

HACKING DE INSTAGRAM



Instagram

TÉCNICAS Y HERRAMIENTAS OSINT

**Hacking de
Instagram - Técnicas
y Herramientas
OSINT**

INSTRUCTOR

Marco Mendoza

Ingeniero en Sistemas, Téc en Informática y Autodidacta

Sobre mí

Soy ingeniero en sistemas, técnico en informática y autodidacta, a lo largo de mi vida he tenido la oportunidad de trabajar en diferentes campos como la administración de sistemas, diseño y programación web, desarrollo de aplicaciones móviles y también como maestro. hoy en día con el conocimiento que gane por mis años de trabajo, más muchas horas de estudio autodidacta, he llegado a desempeñarme en el área de seguridad informática realizando auditorias de seguridad en diferentes empresas e instituciones de gobierno.

También soy el creador de una pequeña comunidad en YouTube llamada Hacking y Más donde imparto algunos cursos de seguridad y hacking ético.

Redes sociales:

[Página Web](#)

[Facebook](#)

[YouTube](#)

[Telegram](#)

[Instagram](#)

[Twitter](#)

Descuentos en los mejores cursos

Hacking Ético 2022: Pentesting en Android Avanzado

Si quieres aprender como hackear Android 11, 12, 13 y extraer fotos, videos, notificaciones de redes sociales, posición GPS, contactos, SMS, Bases de datos de Whatsapp y tener a disposición cualquier información, este es tu curso.

CUPON DEL 80% DE DESCUENTO AQUÍ EN MI PAGINA WEB: <https://bit.ly/3JcdOlw>

Únete a mis **62.139** estudiantes de **Udemy** y aprende conmigo.

Informática y software > Redes y seguridad

Hacking Ético 2022: Pentesting en Android Avanzado

Aprende a Evaluar y Hackear Vulnerabilidades en Android Para Pentesting y Respuesta a Incidentes.

0.0 ☆☆☆☆ (0 calificaciones) 0 estudiantes

Creado por [Marco Mendoza](#)

Publicado el 🌐 Español



1.249 MX\$

Inscríbete ahora

Garantía de reembolso de 30 días

Este curso incluye:

- 8 horas de video bajo demanda
- 6 recursos descargables
- Acceso de por vida
- Acceso en dispositivos móviles y TV

[Compartir](#) [Aplicar cupón](#)

Lo que aprenderás

- ✓ Aprenderán Cómo Evaluar Vulnerabilidades en Android.
- ✓ Serán Completamente Competentes en el Area de Pentesting De Dispositivos Móviles.
- ✓ Podrán Prevenir Ataques Avanzados a Android.
- ✓ Ejecutarán Geolocalización Por GPS.
- ✓ Serán Capaces de Extraer Contactos y Registros de Llamadas.
- ✓ Podrán Ejecutar Herramientas Avanzadas Para Pentesting.
- ✓ Tendrán Acceso a Todo Tipo de Información de Forma remota y Local.
- ✓ Podrán Mitigar Ataques.
- ✓ Podrán Ejecutar Ataques Avanzados Con Metasploit y Mas Herramientas.
- ✓ Serán Capaces de Extraer Fotos, Videos, Bases de Datos, Audios y Muchos Mas Archivos.
- ✓ Serán Capaces de Hackear las Versiones de Android, 10, 11 y 12.
- ✓ Podrán Extraer Notificaciones de Aplicaciones ya Instaladas.
- ✓ Tendrán la Perspectiva de Un Ataque real Para su Prevención.
- ✓ Serán Capaces de Configurar un Entorno Seguro de Trabajo.
- ✓ Serán Capaces de Ejecutar Ataques Locales Y Mundiales Para Su Evaluación.
- ✓ Tendrán la Capacidad de Identificar

Descripción

La seguridad en dispositivos **Android** se ha vuelto cada vez más importante debido a la gran demanda que hay en el mundo con respecto a Smartphones, Smart tv, relojes, impresoras e incluso computadoras y laptops. Es debido a este incremento de dispositivos inteligentes que usan **Android** que las amenazas para los usuarios han aumentado de una manera desproporcionada, un claro ejemplo de esto es lo sucedido durante la pandemia, ya que la mayoría de las personas empezaron a trabajar desde casa debido a la contingencia, muchos **ciberdelincuentes** aprovecharon esto para revivir viejos **Malware** como crear nuevos **Malwares**, esto provocó una gran cantidad de ataques y nuevas formas de estafas, como resultado muchas personas fueron víctimas de robo de información, fraude y robo bancario, dada la necesidad de más expertos en el tema del **pentesting** de **Android** cree este curso que aborda los temas más básicos como técnicas muy avanzadas de simulaciones de ataques reales, si te interesa ser un experto en el **penstesting** y **hacking** de **Android** te invito a seguirme en el curso. Este curso fue creado pensando en los escenarios más reales que puedan proporcionarte los mejores ejemplos de ataques en la vida real.

Hacking Ético 2022: Curso de Metasploit Framework

Si quieres aprender como los expertos en hacking usan Metasploit como expertos te invito a seguir mi curso con más de **44.333 estudiantes satisfechos**.

CUPON DEL 80% DE DESCUENTO AQUÍ EN MI PAGINA WEB: <https://bit.ly/3KMs4BX>

Únete a mis **62.139** estudiantes de **Udemy** y aprende conmigo.

Informática y software > Redes y seguridad > Hacking ético

Hacking Ético 2022: Curso de Metasploit Framework

Aprende a Usar e Implementar Metasploit Framework Para Hackear Windows 10, Android 11 y Log4Shell

4,2 ★★★★★ (1.298 calificaciones) 44.333 estudiantes

Creado por [Marco Mendoza](#)

🕒 Fecha de la última actualización: 2/2022 🌐 Español 🗣️ Español [automático]



Vista previa de este curso

179 MX\$ ~~1.029 MX\$~~

83 % de descuento

🕒 ¡Esta oferta termina en 22 horas!

[Añadir a la cesta](#)

[Comprar ahora](#)

Garantía de reembolso de 30 días

Este curso incluye:

- 📺 5 horas de vídeo bajo demanda
- 📄 2 artículos
- 📄 4 recursos descargables
- 🔄 Acceso de por vida
- 📱 Acceso en dispositivos móviles y TV
- 📄 Certificado de finalización

[Compartir](#) [Regalar este curso](#) [Aplicar cupón](#)

Lo que aprenderás

- ✓ Las personas que tomen este curso podrán utilizar Metasploit Framework para realizar simulaciones de intrusión en sistemas
- ✓ Podrán comprender en su totalidad metasploit.
- ✓ Aprenderás a hackear la vulnerabilidad de log4shell.
- ✓ Serás capaz de evadir windows defender y los antivirus.
- ✓ Podrás explotar servidores FTP.
- ✓ Aprenderás a ejecutar ataques en un entorno controlado.
- ✓ Seran capaces de hackear windows 10 y android.
- ✓ Comprenderás como troyanizar una app original de la play store.
- ✓ Aprenderás a usar encoders externos.
- ✓ Y mucho más.

Requisitos

Descripción

En este curso aprenderás como usar e implementar Metasploit Framework para que posteriormente puedas acoplarlo en tus pruebas de penetración y evaluación de vulnerabilidades, empezaremos con una pequeña introducción al temario del curso, después pasaremos a configurar todas las máquinas virtuales que usaremos a lo largo del curso, en este caso trabajaremos con Windows 10 y Android 11, enseguida estaremos viendo algunas herramientas que van de la mano de Metasploit Framework y daremos un vistazo rápido a la interfaz gráfica conocida como Armitage, en el siguiente capítulo veremos los módulos que conforman Metasploit Framework y también daremos un vistazo a la carpeta raíz de Metasploit para ver cómo está organizado, paso siguiente pasaremos a ver algunos auxiliares que nos ayudaran a tener una visión más amplia a la hora de buscar información de servicios que se están ejecutando bajo los protocolos más usados en redes locales, después veremos cómo desplegar ataques con Metasploit en sistemas operativos actuales, también veremos la eficiencia y deficiencia de Metasploit desplegado en diferentes entornos así como la forma de integrar nuevos exploits para personalizar nuestro Metasploit Framework, en la sección de ataques veremos como explotar la vulnerabilidad de Log4Shell utilizando drivers y aplicaciones webs vulnerables, paso siguiente troyanizaremos la App original de facebook para hackear android y tener acceso con privilegios, si quieres dominar Metasploit como un maestro te invito a seguir este curso.

Hacking Ético 2022: Curso de Wireshark Para Pentesting

Si quieres aprender cómo detectar malware, ataques DDoS, y ataques de fuerza bruta sin alterar la estructura del equipo y sin usar ingeniería inversa, este es tu curso, únete a mis 18.932 estudiantes satisfechos.

CUPON DEL 80% DE DESCUENTO AQUÍ EN MI PAGINA WEB: <https://bit.ly/2XlvqZf>

Únete a mis 62.139 estudiantes de Udeemy y aprende conmigo.

Informática y software > Redes y seguridad > Pruebas de penetración

Hacking Ético 2022: Curso de Wireshark Para Pentesting

Aprende a Detectar Ataques de Fuerza Bruta, DDoS y Malware Con Wireshark y Kali Linux.

4.5 ★★★★★ (202 calificaciones) 18.932 estudiantes

Creado por [Marco Mendoza](#)

Fecha de la última actualización: 2/2022 🌐 Español 🗣️ Español [automático]

Lo que aprenderás

- ✓ Las personas que tomen este curso podrán utilizar Wireshark para detectar ataques de diferentes tipos, como Malware, DDoS, Fuerza bruta y Escaneos de Puertos.
- ✓ Aprenderán cómo se despliegan los ataques de fuerza bruta.
- ✓ Comprenderán las diferencias entre ataques de Malware.
- ✓ Podrán identificar cuando un equipo está comprometido.

Requisitos

- Necesitan contar con vmware o virtualbox instalado y tener algo de conocimiento sobre la instalación de sistemas operativos

Descripción

Vista previa de este curso

179 MX\$ ~~1.029 MX\$~~
83 % de descuento
⏰ ¡Esta oferta termina en 22 horas!

[Añadir a la cesta](#)

[Comprar ahora](#)

Garantía de reembolso de 30 días

Este curso incluye:

- 📺 5 horas de video bajo demanda
- 📄 2 artículos
- 📁 11 recursos descargables
- 🌐 Acceso de por vida
- 📱 Acceso en dispositivos móviles y TV
- 📄 Certificado de finalización

[Compartir](#) [Regalar este curso](#) [Aplicar cupón](#)

Descripción

Hoy en día las amenazas informáticas han evolucionado de una manera muy drástica, desde Malware inteligente, hasta Ataques a gran escala que pueden provocar el cese de operaciones de una empresa, y pensando en cómo prevenir este tipo de amenazas sin alertar a los atacantes se creó este curso. Iniciaremos con una breve introducción al temario del curso, después comenzaremos con la instalación del entorno virtual que utilizaremos a lo largo de las clases, también repasaremos la importancia de evitar comprometer el sistema y daremos una introducción completa a los ataques más utilizados contra empresas, a continuación daremos un repaso de la interfaz gráfica de Wireshark, continuaremos con el análisis de paquetes para empezar a familiarizarnos con los métodos de filtrado que podemos aplicar con Wireshark, después explicaremos de forma rápida como implementar reglas de firewall y como aplicar una línea base de trabajo para tener una referencia del tráfico que circula por la red, enseguida empezaremos a ver cómo podemos crear y utilizar filtros para agilizar la búsqueda de amenazas, y por ultimo veremos cómo identificar tanto Malware como Ataques de fuerza bruta, si estás interesado en expandir tus conocimientos sobre seguridad, este es tu curso, te invito a que te suscribas para que me acompañes a lo largo de esta aventura.

Contenido

Introducción	1
¿Cómo pueden los hackers hackear cuentas de redes sociales?	1
1. Phishing	1
2. KeyLogging	2
3. Ataques de Man In The Middle	3
4. Ingeniería Social.....	4
5. Secuestro de sesión.....	4
6. Contraseñas guardadas	5
7. Suplantación de DNS.....	5
8. Botnets.....	6
El spyware y cómo lo usan los hackers.....	7
¿Cuáles son las formas más comunes en que se distribuye el spyware?	7
¿Qué hace el spyware una vez que encuentra una forma de entrar en una computadora o una red?	8
¿Cuáles son las razones comunes por las que los hackers usan malware?.....	9
¿Cómo deshacerse del spyware y el malware?.....	9
Los troyanos y como los usan los hackers	10
Definición de troyanos.....	10
Tipos de troyanos	13
Troyano-Backdoor.....	13
Troyano-Exploit.....	13
Troyano-DDoS	13
Troyano-Downloader	14

Contenido

Troyano-FakeAV.....	14
Troyano-Banker.....	15
Troyano-GameThief	15
Trojan-Ransom	15
Troyano-Spy	16
Osintgram	17
Descargo de responsabilidad	18
Instalación	18
Comandos	23
Info	24
Followers.....	24
Followings.....	25
Likes.....	25
Photos	26
Photodes.....	26
Comments.....	27
Hashtags.....	27
Tagged.....	28
Fwersnumber.....	28

Introducción

No podemos negar la importancia de los sitios web de redes sociales en nuestra vida diaria. Una red social o un sitio de redes sociales ayuda a las personas a conectarse con sus amigos, familiares, marcas y celebridades, etc. Compartimos mucha información en estos sitios web, incluidos nuestros datos personales y financieros, como ubicación, fotos y mensajes, etc. la razón por la cual los hackers prefieren hackear cuentas de redes sociales por sus malas intenciones.

¿Cómo pueden los hackers hackear cuentas de redes sociales?

No todos los usuarios de Internet tienen la educación suficiente para comprender cómo proteger sus cuentas de redes sociales. Entonces, aquí, mencionaré algunos de los métodos más populares utilizados por los hackers para piratear cuentas de redes sociales y cómo asegurarse de que no lo pirateen con esos métodos.

1. Phishing

El phishing es muy fácil y se considera una técnica noob, pero es una de las técnicas más efectivas para hackear cuentas de redes sociales. Existe una probabilidad de 50-50 de que un hacker obtenga la contraseña de una víctima mediante Phishing si su víctima no conoce la terminología básica de Internet.

Introducción

Hay varias formas de llevar a cabo un ataque de phishing. El más común es cuando un hacker crea una réplica de una página de inicio de sesión que se parece a la página real de las redes sociales. La víctima entonces pensará que es el inicio de sesión habitual.

El Phishing más común es crear un duplicado de una página de inicio de sesión que se parece a la página de inicio de sesión real. La víctima piensa que es la página de inicio de sesión social habitual, por lo que ingresa sus datos de inicio de sesión en la página de phishing. Una vez que la víctima inicia sesión a través de la página falsa, la dirección de correo electrónico y la contraseña se almacenan en un archivo de texto o en la base de datos del hacker.

¿Cómo detectar una página de phishing?

- Compruebe la URL de la página de inicio de sesión.
- Nunca inicie sesión en su cuenta de red social en otros dispositivos.
- Use navegadores webs modernos que identifiquen la página de phishing.
- Evite los correos electrónicos o mensajes de texto que le soliciten que inicie sesión en su cuenta de red social.

2. KeyLogging

El KeyLogging es una de las formas más fáciles de hackear una cuenta de redes sociales. Un keylogger es un programa que registra y monitorea la entrada del usuario y mantiene un registro de todas las teclas que se ingresan. El keylogger puede enviar activamente sus entradas a los hackers a través de Internet. Debe tener mucho cuidado al tratar con keyloggers porque incluso los expertos en informática se convierten en víctimas del keylogger.

¿Cómo detectar Keyloggers?

- Escanee sus unidades USB antes de usarlas
- Descargar software solo de sitios confiables
- Usa un buen antivirus

3. Ataques de Man In The Middle

En este método, el hacker en secreto altera la comunicación entre el servidor y la víctima que creen que se están comunicando directamente entre sí.

El hacker establece conexiones independientes con las víctimas y transmite mensajes entre ellas para hacerles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación está controlada por el hacker.

El hacker debe poder interceptar todos los mensajes relevantes que pasan entre las dos víctimas e inyectar otros nuevos. Esto es sencillo en muchas circunstancias; por ejemplo, un atacante dentro del rango de recepción del punto de acceso inalámbrico puede insertarse como man-in-the-middle.

¿Cómo evitar los ataques MIME?

- Usar servicios VPN
- Un servidor proxy para acceder a Internet.
- Use un buen antivirus con buenas opciones de firewall

Introducción

4. Ingeniería Social

La ingeniería social es un método simple que se basa en recopilar la mayor cantidad posible de información de las víctimas. La información puede incluir la fecha de nacimiento, el número de teléfono, las preguntas de seguridad, etc. Una vez que un hacker obtiene acceso a esta información, puede forzar la información o usar métodos de recuperación para obtener contraseñas de inicio de sesión.

¿Cómo evitar la Ingeniería Social?

- Nunca comparta información personal por correo electrónico o teléfono
- Evite enlaces de sitios desconocidos o sospechosos

5. Secuestro de sesión

Cuando inicia sesión en su cuenta de redes sociales, su navegador y el servidor de redes sociales mantienen una sesión para la autenticación del usuario. Los detalles de la sesión se guardan en los archivos de cookies de su navegador. En el secuestro de sesión, el hacker roba esas cookies y luego accede a la cuenta de la víctima. El secuestro de sesiones es más común cuando se accede a sitios web de redes sociales en una conexión HTTP (no segura) y se usa ampliamente en conexiones LAN y Wi-Fi.

¿Cómo evitar el secuestro de sesión?

- No use sitios web de redes sociales cuando esté conectado a Wi-Fi o LAN
- Intente borrar las cookies cada 2-3 días o, si es posible, diariamente.

6. Contraseñas guardadas

La mayoría de las veces compartimos nuestros datos de inicio de sesión y de tarjeta de crédito en el navegador web. Cualquiera puede ver su cuenta de redes sociales desde el administrador de contraseñas de su navegador. Un hacker puede obtener acceso físico a su computadora e insertar un USB programado para extraer o recuperar automáticamente las contraseñas guardadas en el navegador de Internet o cualquier otra información que el hacker pueda necesitar.

¿Cómo evitar el hackeo de contraseñas?

- Trate de no guardar contraseñas en los navegadores web
- No comparta su dispositivo con la gente
- Bloquear los conectores del dispositivo

7. Suplantación de DNS

Si un hacker está en la misma red que está conectada a la víctima, puede cambiar la página original y reemplazarla con su propia página falsa y acceder fácilmente a la cuenta de redes sociales de la víctima.

¿Cómo evitar la falsificación de DNS?

- Administre sus servidores DNS de forma segura

Introducción

8. Botnets

Básicamente, las botnets son redes hechas de computadoras o bots controlados a distancia. Estos bots han sido infectados con malware que permite controlarlos de forma remota. Es costoso configurar botnets y esto hace que se utilicen mínimamente en casos de hacking de cuentas.

¿Cómo evitar las Botnets?

- Mantenga todo su software actualizado
- Asegúrese de que su firewall esté siempre activo

El spyware y cómo lo usan los hackers

El spyware y registra el uso y la actividad de su computadora. Observa el comportamiento de los usuarios y encuentra vulnerabilidades que le permiten al hacker ver datos y otra información personal que normalmente consideraría privada o confidencial.

¿Cuáles son las formas más comunes en que se distribuye el spyware?

Como ya dijimos, los hackers son cada vez más sofisticados. Esta idea no se pierde en cómo se distribuye el spyware. La forma más común en que se distribuye el spyware es a través de descargas en línea que normalmente serían inofensivas. Otro método común es a través de conexiones Wifi gratuitas no seguras (no se necesita contraseña) o fáciles de hackear. Para la mayoría de los hackers, esto es todo lo que necesitan para tener acceso completo NO SOLO a su computadora o red, sino a cualquier dispositivo conectado en su oficina u hogar. Y luego se aprovechará de las descargas, los archivos, etc. y se ejecutará sin ser detectado recopilando información sobre usted, sus clientes y su sistema hasta que sea descubierto y destruido.

El spyware y cómo lo usan los hackers

Importante: el spyware casi siempre se descarga sin saberlo o se disfraza como algo confiable. Esto significa que casi nunca es intencional. Y la mayoría de las veces, el software espía es introducido en su sistema por un empleado que pensó que estaba haciendo lo correcto, pero sin darse cuenta infecta una computadora o una estación de trabajo y luego finalmente se propaga por todo el sistema.

¿Qué hace el spyware una vez que encuentra una forma de entrar en una computadora o una red?

El software espía está programado para adjuntarse a archivos, correos electrónicos, etc. en su computadora o dispositivo sin su autorización. Luego, comenzará a monitorear y buscar tipos específicos de información que sería importante para el hacker, como información de tarjetas de crédito, números de teléfono, direcciones de correo electrónico, en realidad cualquier cosa que el hacker quiera programar para que esté atento. Cuando encuentra algo para lo que está diseñado, transmite/envía esos datos, generalmente sin ser detectados, a un sistema de base de datos o almacenamiento remoto donde el hacker puede acceder a la información.

Mientras que los hackers son cada vez más sofisticados. Eso no significa que usen métodos complejos. A menudo, los hackers programan software espía para buscar información confidencial y crítica en lugares muy simples y fáciles de proteger, Y, aunque muchos hackers se centran en métodos simples, hay muchos que adoptan un enfoque más agresivo al crear software espía que puede asumir el control de su computadora o dispositivos, para hacer de todo, desde alterar la configuración de Internet o del navegador web hasta realizar actividades ilegales y delictivas.

¿Cuáles son las razones comunes por las que los hackers usan malware?

Los piratas informáticos usan malware específicamente por muchas razones, como:

- Acceder o eliminar documentos
- Modificar o borrar información
- Adquirir y distribuir datos confidenciales, como registros financieros, números de tarjetas de crédito

¿Cómo deshacerse del spyware y el malware?

Tanto el spyware como el malware son difíciles de manejar y casi siempre requerirán un experto que sepa lo que están haciendo y cómo prevenirlo en el futuro. Normalmente, un sistema o red deberá limpiarse y restaurarse con datos respaldados o, como mínimo, se necesitará una reinstalación completa del sistema, incluido otro software importante, para solucionar el problema. A veces, se requiere reemplazar ciertos componentes de hardware, como los discos duros, para asegurar una reparación adecuada.

Los troyanos y como los usan los hackers

Algunas amenazas de ciberseguridad son tan anticuadas que realmente no se oye mucho sobre ellas, e incluso puede parecer que disminuyen con el paso de los años. Pero desde el comienzo de la pandemia de COVID-19, los autores de malware han estado encontrando nuevas formas de explotar la situación en la que se encuentra el mundo. Una de las tácticas más comunes que estamos viendo es el uso de troyanos.

Definición de troyanos

No sería correcto hablar de troyanos si no mencionáramos brevemente los orígenes del término en sí. La historia del Caballo de Troya es bien conocida: narra cómo los soldados griegos lograron apoderarse de Troya, considerada una ciudad inexpugnable. Todo lo que se necesitó para acabar con Troya fue un truco: los atacantes construyeron un caballo de madera que se presentó a los troyanos como regalo, que aceptaron con gusto. Lo dejaron atravesar sus muros protectores, y una vez que estuvo dentro de la ciudad, los guerreros griegos bajaron del caballo mientras no había nadie alrededor y atacaron.

Los troyanos y como los usan los hackers

Incluso después de más de 3.000 años, el caballo de Troya sigue siendo una metáfora, que simboliza cualquier estrategia que permita a los atacantes infiltrarse y finalmente derrotar a su oponente, a través de la cooperación inconsciente del oponente.

Los troyanos en ciberseguridad también utilizan el engaño, o en este caso, la ingeniería social, para engañar a las víctimas para que ejecuten programas aparentemente benignos, a veces incluso familiares, que no tienen contenidos benignos. Estos troyanos son códigos o programas disfrazados de programas legítimos, pero se comportan de manera maliciosa, ocultando efectivamente cualquier ejecución de este tipo. La víctima los instala voluntariamente para realizar una función deseada, pero realizan una dañina una vez instalados.

Si bien a menudo escuchamos el término “virus troyano”, técnicamente no son virus. Un virus tiene la capacidad de propagarse adhiriéndose a otro software, y los troyanos se propagan disfrazándose de otro software.

Los troyanos pueden llegar de cualquier forma: archivos adjuntos de correo electrónico, música gratuita, herramientas, juegos en línea, anuncios o cualquier aplicación aparentemente inofensiva y legítima. Debido a que hay tantas formas en las que los troyanos pueden disfrazarse, hay tantas formas en las que los usuarios pueden infectarse con ellos.

Los troyanos generalmente se instalan en el dispositivo de la víctima mientras la víctima está navegando por Internet, descargando herramientas, programas y utilidades gratuitas o mediante un correo electrónico de phishing. Se disfrazan de software válido; a menudo, incluso software anti-malware, para añadir ironía. La víctima generalmente desconoce la presencia del programa malicioso, pero una vez que está instalado, puede ejecutar código para crear puertas traseras, ejecutar scripts, monitorear actividades, y robar datos personales.

Otra forma en que los autores de troyanos se aprovechan de los usuarios desprevenidos es disfrazar el programa para reflejar las últimas tendencias y

sucesos en todo el mundo. Hemos visto que gran parte de esto tuvo lugar durante la pandemia de COVID-19, con su excepcional magnitud de troyanos.

Como una de las formas más antiguas de amenazas digitales que existen, los troyanos han visto su reaparición generalizada en los últimos años, y 2021 muestra signos de que dominan el panorama de las amenazas cibernéticas una vez más.

En estos primeros meses del año ya hemos visto el troyano ElectroRAT recién descubierto que se ha encontrado dirigido a usuarios de criptomonedas; una campaña de malware que involucra un nuevo troyano Quaverse que atrae a la gente a descargar un archivo adjunto malicioso de correos electrónicos de phishing (que pretenden tener un video escandaloso del presidente de EE. UU.); y Rogue RAT , que se ofrece a la venta en la web oscura y utiliza código fuente de otros dos RAT de Android.

Y no olvidemos el más buscado en ciberseguridad: Emotet, que alguna vez fue un troyano bancario, pero recientemente distribuidor de otras campañas maliciosas. Sigue prevaleciendo como la principal amenaza troyana de 2021, incluso después de los esfuerzos internacionales de aplicación de la ley para tomar el control de su infraestructura.

Si no lo estuviéramos ya, podemos estar seguros ahora de que, por muy “obsoletos” y menos comentados que puedan ser los troyanos, son perdurables y prosperan, sin signos de detenerse. Tampoco oímos hablar de los troyanos de forma independiente; han tomado otra forma como parte del ciclo de vida del ciberataque o de ataques aún mayores, generalmente para ganar un punto de apoyo inicial en el sistema objetivo. Por ejemplo, podemos mirar hacia atrás en 2020 y uno de los casos más peligrosos y de mayor alcance, la brecha de SolarWinds .

Los troyanos y como los usan los hackers

El ataque involucró a atacantes que comprometieron la infraestructura de SolarWinds, la compañía que produce Orion, y luego usaron ese acceso para distribuir actualizaciones troyanizadas a los usuarios del software. Los componentes troyanizados de la actualización de software se denominaron SUNBURST y ahora hay reglas de detección de código abierto disponibles.

Tipos de troyanos

Troyano-Backdoor

Un troyano de puerta trasera crea una “puerta trasera” que permite a los atacantes controlar remotamente el dispositivo infectado de la víctima. Con este acceso remoto, los atacantes pueden enviar, recibir, eliminar o ejecutar archivos, instalar malware adicional, actuar como keylogger e incluso formar parte de un gran grupo de dispositivos infectados que se utilizan como botnet.

Troyano-Exploit

Los troyanos de explotación contienen código o un script que explota una vulnerabilidad conocida en el software del dispositivo infectado.

Troyano-DDoS

Un ataque DDoS implica apagar un dispositivo o una red y dejarlo inaccesible inundándolo con solicitudes de diferentes fuentes. Con los troyanos DDoS, los atacantes infectan una gran cantidad de dispositivos con un troyano, tomando el control sobre ellos y lanzando simultáneamente ataques distribuidos de denegación de servicio en el objetivo, abrumando y finalmente haciendo que deje de funcionar.

Troyano-Downloader

Los descargadores son troyanos que descargan y ejecutan programas maliciosos adicionales, incluidos keyloggers, adware o incluso otros troyanos en el dispositivo infectado. Los atacantes suelen distribuir descargadores como parte de los payload de otro programa malicioso.

Troyano-FakeAV

Los troyanos antivirus falsos se hacen pasar por un software antivirus legítimo que descargarías voluntariamente de Internet. Sin embargo, una vez instalados, solicitarán dinero a la víctima a cambio de escanear su dispositivo en busca de virus y eliminarlos. Si bien a menudo advierten de una amenaza “secreta” detectada, las amenazas son falsas.

Los troyanos y como los usan los hackers

Troyano-Banker

Los troyanos bancarios están diseñados para robar datos financieros: datos bancarios, tarjetas de crédito y débito e información similar. Ejemplos recientes y notorios de troyanos en el mundo real fueron, de hecho, troyanos bancarios: Emotet comenzó en 2014 como un troyano bancario, al igual que TrickBot, otro de los troyanos bancarios más prolíficos de la historia.

Troyano-GameThief

Ya hemos mencionado que descargar juegos en línea es un método común de infección por troyanos y, de hecho, existen troyanos diseñados específicamente para eso. Mientras que los troyanos bancarios tienen como objetivo los datos financieros, los troyanos ladrones de juegos se crean para robar información relacionada con las cuentas de juegos en línea.

Trojan-Ransom

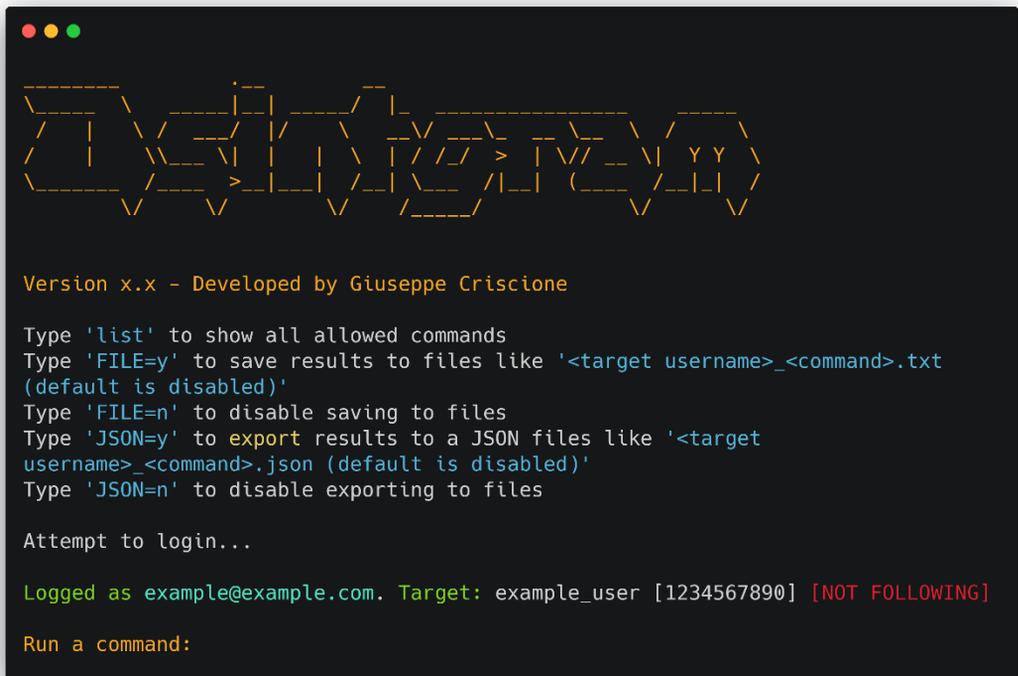
Los troyanos de rescate, una vez instalados, ejecutarán un ataque de ransomware que cifrará un sistema y los datos que contiene, dejándolo inutilizable para la víctima. El cifrado y la devolución segura de datos se pueden proporcionar si se paga una suma.

Troyano-Spy

Un troyano espía instala en secreto programas destinados a espiar o registrar pulsaciones de teclas. Puede monitorear todos los procesos en un dispositivo infectado, rastrear los movimientos de su teclado y robar sus datos.

Osintgram

Osintgram es una herramienta OSINT en Instagram para recopilar, analizar y ejecutar reconocimiento.



```
Version x.x - Developed by Giuseppe Criscione

Type 'list' to show all allowed commands
Type 'FILE=y' to save results to files like '<target username>_<command>.txt'
(default is disabled)'
Type 'FILE=n' to disable saving to files
Type 'JSON=y' to export results to a JSON files like '<target
username>_<command>.json (default is disabled)'
Type 'JSON=n' to disable exporting to files

Attempt to login...

Logged as example@example.com. Target: example_user [1234567890] [NOT FOLLOWING]

Run a command:
```

Descargo de responsabilidad

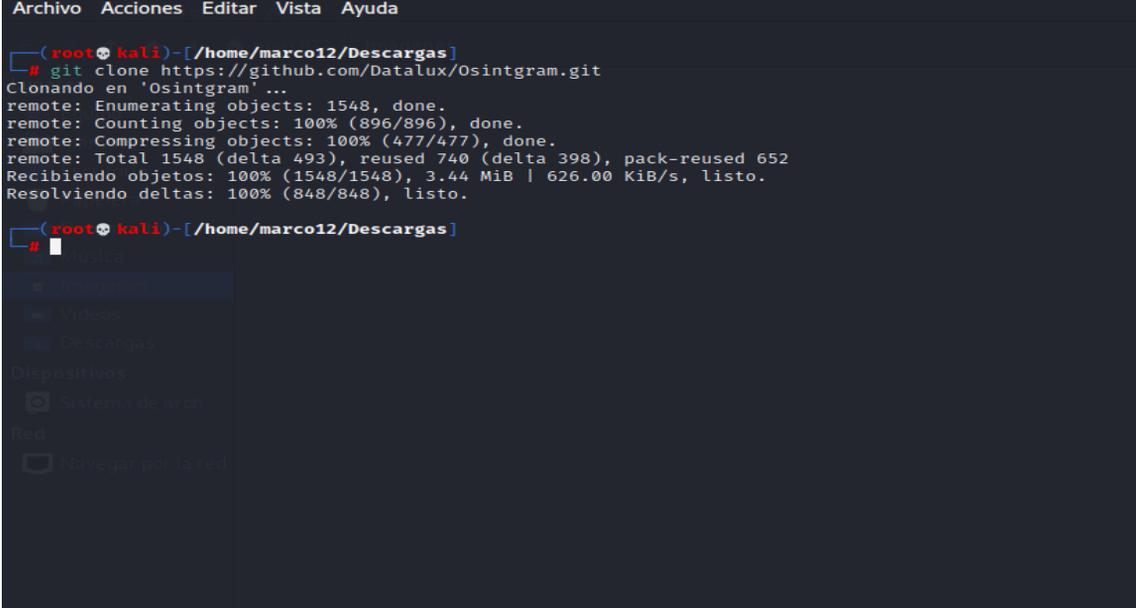
¡SOLO PARA PROPÓSITOS EDUCATIVOS! Los colaboradores no asumen ninguna responsabilidad por el uso de esta herramienta.

Advertencia: Se recomienda no utilizar su cuenta propia/principal al utilizar esta herramienta.

Instalación

- 1) El primer paso es clonar el repositorio con el siguiente comando.

```
1 git clone https://github.com/Datalux/Osintgram.git
```



```
Archivo Acciones Editar Vista Ayuda
(root@kali)~/home/marco12/Descargas
# git clone https://github.com/Datalux/Osintgram.git
Clonando en 'Osintgram' ...
remote: Enumerating objects: 1548, done.
remote: Counting objects: 100% (896/896), done.
remote: Compressing objects: 100% (477/477), done.
remote: Total 1548 (delta 493), reused 740 (delta 398), pack-reused 652
Recibiendo objetos: 100% (1548/1548), 3.44 MiB | 626.00 KiB/s, listo.
Resolviendo deltas: 100% (848/848), listo.
(root@kali)~/home/marco12/Descargas
#
```

Hacking de Instagram - Técnicas y Herramientas OSINT

2) Después tenemos que movernos a la carpeta del repositorio y instalar python3.

1 cd Osintgram

2 sudo apt install python3

```
Archivo Acciones Editar Vista Ayuda
└─(root@kali)-[/home/marco12/Descargas]
└─# cd Osintgram
└─(root@kali)-[/home/marco12/Descargas/Osintgram]
└─# sudo apt install python3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
python3 ya está en su versión más reciente (3.9.7-1).
fijado python3 como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 fonts-roboto-slab libgeos3.10.1 libmms0 libofa0 libperl5.32 libperl5.32:i386 libwmf-0.2-7 libwmf0.2-7 linux-headers-5.15.0-kali-amd64 lin
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.

└─(root@kali)-[/home/marco12/Descargas/Osintgram]
└─#
```

3) También necesitaremos pip.

1 sudo apt install python3-pip

Osintgram

```
Archivo Acciones Editar Vista Ayuda
(root@kali)~/home/marco12/Descargas/Osintgram
# sudo apt install python3-pip
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 fonts-robotoslab libgeos3.10.1 libmms0 libofa0 libperl5.32 libperl5.32:libperl5.32:i386 libwmf-0.2-7 libwmf0.2-7 linux-he
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
 python3-wheel
Se instalarán los siguientes paquetes NUEVOS:
 python3-pip python3-wheel
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1 341 kB de archivos.
Se utilizarán 7 175 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://kali.download/kali kali-rolling/main amd64 python3-wheel all 0.37.1-2 [31.6 kB]
Des:2 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 22.0.2+dfsg-1 [1 309 kB]
Descargados 1 341 kB en 4s (330 kB/s)
Seleccionando el paquete python3-wheel previamente no seleccionado.
(Leyendo la base de datos ... 376487 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../python3-wheel_0.37.1-2_all.deb ...
Desempaquetando python3-wheel (0.37.1-2) ...
Seleccionando el paquete python3-pip previamente no seleccionado.
Preparando para desempaquetar .../python3-pip_22.0.2+dfsg-1_all.deb ...
Desempaquetando python3-pip (22.0.2+dfsg-1) ...
Configurando python3-wheel (0.37.1-2) ...
Configurando python3-pip (22.0.2+dfsg-1) ...
Procesando disparadores para man-db (2.10.1-1) ...
Procesando disparadores para kali-menu (2021.4.2) ...
(root@kali)~/home/marco12/Descargas/Osintgram
#
```

4) Ahora podemos instalar los requerimientos de la herramienta.

1 pip install -r requirements.txt

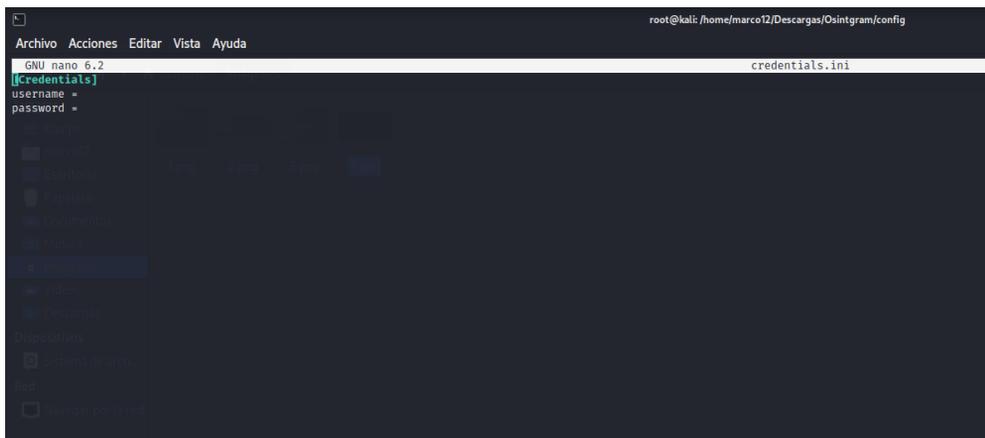
```
Archivo Acciones Editar Vista Ayuda
(root@kali)~/home/marco12/Descargas/Osintgram
# pip install -r requirements.txt
Ignoring pyreadline: markers 'platform_system == "Windows"' don't match your environment
Collecting requests==2.24.0
  Downloading requests-2.24.0-py2.py3-none-any.whl (61 kB)
  61.8/61.8 KB 125.0 KB/s eta 0:00:00
Requirement already satisfied: requests-toolbelt==0.9.1 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (0.9.1)
Collecting geopy>=2.0.0
  Downloading geopy-2.2.0-py3-none-any.whl (118 kB)
  118.9/118.9 KB 158.9 KB/s eta 0:00:00
Collecting prettytable==0.7.2
  Downloading prettytable-0.7.2.zip (28 kB)
  Preparing metadata (setup.py) ... done
Collecting instagram-private-api==1.6.0
  Downloading instagram_private_api-1.6.0.0-py3-none-any.whl (78 kB)
  78.9/78.9 KB 421.7 KB/s eta 0:00:00
Collecting gnureadline>=8.0.0
  Downloading gnureadline-8.0.0.tar.gz (3.1 MB)
  3.1/3.1 MB 628.4 KB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting idna<3, >=2.5
  Downloading idna-2.10-py2.py3-none-any.whl (58 kB)
  58.0/58.8 KB 601.6 KB/s eta 0:00:00
Collecting chardet<4, >=3.0.2
  Downloading chardet-3.0.4-py2.py3-none-any.whl (133 kB)
  133.4/133.4 KB 472.4 KB/s eta 0:00:00
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python3/dist-packages (from requests==2.24.0->-r requirements.txt (line 1)) (2020.6.20)
Collecting urllib3<=1.25.0, >=1.25.1; python_version <= 3.6
  Downloading urllib3-1.25.11-py2.py3-none-any.whl (127 kB)
  128.0/128.0 KB 595.5 KB/s eta 0:00:00
Collecting geographiclib>=2.0
  Downloading geographiclib-1.52-py3-none-any.whl (38 kB)
Building wheels for collected packages: prettytable, gnureadline
  Building wheel for prettytable (setup.py) ... done
  Created wheel for prettytable: filename=prettytable-0.7.2-py3-none-any.whl size=13714 sha256=ca04d6f34b1b9094ea0bef1bd268a3b4ceca1a19dc4e22fd8a25c9f935f
  Stored in directory: /root/.cache/pip/wheels/75/7f/28/77a876f1f8cbeda61aca712815d84d7a32435f8426a2dd7b
  Building wheel for gnureadline (setup.py) ... done
  Created wheel for gnureadline: filename=gnureadline-8.0.0-cp39-cp39-linux_x86_64.whl size=402807 sha256=05036cdd9bc96626fd842df9af29c8222be6a343b84b52bcb11d42ecdfdc28e
  Stored in directory: /root/.cache/pip/wheels/92/f0/93/fdf808790d52b6c6eeea0f2538c5a34ddc23074e57aed125a07
```

Hacking de Instagram - Técnicas y Herramientas OSINT

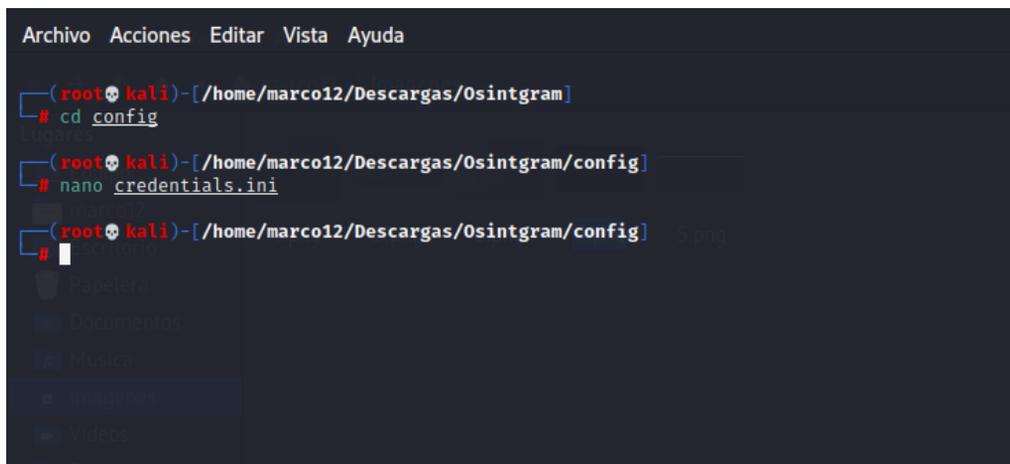
- 5) Este paso es muy importante ya que tenemos que configurar un usuario y contraseña de una cuenta de Instagram que hayamos creado con anterioridad ya que **Osintgram** trabaja con una cuenta vinculada para extraer información, y eso configuraremos en este paso.

1 cd config

2 nano credentials.ini



```
root@kali: /home/marco12/Descargas/Osintgram/config
GNU nano 6.2 credentials.ini
[credentials]
username =
password =
```



```
Archivo Acciones Editar Vista Ayuda
(root@kali)-[/home/marco12/Descargas/Osintgram]
└─# cd config
(root@kali)-[/home/marco12/Descargas/Osintgram/config]
└─# nano credentials.ini
(root@kali)-[/home/marco12/Descargas/Osintgram/config]
└─#
```

Después de poner el usuario y password damos *Ctrl + x* y luego *S* para guardar cambios.

Osintgram

- 6) Ahora podemos empezar a atacar, solo ahí que regresar al directorio raíz de **Osintgram**, recuerda que en el paso anterior entramos en la carpeta **config** pero ya terminamos ahí, después de salir podemos configurar el objetivo que atacaremos.

1 `cd ..` con este comando regresaremos a la carpeta principal.

2 `python3 main.py nombre_objetivo nombre de usuario del objetivo sin arroba.`

```
Archivo Acciones Editar Vista Ayuda
(root@kali)-[/home/marco12/Descargas/Osintgram/config]
└─# cd ..

(root@kali)-[/home/marco12/Descargas/Osintgram]
└─# python3 main.py

Attempt to login ...
ClientCookieExpiredError/ClientLoginRequiredError: Cookie expired at 1628592384

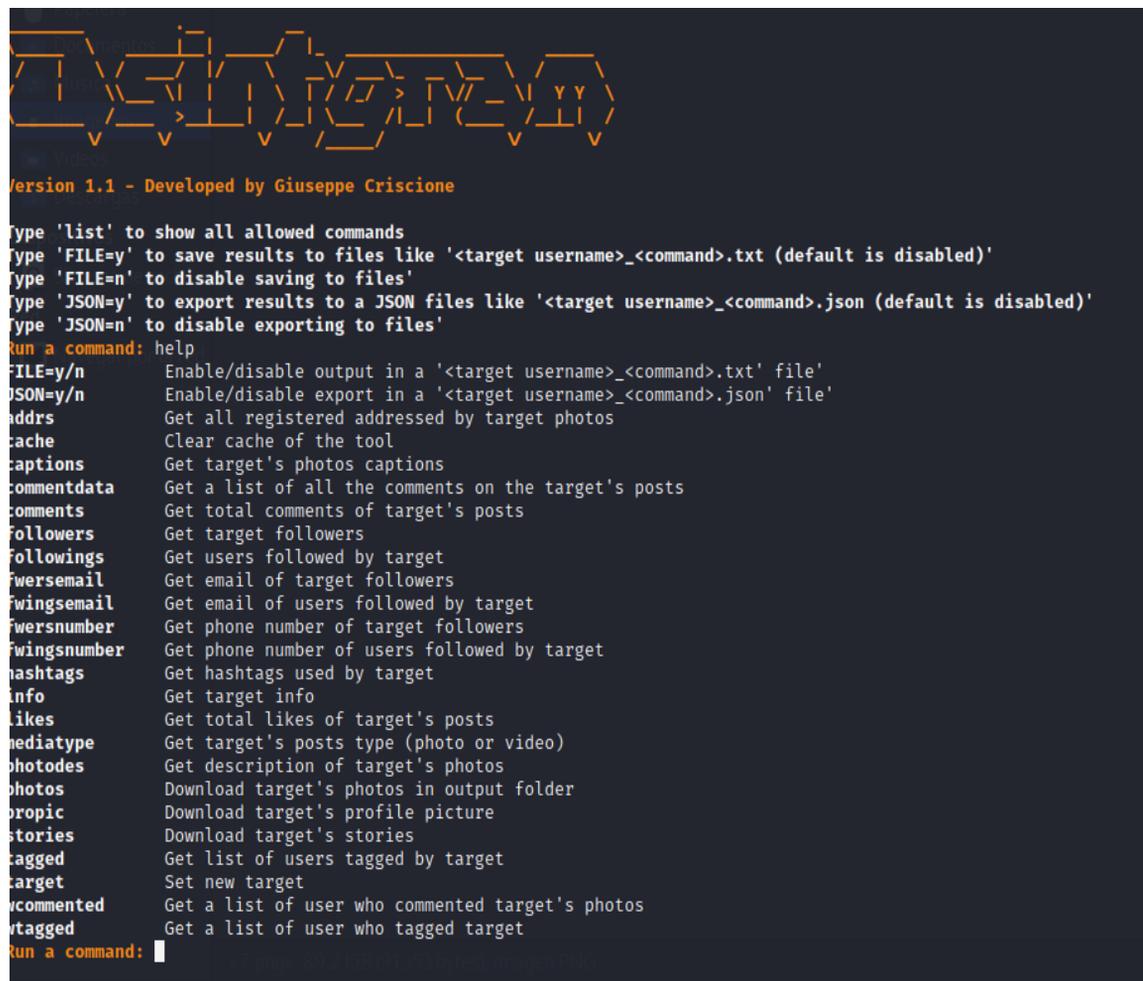
Logged as dragon_inferna@hotmail.es. Target: _lizrodriguezr [1641789341] [FOLLOWING]

Version 1.1 - Developed by Giuseppe Criscione

Type 'list' to show all allowed commands
Type 'FILE=y' to save results to files like '<target username>_<command>.txt (default is disabled)'
Type 'FILE=n' to disable saving to files'
Type 'JSON=y' to export results to a JSON files like '<target username>_<command>.json (default is disabled)'
Type 'JSON=n' to disable exporting to files'
Run a command: █
```

Comandos

No podemos ver todos los comandos, pero veremos 10 de ellos como ejemplo para finalizar este libro.



```
Version 1.1 - Developed by Giuseppe Criscione

Type 'list' to show all allowed commands
Type 'FILE=y' to save results to files like '<target username>_<command>.txt (default is disabled)'
Type 'FILE=n' to disable saving to files'
Type 'JSON=y' to export results to a JSON files like '<target username>_<command>.json (default is disabled)'
Type 'JSON=n' to disable exporting to files'
Run a command: help
FILE=y/n      Enable/disable output in a '<target username>_<command>.txt' file'
JSON=y/n     Enable/disable export in a '<target username>_<command>.json' file'
addr         Get all registered addressed by target photos
cache        Clear cache of the tool
captions     Get target's photos captions
commentdata  Get a list of all the comments on the target's posts
comments     Get total comments of target's posts
followers    Get target followers
followings   Get users followed by target
fwersemail   Get email of target followers
fwingsemail  Get email of users followed by target
fwersnumber  Get phone number of target followers
fwingsnumber Get phone number of users followed by target
hashtags     Get hashtags used by target
info         Get target info
likes        Get total likes of target's posts
mediatype    Get target's posts type (photo or video)
photodes     Get description of target's photos
photos       Download target's photos in output folder
propic       Download target's profile picture
stories      Download target's stories
tagged       Get list of users tagged by target
target       Set new target
commented    Get a list of user who commented target's photos
rtagged      Get a list of user who tagged target
Run a command: █
```


Osintgram

Photos

Este comando descargara todas las fotos de la víctima, dejara una carpeta en la carpeta raíz de la herramienta con el nombre **OUTPUT**.

```
Run a command: photos
How many photos you want to download (default all): Downloading all photos available...
Downloaded 84 photos
Woohoo! We downloaded 84 photos (saved in output folder)
Run a command: █
```

Photodes

Este comando nos dará todas las descripciones de las fotos.

```
Run a command: photodes
Woohoo! We found 12 descriptions
```

Photo	Description
1	[Blurred]
2	[Blurred]
3	[Blurred]
4	[Blurred]
5	[Blurred]
6	[Blurred]
7	[Blurred]
8	[Blurred]
9	[Blurred]
10	[Blurred]
11	[Blurred]
12	[Blurred]

```
Run a command: █
```

Comments

Este comando nos dará todos los comentarios que hizo.

```
Run a command: comments
Searching for target total comments ...
23 comments in 84 posts
Run a command: █
```

Hashtags

Este comando nos dará todos los hashtags que uso la víctima

```
Run a command: hashtags
Searching for target hashtags ...
1. #teamo♥
1. #friends#loveyou
1. #feliz
1. #diablitos♥
1. #MiPrincess
1. #Love
1. #4ever
Run a command: █
```

Osintgram

Tagged

Este comando nos dará una lista de todas las personas etiquetadas por la víctima.

```
Run a command: tagged
Searching for users tagged by target ...

Woohoo! We found 1 (2) users
+-----+-----+-----+-----+
| Posts | Full Name | Username | ID |
+-----+-----+-----+-----+
| 1 | [redacted] | [redacted] | [redacted] |
+-----+-----+-----+-----+

Run a command: █
```

Fwersnumber

Este comando extraerá todos los números de teléfono de los seguidores de la víctima, este comando tardará un rato en terminar.

```
Run a command: fwersnumber
Searching for phone numbers of users followers... this can take a few minutes
Do you want to get all phone numbers? y/n: y
[redacted]
```

Hacking de Instagram - Técnicas y Herramientas OSINT

```
Run a command: fwernumber
Searching for phone numbers of users followers... this can take a few minutes
Do you want to get all phone numbers? y/n: y
Caught 15 followers phone numbers
```

ID	Username	Full Name	Phone

```
Run a command: █
```