# 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?

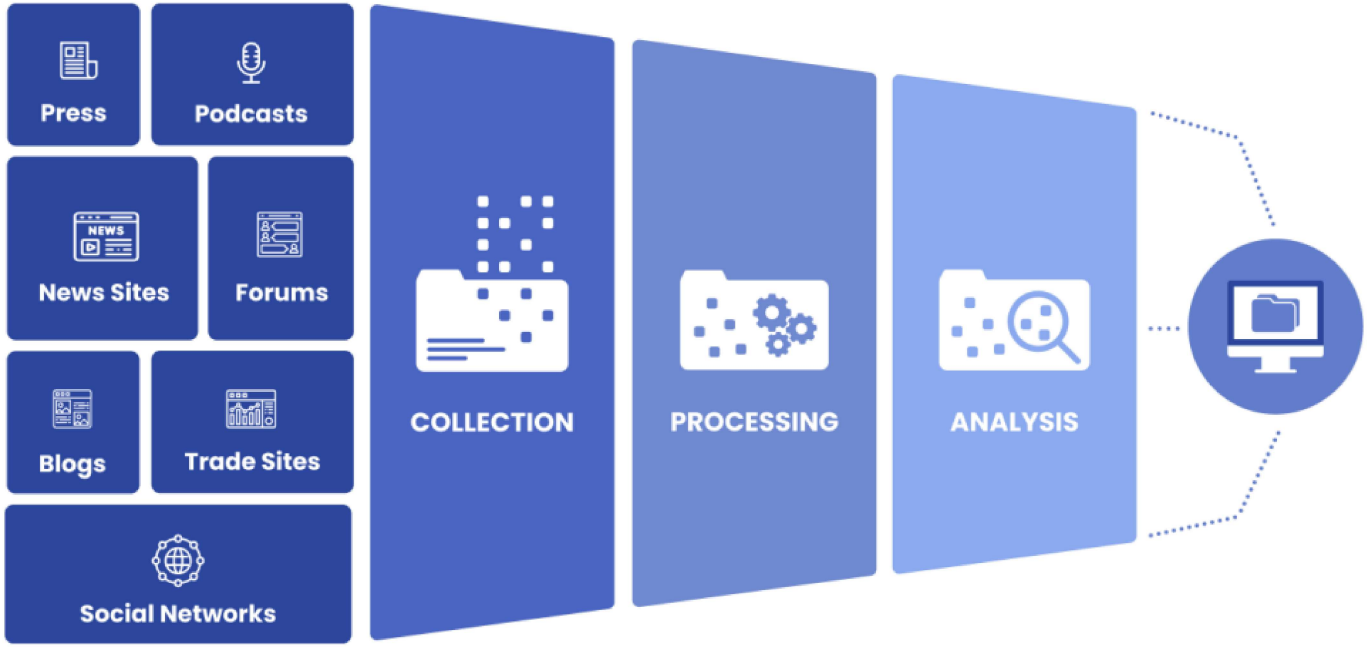
# Introdução

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

# OSINT

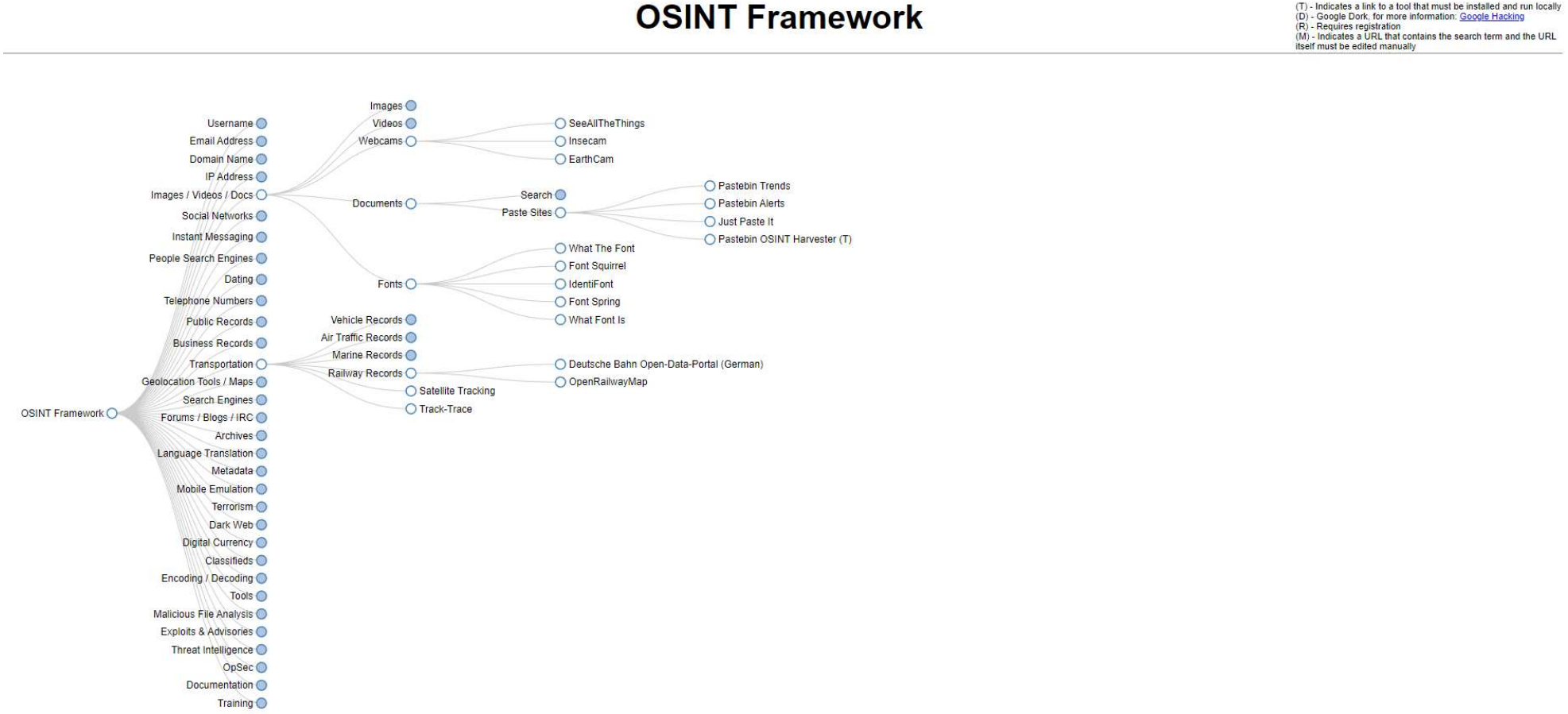
*OSINT* significa *Open Source Intelligence*, ou inteligência de fontes abertas, ou seja, informações abertas na internet ao público.

# OSINT


Press
Podcasts
NEWS
News Sites
Forums
Blogs
Trade Sites
Social Networks
COLLECTION
PROCESSING
ANALYSIS

[9]

# 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 Framework
Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Malicious File Analysis
Exploits & Advisories
Threat Intelligence
OpSec
Documentation
Training
Images
Videos
Webcams
SeeAllTheThings
Insecam
EarthCam
Documents
Search
Paste Sites
Pastebin Trends
Pastebin Alerts
Just Paste It
Pastebin OSINT Harvester (T)
Fonts
What The Font
Font Squirrel
IdentiFont
Font Spring
What Font Is
Vehicle Records
Air Traffic Records
Marine Records
Railway Records
Deutsche Bahn Open-Data-Portal (German)
OpenRailwayMap
Satellite Tracking
Track-Trace

# 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

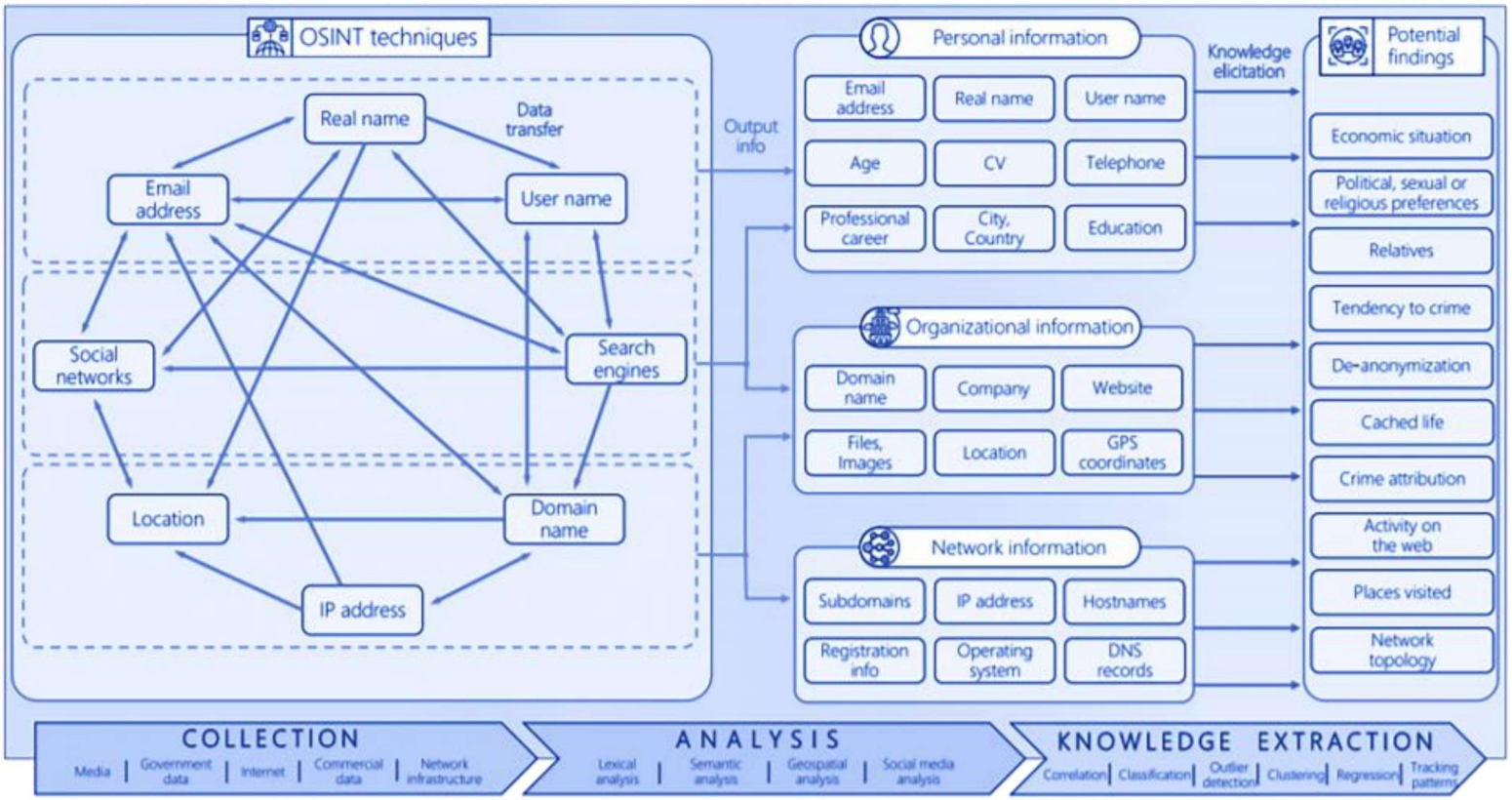
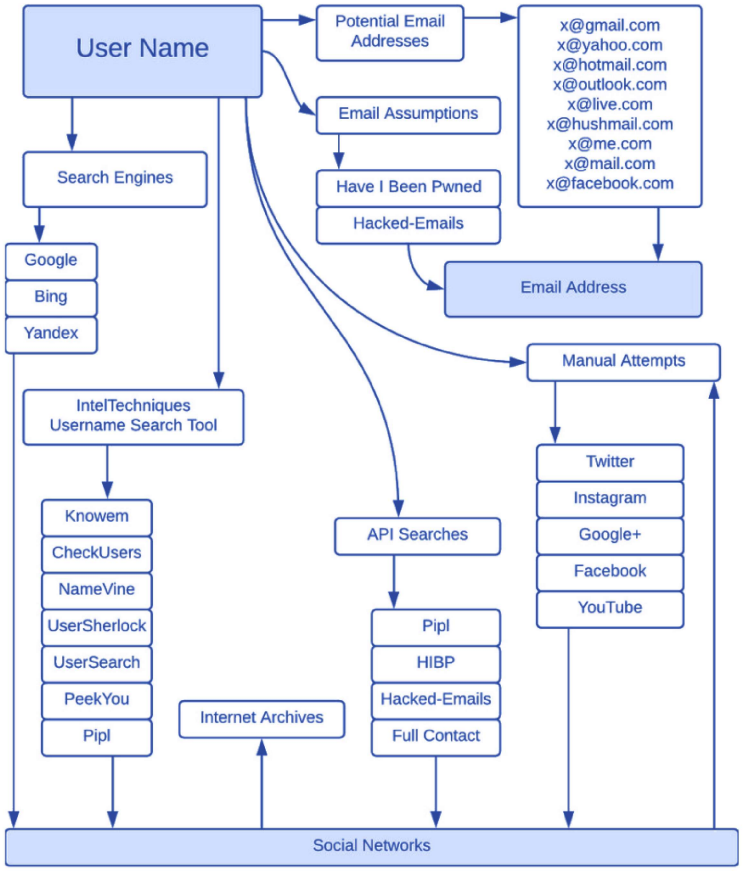



**FIGURE 2. Principal OSINT workflows and derived intelligence.**

[18]

# Técnicas do OSINT



# Conclusão

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

Etapa 2

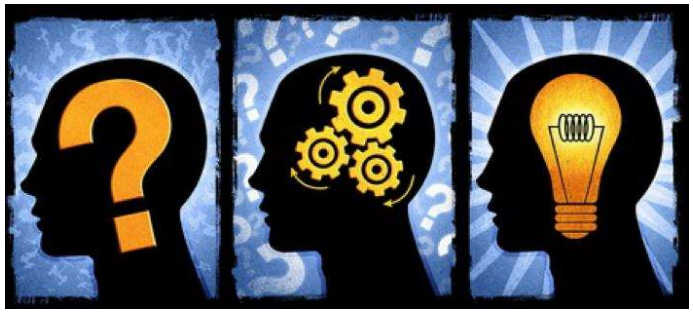
# Pensamento OSINT

# 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?

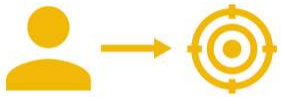
# Mindset OSINT

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

# Mindset OSINT

**OFFENSIVE** 1

Makes direct contact with the target.



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

**PASSIVE** 2

Does not make direct contact with the target.

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

# 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 aquivos 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

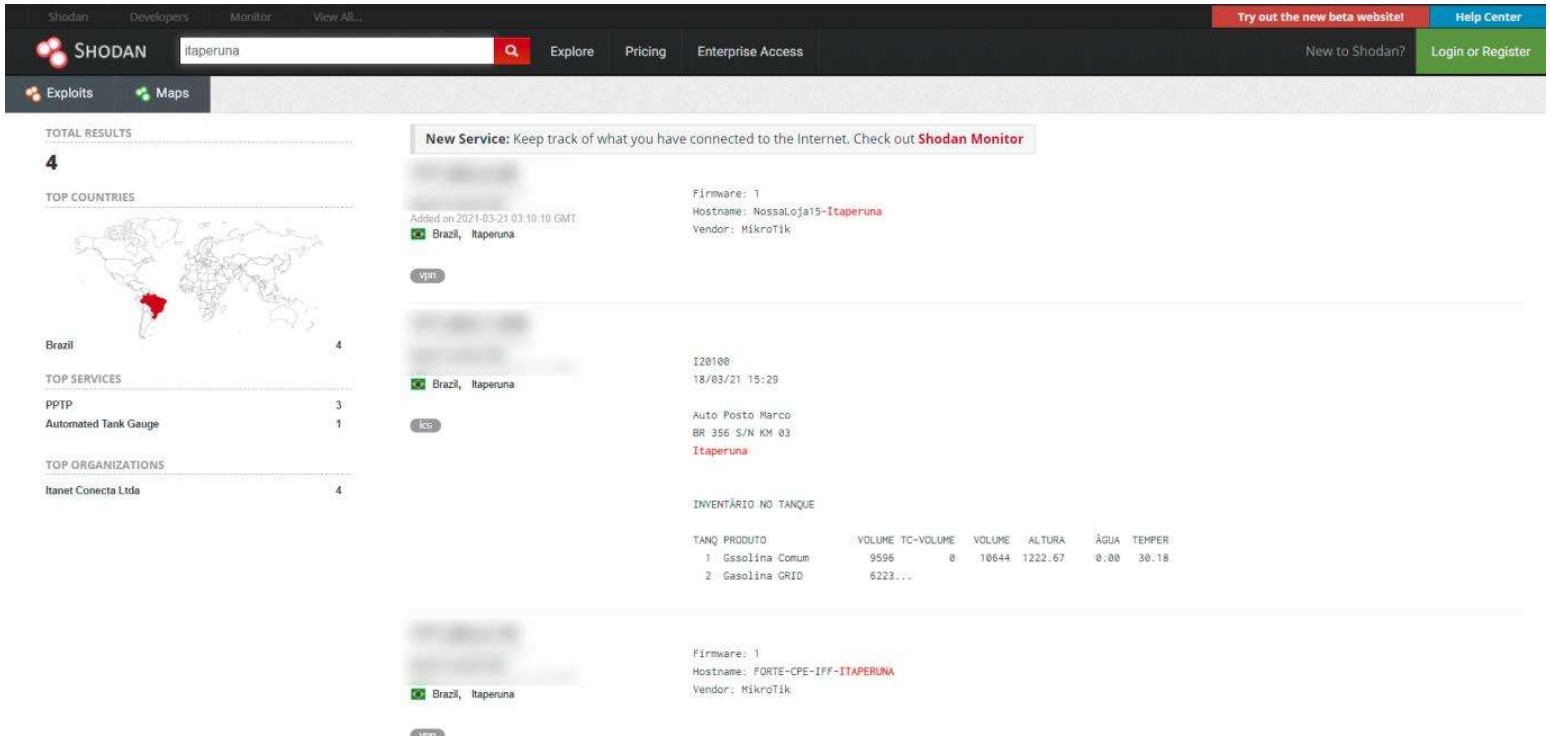
# Introdução

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.

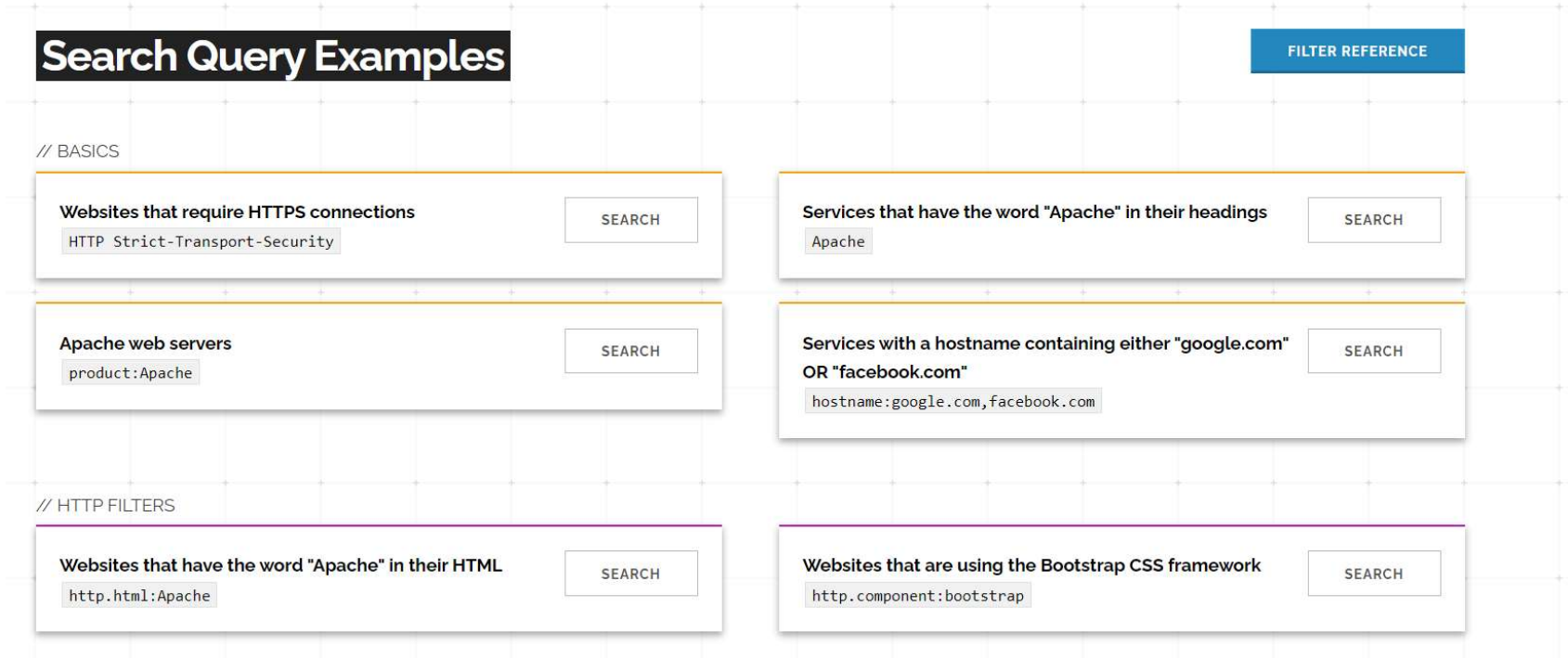
# Shodan


Shodan
Developers
Monitor
View All...
Try out the new beta website!
Help Center
SHODAN
itaperuna
Explore
Pricing
Enterprise Access
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
Firmware: 1
Hostname: NossaLoja15-Itaperuna
Vendor: MikroTik
vpn
Brazil, Itaperuna
I20100
18/03/21 15:29
Auto Posto Marco
BR 356 S/N KM 03
Itaperuna
INVENTÁRIO NO TANQUE
TANQ PRODUTO VOLUME TC-VOLUME VOLUME ALTURA ÁGUA TEMPER
1 Gssolina Comum 9596 0 10644 1222.67 0.00 30.18
2 Gasolina GRID 6223...
ics
Brazil, Itaperuna
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

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

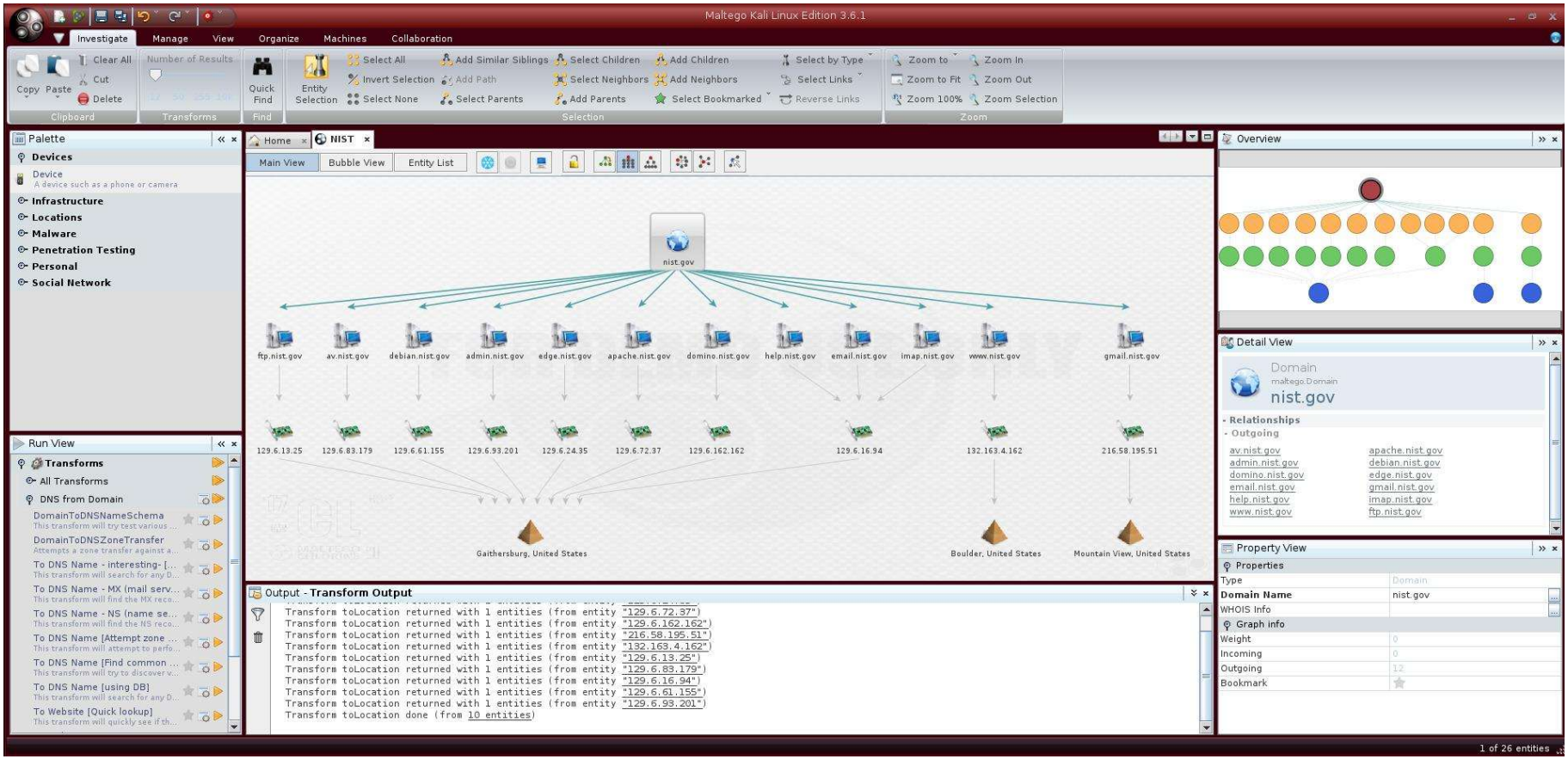
# Maltego

É uma ferramenta GUI que permite coletar informações sobre **qualquer indivíduo**, extraindo 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
Palette
Devices
Infrastructure
Locations
Malware
Penetration Testing
Personal
Social Network
Home
NIST
Main View
Bubble View
Entity List
nist.gov
ftp.nist.gov
av.nist.gov
debian.nist.gov
admin.nist.gov
edge.nist.gov
apache.nist.gov
domino.nist.gov
help.nist.gov
email.nist.gov
imap.nist.gov
www.nist.gov
gmail.nist.gov
Gaithersburg, United States
Boulder, United States
Mountain View, United States
Overview
Detail View
Domain
nist.gov
Property View
Run View
Transforms
Output - Transform Output
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.

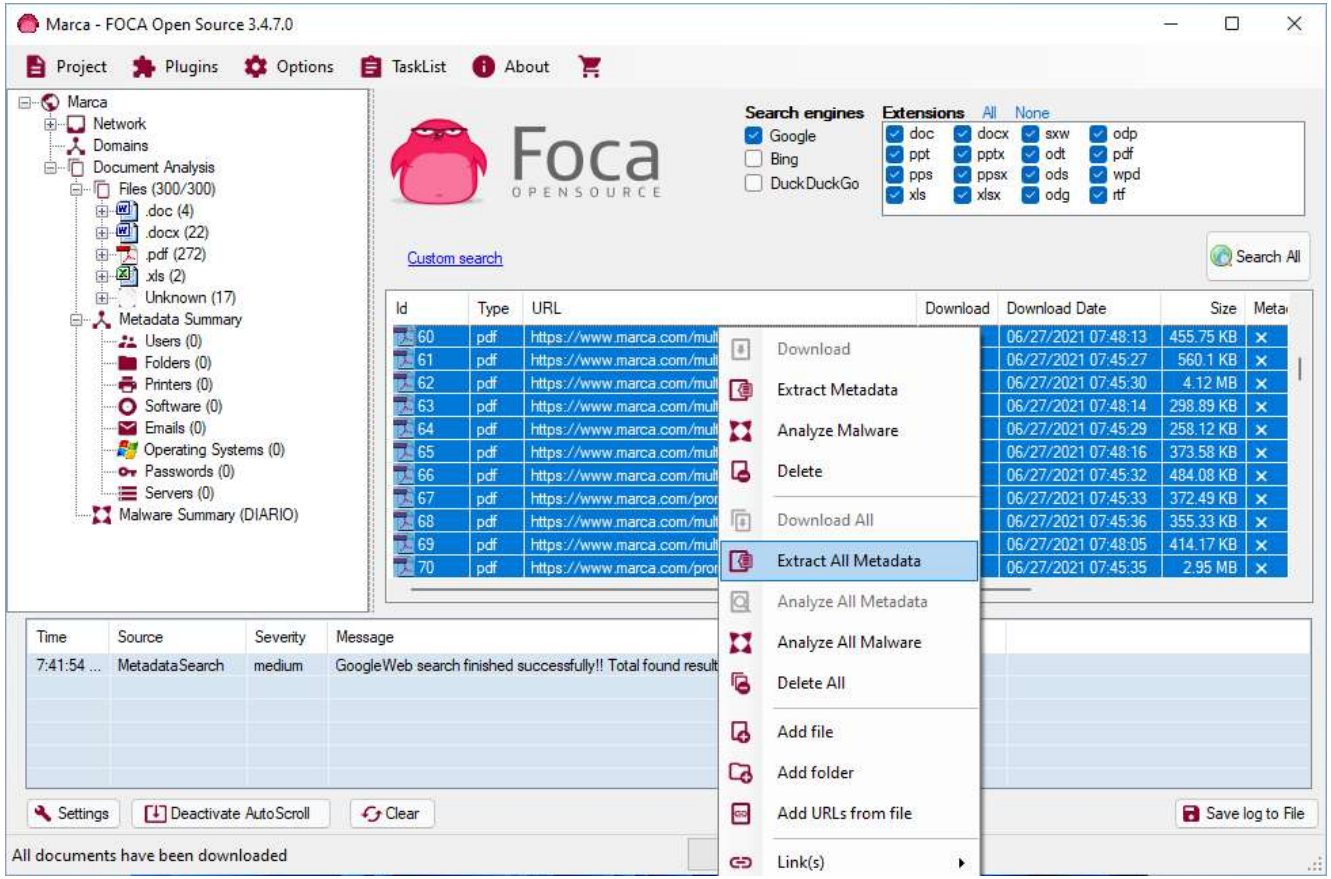
# FOCA

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

# FOCA

Podem ser aquivos 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)
Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Extensions
All
None
doc
docx
sxw
odp
ppt
pptx
odt
pdf
pps
ppsx
ods
wpd
xls
xlsx
odg
rtf
Custom search
Search All
Id
Type
URL
Download
Download Date
Size
60 pdf 06/27/2021 07:48:13 455.75 KB
61 pdf 06/27/2021 07:45:27 560.1 KB
62 pdf 06/27/2021 07:45:30 4.12 MB
63 pdf 06/27/2021 07:48:14 298.89 KB
64 pdf 06/27/2021 07:45:29 258.12 KB
65 pdf 06/27/2021 07:48:16 373.58 KB
66 pdf 06/27/2021 07:45:32 484.08 KB
67 pdf 06/27/2021 07:45:33 372.49 KB
68 pdf 06/27/2021 07:45:36 355.33 KB
69 pdf 06/27/2021 07:48:05 414.17 KB
70 pdf 06/27/2021 07:45:35 2.95 MB
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)
Time
Source
Severity
Message
7:41:54 ... MetadataSearch medium GoogleWeb search finished successfully!! Total found result
Settings
Deactivate AutoScroll
Clear
Save log to File
All documents have been downloaded

# 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)

SCAN ME