OSINT
FUENTE ABIERTA
INTELIGENCIA OSINT

OSINT ofensivo

OWASP
The Open Web Application Security Project

*

OWASP
The Open Web Application Security Project

- **Adán Nurudini**

CEH, ITIL V3, CCNA, CCNP, CASP, PCI-DSS, BSC-IT

Investigador principal de seguridad en Netwatch Technologies

Consultor de proyectos, Information Security Architects Ltd

Miembro, Equipo de Servicio de Resiliencia de Ciberseguridad

Probador de penetración de aplicaciones web

Presidente - Asociación de Estudiantes de la Escuela de Tecnología GIMPA

NETWATCH TECHNOLOGIES

CSRT Cybersecurity Resilience Services Team
MEMBER | www.csrt.org.gh

*

DESCARGO DE RESPONSABILIDAD

Todos los puntos de vista u opiniones presentados en esta presentación son exclusivamente míos y no representan necesariamente a mi empleador.

ÿNo soy abogado ni te doy consejo legal ÿNo te estoy
dando permiso ni autorizándote a hacer nada jamás. ÿDe hecho no hagas nada nunca.

*

Quitar

•

¿Qué **es** OSINT?

• Recopilar datos indirectamente sin conocer otra información • Recopilar datos sobre servidores, ubicación, sistemas operativos, etc. • Inteligencia de amenazas para su organización • Recopilación de datos que podrían protegerlo a usted y a su empresa • Habilidades de GHDB

• Métodos y operaciones de Shodan •

OSINT utilizando solo herramientas gratuitas

OSINT

Open-Source Intelligence (OSINT) es **inteligencia** recopilada de fuentes públicas disponibles

"Abierto" se refiere a fuentes públicas disponibles (a diferencia de las fuentes encubiertas)
No está relacionado con **software de código abierto** o **inteligencia pública .**

Esta información proviene de una variedad de fuentes, incluidas las páginas de redes sociales de su empresa y personal. Estos pueden ser una mina de oro de información, revelando información como el diseño de tarjetas de identificación, el diseño de los edificios y el software utilizado en los sistemas internos.

Fuente: https://en.wikipedia.org/wiki/Open-source_intelligence

OWASP
The Open Web Application Security Project

Inteligencia de código abierto (OSINT)

Campos y Sectores donde mayormente se requiere OSINT.

Gobierno, Finanzas, Telecomunicaciones, Infraestructura Crítica, Empresas de Asesoría en Seguridad Cibernética, Equipos de Inteligencia de Amenazas Cibernéticas, Derecho, Equipos Forenses Cibernéticos, etc.

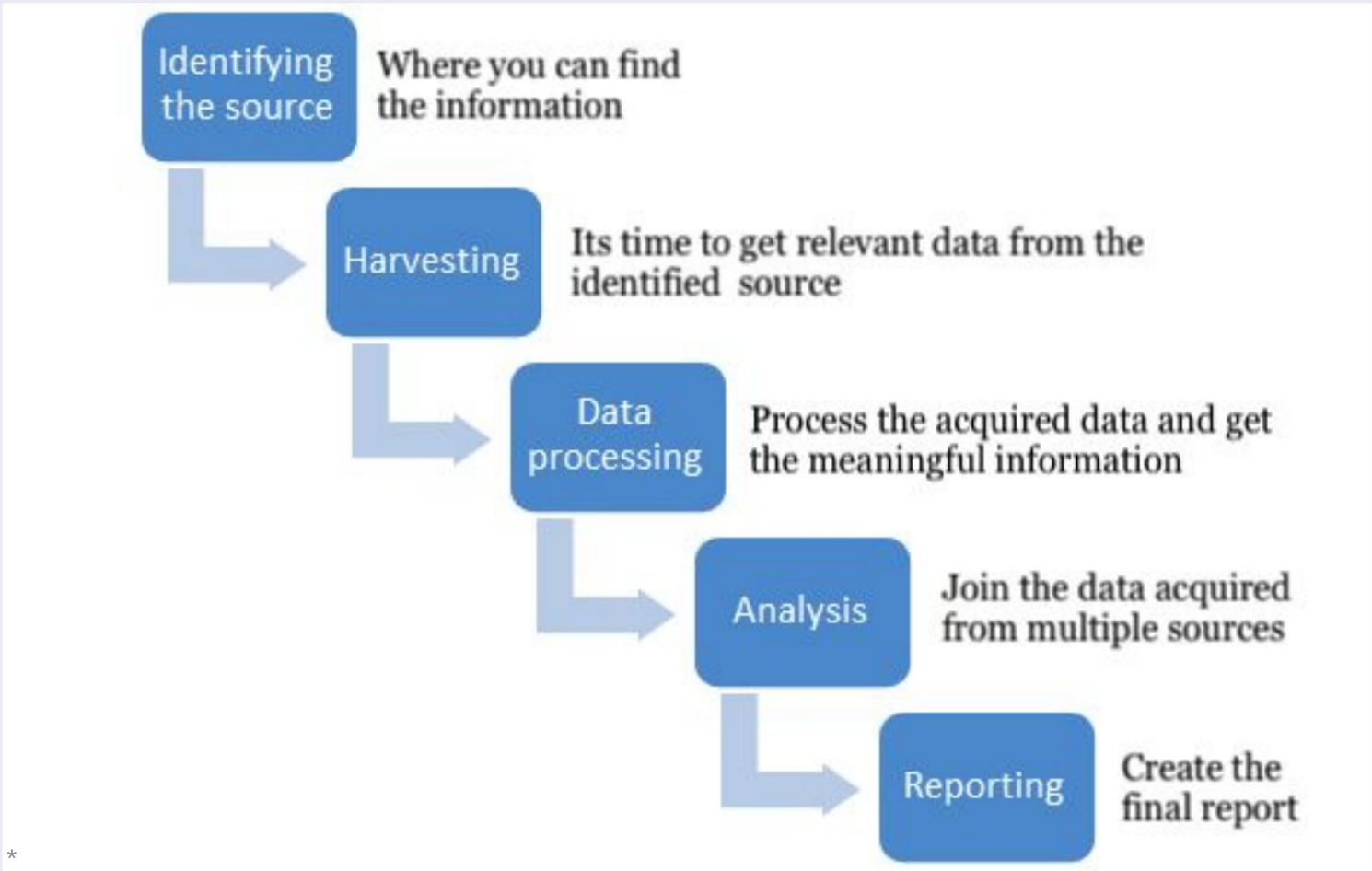
TIPOS DE OSINT Desde

la perspectiva de la Seguridad podemos separar OSINT en: •Ofensivo: Recopilación de información antes de un ataque •Defensivo: Aprendizaje de ataques contra la empresa.

El OSINT da oportunidades tanto al defensor como al atacante; puede conocer la debilidad de una empresa y corregirla mientras que al mismo tiempo la debilidad podría ser explotada.

*

El proceso OSINT



*

OSINT - Qué información buscar

1. IP de infraestructura tecnológica,

nombre de host, servicios, redes, versiones de software/hardware e información del sistema operativo, geolocalización y diagramas de red.

2. Base de datos

Documentos, artículos, presentaciones, hojas de cálculo y archivos de configuración

3. Metadatos

Correo electrónico y búsqueda de empleados (nombre y otra información personal)

OSINT ofensivo – Objetivos finales

La información anterior puede dar lugar a los siguientes ciberataques:

1. Ingeniería Social 2.
Denegación de Servicio
3. Ataques de fuerza bruta de contraseñas
4. Infiltración de objetivos 5.
Las cuentas de usuario toman el control
6. Robo de identidad 7.
Robo de datos

Brace your self demo está comenzando

* Todo el mundo está interesado en algo

OSINT Ofensivo – Recursos y herramientas

1. Motores de búsqueda OSINT

Los atacantes confían en estos motores de búsqueda OSINT para realizar un reconocimiento pasivo.

• Google: https://google.com • Shodan - https://shodan.io • Censys - https://censys.io • Fofa - https://fofa.so • Pila de perros - http://www.dogpile.com • Archivos - https://archive.org/

*

OSINT Ofensivo – Recursos y herramientas

2. Recolección de correo

electrónico La recolección de direcciones de correo electrónico es una técnica OSINT que brinda a los atacantes más información para realizar ataques como el relleno de contraseñas y los ataques de ingeniería social.

La cosechadora https://github.com/laramies/theHarvester

Prowl https://github.com/nettitude/prowl

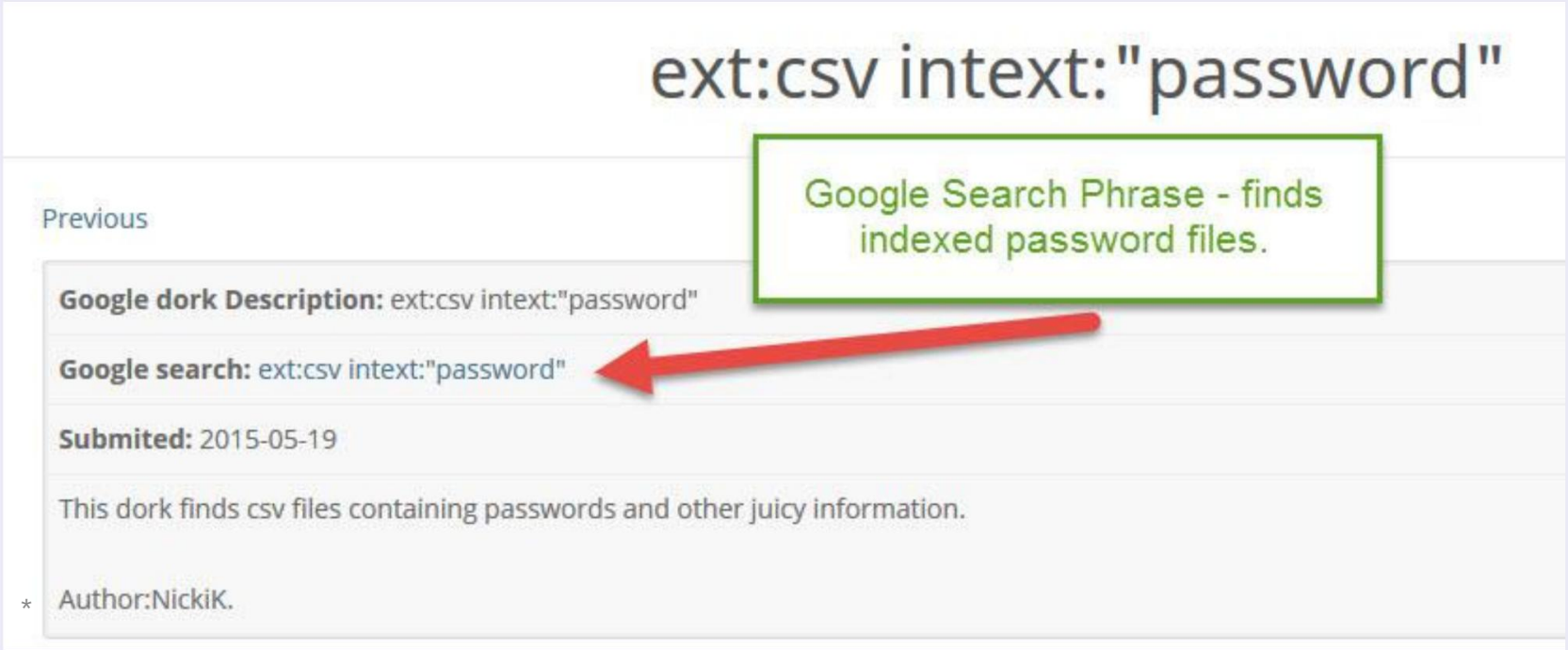
Haveibeenpawned - https://haveibeenpwned.com/

*

OSINT Ofensivo – Recursos y herramientas

3. Base de datos de piratería de Google (GHDB)

El GHDB es un índice de consultas de búsqueda (las llamamos tontos) que se utiliza para encontrar información disponible públicamente. Idiotas - https://www.exploit-db.com



OWASP
The Open Web Application Security Project

OSINT Ofensivo – Recursos y herramientas

3. DNS / Enumeración de subdominios

La enumeración de subdominios es el proceso de encontrar subdominios válidos (que se pueden resolver) para uno o más dominios.

Tener un subdominio no seguro puede generar un riesgo grave para su negocio.

Herramientas para la enumeración de subdominios:

Aquatone - https://github.com/michenriksen/aquatone

Sublister - https://github.com/aboul3la/Sublist3r

Facebook - https://developers.facebook.com/tools/ct

Comprobador de DNS de https://dnsdumpster.com/

OWASP
The Open Web Application Security Project

OSINT es importante y los atacantes y defensores aún lo pasan por alto

Espero que hayas encontrado útil esta charla.

Referencias

https://www.slideshare.net
https://resources.infosecinstitute.com
https://google.com https://www.exploit-db.com https://www.wikipedia.org/

OWASP
The Open Web Application Security Project

Gracias

preguntas y respuestas

Conectemos

Twitter: @Bra__Qwesi___

Correo electrónico: adam.nurudini@st.gimpa.edu.gh

*