

# Hacking Ético

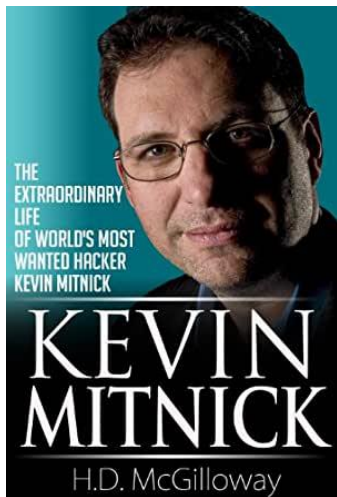
Ing. Iver Adolfo Vargas  
Villanueva



# ¿Qué es un hacker?



# Hacker famosos



# Tipos de hacker



# Pilares de decisión

Leyes del país

Leyes de la organización

Valores





# Vulnerabilidades



## EL FC BARCELONA SUFRE UN ATAQUE DE RELLENO DE CREDENCIALES EN SU CUENTA DE Twitter

El grupo OurMine, mismo que atacó las cuentas de múltiples equipos de la NFL en Enero, ha atacado las cuentas de Twitter del FC Barcelona y del Comité Olímpico Internacional este 15 de febrero.



## FALLO CRIPTOGRÁFICO DE SEGURIDAD

La vulnerabilidad crítica denominada CVE-2020-0601, que fue descubierta por la NSA de Estados Unidos, afecta a un componente conocido como CryptoAPI (Crypt32.dll).



## 500 EXTENSIONES MALICIOSAS DE CHROME AFECTAN A MILLONES DE USUARIOS

Las extensiones maliciosas de Chrome recopilaban en secreto los datos del navegador de los usuarios y los redirigían a sitios web con malware.



## Microsoft

## 250 MILLONES DE REGISTROS DE SOPORTE EXPUESTOS

Cerca de 250 millones de registros de Servicio al Cliente y Soporte (CSS) de Microsoft se encontraron expuestos a Internet en cinco bases de datos inseguras de Elasticsearch, informa Comparitech.



EL HOMBRE MÁS RICO DEL MUNDO

## HACKED

El archivo fue enviado por el príncipe heredero Salman que tenía una conversación con Jeff Bezos vía Whatsapp, por lo cual recibió un archivo de video malicioso el cual se trataba de un archivo MP4 según los forenses digitales.



## CIBERDELINCUENTE PIDE \$5 MILLONES EN RESCATE

Compañía petrolera en México ha sido atacada por un ransomware y el ciberdelincuente exige \$5 millones de dólares.



## FIN DEL SOPORTE PARA WINDOWS 7 Y SERVER 2008

El soporte de Windows 7 y Windows Server 2008 finaliza el 14 de enero de 2020.



VULNERABILIDAD CRÍTICA EN BLUETOOTH PERMITE EL CONTROL TOTAL DE

## Android

Vulnerabilidad en el sistema Bluetooth de Android que permite a un atacante ejecutar código arbitrario en forma remota utilizando la MAC del dispositivo. Esta vulnerabilidad afecta a la versión Android Oreo 8.0 y Android Pie 9.0.



## ERROR CRÍTICO DEL PLUGIN DE WORDPRESS AFLIGE 700,000 SITIOS

Un popular plugin de WordPress, que ayuda a que los sitios web cumplan con el Reglamento General de Protección de Datos (RGPD), ha publicado correcciones para una falla crítica.



## SHLAYER, EL VIRUS QUE LLEVA DOS AÑOS ATACANDO A LOS USUARIOS DE MacOS

Shlayer es malware tipo troyano el cual su función es descargar e instalar adware o aplicaciones no deseadas en una Mac infectada.



## VULNERABILIDAD PERMITE SEQUESTRAR VPN CIFRADAS

Un equipo de investigadores de ciberseguridad, ha revelado una vulnerabilidad grave en VPN



## SITIO DE GOBIERNO AMERICANO HACKEADO

El sitio fdip.gov operado por el gobierno de EE. UU. ha sido víctima de defacement por parte de un grupo que afirma representar al gobierno de Irán.



## BANCO NACIONAL DE ISLAS CAÍMAN HACKED

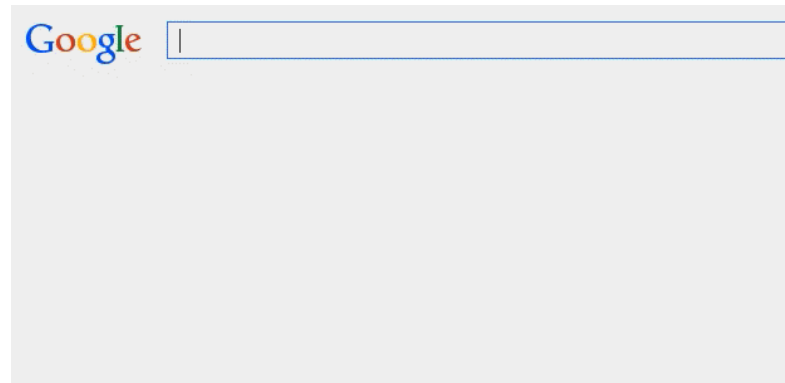
En ella figuran, por ahora, más de 1.400 cuentas de clientes procedentes principalmente de la Unión Europea y América.

# Fases del Hacking Ético



# Reconocimiento

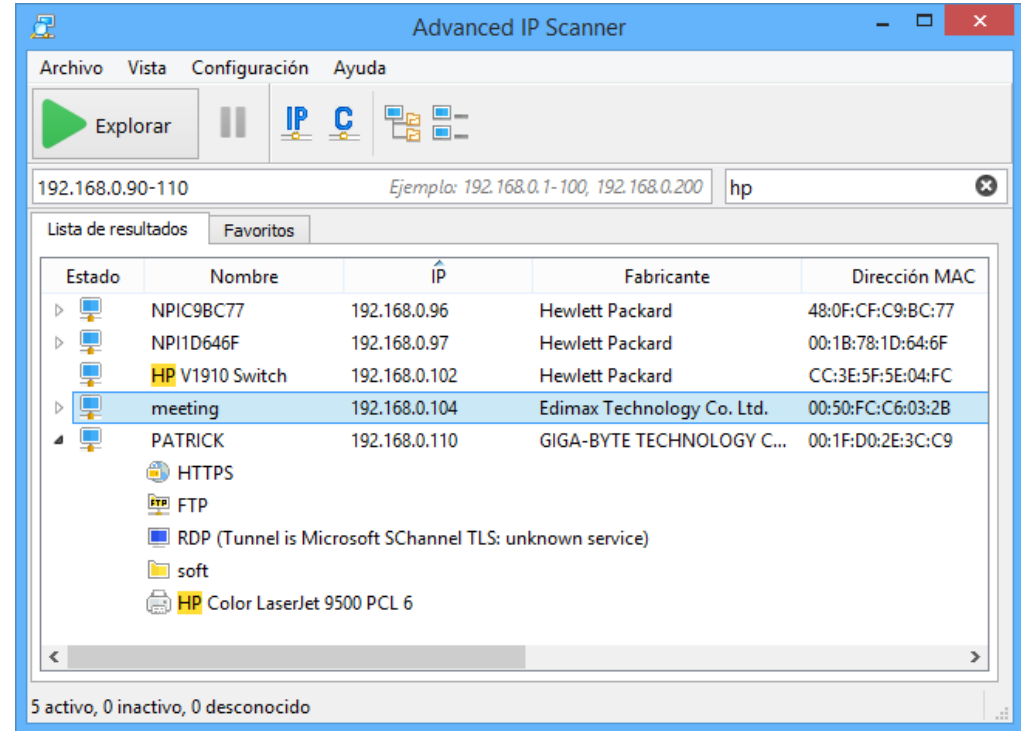
- **Pasivo - footprinting**
  - Recopilar información
  - Sniffing de la red
- **Activo - fingerprinting**
  - Sondear la red
  - Ingeniería Social





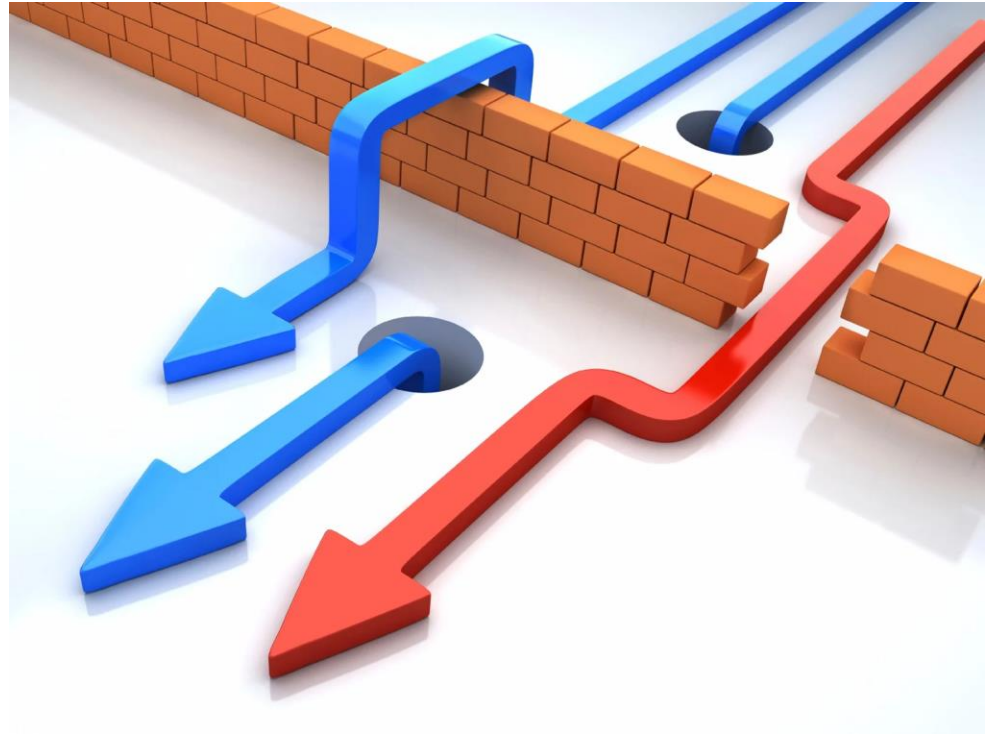
# Escaneo

- Escáneres de puertos
- Escáneres ICMP (Protocolo de Mensajes de Control de Internet)
- Barrido de ping
- Mapeadores de red
- Barrido de SNMP (Protocolo de manejo simple de red)
- Escáneres de vulnerabilidades



# Obtener acceso

- Explotar vulnerabilidades
  - LAN
  - Internet
  - Aplicación
  - Servidor
  - Computadora



# Mantener acceso

- Backdoor
- Troyanos
- Spyware

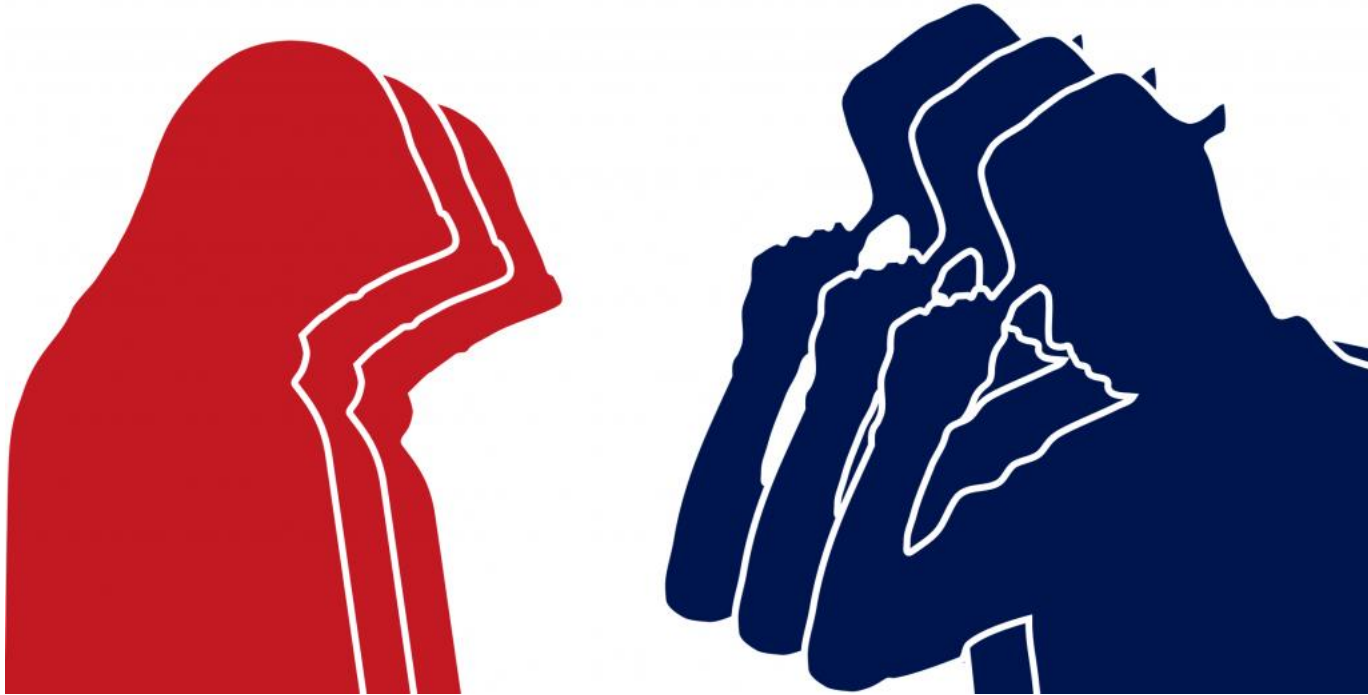


# Limpiar huellas

- Eliminar logs
- Eliminar alertas
  - Sistema Operativo
  - Antivirus
  - IDS



# Roles de un Ethical Hacking



# Técnicas de Hackeo - SQL Injection

## SQL INJECTION



WEB PAGE

USERNAME:

WUM

PASSWORD:

\*\*\*\*\*

Select \* from wum\_Table where user-d='wum' and password 'wumtool';



WEB PAGE

USERNAME:

'1' OR '1' = '1'

PASSWORD:

\*\*\*\*\*

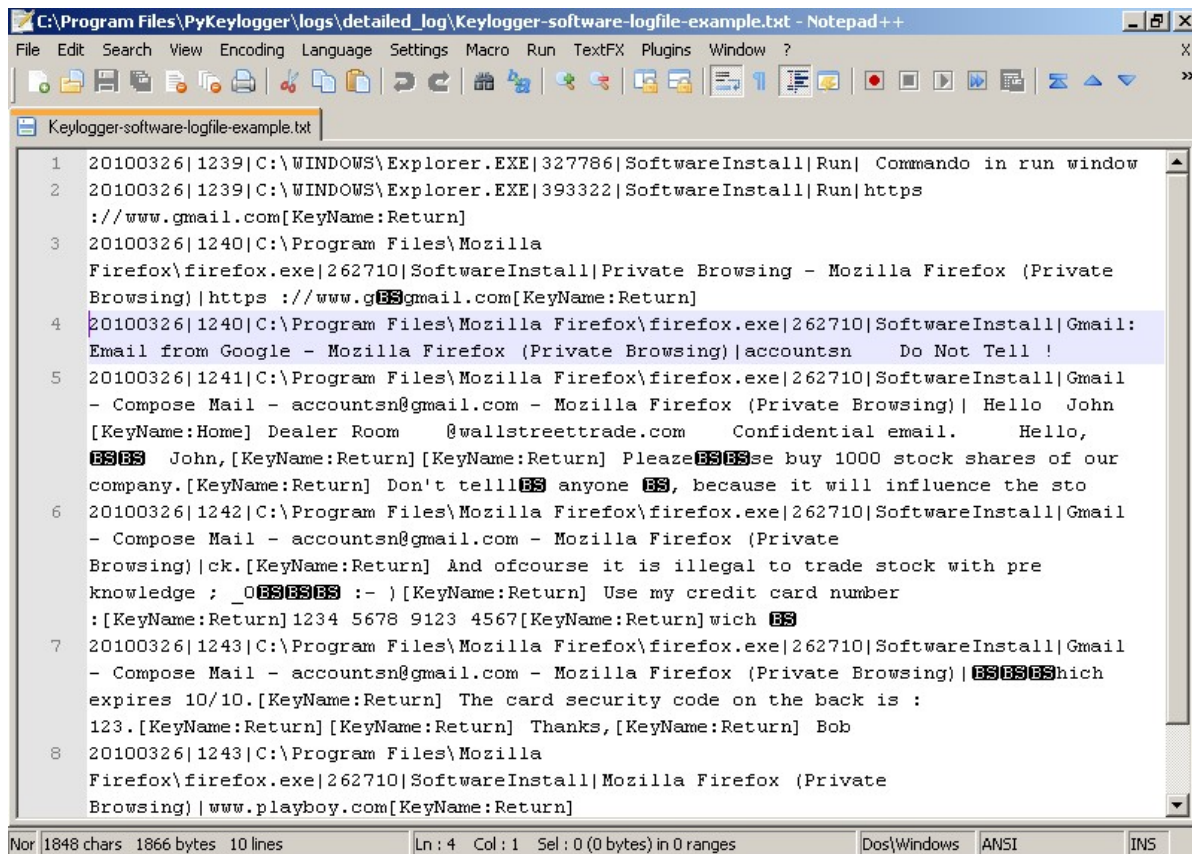
Select \* from wum\_Table where user-d='1' OR '1' = '1' and password '1' OR '1' = '1';



# Técnicas de Hackeo -Phishing



# Técnicas de Hackeo - Keylogger



```
C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
1 20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
2 20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
  ://www.gmail.com[KeyName:Return]
3 20100326|1240|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
  Browsing)|https ://www.gBSgmail.com[KeyName:Return]
4 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
  Email from Google - Mozilla Firefox (Private Browsing)|accounts Do Not Tell !
5 20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts@gmail.com - Mozilla Firefox (Private Browsing)| Hello John
  [KeyName:Home] Dealer Room @wallstreettrade.com Confidential email. Hello,
  BSBS John,[KeyName:Return][KeyName:Return] PleaseBSBS use buy 1000 stock shares of our
  company.[KeyName:Return] Don't tellBS anyone BS, because it will influence the sto
6 20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts@gmail.com - Mozilla Firefox (Private
  Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre
  knowledge ; _0BSBSBS :- )[KeyName:Return] Use my credit card number
  :[KeyName:Return]1234 5678 9123 4567[KeyName:Return]wich BS
7 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts@gmail.com - Mozilla Firefox (Private Browsing)|BSBSBShigh
  expires 10/10.[KeyName:Return] The card security code on the back is :
  123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
8 20100326|1243|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
  Browsing)|www.playboy.com[KeyName:Return]
```

Nor 1848 chars 1866 bytes 10 lines Ln: 4 Col: 1 Sel: 0 (0 bytes) in 0 ranges Dos\Windows ANSI INS

# Técnicas de Hackeo - Ataque DDOS



# Técnicas de Hackeo - Vishing

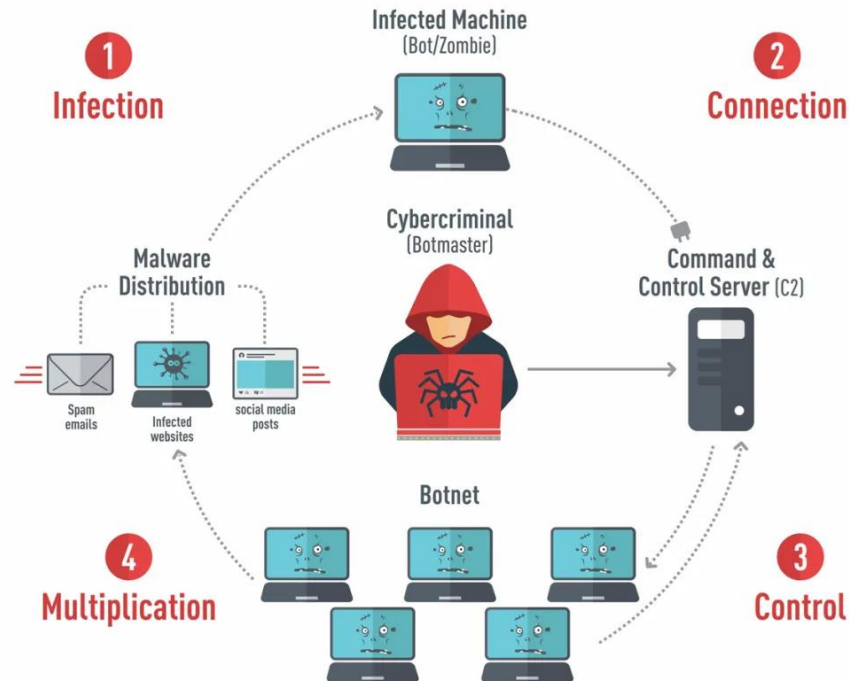


# Técnicas de Hackeo - Baiting



# Técnicas de Hackeo - Botnet

## How a Botnet works





# Técnicas de Hackeo – Ingeniería Social



# Hardware para Hacking ético



# DEMOS



# Conclusiones

# Recomendaciones

# ¡¡ Muchas Gracias !!



This work is licensed under a Creative Commons Attribution-ShareAlike 3.0  
Marzo 2020  
Disponible en: <https://github.com/ingivargas84/presentaciones>