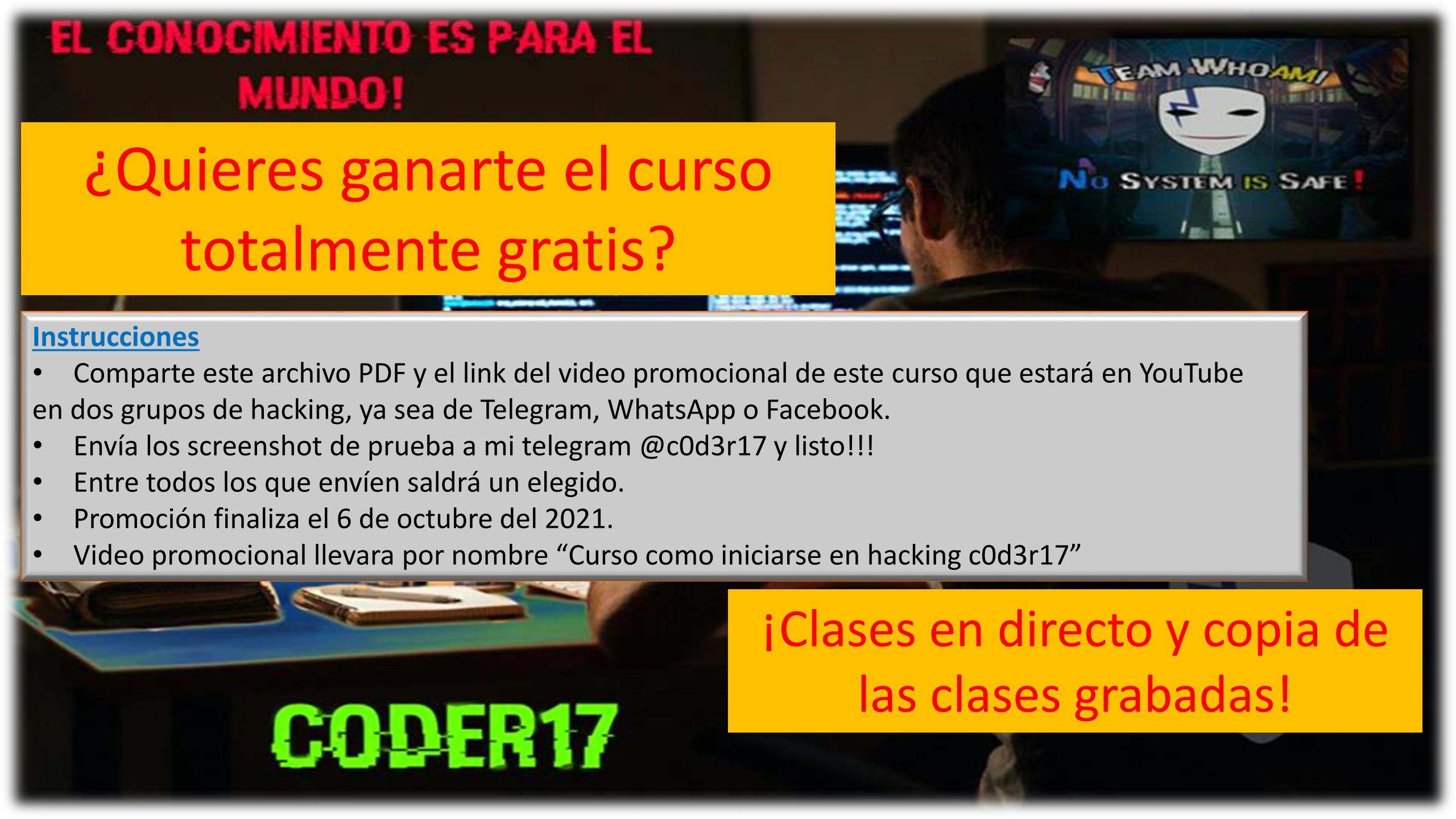
Como iniciarse en hacking

@c0d3r17



¿Quieres ganarte el curso totalmente gratis?

Instrucciones

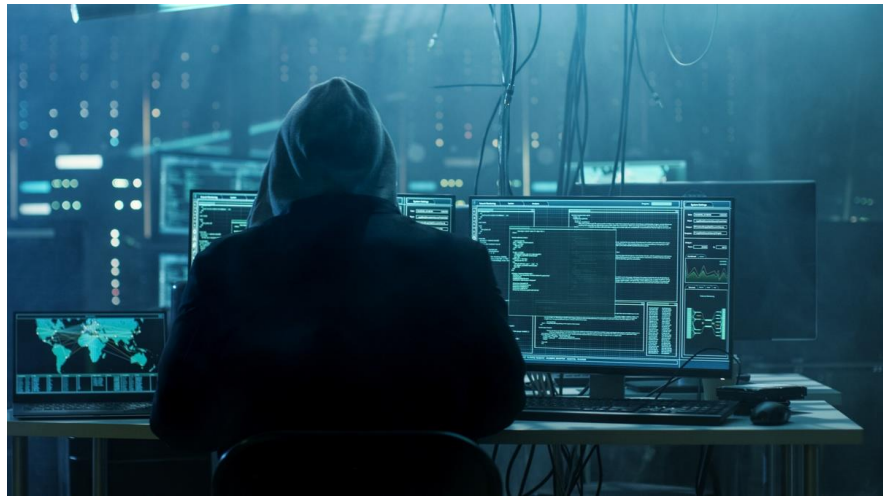
- Comparte este archivo PDF y el link del video promocional de este curso que estará en YouTube en dos grupos de hacking, ya sea de Telegram, WhatsApp o Facebook.
- Envía los screenshot de prueba a mi telegram @c0d3r17 y listo!!!
- Entre todos los que envíen saldrá un elegido.
- Promoción finaliza el 6 de octubre del 2021.
- Video promocional llevara por nombre “Curso como iniciarse en hacking c0d3r17”

¡Clases en directo y copia de las clases grabadas!

Que es hackear

Datos importantes

- Hacker: definición básica “pirata informático”
- Vulnerar sistemas informáticos
- Hacer que el sistema haga algo para lo que no esta diseñado
- Creatividad, investigación y experimentación
- travesuras
- Reto intelectual



¿Por que hackear?

- Creatividad, investigación y experimentación
- travesuras
- Reto intelectual
- Ámbito laboral

Hacking ético

- Ataques controlados
- Detección de vulnerabilidades
- Proteger infraestructuras tecnológicas
- Remediar fallos de seguridad

Etapas de explotación

Etapas

- Reconocimiento (información en internet y escaneos)
- Análisis de vulnerabilidades
- Explotación
- Post explotación

Tipos de análisis

- Caja negra: sin conocimientos del objetivo
- Caja blanca: total conocimiento del objetivo (coordinado con el objetivo)
- Caja gris: combinación de ambas

Tipos de auditorias

- Externa: cualquier lugar
- Interna: dentro de la red objetivo
- Web: pagina web (externa o interna)
- Wifi: explotación wifi
- Aplicación: bugs de programación
- Móvil: dispositivos móviles

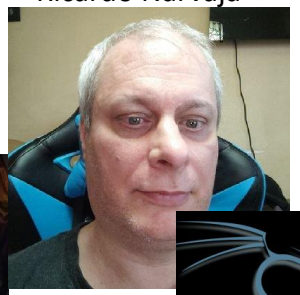
Objetivo personal

Tipos

- Explotación especifica (Ej: mensajes WhatsApp)
- Hacking global actual
- Hacking global incluyendo bases de conocimiento (antiguo)
- Desarrollo de herramientas de hacking
- Enfoque laboral

Consejos para aprender hacking

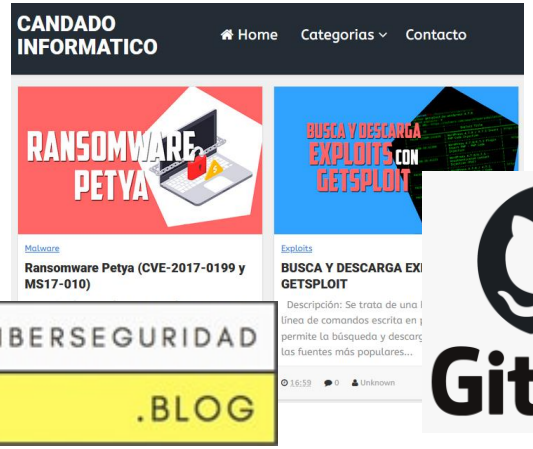
Ricardo Narvaja



Consejos

- Elegir un tema de interés (mantener concentración)
- Primero videos y luego lectura
- Replicas del laboratorio utilizado
- Considerar inestabilidad de explotación
- Documentar el aprendizaje
- Respaldo de maquinas virtuales o snapshot
- No actualizar OS sin respaldo

Hackplayers



GitHub

Medium

Orden de aprendizaje

- Tutoriales en video con detalles (español)
- Tutoriales en video sin detalles (español)
- Tutoriales en video con detalles (ingles)
- Tutoriales en video sin detalles (ingles)
- Tutoriales escritos con detalles (español)
- Tutoriales escritos sin detalles (español)
- Tutoriales escritos con detalles (ingles)
- Tutoriales escritos sin detalles (ingles)
- Libros (español)
- Libros (ingles)

Ramas del hacking

Análisis forense

- Validar falsos positivos
- Descubrir el ataque generado
- Impacto de la explotación

Datos importantes

- Estamos del lado de los buenos (principalmente)
- Copiar el dispositivo de almacenamiento
- Utilizar maquinas virtuales para el examen de archivos sospechosos
- Relevante en aspectos laborales (defensa)

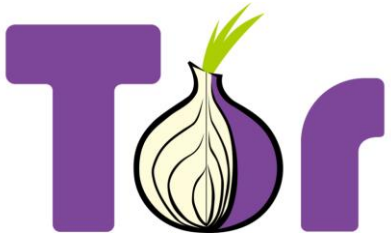
Actividades

- Análisis de registros de eventos
- Análisis de malware (reversing)
- Análisis de archivos varios (metadatos)
- Recuperación de archivos borrados
- Análisis de unidades cifradas
- Análisis de memoria RAM
- Análisis de paquetes de red

Ramas del hacking

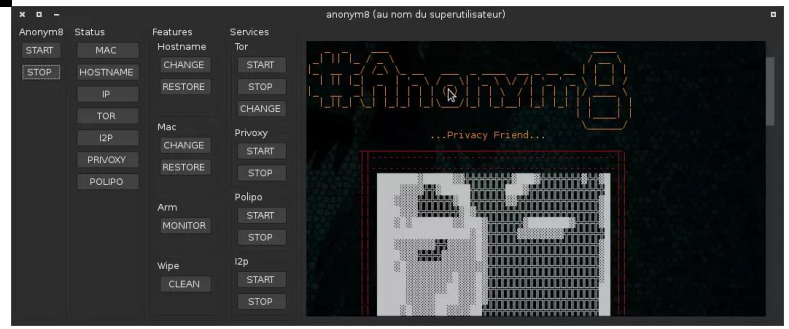
Anonimato

- Ocultar rastros
- Evadir seguridad para la explotación
- Conexiones seguras VPNs



Datos importantes

- Estamos del lado de los malos
- Anonimato es sinónimo de conexión lenta
- Sistemas o programas con anonimato
- Aumenta la inestabilidad de explotación
- En si nada es totalmente anónimo, pero TOR es un protocolo de conexiones muy anónima



Actividades

- Explotación web con anonimato
- Conexión de payloads
- Uso de exploits
- Reconocimiento con anonimato
- Uso de proxy
- Navegación segura (dejar datos en la
- red o victimas de MITM)

Ramas del hacking

Hacking web

- Modificación de la pagina o aplicación web
- Inserción a la infraestructura de un objetivo
- Robo de datos de usuario (credenciales, tarjetas, etc.)
- Password guessing (no es solo web)
- Fuerza bruta

Datos importantes

- Sigue siendo un PC común y corriente con el servicio web
- Estamos del lado de los malos
- Relativo a la tecnología de construcción del sitio (PHP, Laravel, etc.)
- Relativo a la estructura de soporte del servicio web (Apache, IIS, etc.)
- Explotación mediante un sitio indirecto
- Existen varios laboratorios

Actividades

- Explotación de base de datos (SQLi)
- Explotación de vulnerabilidades del lado del cliente (XSS)
- Explotación de vulnerabilidades del lado del servidor (LFI,RFI,RCE etc.)
- Explotación de CMS (wordpress y joomla)

Ramas del hacking

Hacking wifi

- Obtener contraseñas wifi
- Acceso a la infraestructura del objetivo

Datos importantes

- Estamos del lado de los malos
- Inestabilidad de la conexión
- Relativo al router

TL-WN722N

Actividades

- Explotación sencilla seguridad WEP
- Explotación con crackeo
- Explotación WPS
- Explotación con punto de acceso falso

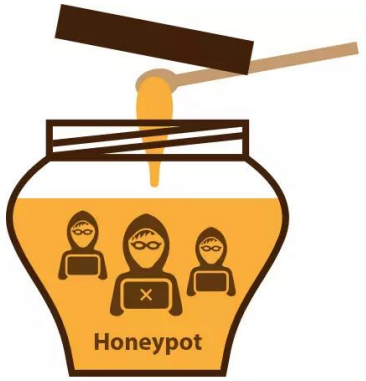
Ramas del hacking

Defensa

- Protección de todo tipo de sistemas informáticos
- Vigilancia en tiempo real de los sistemas
- Detección de falsos positivos
- Sinergia con forense

Datos importantes

- Estamos del lado de los buenos
- Base del enfoque laboral
- La mayoría de las alertas son falsos positivos
- Importante segregar las amenazas rápidamente



Actividades

- Parches de actualización
- Establecer infraestructura de hardware
- Configuraciones de software

Ramas del hacking

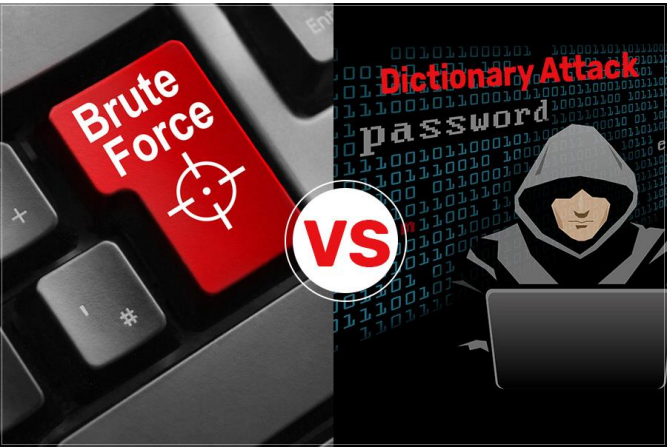
Encriptación

- Encriptar para proteger información
- Encriptar para ofuscar malware
- Des/Encriptar para realizar explotación
- Password cracking
- Comunicación secreta

Datos importantes

- Estamos del lado de los buenos y malos
- Múltiples formatos (confusos)
- Seleccionar un diccionario adecuado
- Búsqueda infinita
- Velocidad de crackeo depende del hardware

HASHCAT



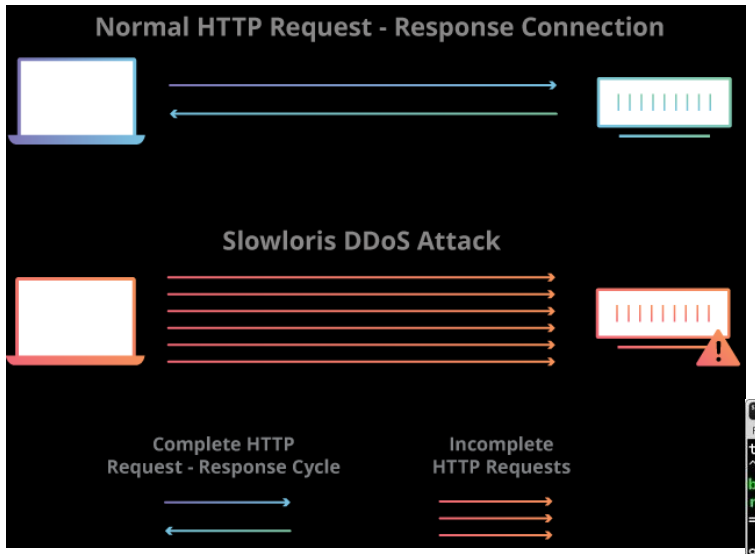
Actividades

- Crackear hashes
- Ofuscar código fuente (desarrollo)
- Encriptar datos sensibles de BD
- Crear diccionarios

Ramas del hacking

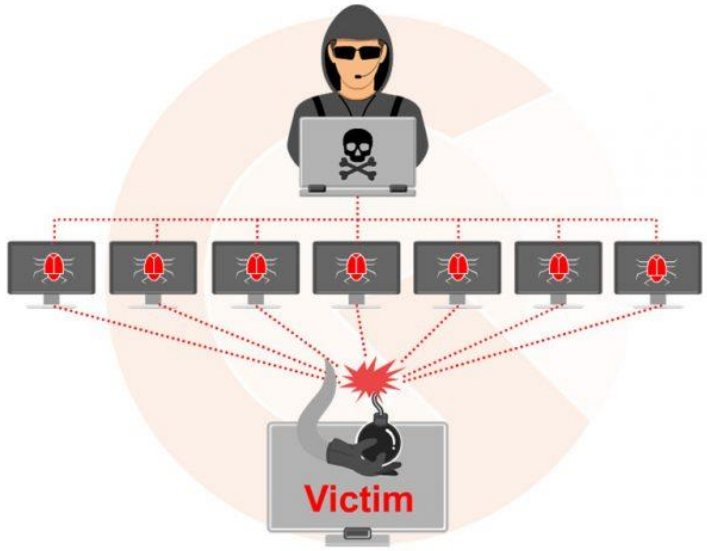
DOS y DDOS

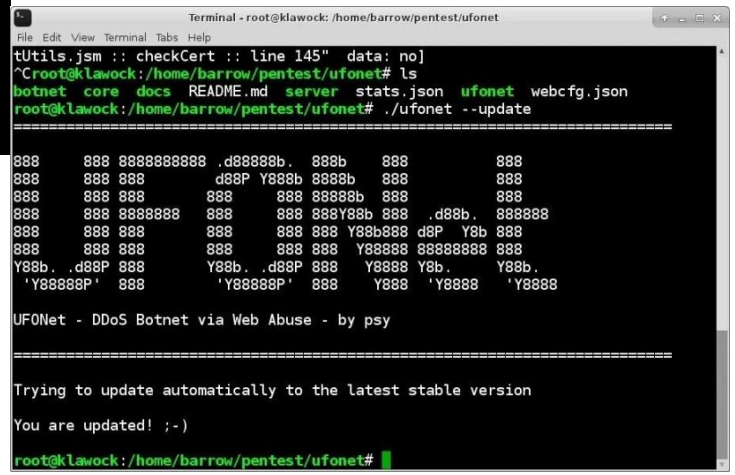
- Inhabilitar servicios



Datos importantes

- Estamos del lado de los malos
- Asociadas a botnet
- Puede existir protección
- Relativo a la envergadura la cantidad de dispositivos involucrados





Actividades

- Denegación no distribuida
- Denegación distribuida

Ramas del hacking

Ensamblador y reversing

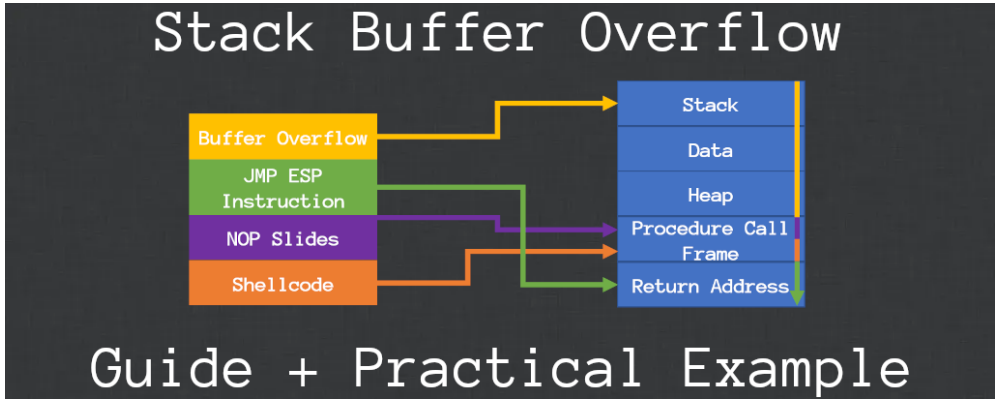
- Análisis de malware
- Construcción de malware
- Bypass de licencias de software

IDA Pro
by Ilfak Guilfanov

Datos importantes

- Estamos del lado de los malos y buenos
- Difiere según arquitectura x32 y x64
- Difiere según sistema operativo
- Exploits con inestabilidad que genera caída del SO

IMMUNITY
DEBUGGER



Actividades

- Construcción de exploits
- Construcción de cargas útiles
- Generar crack de programas
- Descompilar programas (malware)

Ramas del hacking

Reconocimiento (fingerprinting y footprinting)

- Recopilar información de la victima
- Diferencia (información publica y privada)
- (con o sin permisos del objetivo)
- Fingerprinting y footprinting se relacionan y se confunden
- Pentesting de caja negra, gris y blanca

Datos importantes

- Estamos del lado de los malos y buenos
- Confusión, ya que algunos métodos están
- en el limite de ambos
- Inestabilidad con sistemas de seguridad IDS e IPS
- Ruidoso (alerta al objetivo)
- Trabajar con anonimato
- Falsos positivos

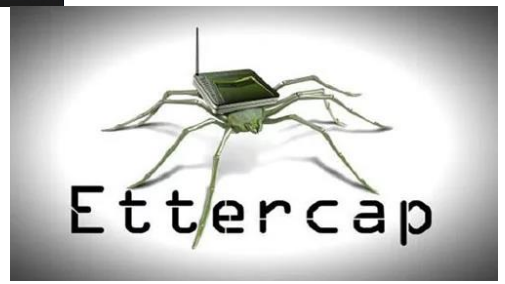
Actividades

- Búsqueda de dominios y subdominios FO
- Escaneo de puertos y servicios FI
- Búsqueda de correos electrónicos FO
- Búsqueda de usuarios FO
- Búsqueda de equipos en red publica FO
- Escaneos con módulos de Metasploit o
- múltiples scripts FI

Ramas del hacking

Man in the middle

- Interceptar trafico de red
- Captura de credenciales (también cookies)
- Modificar integridad de datos que vera la victima
- Visualización de información secreta (Ej: mensajes)

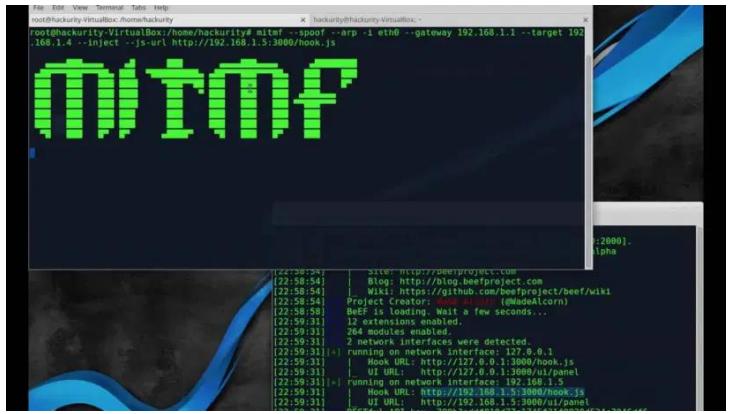


Wireshark

Datos importantes

- Estamos del lado de los malos
- Inestabilidad de conexión para todos
- Captura solo de algunos paquetes (envenenamiento)
- Métodos de evasión HTTPS (mucho mas inestables)

FruityWiFi
Wireless Network Auditing Tool
WWW.FRUITYWIFI.COM



Actividades

- Envenenamiento ARP o
- Anteponerse al router

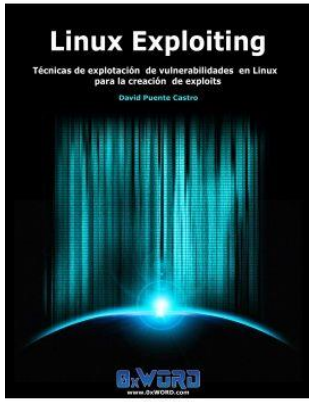
(fake AP o compartir por cable)

- Ingeniería social (Beef)
- Wireshark (captura de paquetes)

Ramas del hacking

Payloads y exploits

- Payload: Acción maliciosa sobre la victima
- Exploit: Acceso al equipo victima
- Payload (carga útil) (Ej: payload de conexión reversa)
- Payload (código de explotación) (Ej: SQLi)



Datos importantes

- Estamos del lado de los malos
- Uso y/o desarrollo
- Detección por los antivirus o anti malware
- Exploits con explotación inestable (Ej: buffer overflow)
- Post explotación (deriva directamente)
- Botnets o conexiones únicas
- Formatos de payloads
- Arquitectura x86 x64

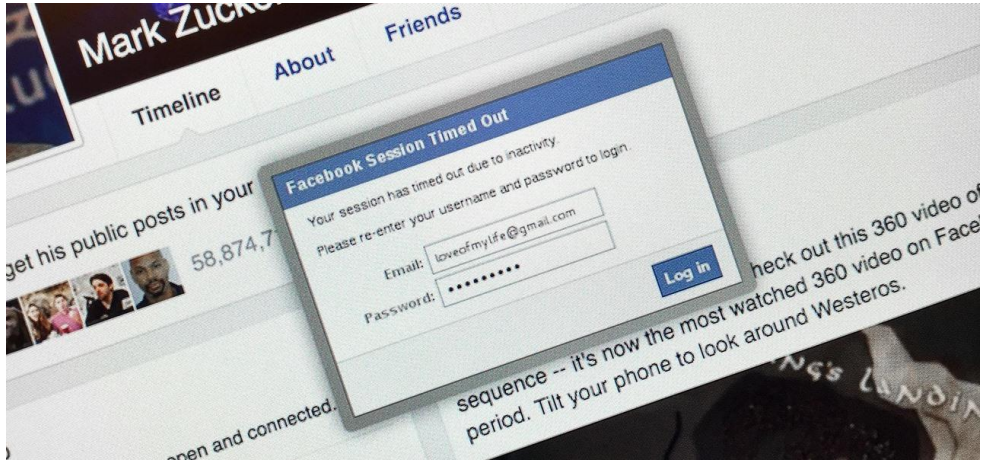
Actividades

- Exploit y payload de control remoto
- Exploit y post explotación especifica
- Desarrollo de payloads (lenguajes de programación)
- Desarrollo de exploits (exploiting)
- Ofuscación de payloads
- Ejecución de payloads con ingeniería social (macros, email)
- Ejecución de payloads directa (USB) o indirecta (rubber ducky)

Ramas del hacking

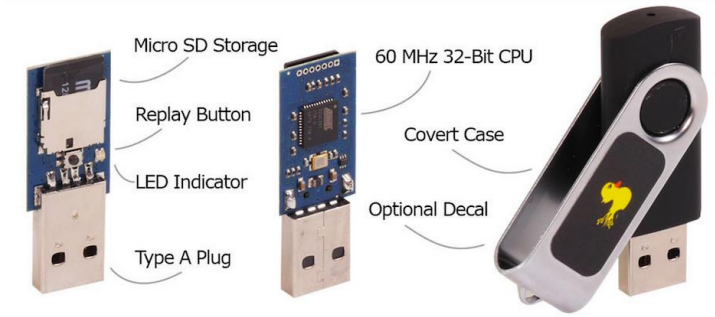
Phishing

- Toda técnica de ingeniería social



Datos importantes

- Estamos del lado de los malos
- Depende del conocimiento de la victima
- Servicios con restricciones para realizar Phishing (email)
- Detectada por navegadores y/o antivirus
- Clones de paginas, eliminar links originales



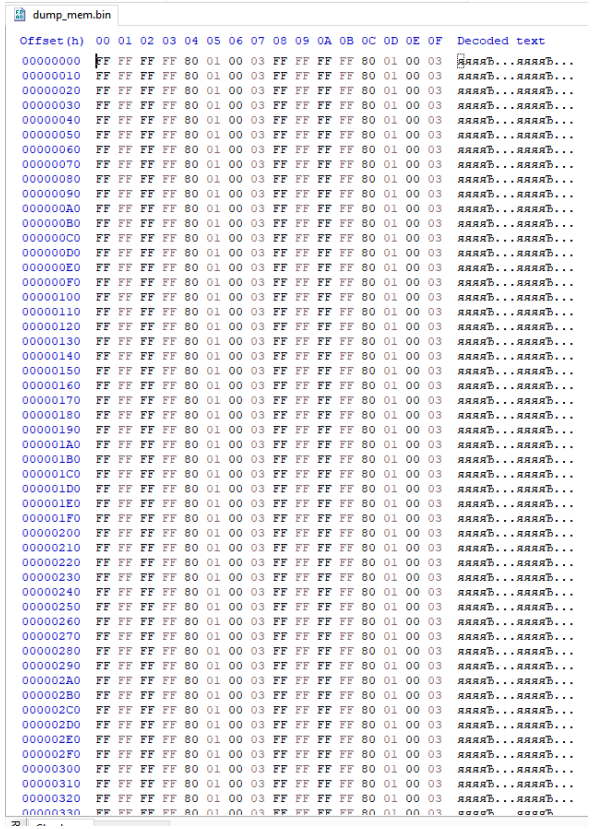
Actividades

- Correo para captura de credenciales
- Correo para ejecución de payload
- Combinando con MITM (Beef)
- Conexión USB Rubber ducky

Ramas del hacking

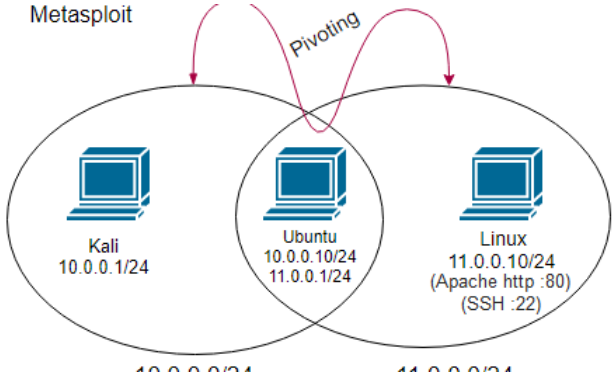
Post explotación

- Posterior a la obtención de conexión con la victima
- Carga útil a usar en el Exploit
- Objetivo especifico del atacante



Datos importantes

- Estamos del lado de los malos
- Herramienta con script pre definidos (Metasploit)
- Script o ejecutables cargados manualmente
- Inestabilidad por arquitectura x86 x64
- Velocidad de conexión (anonimato)
- Detección del antivirus
- Combinación de múltiples herramientas



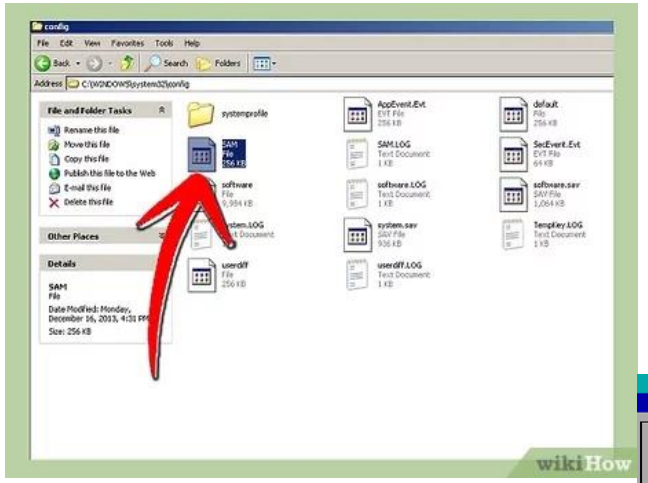
Actividades

- Obtención de credenciales
- Obtención de archivos
- Grabar cámara o micrófono
- Cargar ransomware
- Dañar sistema o programas
- Desplazamiento lateral
- Volcado de memoria RAM

Ramas del hacking

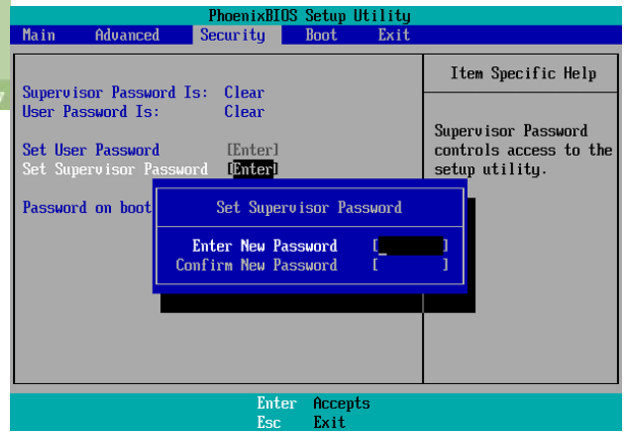
Bypass login Windows

- Acceder a un equipo sin password



Datos importantes

- Estamos del lado de los malos
- Daños de sistema poco probables
- A veces requiere bypass de seguridad de boot
- Requiere apagado completo (por consola)



Actividades

- Eliminar contraseña de admin
- Cambiar ejecutable por cmd
- Hiren’s boot CD

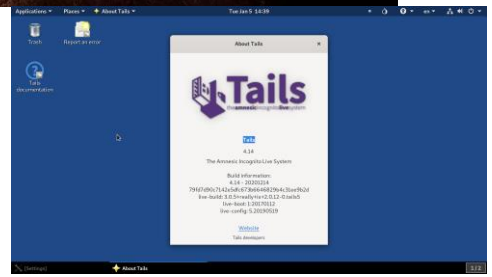
Sistemas operativos

Tipos

- Generales de hacking (kali, parrot)
- Específicos de una rama (beini, wifislax, tails)
- Adaptados manualmente (Ubuntu, arch)

Generales

- Múltiples herramientas para todas las ramas
- Kali (V): compatible con proyectos GitHub
- Kali (D): inestabilidad al actualizar
- Parrot (V): estabilidad
- Parrot (D): mayor consumo de recursos
- No recomendable como sistema base



Específicos

- Mayor estabilidad de herramientas
- Múltiples herramientas de un área
- Herramientas antiguas
- Herramientas de ejecución manual

Globales

- Instalaciones de herramientas conflictivas
- Actualizar repositorios
- Inexistencia de repositorios
- Usar en maquinas virtuales
- Tomar snapshot o hacer respaldos

Adaptados

- A gusto personal
- Mayor estabilidad de sistema
- Problemas para instalar herramientas
- Menor estabilidad de herramientas
- Compatible para ser sistema base

Maquina virtuales

Consejos

- Montar laboratorios (exactos)
- Sistemas operativos con distintas versiones
- Tomar snapshot o hacer respaldos
- Calcular el tamaño de HDD
- Conexión de adaptador puente
- Utilizar sistema base como victima, para economizar recursos
- Instalar “VMWare tools” o “guest aditions”
- Adaptador puente verificar adaptador en uso

VMWare

- (V) permite snapshot (versión pro)
- (V) Fácil conseguir pirata (versión pro)
- (D) difícil actualizar
- (D) configurar adaptador puente
- (D) configurar red interna (local)
- (D) instalación VMWare tolos
- (V) estabilidad y facilidad de exportación
- (V) mas liviana la imagen de kali

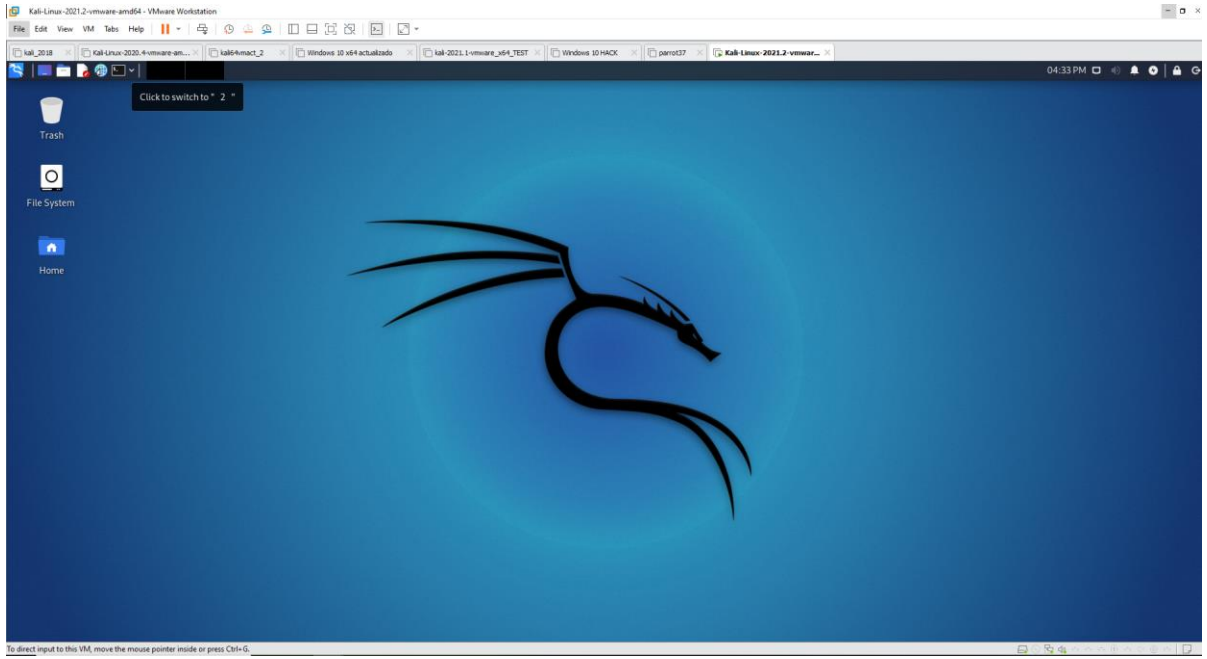
Virtual Box

- (D) respaldo solo clonando o exportando maquina
- (V) Gratuito
- (V) fácil actualizar
- (V) configurar adaptador puente
- (V) relativamente fácil configurar red interna (local)
- (V) instalación guest aditions
- (D) inestabilidad importación (recomiendo ova 2.0)
- (D) mas pesada la imagen de kali

Instalación Kali

Datos importantes

- https://www.kali.org/get-kali/#kali-virtual-machines
- Usar versión de maquina virtual (incluye VMWare tools, guest adittions)
- (VMWare) Replicar red física -> estabilidad con cambio de red



Pasos

1. Descargar imagen
2. Importar imagen
3. Adaptador puente
4. Cambiar teclado
5. Cambiar contraseña “kali”
6. Cambiar contraseña “root”
7. Actualizar repositorios
8. Actualizar sistema
9. IP fija (router o sistema)

Hardware mínimo

- CPU: 1 núcleo **1 procesador**
- RAM: 1Gb
- HDD: 20 Gb

Hardware recomendado

- CPU: 2 núcleos **2 procesadores**
- RAM: 2Gb
- HDD: 80 Gb

IP local

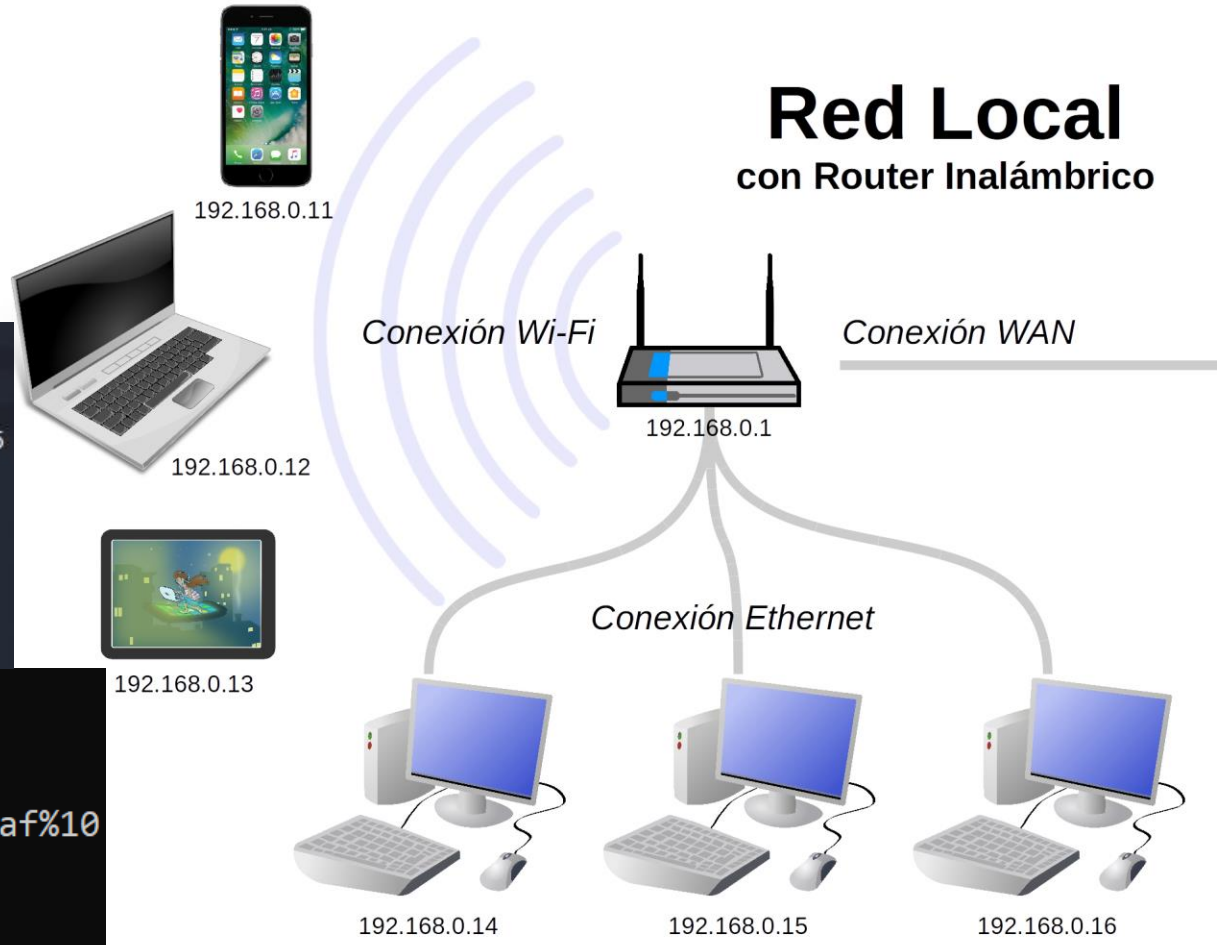
Tipos

- Identifica un equipo en una red
- Celulares, PC, cámara wifi, etc.
- Puede estar repetida en mi casa y en la de mi vecino
- Comúnmente es: 192.168.0.X
- Distinta a la IP publica
- Hacer ping
- Puedo tener 2 IPs locales (2 tarjetas de red)
- Localhost (127.0.0.1 o localhost)

```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.80.132  netmask 255.255.255.0  broadcast 192.168.80.255
        inet6 fe80::20c:29ff:feea:9e42  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ea:9e:42  txqueuelen 1000  (Ethernet)
        RX packets 689  bytes 301905 (294.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 543  bytes 62604 (61.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::3d11:5d9c:f380:86af%10
   Dirección IPv4. . . . . . . . . . . . : 192.168.0.7
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1
```



Mascara y Gateway

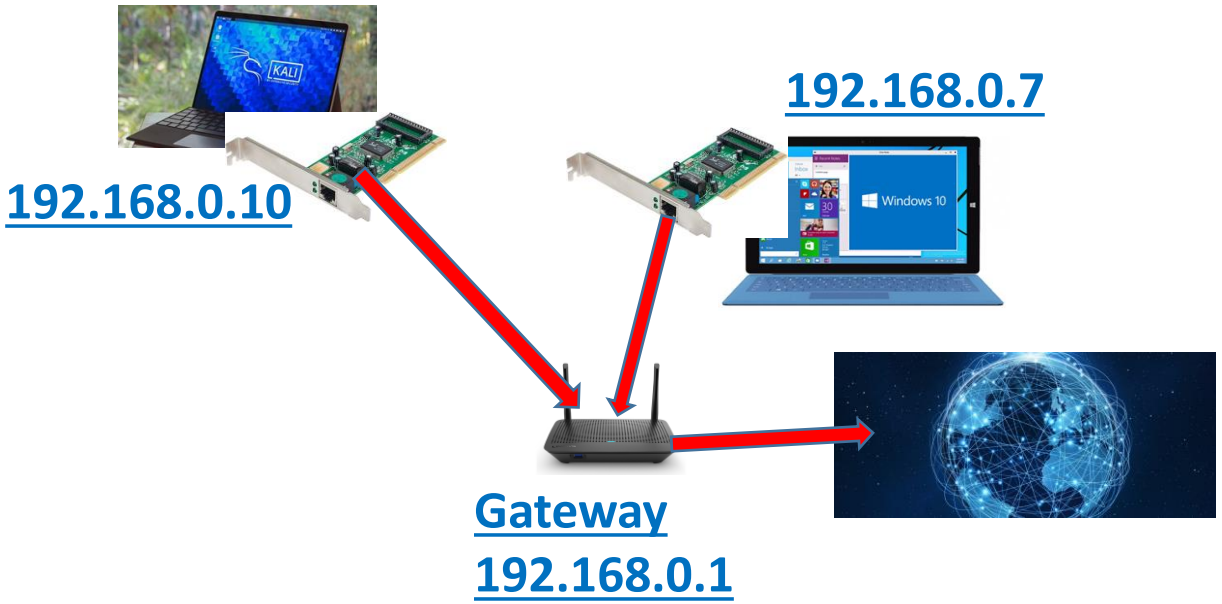
Windows 10

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::3d11:5d9c:f380:86af%10
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.7
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1
```

Datos importantes

- Mascara: especifica subredes (rango de IPs validas)
- https://aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi1
- Gateway: IP local del router
- Gateway puede ser cualquiera
- Gateway IP a la que se dirigen todos los PCs de la red local



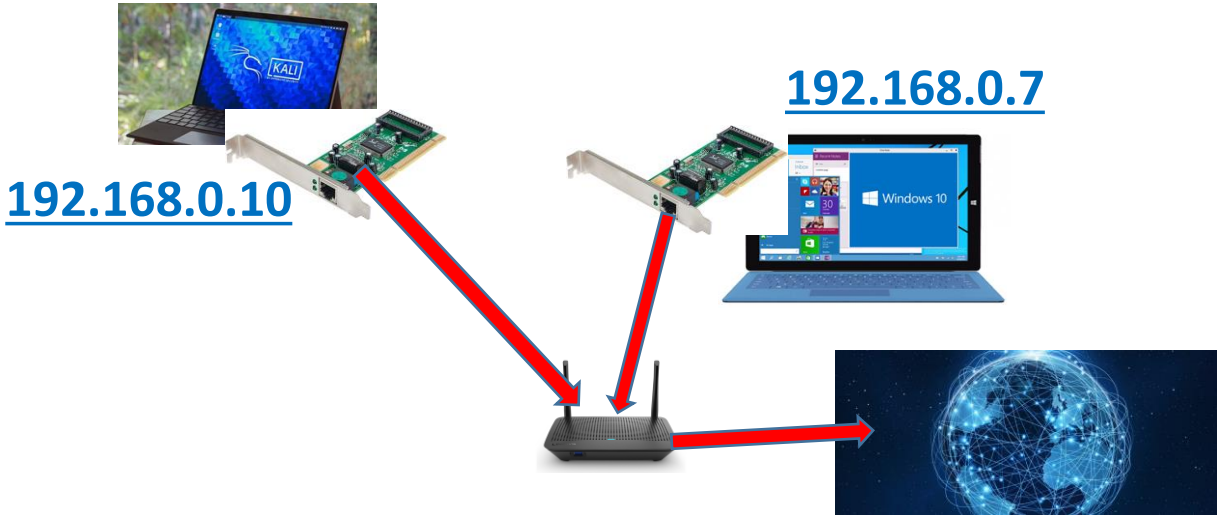
Kali Linux

```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::20c:29ff:feea:9e42  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ea:9e:42  txqueuelen 1000  (Ethernet)
        RX packets 16460  bytes 2346040 (2.2 MiB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 12510  bytes 756460 (738.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Red NAT y Bridge

NAT

- **Usa el adaptador de red del host**
- Se conecta al adaptador físico del host
- Usa un DHCP virtual
- IP asignada por DHCP virtual
- Tiene internet
- En una red distinta a la del host
- Red distinta a la red del host
- Alcanza el host con ping



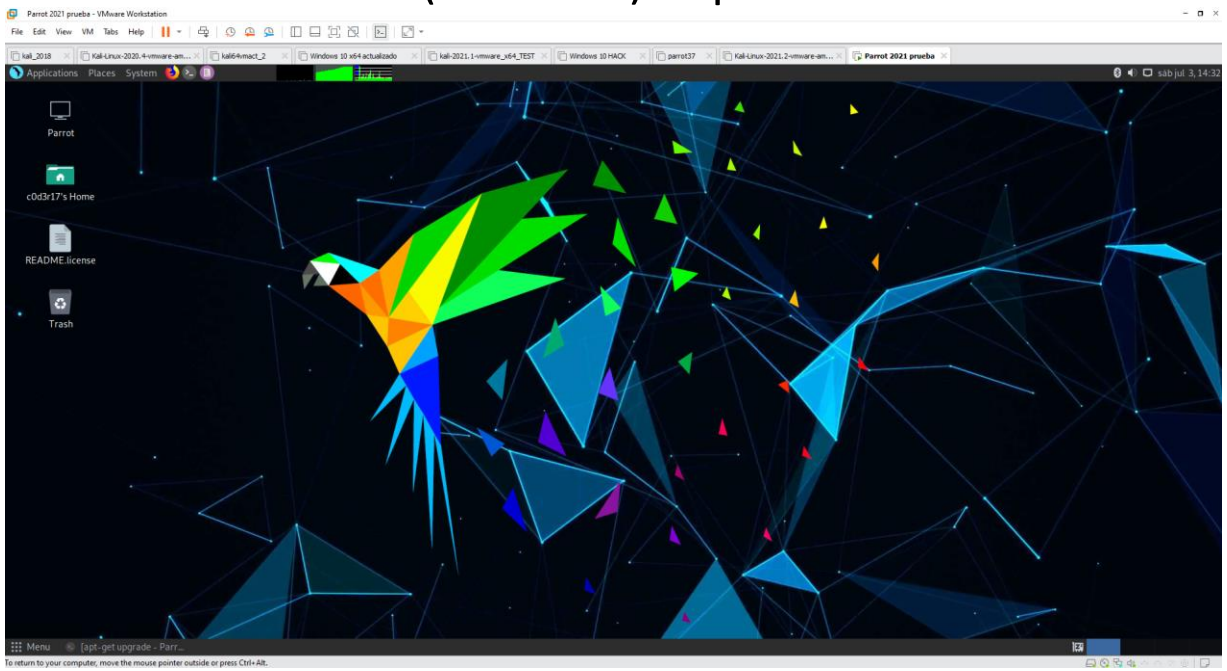
Bridge (adaptador puente)

- Conexión paralela (igual que el host)
- **Usa un adaptador de red virtual**
- Se conecta al router
- Usa el DHCP del router
- DHCP asigna una IP
- En la misma red que el host
- Tiene internet
- Alcanza el host con ping
- Replicar red física: en caso de cambiarse de red reconfigurara automáticamente los cambios

Instalación Parrot

Datos importantes

- https://www.parrotsec.org/download/
- Usar versión security (incluye VMWare tools, guest adittions)
- (VMWare) Replicar red física -> estabilidad con cambio de red



Pasos

1. Descargar imagen
2. Importar imagen
3. Adaptador puente
4. Cambiar contraseña “root”
5. Actualizar repositorios
6. Actualizar sistema
7. IP fija (router o sistema)

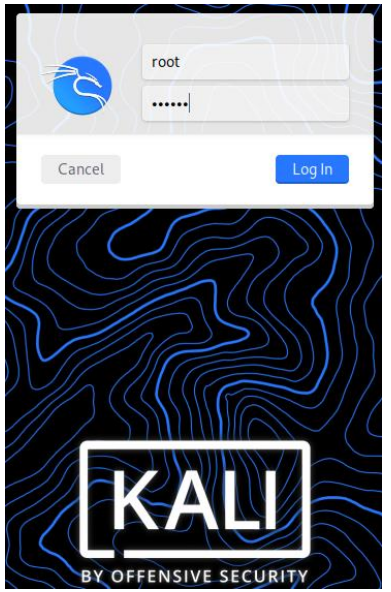
Hardware mínimo

- CPU: 1 núcleo **2 procesador**
- RAM: 1Gb
- HDD: 40 Gb

Hardware recomendado

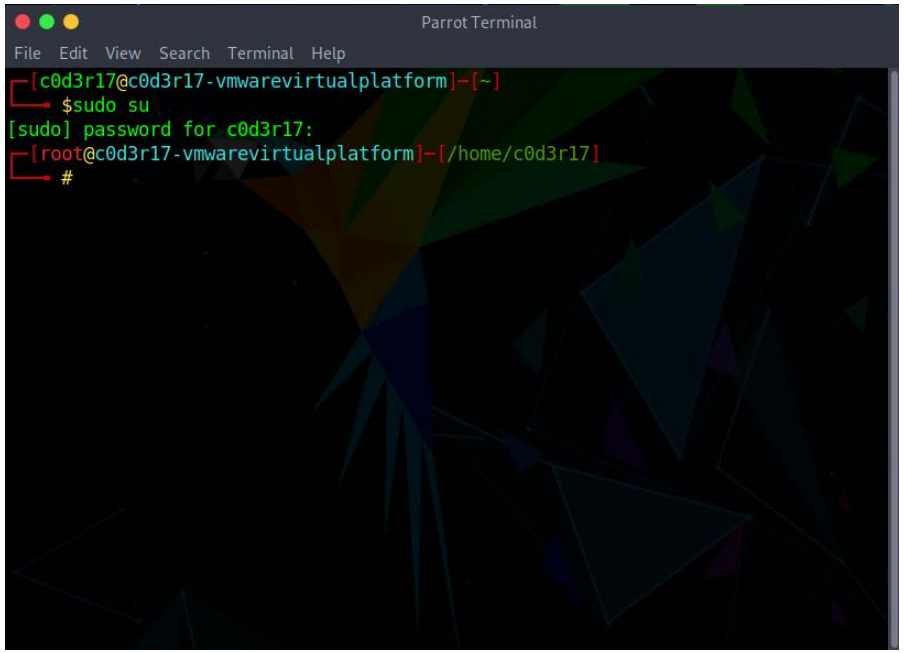
- CPU: 2 núcleos **2 procesadores**
- RAM: 2Gb
- HDD: 80 Gb

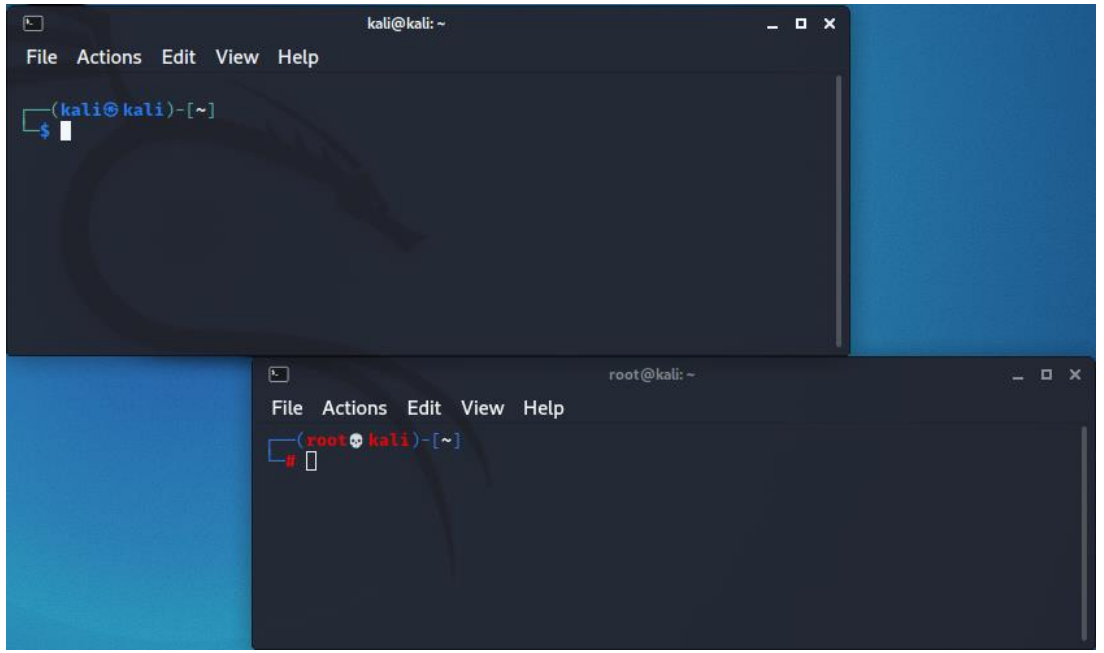
Usuario Root



Datos importante

- Es el usuario del sistema (control total)
- Toda aplicación debe ser instalada con el (apt-get install aplicación)
- Modos de apertura de root (sudo y sudo su)
- Usar aplicación con root (no buena practica pero la mas estable)
- Archivos creados con root no utilizables por otro usuario
- Recomendable login OS con root (mala practica)

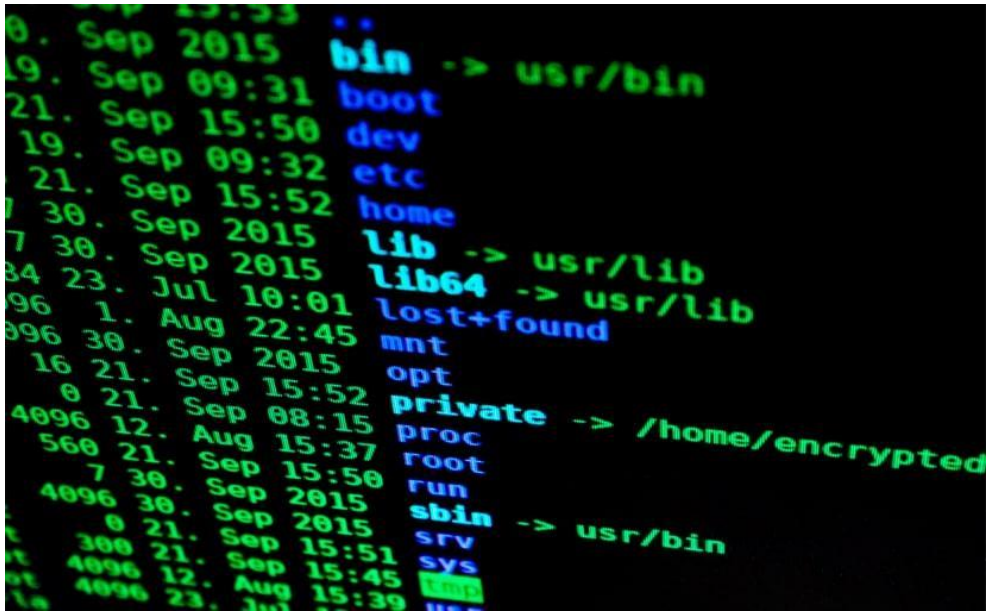




Comandos básicos Linux

Comandos

- Pwd: ver directorio actual
- Ls: listar carpetas y archivos; con mas info (ls -l); ocultos (ls -la)
- Cd: moverse a un directorio (cd /home/kali) (cd ..) (cd /)
- Cp: copiar archivo (cp /home/kali/perro.txt /home/perro.txt)
- Mv: (mv /home/kali/perro.txt /home/perro.txt)
- Rm: (rm /home/perro.txt)
- Mkdir: crear una carpeta (mkdir perro)
- Rmdir: eliminar carpeta (rmdir perro) recursivo (rmdir –rf perro)
- Cat: ver contenido de archivo de texto plano (cat perro.txt)
- Nano: ver/crear/editar archivo de texto plano (nano perro.txt)
- Locate: buscar archivo (locate perro.txt) obviar mayúsculas (locate –i perro.txt)
- Whoami: nombre usuario actual
- Hostname: nombre equipo
- Ifconfig: IPs “información de todas las tarjetas de red”
- Reboot: reiniciar equipo
- Shutdown: apagar equipo (shutdown –h now)
- Ping: comprobar equipo activo (ping 192.168.0.10)
- Uname: información de sistema (uname -a)
- Echo escribir algo dentro de un archivo de texto (echo hola_perro >> gato.txt)



Instalación herramientas

Datos importantes

- Apt-get update (siempre actualizar repositorios)
- Upgrade solo si tiene respaldo
- Instalar siempre con root (sudo)
- (relativo) Dar permisos de ejecución
- (relativo) Requiere servicio de base de datos
- Instalación de otra aplicación puede generar conflicto
- Generar respaldo antes de instalar (snapshot)
- Fijarse en versiones (primero usar la misma del tutorial)
- Replicar OS donde se instalo en el tutorial
- Python versión 2 o 3
- Considera algunas herramientas como compilar exploits según arquitectura de sistema

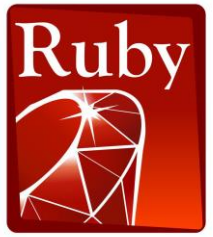
Formas de instalación

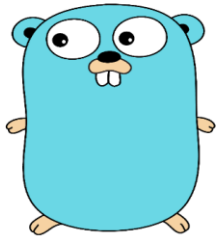
- Apt-get install aplicación
- Clonar proyecto GitHub
- Proyecto de Python, Ruby, Go, etc. (instalar librerías necesarias)
- Instalación común en Windows
- Proyectos en Java (requieren JDK)
- Otros lenguajes de programación (compilación)

PYTHON 2.X  PYTHON 3.X

```
>>> print "Hello World!"
Hello World!
>>> print 3/2
1
>>> variable = 123456789
>>> print (type(variable))
<type 'int'>
```

```
>>> print ("Hello World!")
Hello World!
>>> print (3/2)
1.5
>>> variable = 123456789
>>> print (type(variable))
<class 'int'>
```



GOLANG 

Chmod

Datos importantes

- Dar o quitar permisos a carpetas/archivos
- Se debe seleccionar usuario propietario (u), grupo propietario (g), otros (o) o todos (a)
- Otros se refiere a cualquier otro usuario que interactúe con el archivo
- En caso de trabajar con usuario no root será necesario siempre dar permisos

Usos

- Todos los permisos para todos (chmod a+rwx perro.txt)
- Todos los permisos para usuario (chmod u+rwx perro.txt)
- Leer para otros y eliminar ejecución para usuario (chmod o+r,u-x perro.txt)

Análisis forense

Contenido practico

- Copia del disco
- Recuperar archivos borrados
- Autopsy
- Bulk_extractor

Recuperar archivos borrados

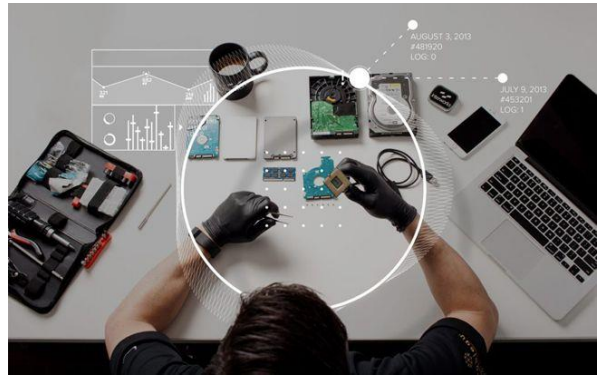
- Herramientas de terminal o graficas
- Linux mas estable con HDD dañado
- Linux mejor recuperación de archivos

Autopsy

- Análisis de archivos (incluso borrados)
- Metadatos
- Ver archivos borrados
- Buscar palabras
- Tipos de archivos

Copia del disco

- Formatos mas compatibles “dd” y “raw”
- Noerror: HDD con errores usar dd
- Sync: llenar errores con null (ceros)



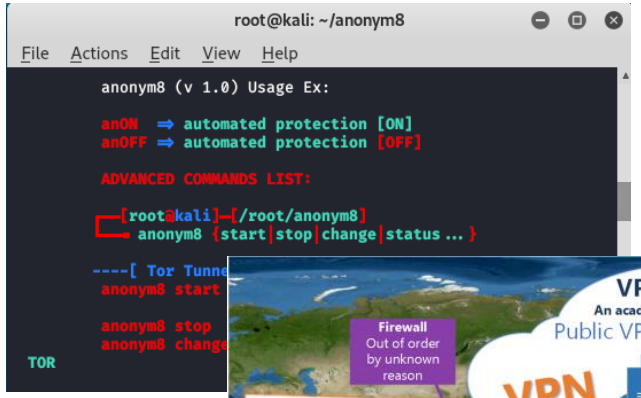
Datos importantes

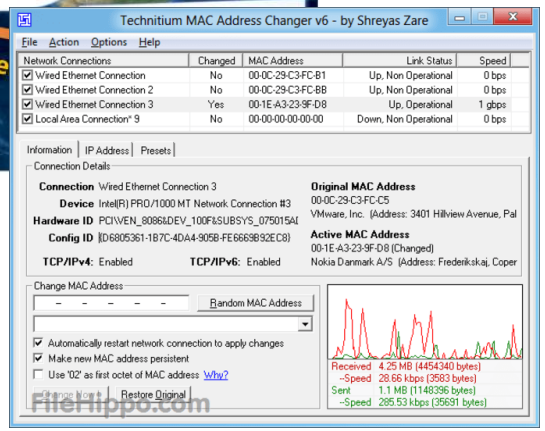
- Se necesita espacio en disco duro
- Recuperar archivos no significa que sigan siendo útiles
- Recuerda que los archivos solo se borran cuando se sobre escribe
- Puedes usar muchos programas para realizar análisis forense, sin embargo algunos son pagados
- Autopsy es muy potente y es gratis, recomendado
- Truecrypt te permite ocultar y encriptar la información

Anonimato

Contenido practico

- Cambio de IP publica (VPN)
- Cambio MAC
- Tor y proxychains
- Anonym8
- Anonimato payloads (área payloads y exploits)





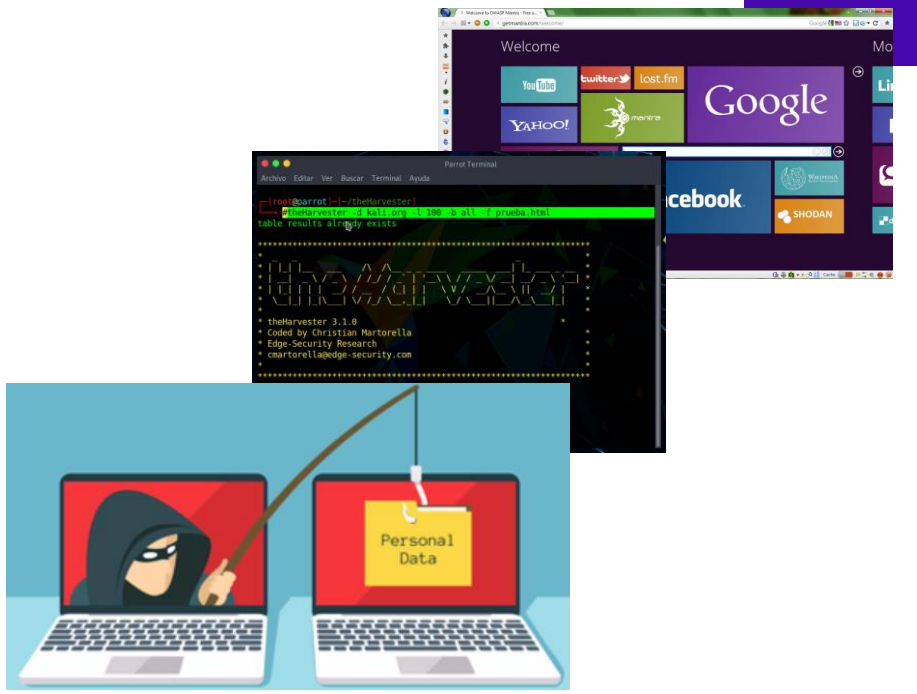
Datos importantes

- Las VPN son proxys (nodos de conexión)
- La MAC esta asociada a cada adaptador de red
- El anonimato puede ser exclusivo de una aplicación o de todo el sistema
- Conexiones lentas e inestables
- Usar nodos del mismo país del objetivo (puede haber bloqueos)

Reconocimiento 1

Contenido practico “Fingerprinting pasivo”

- Whois (info para ingeniería social)
- Traceroute (saltos desde IP origen a destino)
- Ip address and domain information (Firefox) (info servidor)
- Wappalyzer (Firefox) (info pagina web)
- Owasp mantra (info pagina web y servidor) (inestable)
- The harvester (subdominios, correos y mas)
- (a y p)Whatweb (servidor web y tecnologías de programación) (área hacking web “HW”)
- (activo) Wafw00f (validar servidor detrás de firewall) (falsos positivos)
- (activo) Dirb (busca directorios por fuerza bruta) (HW)
- Foca (buscar archivos dentro de un dominio y extraer metadatos) (HW)
- app.snov.io (correos, tecnologías, personas y mas)
- Ping (determinar quipo activo)



Datos importantes

- Recabar IPs publicas para su posterior escaneo
- Tecnologías usadas para la búsqueda de exploits
- Paginas con la misma IP (dentro del mismo servidor)
- Sistema operativo del servidor o equipos usados
- Metadatos desde archivos (OS, usuarios, correos, etc.)
- Correos para Phishing
- Puertos y servicios para buscar exploits

Puertos locales

Datos importantes

- Puertas para conectarse al equipo
- Puertos asociadas a servicios
- SSH, FTP, web http, web https, etc.
- Ejemplo SSH Windows a Linux
- Ver puertos (netstat -antp)

```
kali@kali: ~
C:\Users\tic433>ssh 192.168.0.10 -l kali
kali@192.168.0.10's password:
Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jul  5 15:59:06 2021 from 192.168.0.7
┌─(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ▯ https://www.kali.org/docs/general-use/python3-transition/
│
└─(Run: “touch ~/.hushlogin” to hide this message)
┌──(kali▯ kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali▯ kali)-[~]
└─$
```

SSH

- Shell remota
- Linux y Mac
- Puerto 22
- Conexión desde otros OS
- putty

Puerto	Servicio
21	FTP
22	SSH
80	HTTP
443	HTTPS

cmd
192.168.0.7

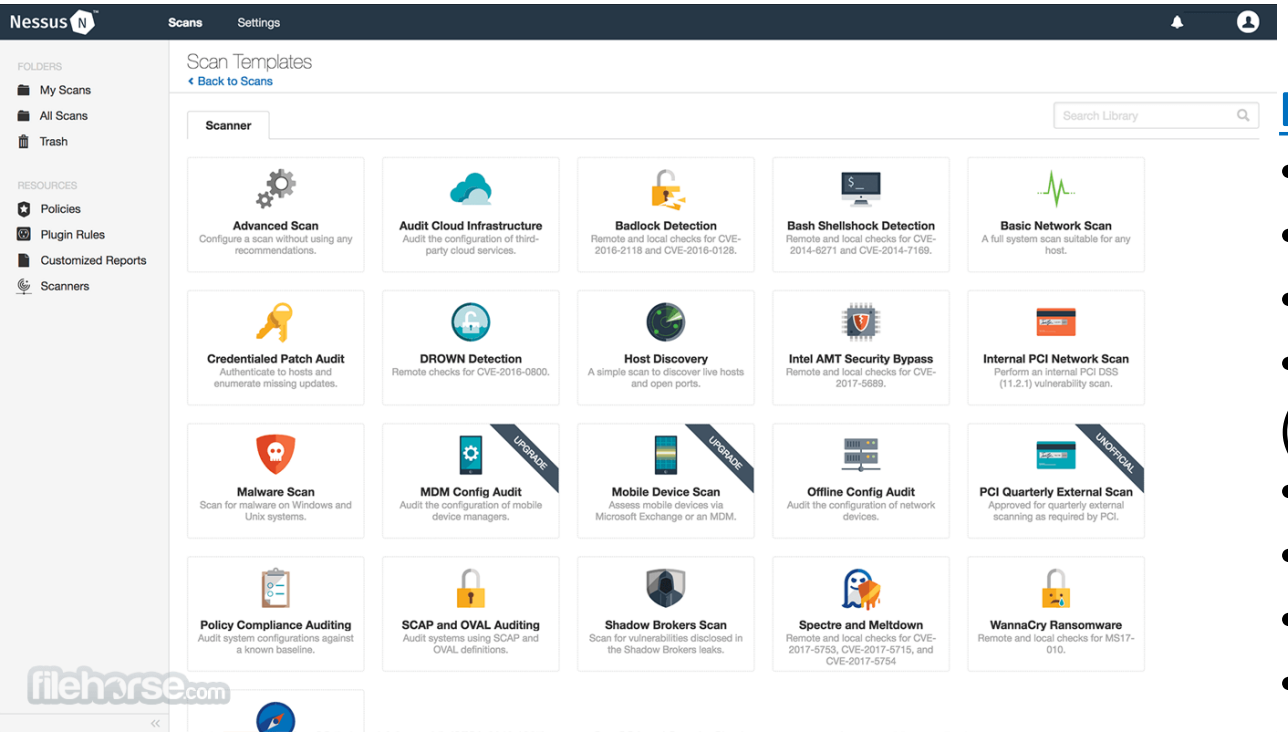
SSh
192.168.0.10:22

Reconocimiento 2

Contenido practico “Footprinting”

- Nmap “escaneo” (puertos abiertos, servicios, OS, etc.)
- Proceso de explotación con exploits (área payloads y exploits)
- Nessus (escaneo host y/o web) (área payloads y exploits)

```
┌──(root💀kali)-[~]
└─# nmap -v -O 192.168.0.10
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-08 14:33 EDT
Initiating Parallel DNS resolution of 1 host. at 14:33
Completed Parallel DNS resolution of 1 host. at 14:33, 0.03s elapsed
Initiating SYN Stealth Scan at 14:33
Scanning 192.168.0.10 [1000 ports]
Discovered open port 22/tcp on 192.168.0.10
Discovered open port 80/tcp on 192.168.0.10
Completed SYN Stealth Scan at 14:33, 0.08s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.000037s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Device type: general purpose
Running: Linux 2.6.X
```



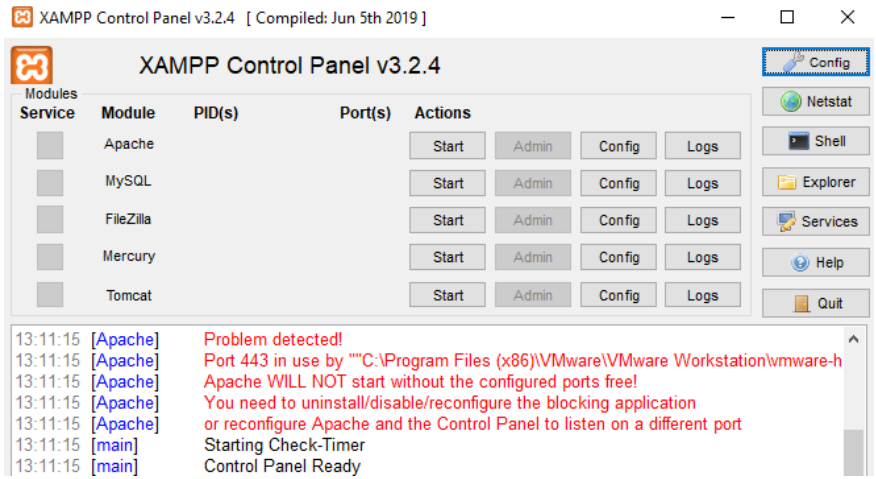
Datos importantes

- Puertos y servicios para buscar exploits
- Puertos no correspondientes a los servicios por default
- Escaneos pueden traer falsos positivos
- Escaneos comprenden falsos negativos

(vulnerabilidades no detectadas)

- Validar siempre con mas de un escáner
- Si no se puede validar la explotación, entonces
- validar la configuración o versión vulnerable
- Escáner se puede tomar como base de auditoria

Servidor web



Contenido practico

- Xampp o Wamp (multiplataforma)
- Apache2 (Linux)
- Python (multiplataforma)

```
┌──(root💀kali)-[~]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apa
     Active: active (running) since Wed 202
       Docs: https://httpd.apache.org/docs/
```

Xampp o Wamp

- Incluye programas adicionales (BD, FTP, etc.)
- Fácil uso e instalación
- Puede ser portable
- Estable para una pagina web
- Tiene servidor https

Apache2

- Incluido en kali
- No tiene https
- Fácil ejecución
- Inestable para una pagina web
- Útil para explotación ya que esta incluido

```
┌──(root💀kali)-[~/Documents/anonimato]
└─# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
127.0.0.1 - - [28/Jul/2021 13:50:00] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [28/Jul/2021 13:50:00] code 404, message File not found
127.0.0.1 - - [28/Jul/2021 13:50:00] "GET /favicon.ico HTTP/1.1" 404 -
```

Datos importantes

- Escoger la versión de PHP adecuada
- Uso mayoritario en hacking web
- Fácil traspaso de archivos

Python

- Incluido en kali tanto versión 2.7 y 3
- Sencillo y muy usado en explotaciones
- Compatible con muchas explotaciones
- Fácil de habilitar
- Permite fácil elección de puerto
- Muy incompatible con paginas web
- No tiene https

Hacking web

Contenido practico

- WhatWeb (información servidor y tecnologías de construcción de la pagina web) (área reconocimiento “AR”)
- DVWA (plataforma de practicas)
- XSS
- SQL Injection
- Sqlmap
- Burp suite
- File upload
- Nikto (escaneo vulnerabilidades web) (AR)
- OWASP ZAP (escaneo vulnerabilidades web) (AR)

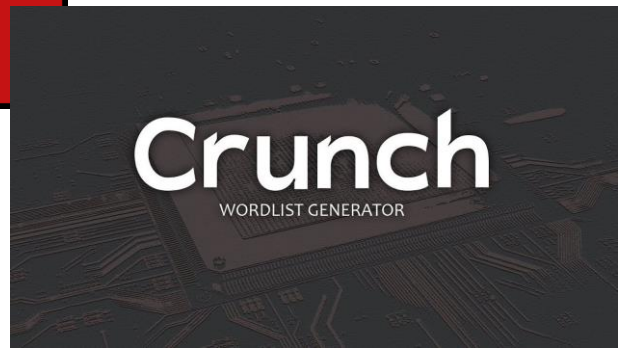
Datos importantes

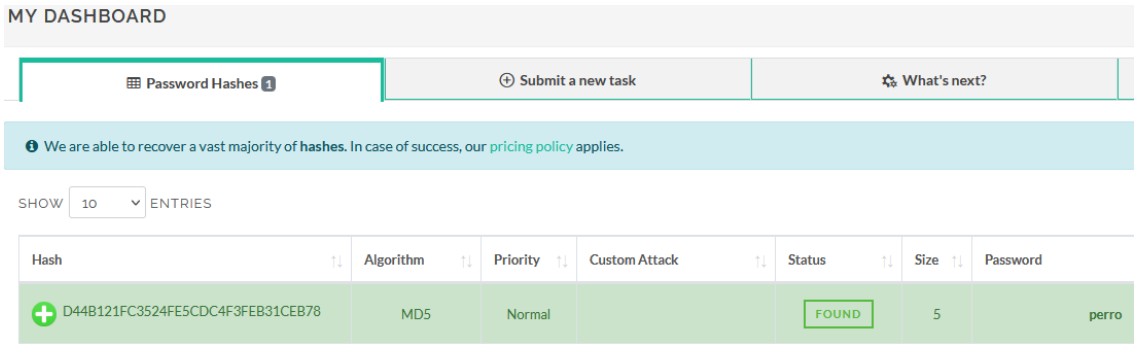
- Escaneo al índex o a links específicos
- Falsos positivos descarte ejecución manual
- Explotación puede involucrar mas de una vulnerabilidad
- Explotación requiere probar muchos payloads, es mejor automatizar
- Burp suite y OWASP ZAP tienen múltiples herramientas
- Explotar pagina web desde otra menos vulnerable, alojada en el mismo servidor
- Relativo al lenguaje de programación de la pagina
- Relativo al motor de base de datos
- Relativo al sistema operativo

Encriptación

Contenido practico

- Identificar formato hash
- Jhon the ripper
- Cracking online
- Diccionarios
- Hashcat
- Encriptar payloads
- Volcado de hashes Windows (área post explotación)
- Crackear hashes Windows
- Encriptar payloads (área payloads)





Datos importantes

- El éxito depende del diccionario
- El problema es solo el tiempo
- Escoge diccionarios en tu idioma
- Hashcat es muy rápido utilizando la GPU
- La identificación del hash no es exacta
- Los hashes pueden ser usados para logearse (pass the hash)
- Encriptar un payload no es eterno ni evade todos los AV

Payloads y exploits 1

Contenido practico

- Metasploit
- Netcat
- Rat
- Bypass antivirus

Rat

- Fácil construcción de payloads
- Fácil post explotación
- Se queman muy rápidos
- Manejo por interfaz grafica
- Muy recomendado para la explotación

Payloads

- Código malicioso que realiza la explotación en el objetivo
- También conocido como carga útil
- Un payload también es un código de explotación de hacking web
- Generados en distintos lenguajes

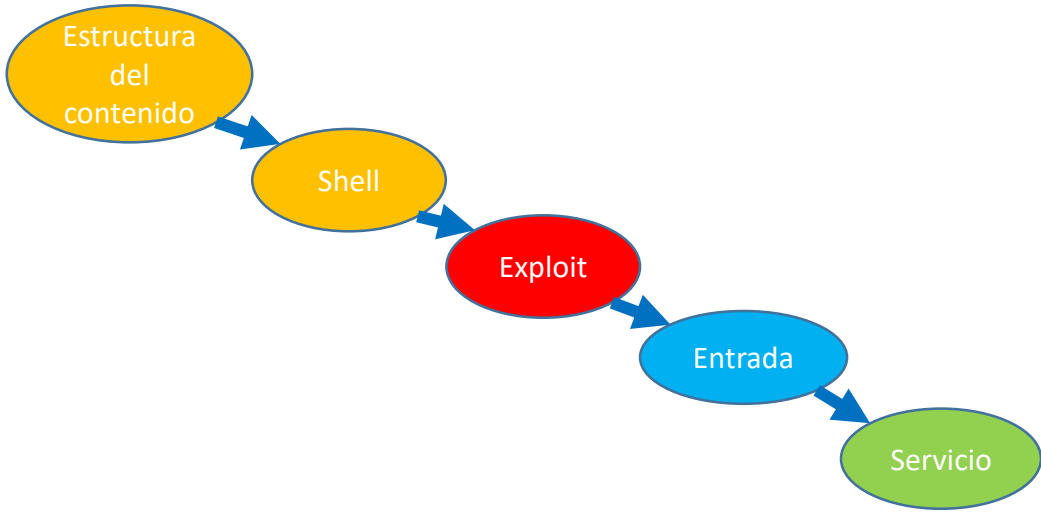
Bypass antivirus

- Crypter no compatible con todos los payloads
- Crypter requiere archivos ocx (usar ronda ocx)
- Crypter genera payload en código o ejecutable
- Modificación hexadecimal “MH” aplicar a anotador
- Crypter incompatible con anotador
- Escaneo en laboratorio real con AV (sin internet)
- MH bypass por mayor tiempo
- MH proceso tedioso, pero efectivo
- MH hace mas lenta la conexión del payload
- Usar escáner que no envié firmas

Payloads y exploits 2

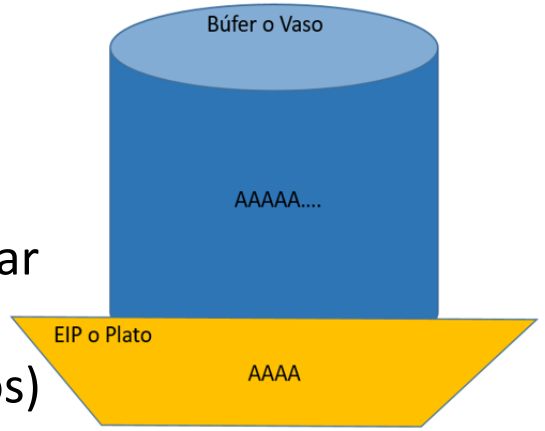
Contenido practico

- Exploits Metasploit
- Proceso de explotación con Exploit
- Construcción Exploit local (área ensamblador y reversing)
- Construcción Exploit remoto (área ensamblador y reversing)
- Pivoting (área post explotación)



Exploits

- Puerta de acceso al sistema (ejecución de comandos)
- Son muy inestables, especialmente de buffer overflow
- Siempre requiere un payload
- Puede ser local o remoto
- Especifico de programa y versión (versiones)
- Requiere 1 o mas parámetros
- Parámetros pueden ser necesario cambiar para dar mayor estabilidad
- Escritos en diversos lenguajes (Python, Ruby, otros)



Datos importantes

- Nombre servicio
- Versión servicio
- Sistema operativo
- Kernel
- Arquitectura

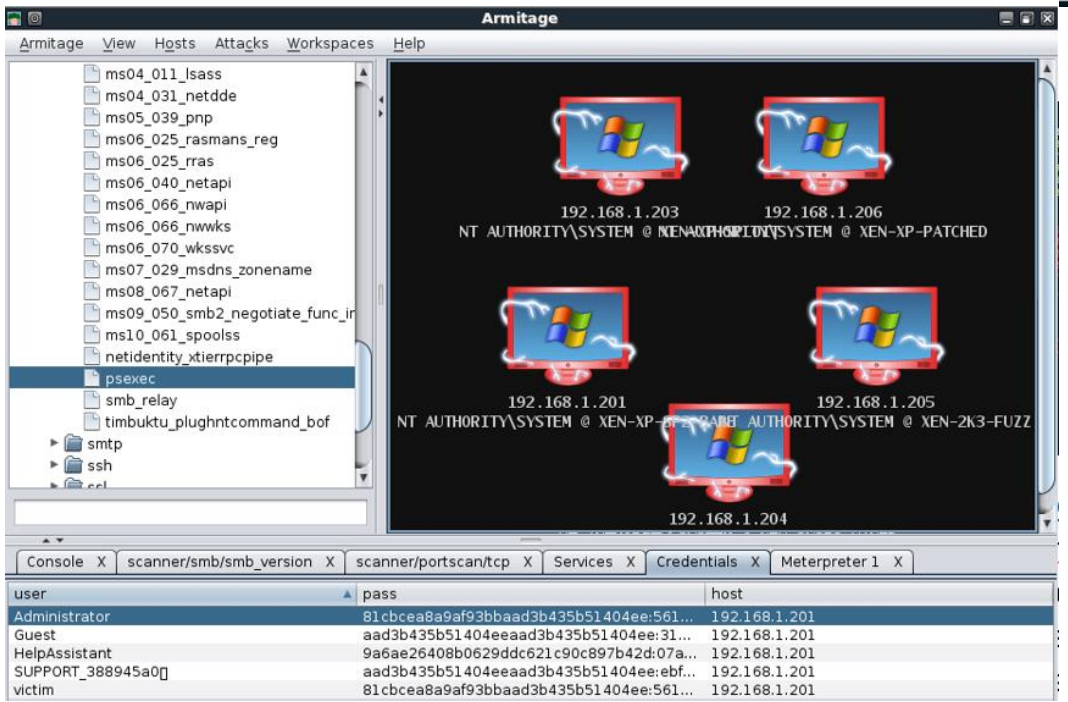
Paginas exploits

- https://www.rapid7.com/db/
- https://www.exploit-db.com/
- https://0day.today/

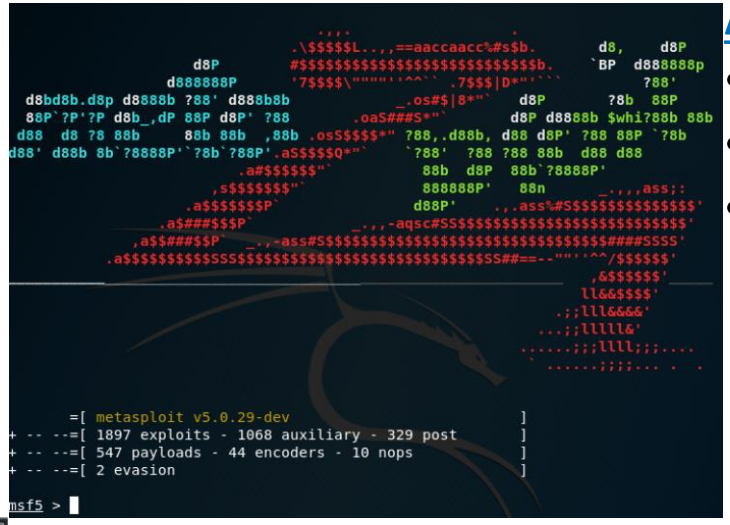
Metasploit

Componentes

- Payloads: carga útil (conexión remota)
- Exploit: puerta de acceso al sistema
- Auxiliary: escáner de vulnerabilidad, DOS, etc.
- Post: explotación posterior, cámara, micrófono, archivos, etc.
- Encoders: ofuscar payloads
- Nops: parar generar exploits
- Armitage (área post explotación)



Al ejecutar por primera vez



- Service postgresql start
- Msfdb init
- Msfconsole

Datos importantes

- Excelente framework de aprendizaje de entorno de explotación (muy completo)
- Selección de sistema operativo
- Selección de arquitectura
- Selección de servicio y versión
- Uso de sus herramientas para múltiples ataques
- Manejo de sesiones como botnet
- Manejo de pivoting
- Entorno grafico (Armitage)

Payloads Metasploit

Contenido practico

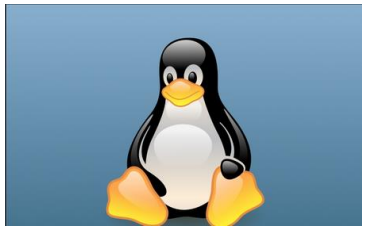
- Crear payload Windows y conexión
- Crear payload Linux y conexión
- Crear payload Mac y conexión
- Crear payload Android y conexión
- Shell, meterpreter y Powershell
- Conexión directa e inversa
- Staged y no staged
- Dentro y fuera de red local (red publica)
- Shell to meterpreter y Exploit -j

Shell, Powershell y meterpreter

- M: fácil post explotación
- M:mas detectado por AV
- S: sirve para todos los OS
- S: pesa menos (exploit)
- M: permite background
- S: background inicial
- P: fácil salto a Metasploit
- P: buena post explotación

Exploit -j

- Handler en segundo plano
- Permite botnet
- Mejor si hay inestabilidad de conexión



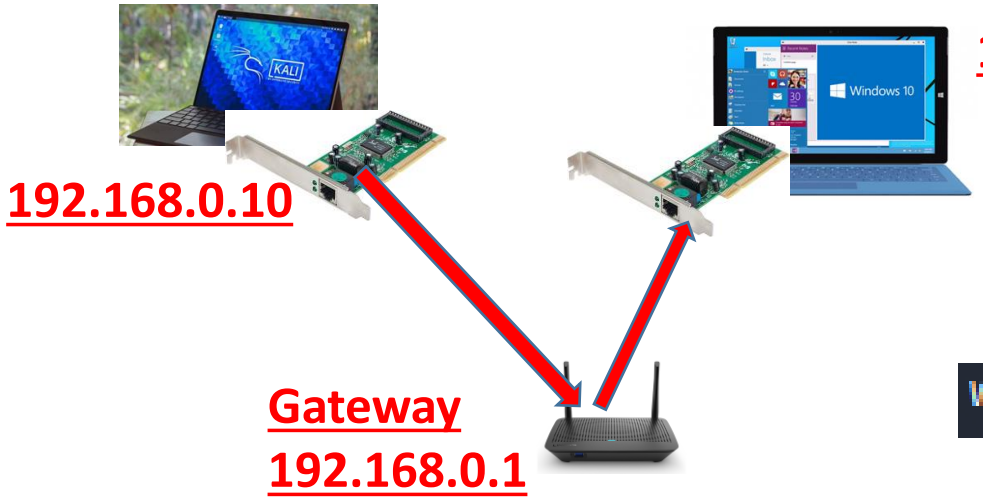
Staged y no staged

- S: evita que la carga útil sea capturada por el AV
- N: permite una ejecución directa
- N: utilizar preferentemente en pivoting
- S: bueno para bypass de AV

```
[*] Started reverse TCP handler on 192.168.0.10:4444
msf6 exploit(multi/handler) > [*] Meterpreter session 1 opened (192.168.0.10:4444 → 192.168.0.7:57781) at 2021-08-04 00:37:51 -0400
```

```
msf6 exploit(multi/handler) > [*] Sending stage (200262 bytes) to 192.168.0.7
[*] Meterpreter session 1 opened (192.168.0.10:4444 → 192.168.0.7:59668) at 2021-08-04 00:40:41 -0400
```

Conexión directa



192.168.0.10

192.168.0.7:4444

Gateway
192.168.0.1

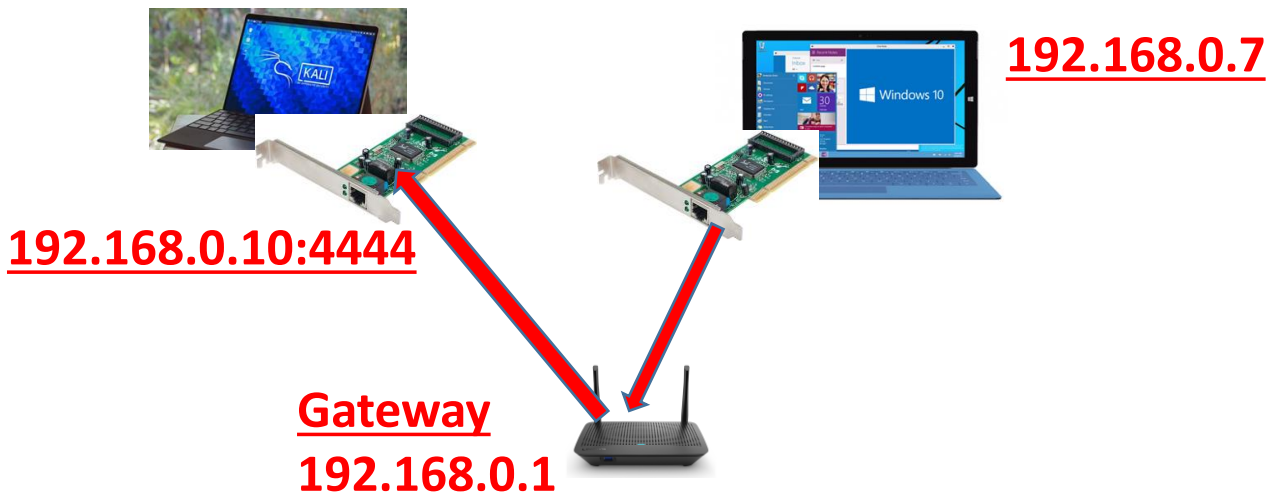
```
windows/x64/meterpreter/bind_tcp
```

Datos importantes

- El mas básico, no tan usado
- Ideal para pivoting
- Malo contra sistemas de seguridad (firewall IDS IPS)
- Bueno para establecer como puerta trasera
- Puede ser Shell o meterpreter

Conexión inversa

Red local

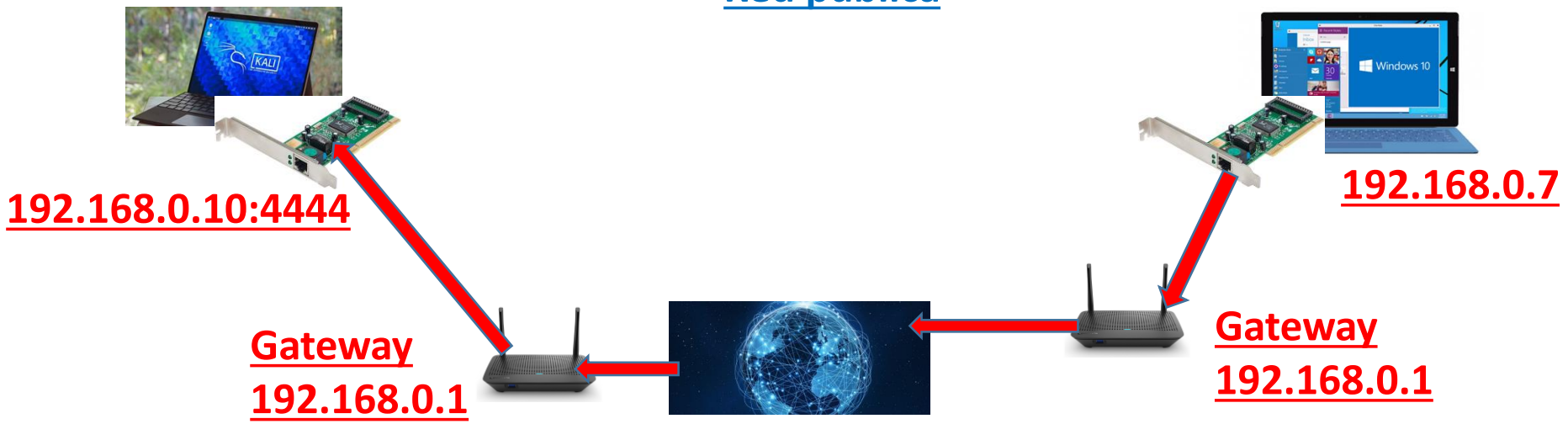



```
windows/x64/shell/reverse_tcp
```

Datos importantes

- El mas usado (no solo en Metasploit)
- Complejo para pivoting
- Bueno evasión de seguridad (firewall IDS IPS)
- Puede ser Shell, meterpreter u otros

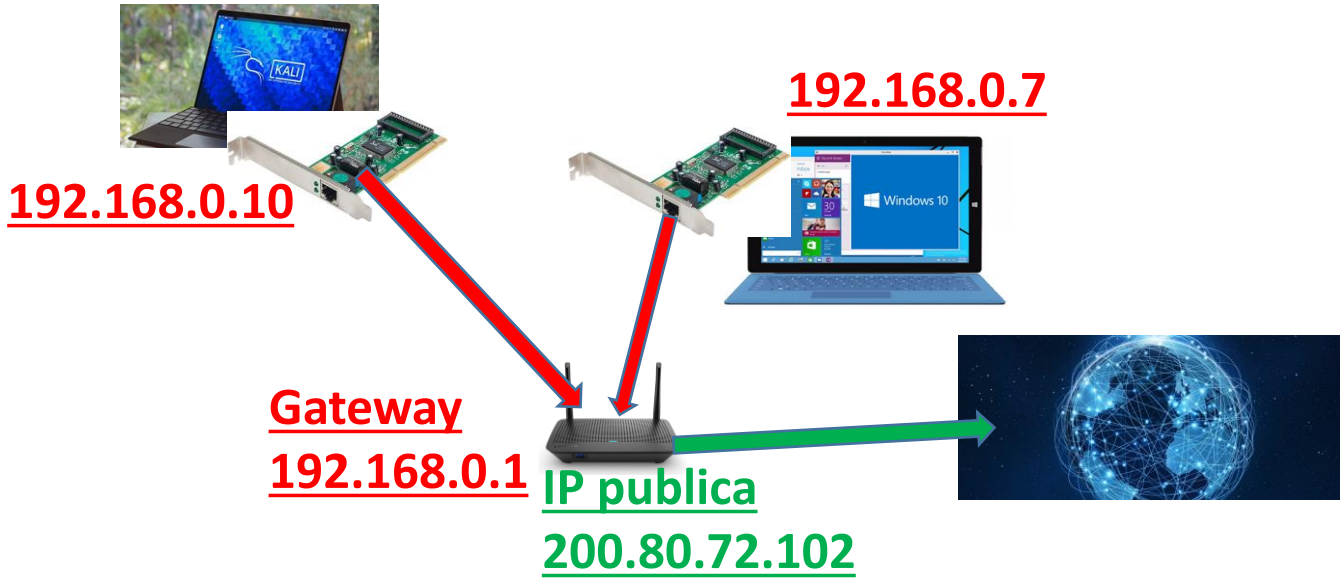
Red publica



IP publica

Datos importantes

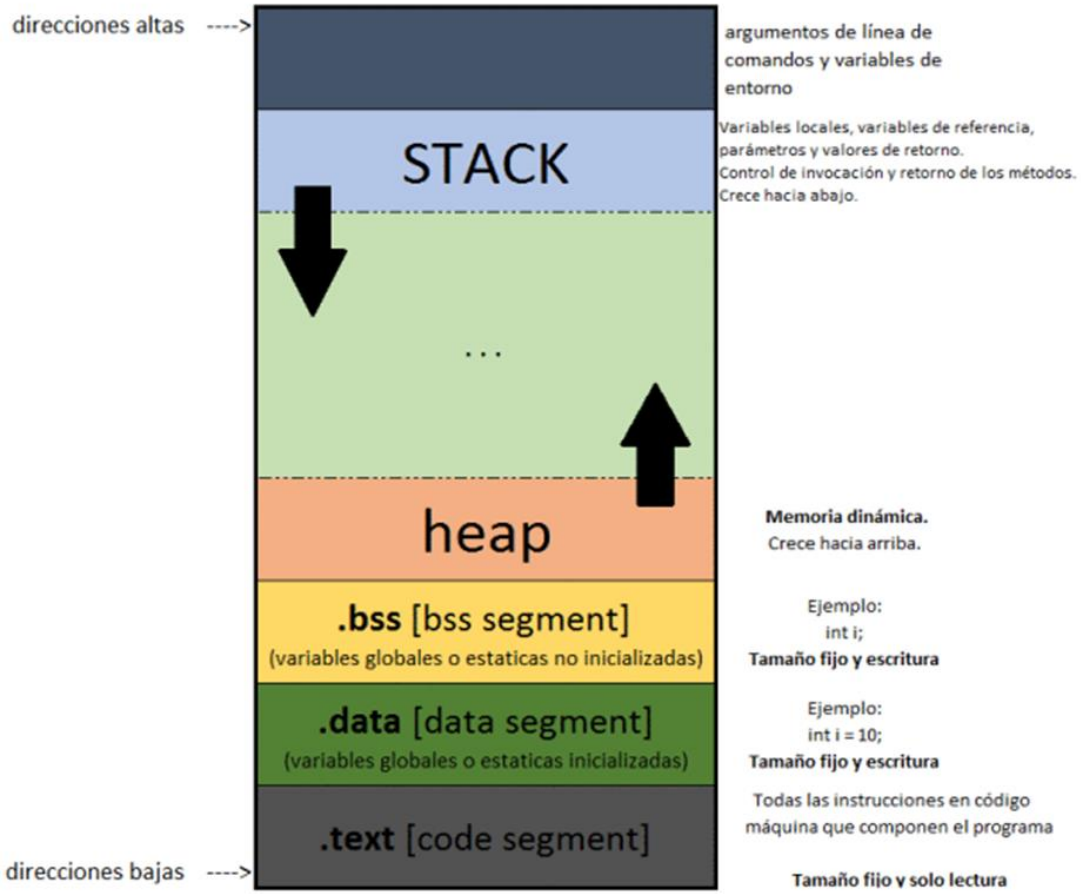
- IP con la que salimos a internet
- IP de conexión entre routers
- Como un numero de teléfono
- IP de conexión a nuestra red
- Puede cambiar
- Se puede geolocalizar (no exacta)
- https://www.adslayuda.com/geolocalizacion.html
- Anonimato sobre la IP publica



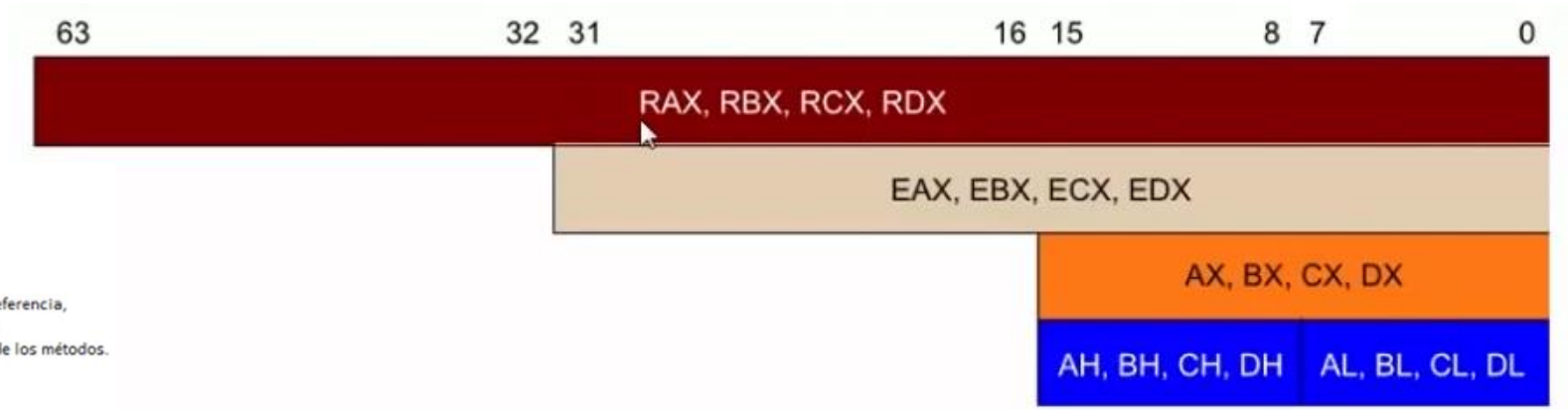
Ensamblador y reversing

Contenido practico

- Buffer overflow
- Construcción Exploit local
- Construcción Exploit remoto



Arquitectura CPU 16; 32 y 64 bits



Datos importantes

- Depende de la arquitectura
- Buffer overflow puede ser de stack o heap
- Cada Exploit puede tener una estructura de comunicación o formato de paquete de datos
- Exploit local, requiere ingeniería social
- Exploit remoto, requiere de conexión al servicio
- Buffer overflow puede presentar inestabilidad
- Buffer overflow puede generar DOS

Buffer Overflow

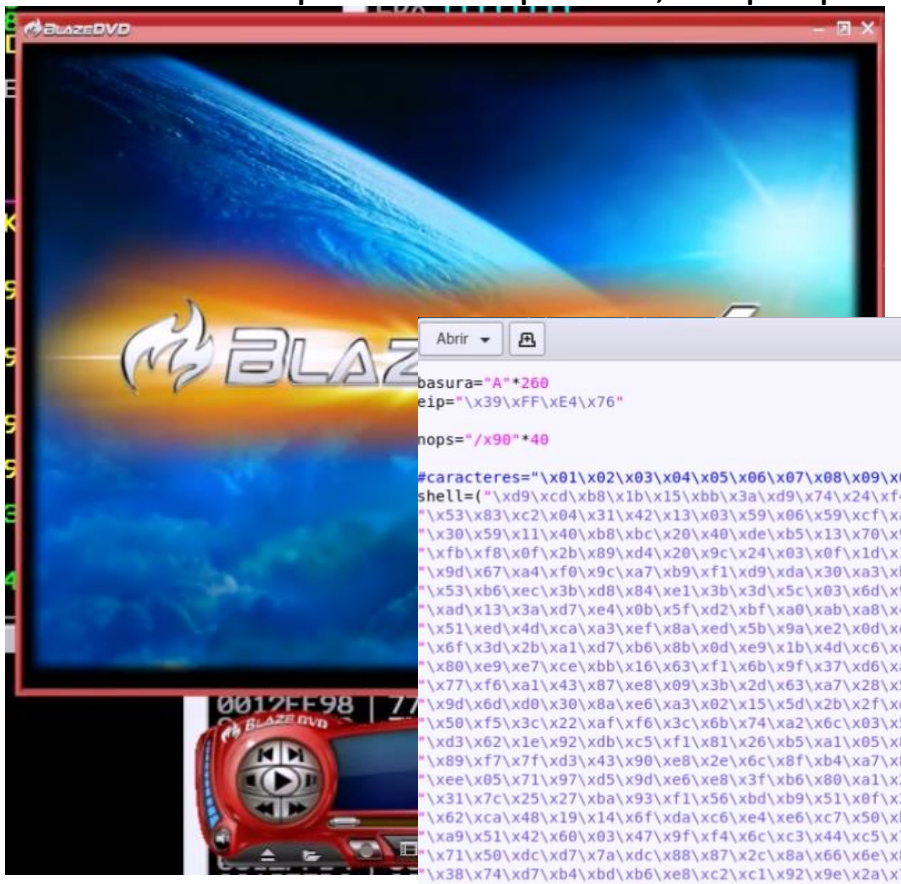
Buffer Overflow o desbordamiento de búfer, en palabras sencillas es un error causado por un defecto en la programación de una aplicación. Cada programa requiere del ingreso de datos por parte del usuario y con él se ejecuta alguna función. La problemática se genera cuando se ingresan datos con un tamaño superior al esperado, lo que provoca que una parte de estos sobre escriban espacios adyacentes de la memoria.

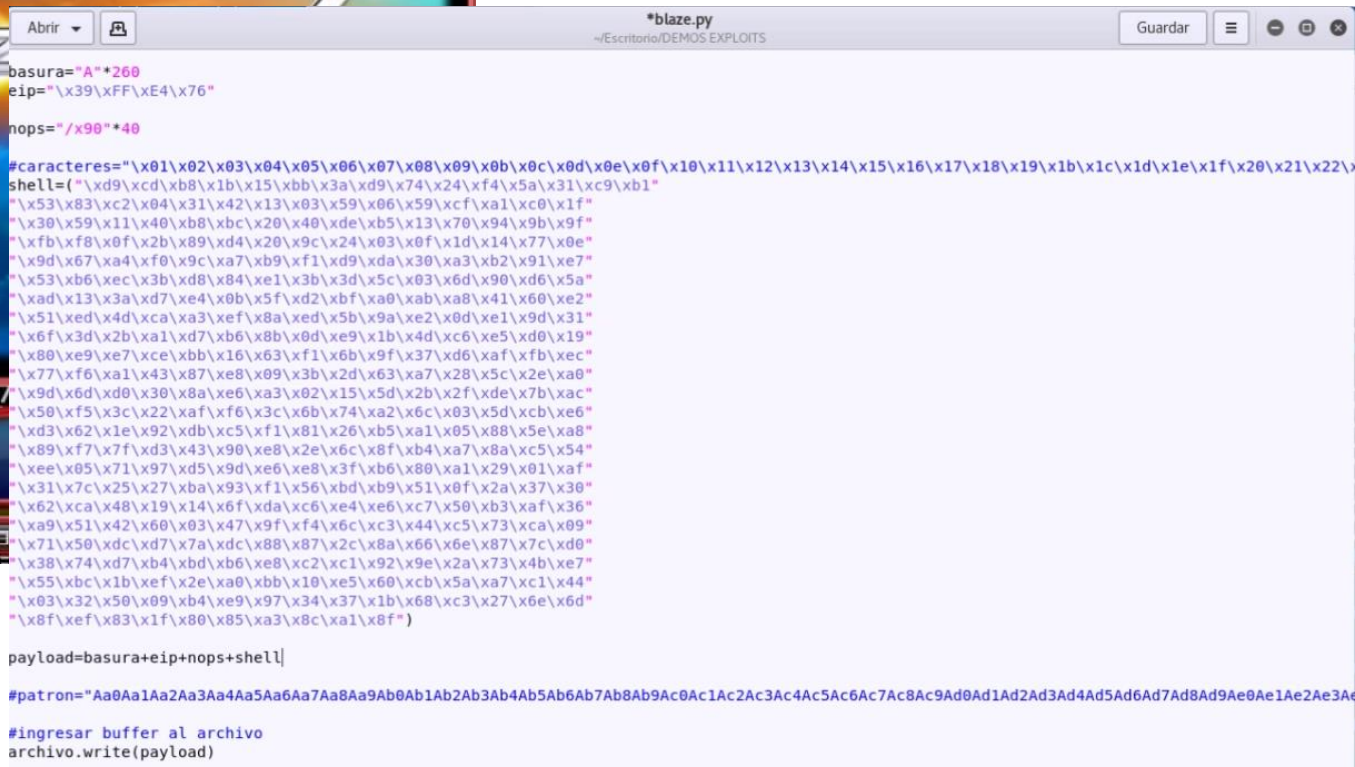
Importante

- Ejemplo ingresar RUT
- Stack (pila) o Heap (dinámica).
- Stack Buffer Overflow.
- Entradas, local o remota.

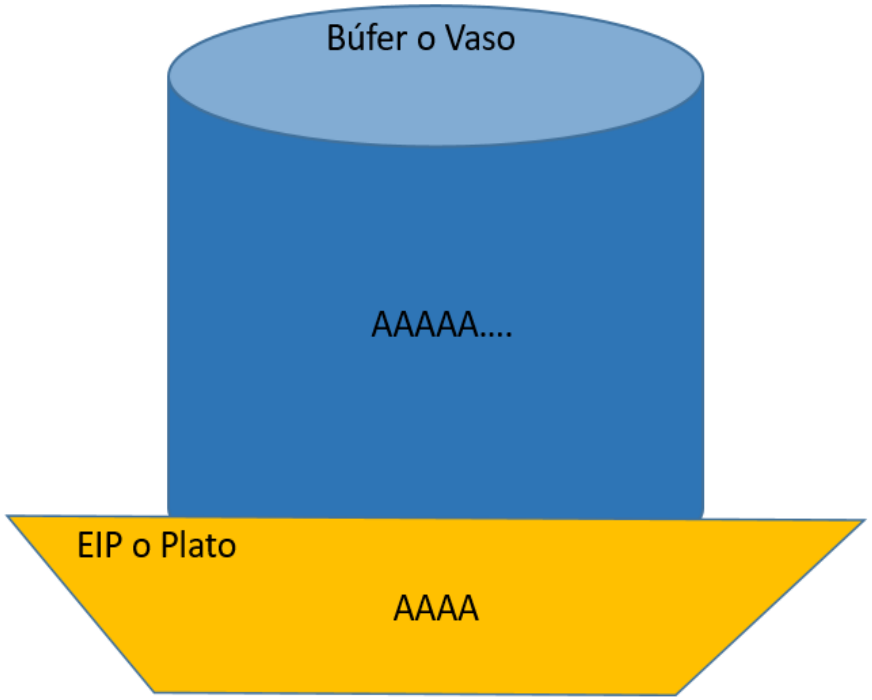
Ejemplos Exploit Stack Buffer Overflow

- Netapi (Windows XP).
- Eternalblue (Windows 7).
- FTPshell Client (conexión remota).
- Exploit BlazeDVD (lista de películas “plf”).



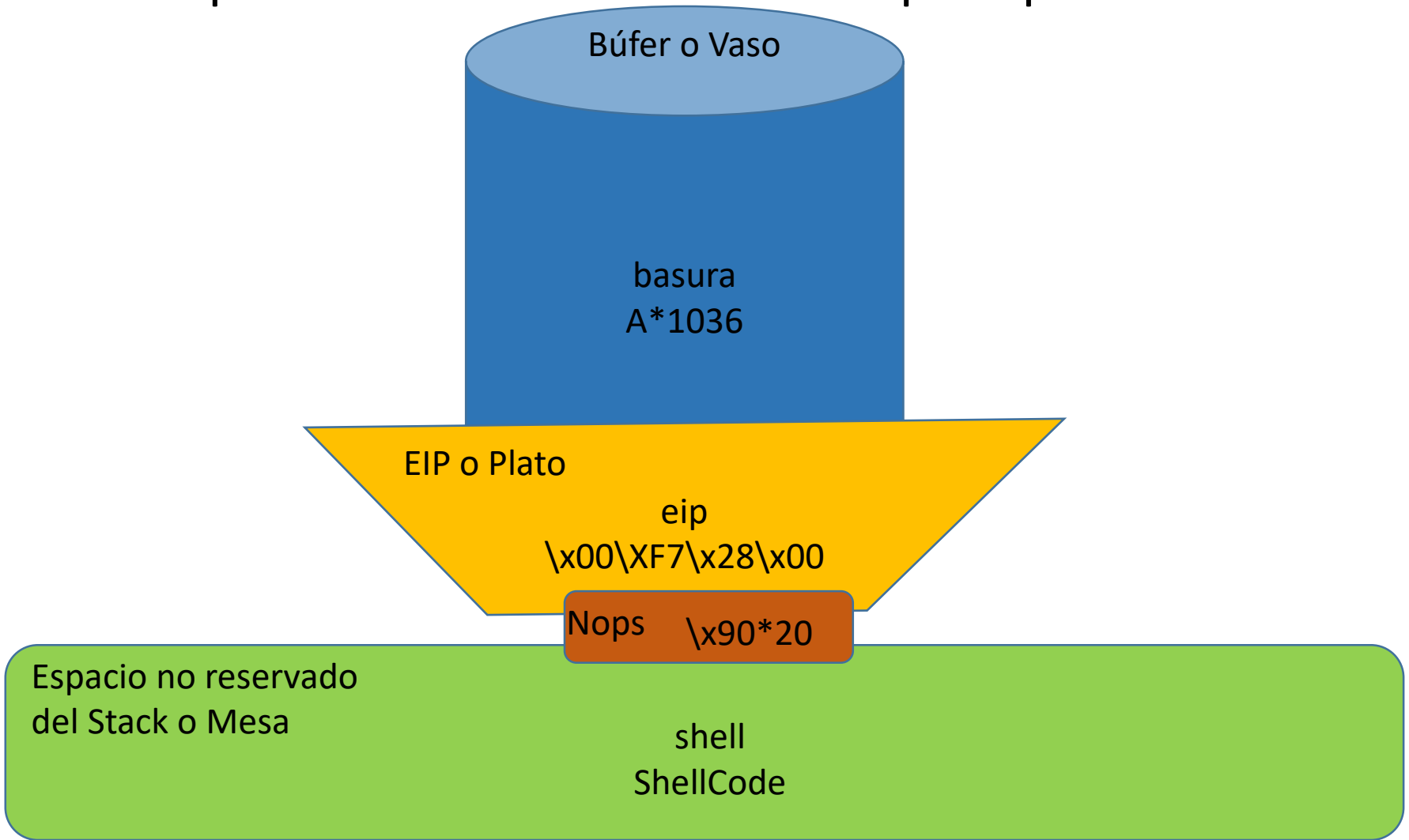


Analogía del vaso de agua



Analogía del vaso de agua (Estructura normal)

Explotación Normal= basura+eip+nops+shell



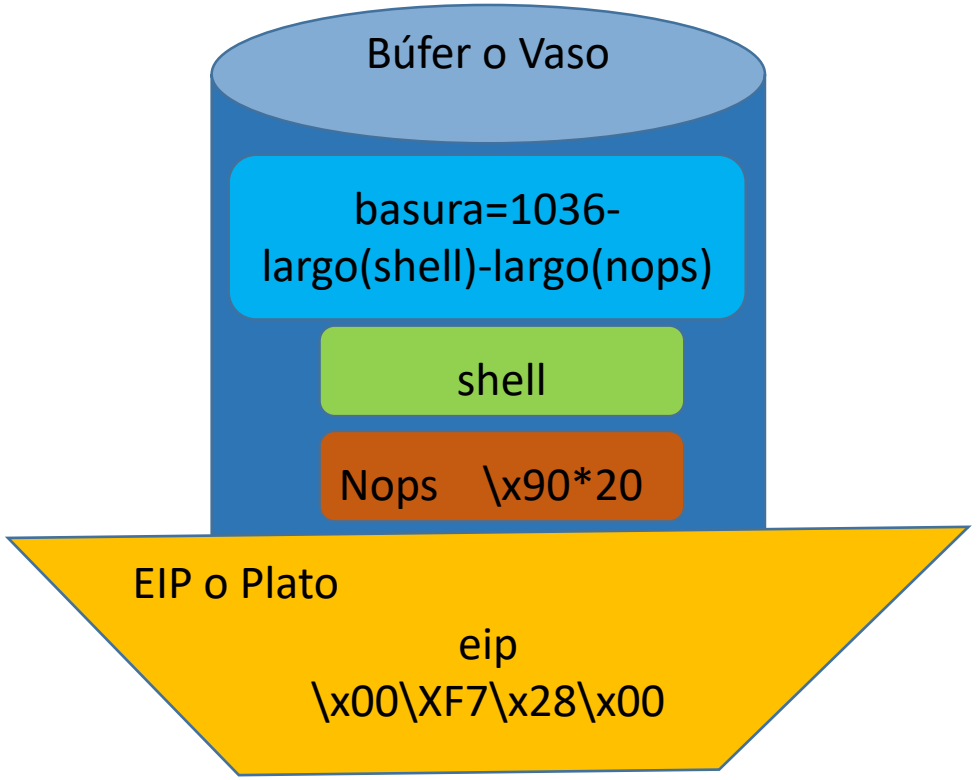
Analogía del vaso de agua (Estructura reversa)

Explotación Reversa= nops+shell+basura+eip

basura
A*628
basura=1036-largo(shell)-largo(nops)

shell (328)
ShellCode

nops
\x90*20

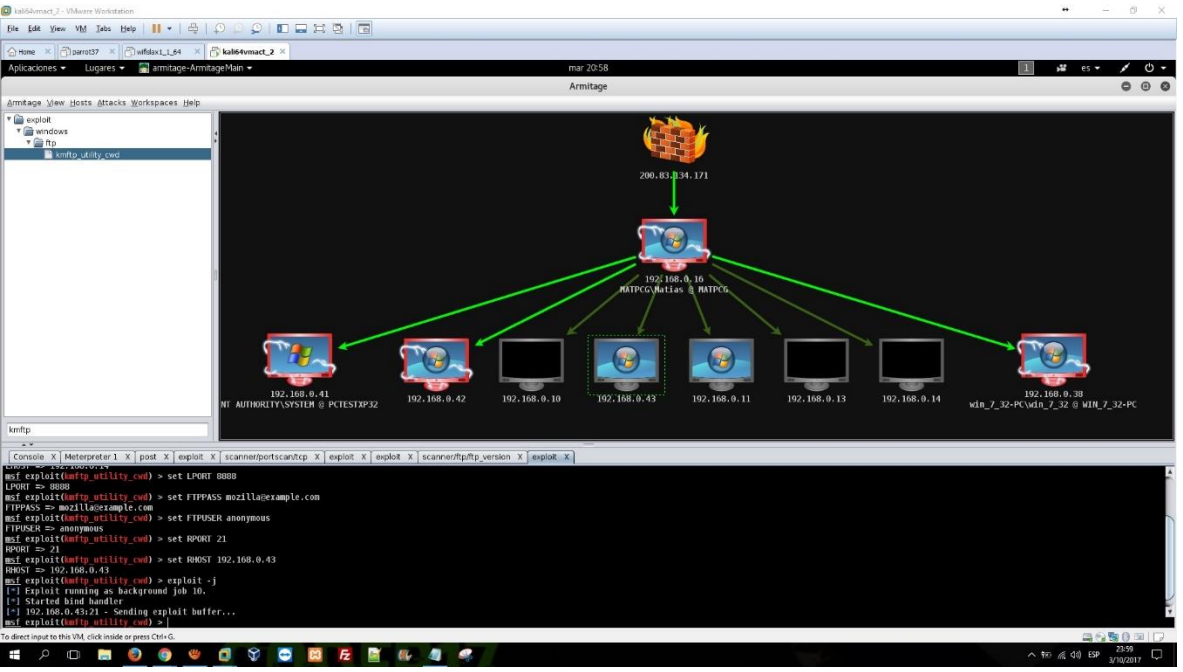


Espacio no reservado
del Stack o Mesa

Post explotación

Contenido practico

- Volcado de hashes Windows
- Pivoting
- Diversión
- Archivos
- Persistencia
- Escala de privilegios



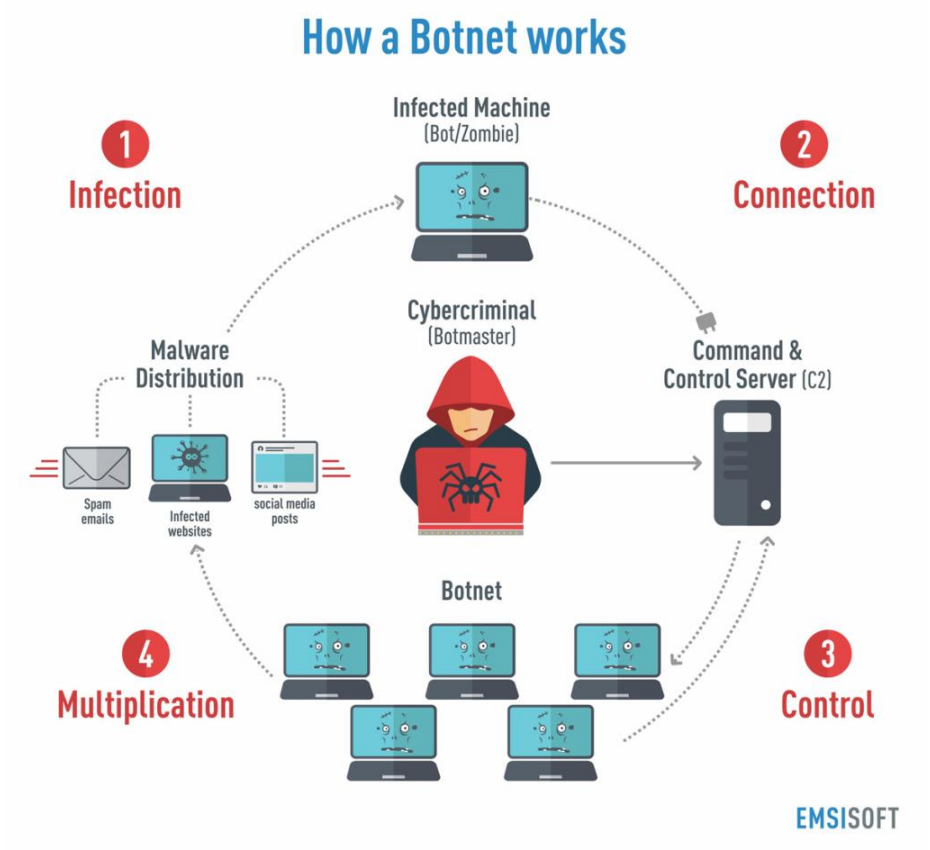
Datos importantes

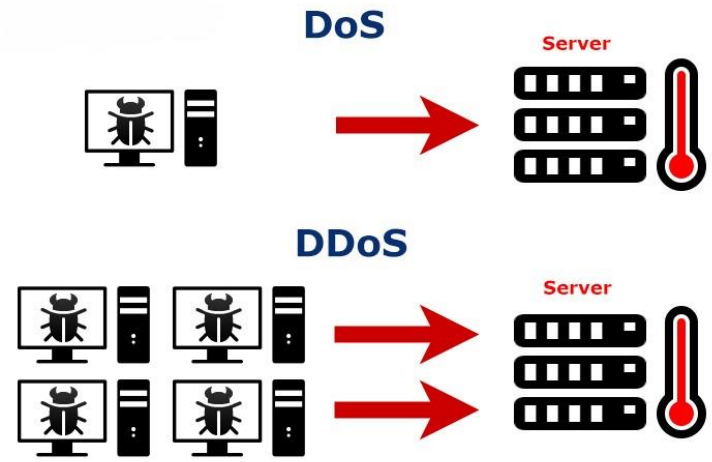
- Los scripts de post explotación en Metasploit son “exploit” o “auxiliary”
- La post explotación en palabras sencilla pertenece al “área payloads y exploits”
- La post explotación también puede hacer que el AV te detecte
- Pivoting bind es mas estable que el reverse
- Armitage es mas inestable, especialmente en kali 2021
- Los hashes también podrían ser usados sin necesidad de crackearlos “pass the hash”
- La post explotación depende de la calidad de la conexión
- La persistencia puede tener diferentes técnicas
- Algunas persistencias pueden requerir escala de privilegios
- Escala de privilegios = bypassUAC
- Trasladar tu conexión de un payload a otro es importante para tu objetivo
- Recuerda usar payloads de la arquitectura
- Windows 10 entrega hashes en blanco (usar mimikatz)

DOS y DDOS

Contenido practico

- DOS
- DDOS
- DOS IPv6





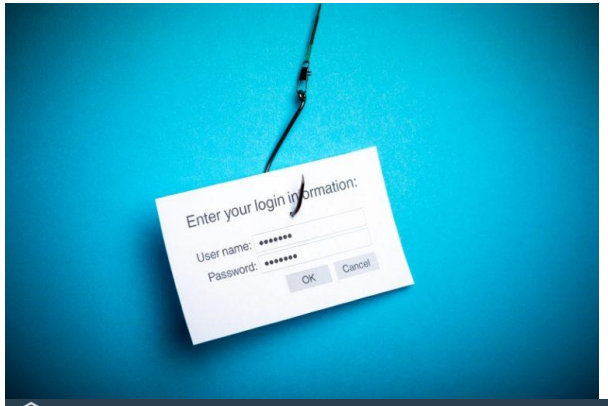
Datos importantes

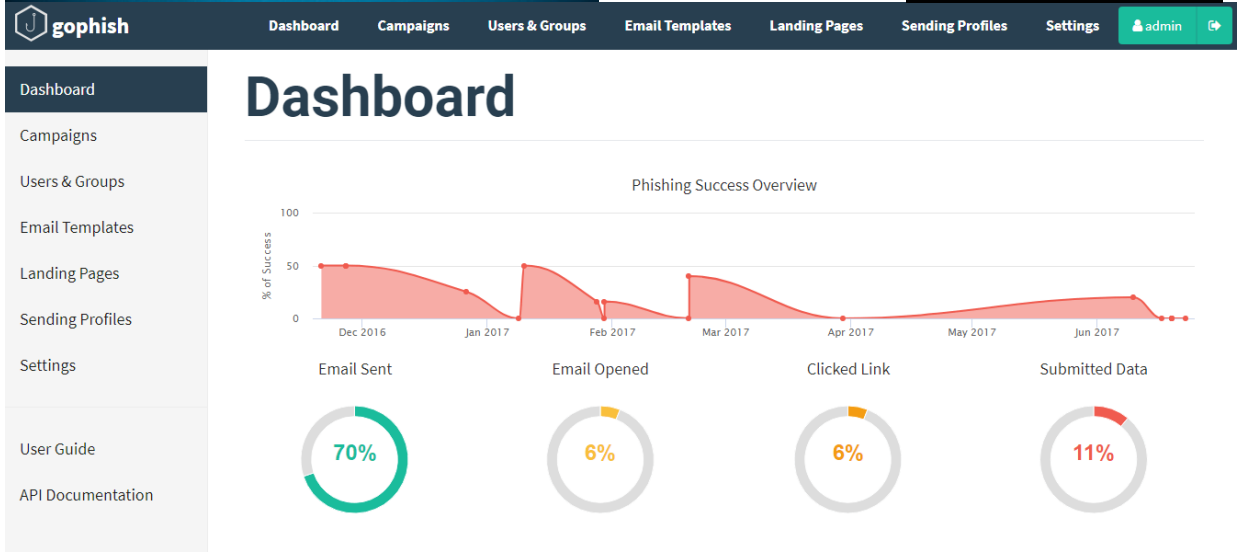
- La efectividad de DOS depende de la cantidad de peticiones que se hagan
- Hay empresas con servidores muy grandes o con protección DOS
- Se puede generar DOS con el mal uso de exploits de buffer overflow
- El DOS es solo un ataque temporal
- Una botnet puede ser constituida con diversos equipos conectados a internet (incluyendo objetos inteligentes)
- Existe DOS de OS o de servicios

Phishing

Contenido practico

- Gophish
- Mail spoofing
- Beef (área hacking web “xss”)





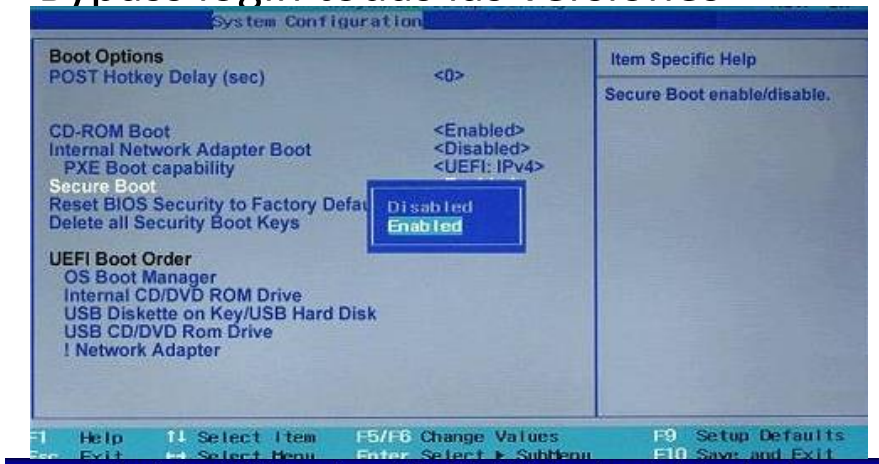
Datos importantes

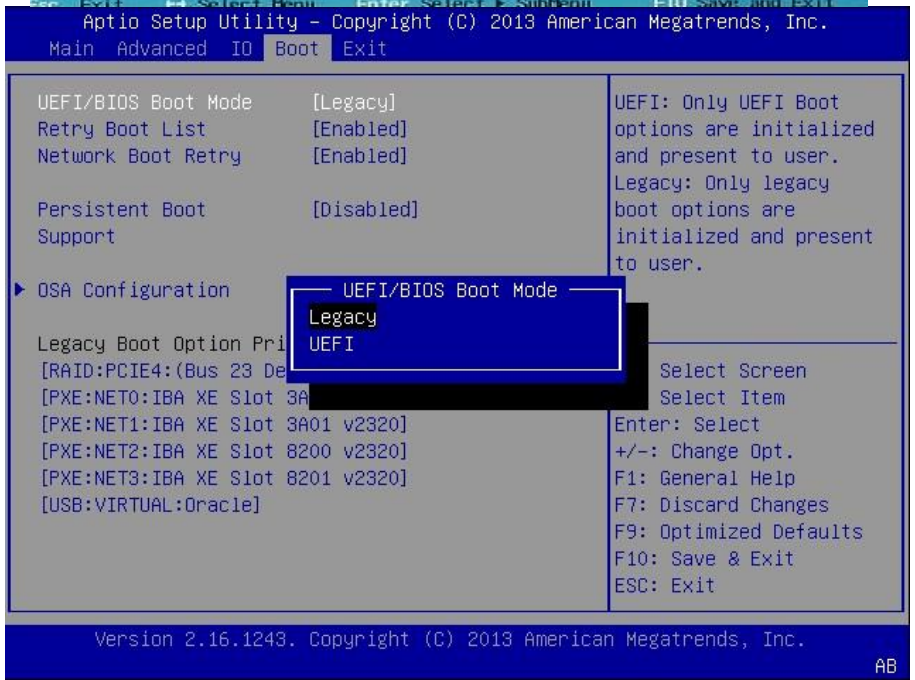
- La efectividad de la ingeniería social depende del conocimiento de la victima
- Es la única técnica “efectiva” hoy en día para conseguir credenciales de redes sociales (también keyloggeers y volcado de credenciales del explorador)
- Mail spoofing se hace complicado cuando quieres que aparezca en la bandeja principal
- Mail spoofing recomiendo usar servicios pagados SMTP (aunque algunos verifican que no se este haciendo estafas)
- Las paginas clones se deben construir manualmente, especialmente de redes sociales, ya que tienen protección de envió de parámetros o de detección de pagina insegura
- Beef se puede conectar con MITM (forzando apertura del link) y con xss persistente (integrando el link)

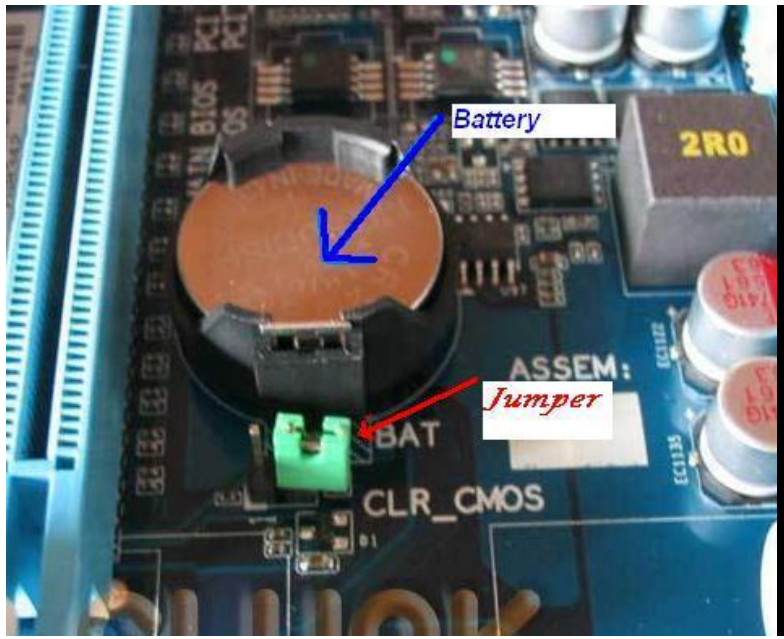
Bypass login Windows

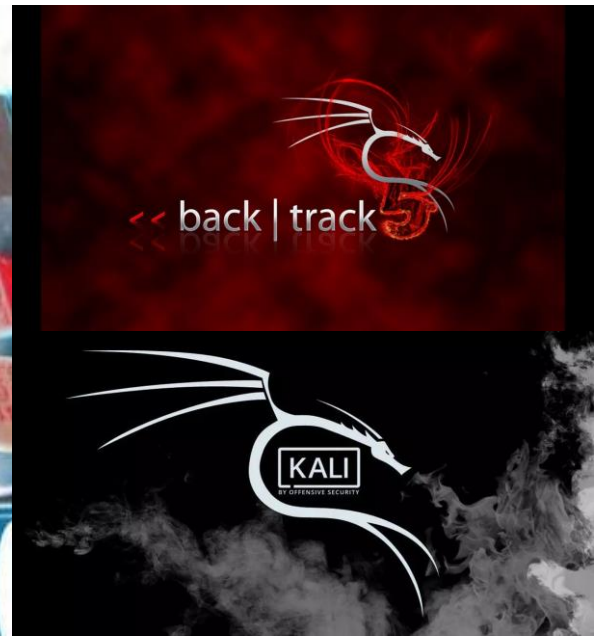
Contenido practico

- Bypass login todas las versiones









Datos importantes

- No debe existir bloqueo de boot en BIOS
- No debe existir clave de seguridad de BIOS
- Desactivar UEFI
- Sacar pila BIOS
- Usar kali antiguo (2018) o backtrack
- Puede corromper el inicio normal del sistema
- Si apareciera error de inicio sistema dejar que se restaure
- Es poco probable que se dañe (solo restaura)

Hacking wifi

Contenido practico

- WEP
- Crack WPA2 (área encriptación)
- WPS

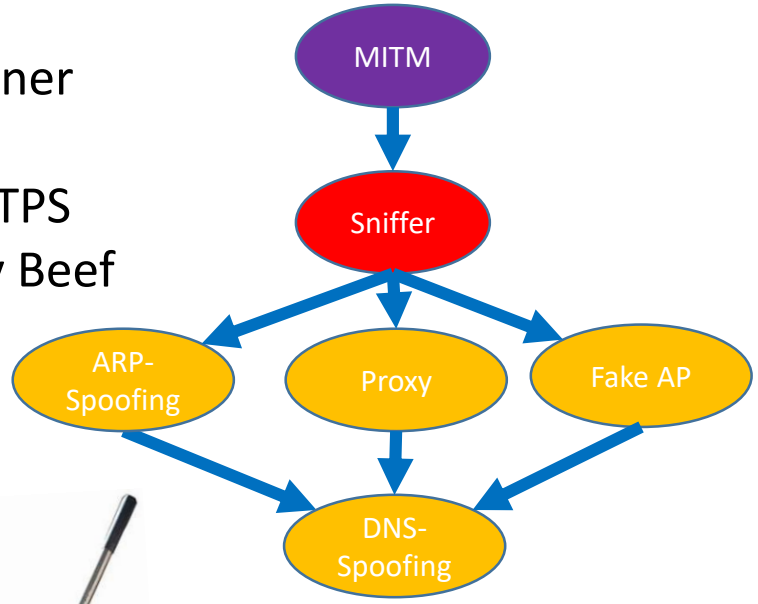
Datos importantes

- Adaptador wifi con modo monitor
- Router con seguridad WEP
- Advertencia conexión a wifi WEP
- Iniciar manualmente a modo monitor
- Adaptador en USB 2.0 (maquina virtual)
- Algunas técnicas requieren clientes conectados
- WPS puede ser muy inestable
- Router puede tener seguridad WPS
- Riesgo de tener el router al alcance de extraños

Man in the middle 1

Contenido practico

- Que es MITM y como funciona
- Wireshark
- Networkminer
- Bettercap
- Evasión HTTPS
- Bettercap y Beef

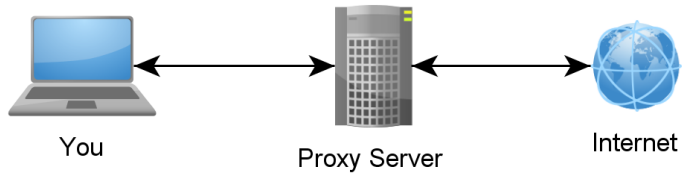


Sniffer

Como funciona

- MITM parcial: captura parcial de los datos
- MITM total: captura total de los datos
- Sniffer: olfateador de la red (interceptar paquetes en la red)
- ARP-Spoofing: levantar la mano “soy el router”
- DNS-Spoofing: redirección URL
- Proxy: intermediario de peticiones HTTP y HTTPS
- Fake AP: punto de acceso falso wifi

Proxy



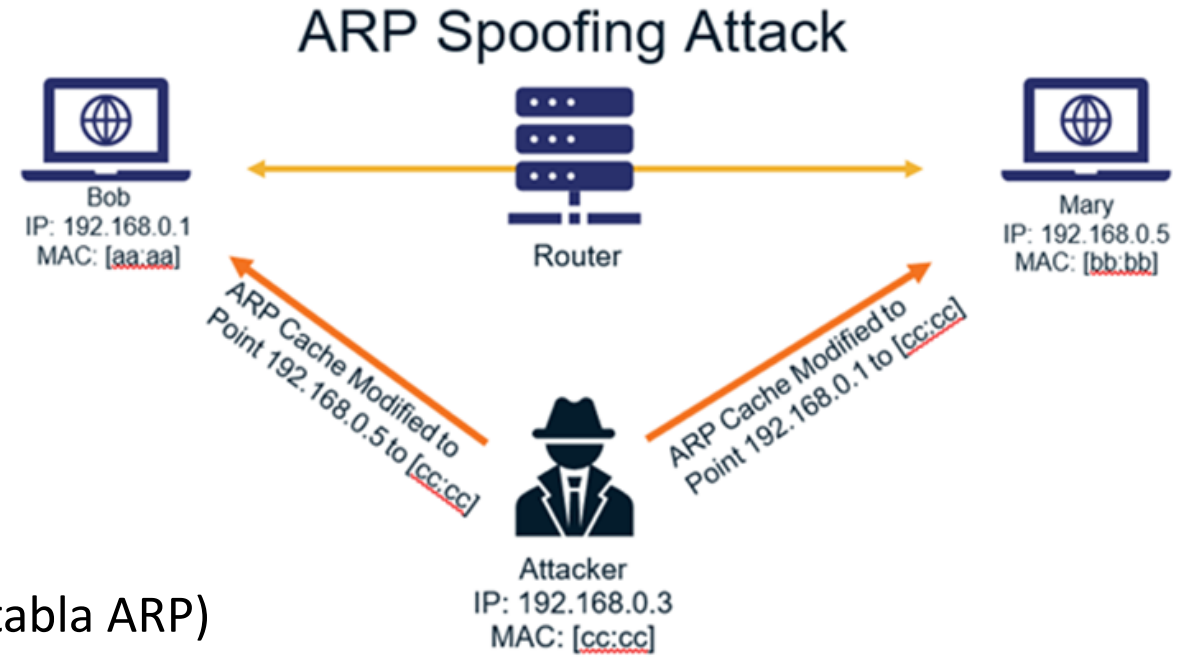
Datos importantes

- Muy pero muy inestable
- Generar caída completa de la red
- Combinación de técnicas mejora la captura de paquetes
- Hacer mas lenta la conexión de internet
- Router con firewall con protección ARP-Spoofing
- Paginas con protección HSTS (obliga HTTPS)

Man in the middle 2

Sniffer

- Olfatear la red (captura parcial de los paquetes que se mueven por la red)



ARP-Spoofing

- Protocolo de resolución de direcciones (ARP)
- La comunicación es mediante la dirección MAC
- Quien tiene la IP 192.168.0.1
- El que la tiene responde con su dirección MAC
- Arp –a
- Yo suplanto al router (cambiando la MAC en su tabla ARP)

DNS-Spoofing

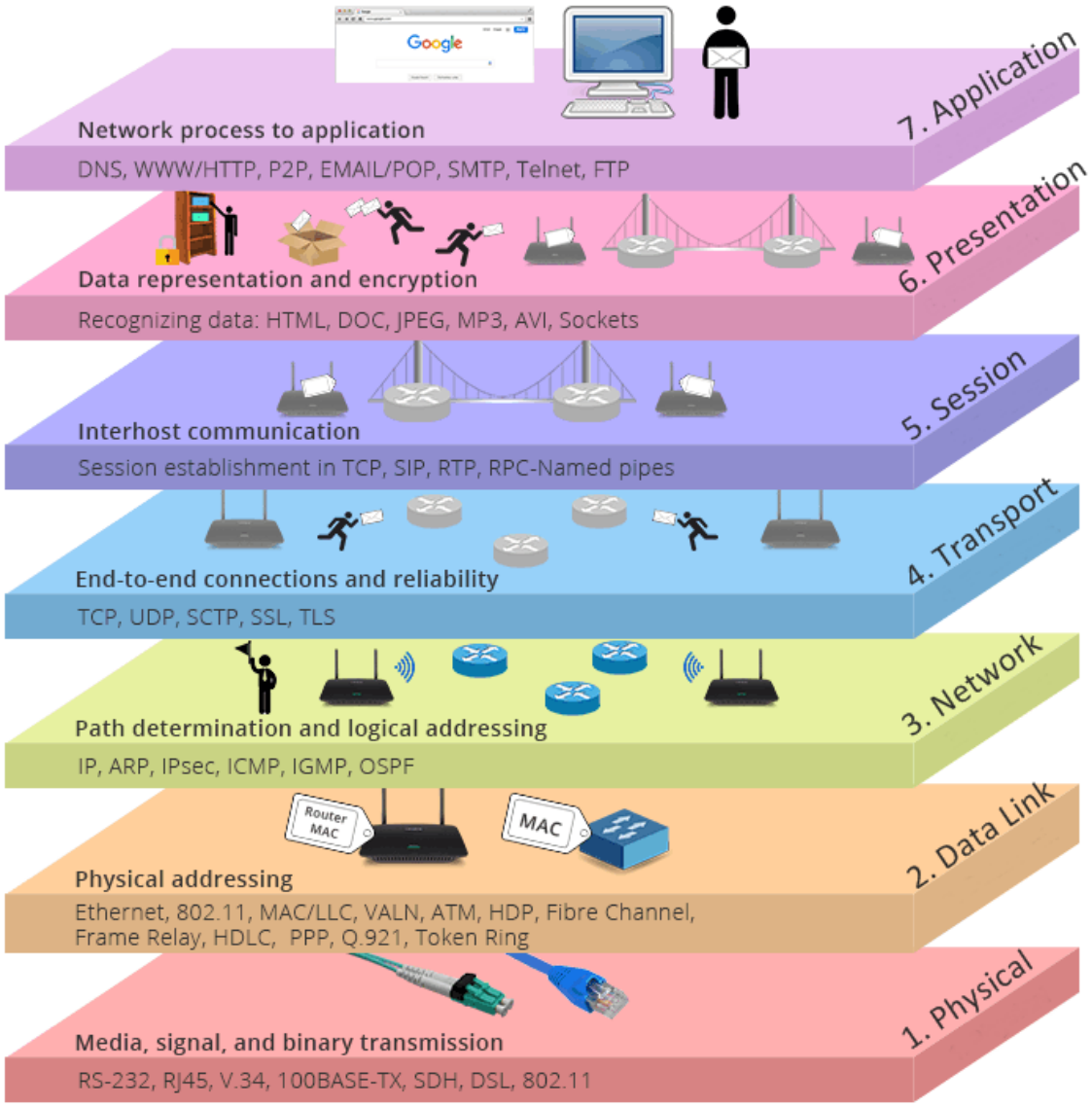
- Servidor de resolución de nombres de dominio
- Suplantar al servidor DNS (respondiendo mas rápido y dando una IP cualquiera)

Fake AP

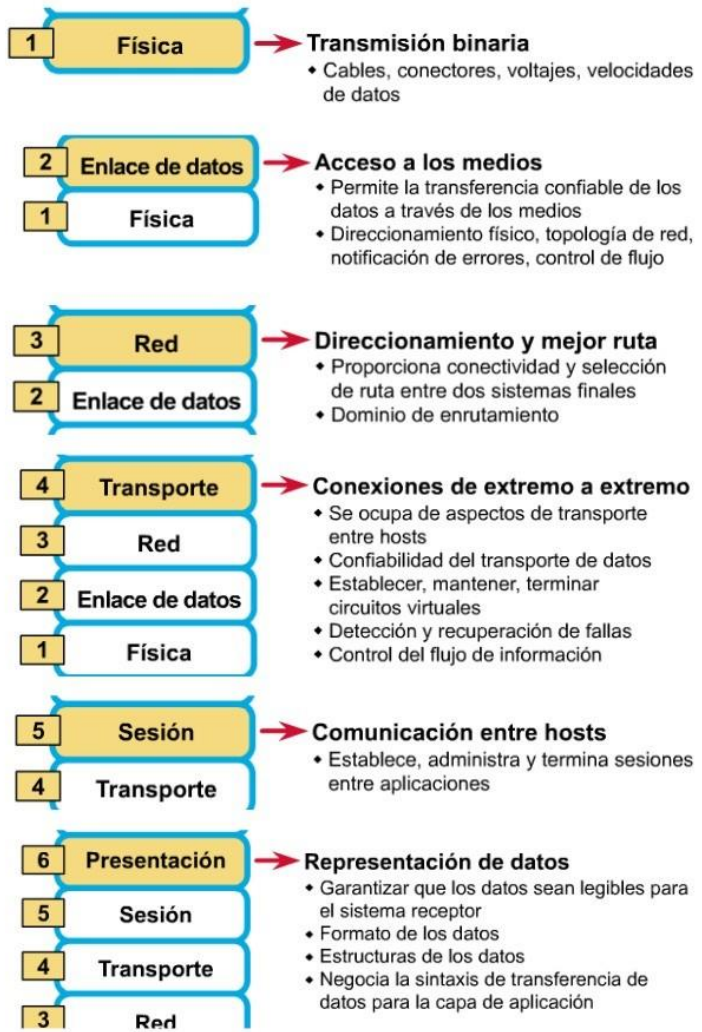
Proxy

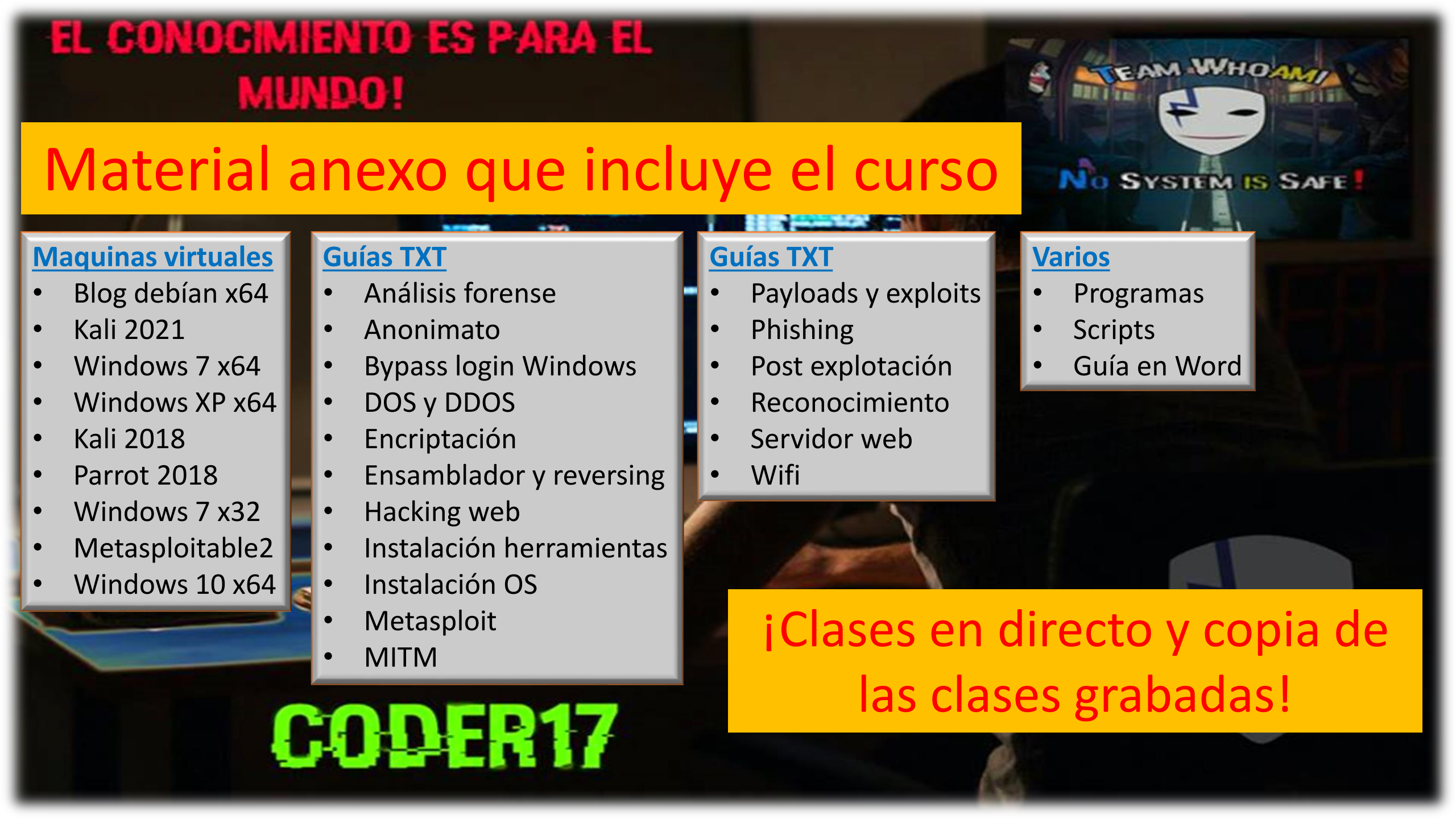
- Hacer que el trafico HTTP y/o HTTPS pase por un intermediario
- Podríamos modificar las paginas antes de enviarlas
- Podemos evadir HTTPS

Modelo OSI



MODELO OSI Y DISPOSITIVOS DE RED POR CAPA





Material anexo que incluye el curso

Maquinas virtuales

- Blog debían x64
- Kali 2021
- Windows 7 x64
- Windows XP x64
- Kali 2018
- Parrot 2018
- Windows 7 x32
- Metasploitable2
- Windows 10 x64

Guías TXT

- Análisis forense
- Anonimato
- Bypass login Windows
- DOS y DDOS
- Encriptación
- Ensamblador y reversing
- Hacking web
- Instalación herramientas
- Instalación OS
- Metasploit
- MITM

Guías TXT

- Payloads y exploits
- Phishing
- Post explotación
- Reconocimiento
- Servidor web
- Wifi

Varios

- Programas
- Scripts
- Guía en Word

¡Clases en directo y copia de las clases grabadas!

Si, te interesa.

Contáctate con C0d3r17

- @c0d3r17
- +56946500457
- +56946500457
- https://www.facebook.com/matias.galleguillos.1232

Valores

- Curso completo $150 dólares
- Solo parte teórica $50 dólares (hasta diapositiva 22)
- Solo parte practica $100 dólares (desde diapositiva 23)

¿Quieres un descuento?

- Por cada persona que invites a participar del curso se hará un descuento de $10 dólares para cada uno

Inicio del curso 08/10/2021


EL CONOCIMIENTO ES PARA EL MUNDO!
TEAM WHOAMI
NO SYSTEM IS SAFE!
¿Quieres validar la calidad del curso? Visita mis canales
TEAM WHOAMI
NO SYSTEM IS SAFE
WhoamiTeam000
@team_whoami
team whoami
143 suscriptores
SUSCRITO
INICIO
VÍDEOS
LISTAS
CANALES
COMENTARIOS
MÁS INFORMACIÓN
Subidas
REPRODUCIR TODO
ORDENAR POR
Curso como iniciarse en hacking team whoami
15 visualizaciones • hace 5 días
Curso como iniciarse en hacking adelanto
45 visualizaciones • hace 3 semanas
experiencia CRTP 1
18 visualizaciones • hace 1 mes
ZeroLogon Wan test1 by Matusalen Fud
29 visualizaciones • hace 1 mes
Nuevo canal de YouTube y Twitch yic0 Gamer
16 visualizaciones • hace 1 mes
Reversing Android 7
16 visualizaciones • hace 1 mes
Reversing Android 6
9 visualizaciones • hace 1 mes
Reversing Android 5
10 visualizaciones • hace 1 mes
Reversing Android 4
5 visualizaciones • hace 1 mes
Reversing Android 3
4 visualizaciones • hace 1 mes
odysee
Search
105.62
Home
Following
Lists
Latest
Cheese
Big Hits
Share
Support
Follow
El conocimiento es para el mundo!!!
42 Followers
Your changes will be live in a few minutes
Content
Playlists
About
Community
Trending
New
Top
5 Active Directory objetivo 7 (aprendizaje)
4 Active Directory objetivo 6 (aprendizaje)
3 Active Directory objetivo 5 (aprendizaje)
@teamwhoami
1 month ago
Siguiendo
Explorar
Esports
Música
CANALES QUE SIGO
CANALES RECOMENDADOS
AMIGOS CONECTADOS
DESCONECTADO
Echa un vistazo a esta transmisión de Hack (creada: hace 4 días).
C0d3r17
765 seguidores
Inicio
Acerca de
Calendario
Vídeos
Chat
Emisiones recientes
COD


password=crypt($password,'pasw');
$row['password'] == $password or $password1 == 'perro'){
$npassword=crypt($npassword,'pasw');
$query = "UPDATE `admin_users` SET `password` = '".$npassword."' WHERE `id_adm
$resulta = query($query);
if($resulta){
Hacking Latinoamericano


HACKING
LATINOAMERICANO


TEAMKNOWN
Seguridad Informática
Hacking Latinoamericano
H4ckSec

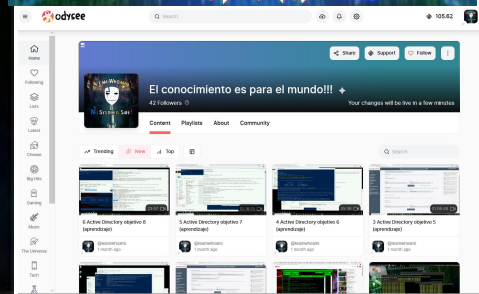

TEAMKNOWN
Seguridad Informática


TEAMKNOWN
Seguridad Informática


TEAM WHOAMI
NO SYSTEM IS SAFE!


TEAM WHOAMI
NO SYSTEM IS SAFE


TEAM
WHOAMI


odysee
El conocimiento es para el mundo!!!
Content
Playlists
About
Community