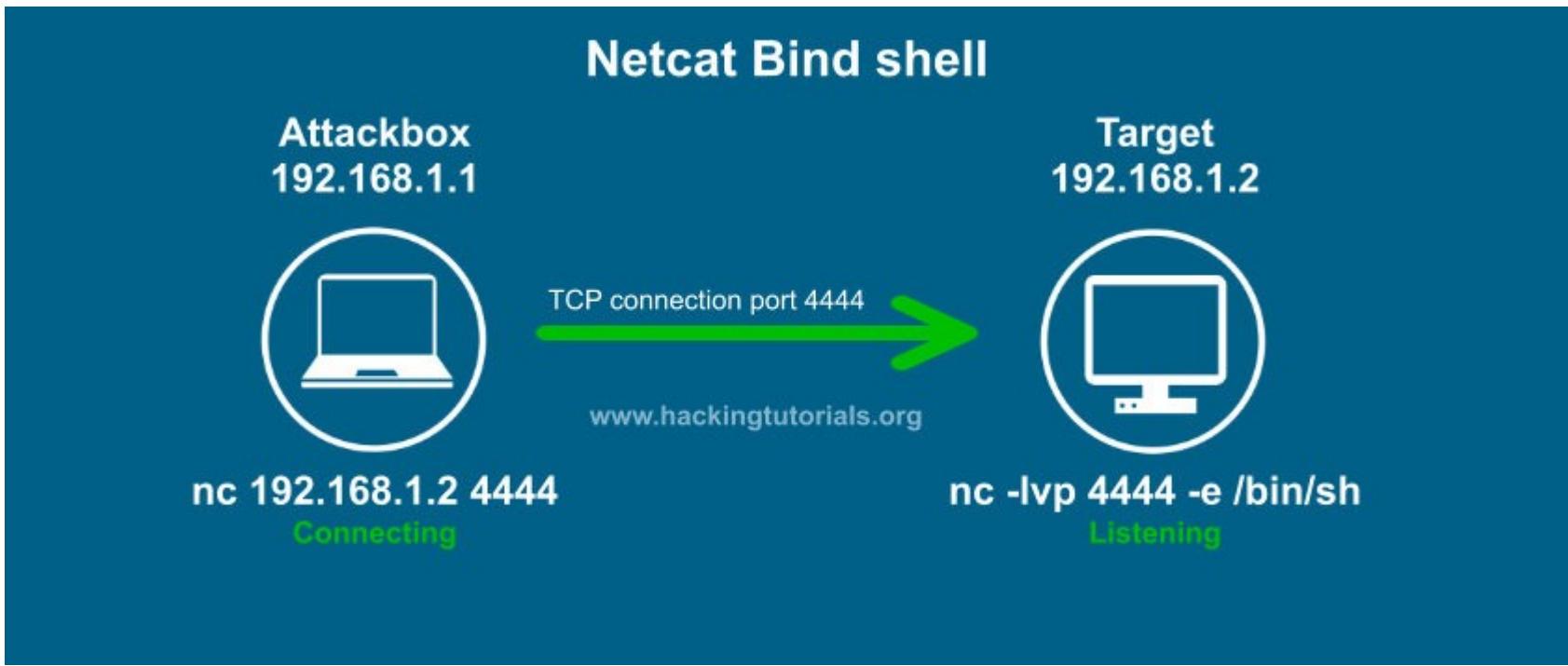
Netcat reverse shell

- lvp: listen verbose port
- nc = netcat
- Puerto default de conexión de nc



Netcat bind shell

- lvp: listen verbose port
- nc = netcat
- Puerto default de conexión de nc



- En ambientes de evaluación interna el 95% se busca utilizar reverse shells
- En ambientes de evaluación externa se prefiere utilizar bind shells, sin embargo, es complejo utilizar este tipo de shells debido a que hay que saltarse bloqueos de Firewalls u otras medidas perimetrales

b) Payloads

- Enviar al equipo objetivo una serie de comandos para obtener una terminal y escalar privilegios
- Tipos de payloads
 - Por etapas: envia el código del payload por fases: windows/meterpreter/reverse_tcp
 - Sin etapas: envia todo el código en la primera conexión: windows/meterpreter_reverse_tcp
- Sugerencia: probar distintos tipos de payloads hasta obtener el resultado esperado

Escalamiento de privilegios

- DEMO usando el protocolo SMB para elevación de privilegios en Kloprix V1



Por hacer

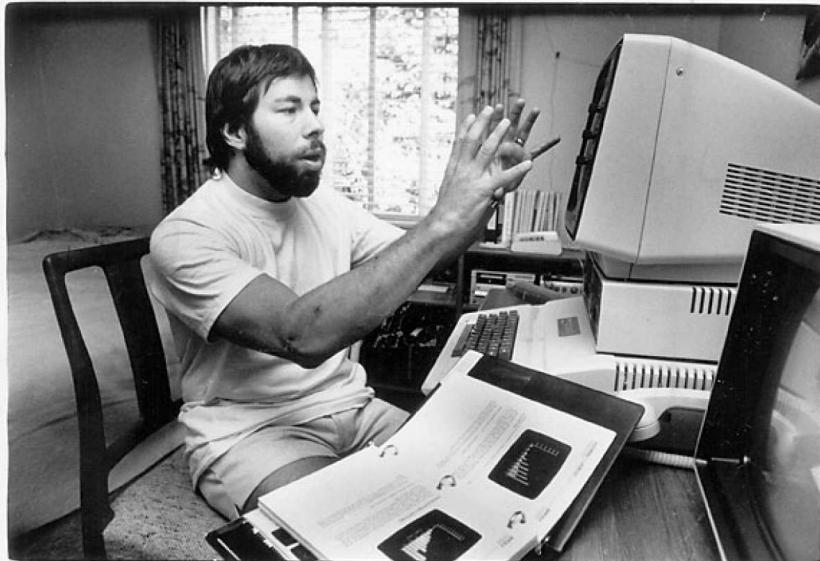
- Password spraying
- Credential stuffing
- Ataques de fuerza bruta a distintos puertos y servicios

FAQs

- Debo tener una formación en Tecnologías de Información antes de entrar en alguna de las áreas de Infosec?
- Debo ser desarrollador de aplicaciones antes de entrar en alguna de las áreas de Infosec?
- Debo tener una super computadora y una super conexión a internet antes de entrar en alguna de las áreas de Infosec?
- Si logro escalar Kloprix ya soy un hacker?
- Todos los hackers son malos?

FAQs

- Todos los hackers son así?



- O así?

Cuidado con...

- Quebrantar leyes, propiedad privada o intelectual para demostrar lo hábil que eres
- Nunca realices ninguna actividad de hacking ético o pruebas de penetración sin un contrato que delimite tus acciones y responsabilidades
- El síndrome del impostor



Happy Hacking!

- @heftamayo

