

OSINT

Cassiano Peres

DIO Tech Education Analyst

 cassiano-dio

 peres-cassiano

Objetivo Geral

Nesta aula vamos falar sobre OSINT, ou inteligência de fontes abertas e como obter dados sobre alvos.

Pré-requisitos

Este curso requer algum conhecimento de programação básica.

Percurso

Etapa 1

O que é OSINT?

Etapa 2

Pensamento OSINT

Etapa 3

Google Hacking

Percurso

Etapa 4 Conhecendo o Shodan

Etapa 5 Maltego

Etapa 6 FOCA

Etapa 1

O que é OSINT?

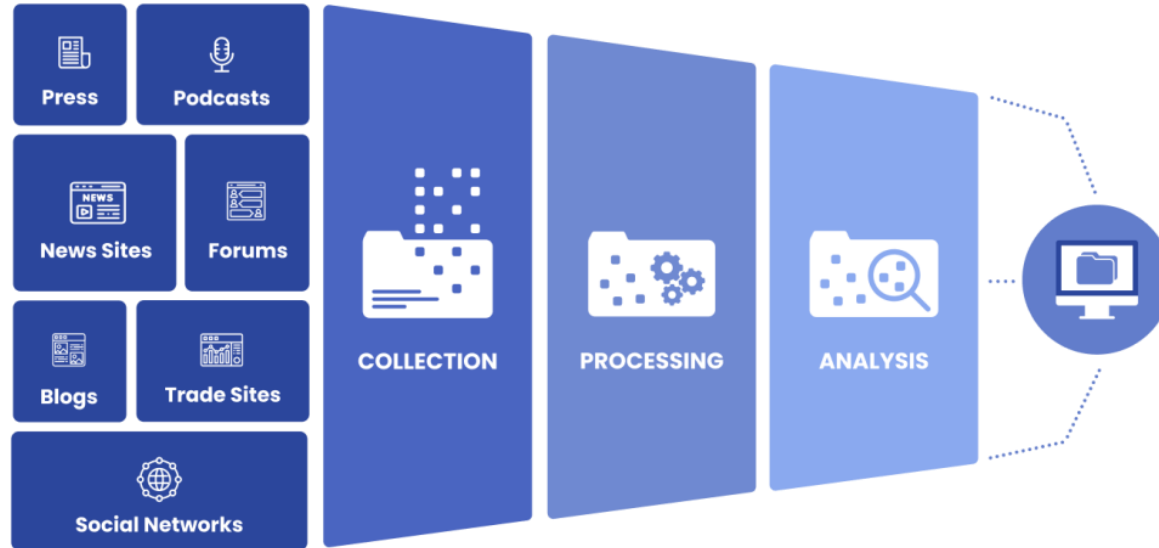
Introdução

Nesta aula vamos conhecer o framework OSINT, a inteligência de fontes abertas.

OSINT

OSINT significa *Open Source Intelligence*, ou inteligência de fontes abertas, ou seja, informações abertas na internet ao público.

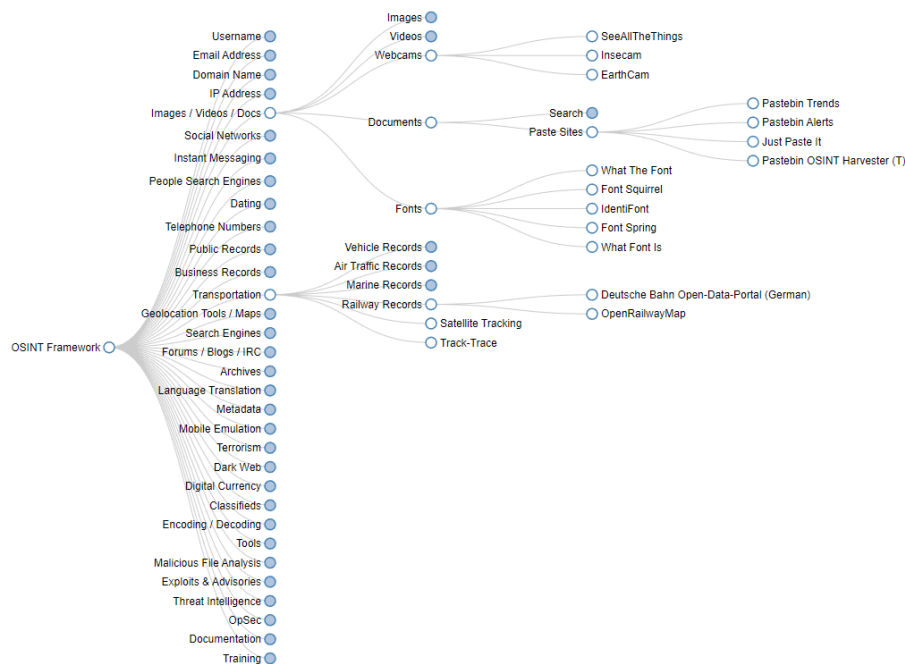
OSINT



OSINT

OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: [Google Hacking](#)
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually



OSINT

Para o OSINT são utilizadas ferramentas voltadas para:

- Coleta de informações;
- Mapeamento e enumeração de serviços;
- Análise de vulnerabilidades;
- Análise de arquivos;
- Extração de metadados.

Tipos de fontes

- Blogs;
- Fóruns,
- Mídias sociais;
- Mídias tradicionais;
- Registros governamentais;
- Etc.

Uso de OSINT

USE CASES OF OSINT INVESTIGATIONS



Network
Footprint



Person
of Interest



Cryptocurrency
Activities



Malware
& Threats



Phishing
& Fraud

Uso de OSINT

- Legislações;
- Combate a frauds;
- Recursos humanos;
- Cibersegurança;
- Operações militares.

Importância do OSINT

- Identificar violações de dados;
- Due Diligence do Cliente (CDD);
- Descobrir vulnerabilidades;
- Apoio aos processos de tomada de decisão;
- Atualizações.

Benefícios do OSINT

- Camada extra de segurança;
- Economia nos processos de decisão;
- Dados analisados conforme são atualizados.

Contratempos do OSINT

- Dificuldade de filtrar os dados inúteis;
- Sem ferramentas o trabalho é moroso;
- Alta necessidade de comandos humanos;
- Não há um padrão ideal definido sobre a quantidade de informações coletadas e analisadas.

Técnicas do OSINT

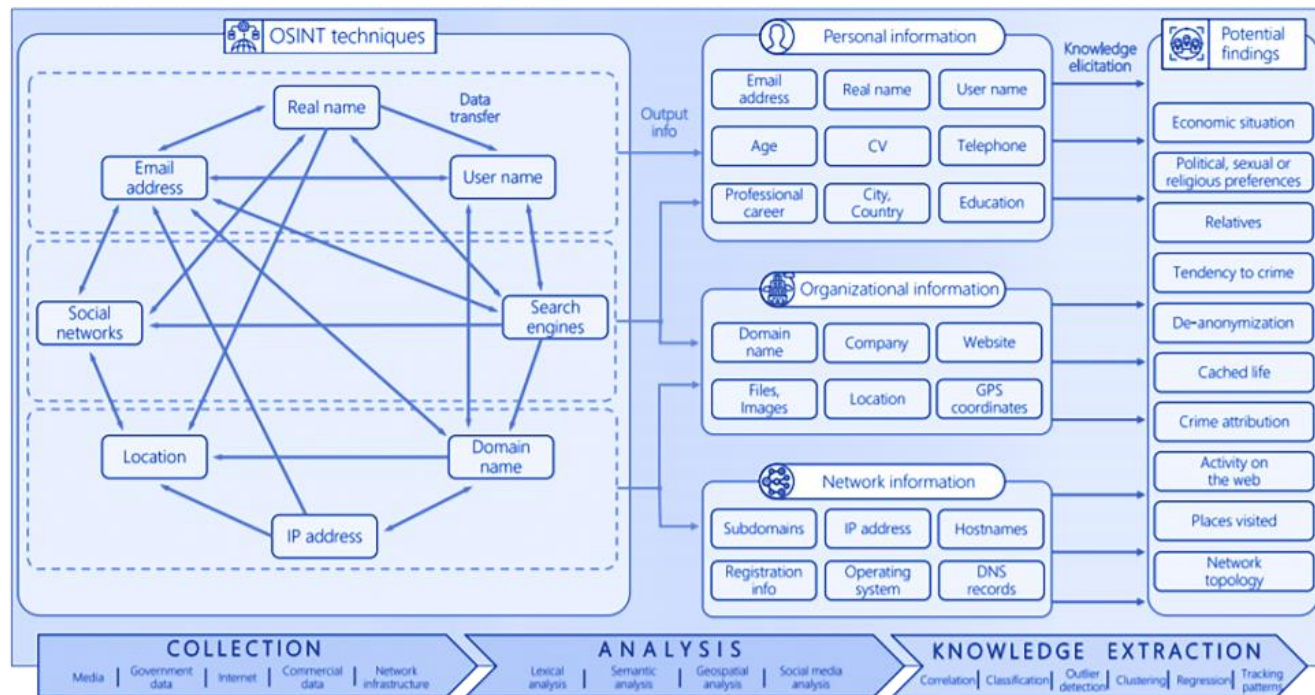


FIGURE 2. Principal OSINT workflows and derived intelligence.



Conclusão

OSINT pode ser considerado um canivete suíço do pentester, sendo extremamente útil para preparar a defesa contra ataques maliciosos.

Etapa 2

Pensamento OSINT

Introdução

Além de ter em mãos as fontes e ferramentas para análise de dados, precisamos saber como utilizá-los da forma mais efetiva possível

Mindset OSINT

OSINT requer uma mentalidade especial, incluindo habilidades analíticas, flexibilidade de pensamento e paciência.



Mindset OSINT

- Quais as fontes escolhidas?
- Qual a confiabilidade das fontes?
- Quais palavras chaves utilizar?
- Quais as melhores ferramentas?

Mindset OSINT

Não adianta ter as melhores fontes e ferramentas se não souber como utilizá-las.

Mindset OSINT

OFFENSIVE

Makes direct contact with the target.



- ▶ **Real-time** / more accurate data
- ▶ **Higher Risk** of being detected by target

1

PASSIVE

Does not make direct contact with the target.



- ▶ **Historical** 3rd-party records
- ▶ **Low Risk** of being detected

2

Mindset OSINT

- Escolher o assunto pesquisado;
- Definição de fontes;
- Reunir palavras-chave;
- Escolher a ferramenta OSINT;
- Refinar as informações contradas;
- Cuidado com informações falsas.

Etapa 3

Google Hacking

Introdução

Nesta aula vamos falar sobre o uso de técnicas de pesquisas avançadas utilizadas no Google para encontrar informações.



Introdução

O Google Hacking nada mais é que uma prática para encontrar arquivos e/ou falhas a partir do Google, usando ele como uma espécie de scanner, com comandos de buscas avançadas por strings chamadas de “**dorks**” ou “**operadores de pesquisa**”.

Dorks

Com a composição de dorks podemos retornar domínios específicos, títulos, palavras, arquivos, etc.

Dorks

- “**site:**” Busca em um site específico:

site:exemplo.com.br

- “**intitle:**” Busca por título de páginas:

intitle:"< Fazer login"

- “**inurl:**” Busca de termos presentes na url:

inurl:/wp-admin

Dorks

- “**intext:**” Busca por texto no conteúdo do site:

intext:adminpass

- “**filetype:**” Busca por formato de arquivos (.jpg,.zip,.txt):

filetype:.txt

- “**inurl:**” Busca de termos presentes na url:

inurl:/wp-admin

Dorks

- “**-termo**”: O sinal de “-” exclui um termo da pesquisa
- “**2021...2022:**” Busca entre datas

Bancos de dados de Dorks

São sites com várias Dorks voltadas à exploração de vulnerabilidades em sites.

- Exploit-db
- InurlBR

Construindo Dorks

Vamos explorar algumas Dorks e obter informações com o Google Hacking.

Conclusão

Nesta aula tivemos uma noção do quão abertos são os sistemas e o perigo que isso representa.

Etapa 4

Conhecendo o Shodan

Introdução

Nesta aula vamos conhecer o Shodan, o “Google dos Hackers”, utilizado para encontrar dispositivos conectados à internet.



Shodan

- Lançado em 2009, é um mecanismo de busca desenvolvido pelo programador John Matherly;
- Acessado por meio de um endereço na web, busca diversos tipos de dispositivos conectados à internet;
- Esses dispositivos podem ser desde computadores, servidores, mobile até câmeras abertas.

Shodan

Shodan Developers Monitor View All...


SHODAN itaperuna [Explore](#) [Pricing](#) [Enterprise Access](#) [Try out the new beta website!](#) [Help Center](#)

[New to Shodan?](#) [Login or Register](#)

[Exploits](#) [Maps](#)

TOTAL RESULTS
4

TOP COUNTRIES



Brazil 4

TOP SERVICES

PPTP 3
Automated Tank Gauge 1

TOP ORGANIZATIONS

Itanet Conecta Ltda 4

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Added on 2021-03-21 03:10:10 GMT
Brazil, Itaperuna

ipmi

Firmware: 1
Hostname: Nossaloja15-Itaperuna
Vendor: Mikrotik

120100
18/03/21 15:29

Brazil, Itaperuna

Auto Posto Marco
BR 356 S/N KM 03
Itaperuna

INVENTÁRIO NO TANQUE

TANQ	PRODUTO	VOLUME	TC-VOLUME	VOLUME	ALTURA	ÁGUA	TEMPER
1	Gssolina Comun	9596	0	10644	1222.67	0.00	30.18
2	Gasolina GRID	6223...					

Firmware: 1
Hostname: FORTE-CPE-IFF-ITAPERUNA
Vendor: Mikrotik

Shodan

Permite listar e filtrar dispositivos por localização, tipo de servidor, portas.

Shodan

Search Query Examples

[FILTER REFERENCE](#)

// BASICS

Websites that require HTTPS connections

`HTTP Strict-Transport-Security`

SEARCH

Services that have the word "Apache" in their headings

`Apache`

SEARCH

Apache web servers

`product:Apache`

SEARCH

Services with a hostname containing either "google.com"
OR "facebook.com"

`hostname:google.com,facebook.com`

SEARCH

// HTTP FILTERS

Websites that have the word "Apache" in their HTML

`http.html:Apache`

SEARCH

Websites that are using the Bootstrap CSS framework

`http.component:bootstrap`

SEARCH

Prática

Vamos praticar alguns comandos de filtros e listagens no Shodan.

Etapa 5

Maltego

Introdução

Nesta aula vamos falar de outra ferramenta de OSINT, o Maltego.



MALTEGO

Maltego

É um dos frameworks OSINT mais famosos para reconhecimento **pessoal e organizacional**.

Maltego

É uma ferramenta GUI que permite coletar informações sobre **qualquer indivíduo**, extraíndo as informações que estão **publicamente disponíveis na internet** por diferentes métodos.

Maltego

1



Mapping the
online footprint
of the person of
interest

2



Finding
personal detail
from known
online presence

3



Using identity
intelligence to
understand the
target's profile

Maltego

Maltego Kali Linux Edition 3.6.1

Investigate Manage View Organize Machines Collaboration

Clipboard Transforms Find Selection Zoom

Copy Paste Cut Delete

Number of Results

Quick Find

Entity Selection

Select All Add Similar Siblings Select Children Add Children Select by Type

Invert Selection Add Path Select Neighbors Add Neighbors Select Links

Select None Select Parents Add Parents Select Bookmark Reverse Links

Zoom to Zoom in Zoom to Fit Zoom Out Zoom 100% Zoom Selection

Overview

Detail View

Domain maltego Domain nist.gov

Relationships

Outgoing

av.nist.gov admin.nist.gov edje.nist.gov gmail.nist.gov help.nist.gov www.nist.gov

apache.nist.gov debian.nist.gov email.nist.gov imap.nist.gov

Domain Name nist.gov

WHOIS Info

Graph info

Weight 0

Incoming 0

Outgoing 12

Bookmark

Output - Transform Output

Transform toLocation returned with 1 entities (from entity "129.6.72.37")

Transform toLocation returned with 1 entities (from entity "129.6.162.162")

Transform toLocation returned with 1 entities (from entity "216.58.195.51")

Transform toLocation returned with 1 entities (from entity "132.163.4.162")

Transform toLocation returned with 1 entities (from entity "129.6.13.25")

Transform toLocation returned with 1 entities (from entity "129.6.83.179")

Transform toLocation returned with 1 entities (from entity "129.6.16.94")

Transform toLocation returned with 1 entities (from entity "129.6.61.155")

Transform toLocation returned with 1 entities (from entity "129.6.93.201")

Transform toLocation done (from 10 entities)

1 of 26 entities

Maltego

Possui versões pagas e *community*, gratuita para uso mas com funcionalidades a menos.

O que o Maltego encontra?

- Pessoas
- Grupos de pessoas (redes sociais)
- Empresas
- Organizações
- Sites

O que o Maltego encontra?

- Domínios
- Nomes DNS
- Blocos de rede
- Endereços IP
- Afiliações
- Documentos e arquivos

Benefícios do Maltego

O Maltego pode ser útil para a fase de coleta de informações de todos os trabalhos relacionados à segurança, gerando economia de tempo, adicionando mais precisão e inteligência.

Prática

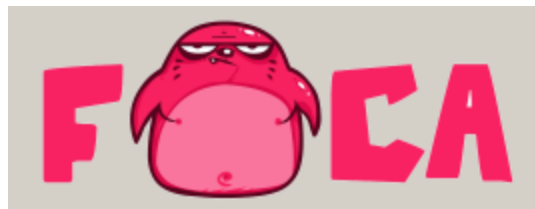
Vamos instalar e fazer algumas pesquisas com o Maltego.

Etapa 6

FOCA

Introdução

Nesta aula vamos falar de outra ferramenta de OSINT, o FOCA.



FOCA

FOCA significa *Fingerprinting & Organisation with Collected Archives*, sendo uma ferramenta utilizada para encontrar, fazer download, analisar e extrair metadados de arquivos.

FOCA

Podem ser arquivos como MS Office, PDF, Open Office, SVG e uma infinidade de formatos.

FOCA

Marca - FOCA Open Source 3.4.7.0

Project Plugins Options TaskList About

Marca

- Network
- Domains
- Document Analysis
 - Files (300/300)
 - doc (4)
 - docx (22)
 - pdf (272)
 - xls (2)
 - Unknown (17)
 - Metadata Summary
 - Users (0)
 - Folders (0)
 - Printers (0)
 - Software (0)
 - Emails (0)
 - Operating Systems (0)
 - Passwords (0)
 - Servers (0)
 - Malware Summary (DIARIO)

Search engines

Extensions

Search All

Id	Type	URL	Download	Download Date	Size	Meta
60	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107481345575KBx		06/27/2021 07:48:13	455.75 KB	x
61	pdf	https://www.marca.com/multimedia/2021/06/27/062720210745275601KBx		06/27/2021 07:45:27	560.1 KB	x
62	pdf	https://www.marca.com/multimedia/2021/06/27/06272021074530412MBx		06/27/2021 07:45:30	4.12 MB	x
63	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107481429889KBx		06/27/2021 07:48:14	298.89 KB	x
64	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107452925812KBx		06/27/2021 07:45:29	258.12 KB	x
65	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107481637358KBx		06/27/2021 07:48:16	373.58 KB	x
66	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107453248408KBx		06/27/2021 07:45:32	484.08 KB	x
67	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107453337249KBx		06/27/2021 07:45:33	372.49 KB	x
68	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107453635533KBx		06/27/2021 07:45:36	355.33 KB	x
69	pdf	https://www.marca.com/multimedia/2021/06/27/0627202107480541417KBx		06/27/2021 07:48:05	414.17 KB	x
70	pdf	https://www.marca.com/multimedia/2021/06/27/06272021074535295MBx		06/27/2021 07:45:35	2.95 MB	x

Download

Extract Metadata

Analyze Malware

Delete

Download All

Extract All Metadata

Analyze All Metadata

Analyze All Malware

Delete All

Add file

Add folder

Add URLs from file

Link(s)

Settings Deactivate AutoScroll Clear

Save log to File

All documents have been downloaded

Time Source Severity Message

7:41:54 ... MetadataSearch medium GoogleWeb search finished successfully!! Total found results

FOCA

Permite encontrar metadados como:

- Usuários do software;
- Versão do software;
- Pastas;
- Sistemas operacionais;
- Etc.

FOCA

Vamos instalar o foca e analisar alguns arquivos para extração de metadados.

Dúvidas?

- > Fórum/Artigos
- > Comunidade Online (Discord)

