



FUNDAMENTOS DE OSINT

PROF. JOAS ANTONIO



OBJETIVO DO EBOOK

- Ensinar o básico do OSINT
- Passar os conceitos teóricos e práticos de OSINT
- Pequeno guia para quem está começando

SOBRE O PROFESSOR

- Pesquisador de Segurança da Informação
- Assistente de Professor pela Cybrary
- PenTester pela ExperSec
- + 25 certificações e 190 cursos
- Professor e Palestrante



- **OSINT** (sigla para *Open source intelligence* ou Inteligência de Fontes Abertas) é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através dados disponíveis para o público em geral, como jornais, revistas científicas e emissões de TV. OSINT é uma das fontes de inteligência. É conhecimento produzido através de dados e informações disponíveis e acessíveis a qualquer pessoa.
- **Open Source Intelligence (OSINT)**. É um modelo de inteligência que visa encontrar, selecionar e adquirir informações de fontes públicas e analisá-las para que junto com outras fontes possam produzir um conhecimento. Na comunidade de inteligência (IC), o termo "aberto" refere-se a fontes disponíveis publicamente.
- As fases que abrangem a coleta especializada segundo fontes e meios utilizados para a obtenção das informações englobam basicamente quatro técnicas. Convencionalmente separadas em três de cunho sigiloso e uma de natureza ostensiva. Nos países centrais, cerca de 80 a 90% dos investimentos governamentais na área de Inteligência são absorvidos por este estágio do ciclo. Os trabalhos acadêmicos que versam sobre Inteligência definem as técnicas de coleta através de acrônimos derivados do uso norte-americano: HUMINT (Inteligência de fontes humana), SIGINT (Inteligência de sinais), IMINT (Inteligência de imagens) e OSINT (Inteligência de fontes abertas).



História da Inteligência de fontes abertas

- O Foreign Broadcast Information Service (FBIS) foi serviço norte-americano pioneiro no trato com OSINT. Iniciou suas atividades ao final da década de 1930, na Universidade de Princeton. Durante a Segunda Guerra Mundial, teve como função analisar os noticiários internacionais captados por rádio e durante a Guerra Fria, monitorar publicações oficiais provenientes da União das Repúblicas Socialistas Soviéticas, como o Pravda e o Izvestia. Com o fim da Guerra Fria, o FBIS passou por um período de ostracismo, até que os atentados, em setembro de 2001, contra o World Trade Center e o Pentágono, trouxeram à tona a importância da utilização das fontes abertas.
- Em oito de novembro de 2005, John Negroponte, o czar da Inteligência norte-americana, anunciou a criação de um departamento voltado exclusivamente para a coleta, reunião e produção de conhecimento a partir de fontes abertas - processo conhecido na literatura especializada como Open Source Intelligence (OSINT). O departamento, integrante da estrutura da Agência Central de Inteligência (CIA), foi criado com a incumbência de funcionar como um centro especializado da Agência. A institucionalização do Centro de Fontes Abertas (Open Source Center – OSC) insere-se nos esforços de modernização e reforço da Inteligência dos Estados Unidos da América.



Por que utilizar fontes abertas?

- As informações coletadas por meio de fontes abertas, possuem baixo custo, se comparado as onerosas operações de campo.
- A maior parte dos gastos com espionagem seria, portanto, desnecessária, ocorrendo principalmente porque autoridades e acadêmicos tendem a confundir Inteligência com segredo.
- No entanto, a separação entre o que é secreto e o que é ostensivo é incerta; Notícias em jornais muitas vezes são baseadas em informações consideradas secretas. Como exemplo de Vazamento, podemos citar o caso WIKILEAKS.
- Fica óbvio que a grande vantagem das fontes abertas é o alto grau de oportunidade e o baixo custo para obtê-las. A OSINT torna-se atraente principalmente em épocas de contingenciamento orçamentário na atividade de Inteligência.


```
language_attributes(); ?>>
charset="<?php bloginfo( 'charset' ); ?>" /> />
name="viewport" content="width=device-width" />
rel="profile" href="http://gmpg.org/xfn/11" /> />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = esc_attr($theme_options['responsive_menu_type']);
    $responsive_menu_class = fruitful_get_class($responsive_menu_type);
```

HUMINT



- **HUMINT** (do inglês *Human Intelligence*) é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações (como em serviço de inteligência ou serviço de informações) obtidas por meio de seres humanos, como os espiões tradicionais.
- Historicamente, HUMINT é a maior fonte de informação dos serviços secretos, porém desde o advento das telecomunicações a SIGINT foi assumindo o papel de principal fonte e acabou por tornar-se mais importante.
- A HUMINT (*Human Intelligence*) é a inteligência de fontes humanas, como declarações e depoimentos de pessoas durante entrevistas, sob qualquer história-cobertura ou pretexto. A HUMINT é a mais antiga fonte de inteligência e permanece como a mais eficaz, não pela quantidade de dados e informações, mas, por sua precisão e *oportunidade*. O Capítulo XIII *O emprego de espiões* de *A Arte da Guerra* do general Sun Tzu descreve várias categorias de espiões; todos, porém, são fontes humanas de inteligência



HUMINT: TIPOS DE FONTE DE INFORMAÇÃO



- As fontes de **HUMINT** não são necessariamente apenas agentes envolvidos em ações clandestinas ou secretas. As pessoas fornecendo as informações podem ser neutras, amigas ou hostis (em relação a um país). Exemplos típicos de **HUMINT** incluem:
- Forças amigas (patrulhas, polícia militar)
- Prisioneiros de Guerra
- Refugiados
- Civis
- Desertores
- Organizações não governamentais (ONGs)
- Jornalistas


```
charset="<?php bloginfo( 'charset' ); ?>"  
name="viewport" content="width=device-width"  
rel="profile" href="http://gmpg.org/xfn/11"  
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>"  
fruitful_get_favicon(); ?>  
wp_head(); ?>  
<?php body_class();?>  
<div id="page-header" class="hfeed site">  
<?php  
$theme_options = fruitful_get_theme_options();  
$logo_pos = $menu_pos = '';  
if (isset($theme_options['logo_position']))  
$logo_pos = esc_attr($theme_options['logo_position']);  
if (isset($theme_options['menu_position']))  
$menu_pos = esc_attr($theme_options['menu_position']);  
$logo_pos_class = fruitful_get_class($logo_pos);  
$menu_pos_class = fruitful_get_class($menu_pos);  
$responsive_menu_type = fruitful_get_class($menu_pos);  
$responsive_menu_class = fruitful_get_class($menu_pos);
```

IMINT



- **IMINT** (sigla para *imagery intelligence*) é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência (ou *serviço de informações*), obtida através da obtenção de imagens, como por meio de satélites e aeronaves como o U-2 e o SR-71.


```
charset="<?php bloginfo( 'charset' ); ?>"  
name="viewport" content="width=device-width" />  
<?php wp_title( '|', true, 'right' ); ?>  
rel="profile" href="http://gmpg.org/xfn/11" />  
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />  
fruitful_get_favicon(); ?>  
wp_head(); ?>  
<?php body_class();?>  
<div id="page-header" class="hfeed site">  
<?php  
$theme_options = fruitful_get_theme_options();  
$logo_pos = $menu_pos = '';  
if (isset($theme_options['logo_position']))  
$logo_pos = esc_attr($theme_options['logo_position']);  
if (isset($theme_options['menu_position']))  
$menu_pos = esc_attr($theme_options['menu_position']);  
$logo_pos_class = fruitful_get_class($logo_pos);  
$menu_pos_class = fruitful_get_class($menu_pos);  
$responsive_menu_type = fruitful_get_class($theme_options['responsive_menu_type']);  
$responsive_menu_class = fruitful_get_class($theme_options['responsive_menu_class']);  
$responsive_menu_id = fruitful_get_class($theme_options['responsive_menu_id']);  
</div>
```

MASINT



- **MASINT**, sigla para *Measurement and Signatures Intelligence* é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através da obtenção de medidas e assinaturas de eventos, como explosões atômicas.


```
charset="<?php bloginfo( 'charset' ); ?>"  
name="viewport" content="width=device-width" />  
<?php wp_title( '|', true, 'right' ); ?>  
rel="profile" href="http://gmpg.org/xfn/11" />  
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />  
fruitful_get_favicon(); ?>  
wp_head(); ?>  
<?php body_class();?>  
<div id="page-header" class="hfeed site">  
<?php  
$theme_options = fruitful_get_theme_options();  
$logo_pos = $menu_pos = '';  
if (isset($theme_options['logo_position']))  
$logo_pos = esc_attr($theme_options['logo_position']);  
if (isset($theme_options['menu_position']))  
$menu_pos = esc_attr($theme_options['menu_position']);  
$logo_pos_class = fruitful_get_class($logo_pos);  
$menu_pos_class = fruitful_get_class($menu_pos);  
$responsive_menu_type = fruitful_get_class($theme_options['responsive_menu_type']);  
$responsive_menu_class = fruitful_get_class($theme_options['responsive_menu_class']);  
$responsive_menu_attr = fruitful_get_class($theme_options['responsive_menu_attr']);  
</div>
```

SIGINT



- **SIGINT** (acrônimo de *signals intelligence*) é o termo inglês usado para descrever a atividade da coleta de informações ou inteligência através da interceptação de sinais de comunicação entre pessoas ou máquinas.
- O nascimento da SIGINT em um senso moderno data da Guerra Russo-Japonesa de 1904~1905. Conforme a esquadra russa preparava-se para o conflito com o Japão em 1904, o navio britânico HMS Diana estacionado no Canal de Suez interceptou sinais sem-fio da marinha russa, destinados para a mobilização dos navios da esquadra; esta foi a primeira vez que algo do tipo ocorreu


```
charset="<?php bloginfo( 'charset' ); ?>"  
name="viewport" content="width=device-width"  
rel="profile" href="http://gmpg.org/xfn/11"  
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>"  
fruitful_get_favicon(); ?>  
wp_head(); ?>  
<?php body_class();?>  
<div id="page-header" class="hfeed site">  
<?php  
$theme_options = fruitful_get_theme_options();  
$logo_pos = $menu_pos = '';  
if (isset($theme_options['logo_position']))  
$logo_pos = esc_attr($theme_options['logo_position']);  
if (isset($theme_options['menu_position']))  
$menu_pos = esc_attr($theme_options['menu_position']);  
$logo_pos_class = fruitful_get_class($logo_pos);  
$menu_pos_class = fruitful_get_class($menu_pos);  
responsive_menu_type = fruitful_get_class($menu_pos);  
responsive_menu_type = fruitful_get_class($menu_pos);
```

SIGINT: SUBDISCIPLINAS



- SIGINT tem as seguintes sub-categorias:
- COMINT, abreviatura de *communications intelligence*, focado nas comunicações humanas
- ELINT, abreviatura de *electronic intelligence*. focado no uso de sensores para obter dados principalmente sobre a rede de defesa inimiga, como alcance de radares.
- FISINT, sigla para *foreign instrumentation intelligence*, focado em comunicações não humanas, como telemetria de mísseis.
- Muitas vezes as atividades de COMINT são descritas como SIGINT, o que pode causar confusão.


```
language_attributes(); ?>>
charset="<?php bloginfo( 'charset' ); ?>" /> />
viewport" content="width=device-width" />
wp_title( '|', true, 'right' ); ?> />
rel="profile" href="http://gmpg.org/xfn/11" />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_class = fruitful_get_class($menu_pos);
```

SIGINT: HISTÓRIA



- Cada vez mais a SIGINT vem se tornando central para os militares, e também para o corpo diplomático, desde o desenvolvimento das telecomunicações e sua aplicação militar, além da mecanização que aumentou a velocidade e raio de atuação das forças, como a blitzkrieg e o uso do submarino e da aviação militar, todos fortes usuários do rádio.
- Vários fatos podem comprovar a importância das SIGINT na guerra moderna:
- A falha dos russos de proteger adequadamente as suas comunicações levou à desastrosa derrota na Batalha de Tannenberg.
- A captura do Telegrama Zimmermann foi fator importante na decisão dos Estados Unidos de entrarem na Primeira Guerra Mundial.
- A quebra do código alemão Enigma é considerada um dos fatores mais importantes para a vitória aliada na Segunda Guerra Mundial.
- A quebra do código japonês PURPLE é considerada um dos fatores mais importantes para a vitória americana no Pacífico que terminou com a Segunda Guerra Mundial, influenciando decisivamente a Batalha de Midway.


```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?> />
rel="profile" href="http://gmpg.org/xfn/11" />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_class = fruitful_get_class($menu_pos);
```

ELINT



- **Electronics Intelligence** ou **ELINT** é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência(*serviço de informações*), obtida através da sensores voltados para a rede de defesa inimiga, como radares e sinais enviados por armas teleguiadas.


```
language_attributes(); ?>>
charset="<?php bloginfo( 'charset' ); ?>" /> />
name="viewport" content="width=device-width" /> />
rel="profile" href="http://gmpg.org/xfn/11" /> />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" /> />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
```

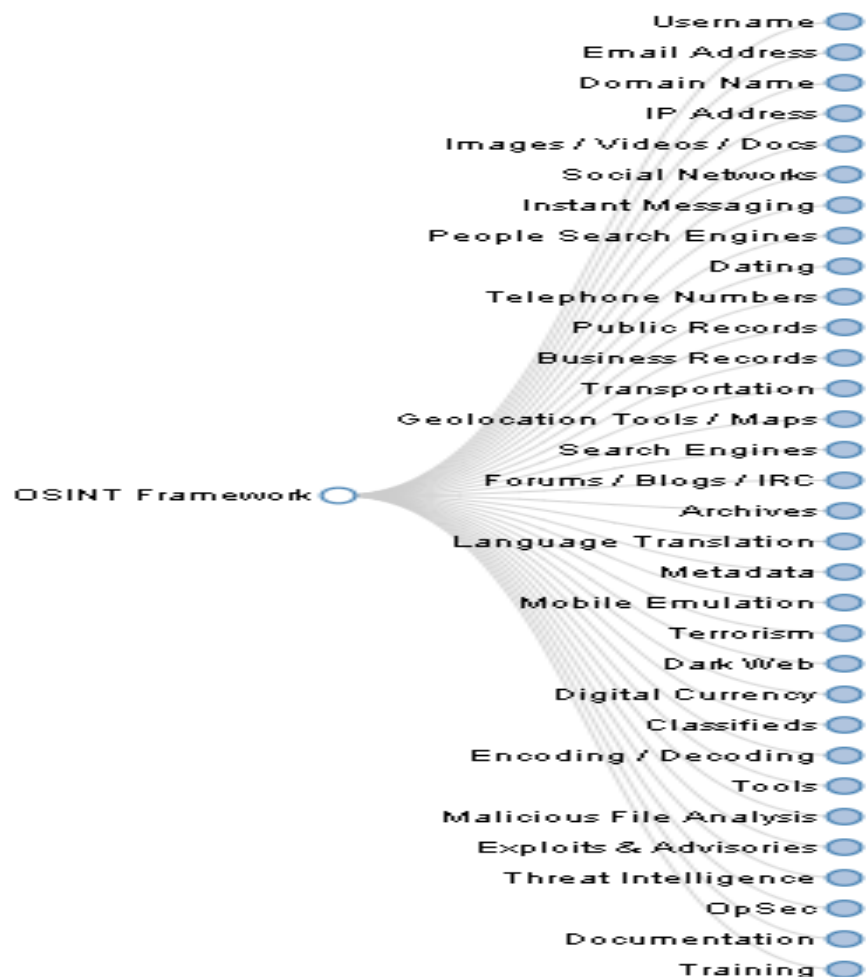
FISINT



- **FISINT**, sigla para *Foreign Instrumentation Signals INTelligence* é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através da monitoração de comunicações não-humanas do inimigo, como sistemas de rádio comando e sistemas Friend or Foe.

ESTRUTURA DO OSINT

<https://osintframework.com/>



NOTAS

- A estrutura OSINT concentrou-se na coleta de informações de ferramentas ou recursos gratuitos. A intenção é ajudar as pessoas a encontrar recursos gratuitos do OSINT. Alguns dos sites incluídos podem exigir registro ou oferecer mais dados para \$\$\$, mas você deve conseguir pelo menos uma parte das informações disponíveis sem nenhum custo.



CONCEITOS PRÁTICOS: OSINT

PROF. JOAS ANTONIO

FERRAMENTAS OSINT

OSINT TOOLS
and how you learn how to use them

1 DATA GATHERING
for intelligence purposes

ANY SITE
is an OSINT data gathering resource

2 LINK ANALYSIS

3 OTHER DATA ANALYSIS

PEOPLE
Consider every possible variation of the person's name.

SOCIAL MEDIA & DATING SITES
Discover what people are talking about if they participate in online forums on social media platforms.

COMMUNITIES & BLOGS
Search these using names, usernames, email addresses and telephone numbers.

IMAGES & VIDEO
Search social sites to find photos, videos, and discussions related to your target.

SPECIALIZED WEB SEARCHERS
Sites that are not mainstream, may be buried, hard to find or simply not indexed by general search engines.

CLASSIFIED LISTINGS
In a theft investigation, the target may be trying to sell a stolen item, or searching for similar items online.

BUSINESS SEARCH SITES
When conducting due diligence investigations, or researching a person that will be interviewed in an investigation.

BACKGROUND CHECKS
Requires specific skills and knowledge of procedures and resources.

GEOLOCATION SEARCHERS
Track a vehicle that has an Automatic Packet Reporting system (APRS), identify the whereabouts of social media activity or the physical location of an IP address.

1. Shodan
2. ThreatPinch Lookup browser plugin
3. NetDB
4. Censys
5. HoneyDB
6. Datasplot
7. OnionScan
8. Advanced Reconnaissance Framework
9. Intel Techniques Search Engine
10. MISP

PALANTIR GOTHAM
Structured data like log files, spreadsheets, and tables. Unstructured data like emails, documents, images, and videos.

PALANTIR METROPOLIS
Large-scale quantitative investigation. Perfect for tracking and analyzing insurance claims data, network traffic flow, and financial trading patterns.

FOSS PROJECT
Open source big data integration, analytics, and visualization platform.

DATASPLOIT
To perform various OSINT techniques, aggregate all the raw data, visualise it on a dashboard, and facilitate alerting and monitoring on the data.

OPEN GRAPHITI
3D data visualization engine for data scientists to visualize semantic networks and to work with them.

peerlyst™
the world is your analyst

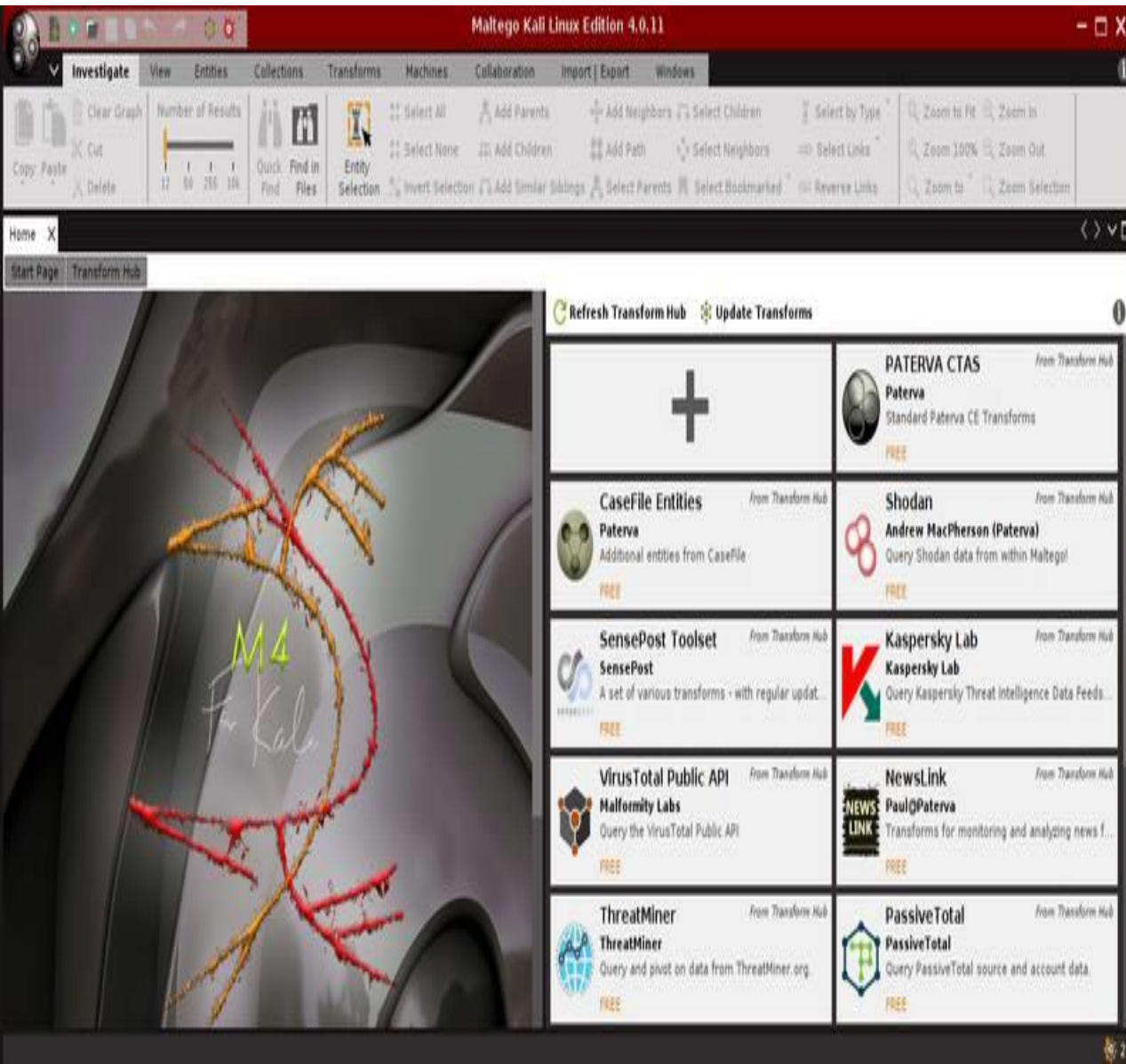
ALGUMAS FERRAMENTAS

- <https://www.shodan.io/>
- <https://www.peerlyst.com/posts/osint-and-threat-intelligence-chrome-plugin-to-look-up-ips-fqdns-md5-sha2-and-cves-matt-brewer>
- <https://censys.io/>
- <https://www.peerlyst.com/tags/honeydb>
- <https://github.com/DataSploit/datasplot>
- <https://github.com/s-rah/onionscan>
- <https://osintframework.com/>
- <https://inteltechniques.com/menu.html>
- <http://www.misp-project.org/>

```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?> />
rel="profile" href="http://gmpg.org/xfn/11" />
fruitful_get_favicon(); ?>
<script src="<?php echo get_template_directory_uri(); ?>
<?php body_class(); ?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $theme_options['logo_position'];
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($responsive_menu_type);
```

MALTEGO

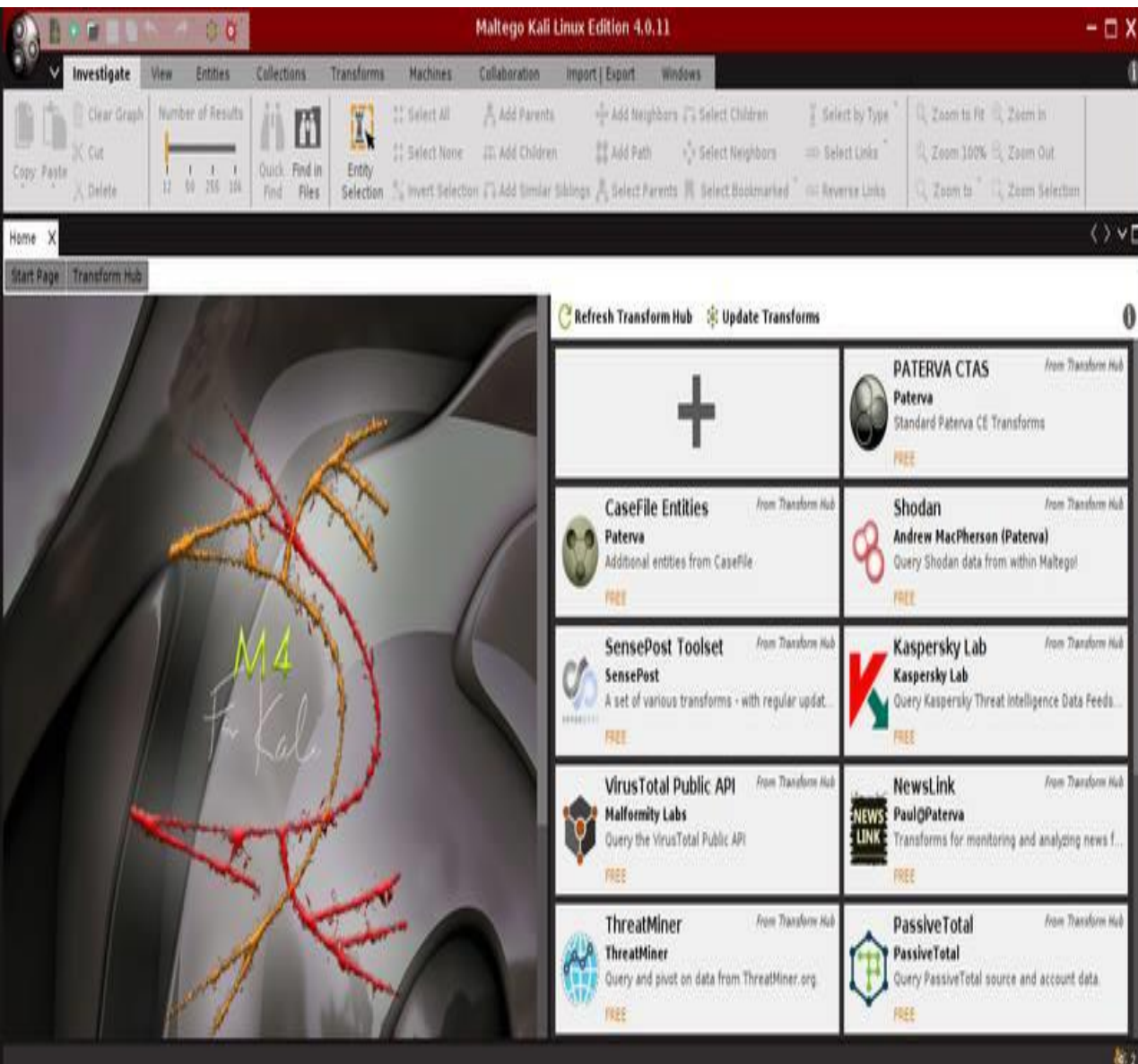
FERRAMENTAS OSINT: MALTEGO



O QUE É MALTEGO?

- O Maltego é desenvolvido pela Paterva e é usado por profissionais de segurança e investigadores forenses para coletar e analisar inteligência de código aberto. Pode facilmente coletar informações de várias fontes e usar várias transformações para gerar resultados gráficos. As transformações são embutidas e também podem ser personalizadas com base no requisito. O Maltego é escrito em Java e vem pré-empacotado no Kali Linux. Para usar Maltego, o registro do usuário é necessário, o registro é gratuito. Uma vez que os usuários registrados podem usar esta ferramenta para criar a pegada digital do alvo na internet.

FERRAMENTAS OSINT: MALTEGO



MATERIAL PARA ESTUDO

- <https://www.youtube.com/watch?v=oSJCUFcgT0>
- <https://pt.slideshare.net/cassioaramos/tutorial-maltego>
- https://www.youtube.com/watch?v=sP-PI_SRQVo
- <https://osintbrasil.blogspot.com/2018/02/como-usar-maltego-para-pesquisa-e-dados.html>
- https://www.youtube.com/watch?v=tC_mUgn5b-c
- https://www.youtube.com/watch?v=wx4mEQZM_0s
- <https://www.computerweekly.com/tip/Maltego-tutorial-Part-1-Information-gathering>
- <http://yahoohackingbr.blogspot.com/2015/04/tutorial-usando-o-maltego-para-o.html>


```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?>" />
rel="profile" href="http://gmpg.org/xfn/11" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
$theme_options = fruitful_get_theme_options();
$logo_pos = $menu_pos = '';
if (isset($theme_options['logo_position']))
    $logo_pos = esc_attr($theme_options['logo_position']);
if (isset($theme_options['menu_position']))
    $menu_pos = esc_attr($theme_options['menu_position']);
$logo_pos_class = fruitful_get_class($logo_pos);
$menu_pos_class = fruitful_get_class($menu_pos);
responsive_menu_type = fruitful_get_class($menu_pos);
```

SHODAN

FERRAMENTAS OSINT: SHODAN

Shodan Developers Book View All...

SHODAN

Explore Developer Pricing Enterprise Access Contact Us

The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture
Websites are just one part of the Internet. There are also refrigerators and much more that can be found with Shodan.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage
Who is using your product? Where are they located? Shodan provides empirical market intelligence.

O QUE É SHODAN?

- O Shodan é um mecanismo de busca que permite ao usuário encontrar tipos específicos de computadores conectados à Internet usando uma variedade de filtros. Alguns também o descreveram como um mecanismo de pesquisa de banners de serviço, que são metadados que o servidor envia de volta ao cliente.

FERRAMENTAS OSINT: SHODAN



MATERIAL PARA ESTUDO

- <https://osintbrasil.blogspot.com/2017/10/um-tutorial-e-um-guia-shodan.html>
- <https://www.youtube.com/watch?v=X0w6GL-lg0k>
- <https://www.youtube.com/watch?v=v2EdwgX72PQ>
- <https://www.youtube.com/watch?v=dcJipmNPxDs>
- <https://www.youtube.com/watch?v=V5f4kqg2Tcs>
- <https://www.youtube.com/watch?v=UNfjqnJS2wk>
- <https://cli.shodan.io/>
- <https://danielmiessler.com/study/shodan/>
- <https://www.defcon.org/images/defcon-18/dc-18-presentations/Schearer/DEFCON-18-Schearer-SHODAN.pdf>



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are refrigerators and much more that can be found with Shodan.



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Shodan provides empirical market intelligence.

```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?>" />
rel="profile" href="http://gmpg.org/xfn/11" />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
<script src="<?php echo get_template_directory_uri(); ?>js/jquery.js" />
</script>
<?php body_class(); ?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $theme_options['logo_position'];
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_class = fruitful_get_class($responsive_menu_type);
```

GOOGLE HACKING

FERRAMENTAS OSINT: GOOGLE HACKING



O QUE É GOOGLE HACKING?

- O Google utiliza uma tecnologia chamada **spiders**, ou **webcrawlers** que são robôs que fazem a varredura na web buscando e** indexando as páginas**. Quando fazemos uma busca pela ferramenta ela procura por este termo nestas páginas indexadas nos retornando **o que estamos procurando de fato**, cada resultado retornado é composto por um **titulo**, uma **url** e uma **descrição**.
- Um servidor mal configurado pode expor informações da empresa no Google. Não é difícil conseguir acesso a arquivos de base de dados através do Google.
- 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, dando comandos e possibilitando manipular buscas avançadas por strings chamadas de “dorks” ou “operadores de pesquisa”.

FERRAMENTAS OSINT: GOOGLE HACKING



MATERIAL PARA ESTUDO

- <https://medium.com/tableless/voc%C3%AA-conhece-o-google-hacking-d8f5c3296a3f>
- <https://www.100security.com.br/google-hacking-database/>
- <https://gbhackers.com/latest-google-dorks-list/>
- <https://www.exploit-db.com/google-hacking-database>
- https://www.youtube.com/watch?v=i9mGAdYo_pk
- <https://www.youtube.com/watch?v=Pku6afMFigY>
- <https://imasters.com.br/devsecops/securitycast-google-hacking-database>
- <https://www.youtube.com/watch?v=qv1eoqvp4ew>
- <https://www.youtube.com/watch?v=d3NzsrnVrlw>


```
charset="<?php bloginfo( 'charset' ); ?>"  
name="viewport" content="width=device-width" />  
<?php wp_title( '|', true, 'right' ); ?>  
rel="profile" href="http://gmpg.org/xfn/11" />  
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />  
fruitful_get_favicon(); ?>  
wp_head(); ?>  
<?php body_class();?>  
<div id="page-header" class="hfeed site">  
<?php  
$theme_options = fruitful_get_theme_options();  
$logo_pos = $menu_pos = '';  
if (isset($theme_options['logo_position']))  
$logo_pos = esc_attr($theme_options['logo_position']);  
if (isset($theme_options['menu_position']))  
$menu_pos = esc_attr($theme_options['menu_position']);  
$logo_pos_class = fruitful_get_class($logo_pos);  
$menu_pos_class = fruitful_get_class($menu_pos);  
$responsive_menu_type = fruitful_get_class($menu_pos);  
$responsive_menu_type = fruitful_get_class($menu_pos);
```

SOCIAL NETWORK

FERRAMENTAS OSINT: SOCIAL NETWORK



MATERIAL PARA ESTUDO

- <https://www.andreafortuna.org/2017/03/20/open-source-intelligence-tools-for-social-media-my-own-list/>

FERRAMENTAS OSINT: SOCIAL NETWORK



SOBRE

- Sites de redes sociais possuem muita informação, mas será tarefa muito chata e demorada se você precisar verificar se um determinado nome de usuário está presente em qualquer site de mídia social. Para obter essas informações, há um site www.checkusernames.com . Ele procurará a presença de um nome de usuário específico em mais de 150 sites. Os usuários podem verificar a presença de um alvo em um site específico para tornar o ataque mais direcionado.
- Uma versão mais avançada do site é <https://knowem.com>, que tem um banco de dados mais amplo de mais de 500 sites, juntamente com mais alguns serviços?

FERRAMENTAS OSINT: SOCIAL NETWORK



MATERIAL PARA ESTUDO

- <https://namechk.com/>
- <https://www.namecheckr.com/>
- <http://www.spinxo.com/username-check>
- <https://securitytrails.com/blog/osint-facebook-tools>
- <https://www.youtube.com/watch?v=q39fy2lpBF8>

```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?> />
rel="profile" href="http://gmpg.org/xfn/11" />
fruitful_get_favicon(); ?>
<script src="<?php echo get_template_directory_uri(); ?>/js/jquery.js"></script>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_class = fruitful_get_class($menu_pos);
```

NUMERO DE TELEFONE

FERRAMENTAS OSINT: NUMERO DE TELEFONE

```
[+] Location:
[+] Carrier: Transatel SA
[+] Line type: mobile
(!) This is most likely a mobile number, but it can still be a VoIP
[-] Running OVH scan...
[-] Running OSINT footprint reconnaissance...
[-] General finding: URL in phone number
[+] Scan URL: https://www.ovh.com/phone
[-] Would you like to use an additional format for this number? (y)
[-] ---- We found the following information for this number:
[-] Searching for footprints on web pages... (limit=10)
[+] Result found: https://freesmscode.com/get-virtual-phone-number-...
[+] Result found: https://freesmscode.com/
[+] Result found: https://freesmscode.com/get-virtual-phone-number-...
[+] Result found: https://smsnumbersonline.com/free-sms-number-online-...
[+] Result found: https://smstibo.com/free-virtual-mobile-number-...
[+] Result found: https://sms24.me/number-...
[+] Result found: https://www.getfreesmsnumber.com/virtual-number-...
[+] Result found: https://smsreceiving.com/receive-sms-online-unit...
```

Find identifying information for phone numbers

SOBRE

- Os números de telefone geralmente contêm pistas sobre a identidade do proprietário e podem trazer muitos dados durante uma investigação do OSINT. Começando com um número de telefone, podemos pesquisar em um grande número de bancos de dados on-line com apenas alguns cliques para descobrir informações sobre um número de telefone. Pode incluir a operadora, o nome e endereço do proprietário e até contas on-line conectadas.

FERRAMENTAS OSINT: NUMERO DE TELEFONE

```
[+] Location:
[+] Carrier: Transatel SA
[+] Line type: mobile
(!) This is most likely a mobile number, but it can still be a VoIP
[-] Running OVH scan...
[-] Running OSINT footprint reconnaissance...
[-] Generating URL in format:
[+] Scan URL: https://www.ovh.com/phone
[-] Would you like to use an additional format for this number? (y)
[-] ---- We
[-] Searching for footprints on web pages... (limit=10)
[+] Result found: https://freesmscode.com/free-virtual-phone-number-
[+] Result found: https://freesmscode.com/
[+] Result found: https://freesmscode.com/get-virtual-phone-number-
[+] Result found: https://smsnumberonline.com/free-sms-number-online-
[+] Result found: https://smstibo.com/free-virtual-mobile-number-
[+] Result found: https://sms24.me/number-
[+] Result found: https://www.getfreesmsnumber.com/virtual-number-
[+] Result found: https://smsreceiving.com/receive-sms-online-unit
```

Find identifying information for phone numbers

MATERIAL PARA ESTUDO

- <https://medium.com/@SundownDEV/phone-number-scanning-osint-recon-tool-6ad8f0cac27b>
- <https://datasploit.readthedocs.io/en/latest/>
- <https://null-byte.wonderhowto.com/how-to/find-identifying-information-from-phone-number-using-osint-tools-0195472/>
- <https://www.youtube.com/watch?v=gDKR1eHIXEA>
- <https://www.youtube.com/watch?v=WW6myutKBYk>
- <https://www.youtube.com/watch?v=GOvuhU02G-s>

FERRAMENTAS OSINT: THE HARVESTER

```
Applications ▾ Places ▾ Terminal ▾ Mon 7:09 PM
root@VdV: ~
File Edit View Search Terminal Help

*****
*
* |H|A|R|V|E|S|T|E|R|
* |G|O|O|G|L|E|
* |P|G|P|
* |B|I|N|G|
*
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

Full harvest..
[-] Searching in Google..
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...
    Searching 200 results...
    Searching 250 results...
    Searching 300 results...
```

MATERIAL PARA ESTUDO

- <https://github.com/laramies/theHarvester>
- <https://tools.kali.org/information-gathering/theharvester>
- https://www.youtube.com/watch?v=NioRu6s4_xk
- <https://www.oanalista.com.br/2016/03/06/coletando-informacoes-com-o-theharvester/>
- <https://www.100security.com.br/theharvester/>
- <https://www.hackingloops.com/theharvester/>

FERRAMENTAS OSINT: METAGOOFIL

```
root@kali:~/usr/share/metagoofil# metagoofil
#####
#
# Metagoofil Ver 2.2
# Christian Martorella
# Edge-Security.com
# cmartorella@edge-security.com
#####

Usage: metagoofil options

-d: domain to search
-t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
-l: limit of results to search (default 200)
-h: work with documents in directory (use "yes" for local analysis)
-m: limit of files to download
-o: working directory (location to save downloaded files)
-f: output file
```

SOBRE

- O **Metagoofil** é uma ferramenta de coleta de informações projetada para extrair metadados de arquivos (pdf, doc, xls, ppt, docx, pptx, xlsx) que pertencem a um domínio alvo.
- A ferramenta irá realizar uma busca no Google para identificar e fazer o download dos documentos para o disco local e, em seguida, irá extrair os metadados com diferentes bibliotecas como Hachoir, PdfMiner e outros. Com os resultados irá gerar um relatório com nomes de usuários, versões de software e servidores ou nomes das máquinas que auxiliaram durante um PenTest na fase de coleta de informações.


```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?> />
rel="profile" href="http://gmpg.org/xfn/11" />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_class = fruitful_get_class($menu_pos);
```

TINEYE

FERRAMENTAS OSINT: TINIEYE

TinEye

Technology Products

Reverse Image Search

Search by image and find where that image appears online

Upload or enter Image URL

[How to use TinEye](#)

TinEye Alerts tracks where your images appear online.

SOBRE

- Tineye é usado para realizar uma pesquisa relacionada à imagem na web. Tem vários produtos como o sistema de alerta tineye, API de pesquisa de cores, motor móvel, etc. Você pode pesquisar se uma imagem está disponível on-line e onde essa imagem apareceu. Tineye usa redes neurais, aprendizado de máquina e reconhecimento de padrões para obter os resultados. Ele usa correspondência de imagem, identificação de marca d'água, correspondência de assinatura e vários outros parâmetros para corresponder à imagem, em vez da correspondência de palavras-chave. O site também oferece extensões de API e extensões de navegador. Você pode simplesmente visitar a imagem e clicar com o botão direito do mouse para selecionar a pesquisa no tineye.

FERRAMENTAS OSINT: TINIEYE

TinEye

Technology Products

Reverse Image Search

Search by image and find where that image appears online

Upload or enter Image URL

[How to use TinEye](#)

TinEye Alerts tracks where your images appear online.

MATERIAL PARA ESTUDO

- <https://www.tineye.com/>
- <https://www.youtube.com/watch?v=5qkbsl9zi8Y>
- <https://www.youtube.com/watch?v=sufLXYuLL9M>

FERRAMENTAS OSINT: WEB SCRAPING

Geeky Baba

WEB SCRAPING



SOBRE

- Web scraping é uma técnica de extração de dados utilizada para coletar dados de sites. Por meio de processos automatizados, implementados usando um rastreador bot, esse tipo de “raspagem” de informações é uma forma de realizar cópias de dados em que informações específicas são coletadas e copiadas da web, tipicamente em um banco de dados ou planilha local central, para posterior recuperação ou análise. Essa ferramenta pode ser considerada muito útil para muitos profissionais, como o de marketing, por exemplo, por facilitar a busca, manipulação e análise de dados para a otimização de vendas e personalização do atendimento a clientes, tanto que diversos negócios legítimos a utilizam com essa finalidade.

FERRAMENTAS OSINT: WEB SCRAPING

Geeky Baba

WEB SCRAPING



MATERIAL PARA ESTUDO

- <https://www.youtube.com/watch?v=pJDJwD8GCIg>
- <http://www.automatingosint.com/blog/category/web-scraping/>
- <https://blog.vulsec.com/web-scraping-for-open-source-intelligence>
- <https://null-byte.wonderhowto.com/how-to/use-photon-scanner-scrape-web-osint-data-0194420/>


```
language_attributes(); ?>>
charset="<?php bloginfo( 'charset' ); ?>"
name="viewport" content="width=device-width"
rel="profile" href="http://gmpg.org/xfn/11"
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>"
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($theme_options['responsive_menu_type']);
    $responsive_menu_class = fruitful_get_class($theme_options['responsive_menu_class']);
```

INFOGA

FERRAMENTAS OSINT: INFOGA



```
|| Infoga - Email Information Gathering
|| Infoga v4.1 - "Mr.Robot"
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/infoga
```

```
Usage: infoga -t [target] -s [source]
```

```
-t --target    Domain to search
-s --source    Data source: [all,google,bing,yahoo,pgp]
-i --info     Get email informatios
-h --help     Show this help and exit
```

```
Examples:
```

```
infoga --target site.com --source all
infoga --target site.com --source [google,bing,...]
infoga --info test123@site.com
```

SOBRE

- Infoga é uma ferramenta que coleta informações de contas de e-mail (ip, nome de host, país, ...) de diferentes fontes públicas (mecanismos de busca, servidores de chave PGP e shodan) e verifica se os e-mails vazaram usando a API haveibeenpwned.com. É uma ferramenta muito simples, mas muito eficaz para os estágios iniciais de um teste de penetração ou apenas para conhecer a visibilidade de sua empresa na Internet.

FERRAMENTAS OSINT: INFOGA



```
|| Infoga - Email Information Gathering
|| Infoga v4.1 - "Mr.Robot"
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/infoga
```

```
Usage: infoga -t [target] -s [source]
```

```
-t --target    Domain to search
-s --source    Data source: [all,google,bing,yahoo,pgp]
-i --info      Get email informatios
-h --help      Show this help and exit
```

Examples:

```
infoga --target site.com --source all
infoga --target site.com --source [google,bing,...]
infoga --info test123@site.com
```

MATERIAL PARA ESTUDO

- <https://github.com/m4ll0k/Infoga>
- <https://www.youtube.com/watch?v=KltbNlyA9IY>
- <https://www.youtube.com/watch?v=2md1JvjDQhs>
- <https://www.youtube.com/watch?v=TUw3JpAA7H8>
- <https://www.youtube.com/watch?v=WYJFSPaAiJI>
- <https://www.youtube.com/watch?v=DDRy3MtQD4g>

FERRAMENTAS OSINT: TORBOT

```

TORBOT V 1.0.0
#####
# TorBot - A python Tor Crawler #
# GitHub : https://github.com/DedSecInside/TorBot #
#####
LICENSE: GNU Public License

Tor Ip Address :
193.70.56.25

Websites Found - 232
-----
http://torlinkbgs6aabns.onion/
http://easycoinsayj7p5l.onion
http://jzn5w5pac26sqef4.onion
http://y3fp1eiezy2sin4a.onion
http://qkj4drtgvpm7eekl.onion
http://ow24et3tetp6tvmk.onion
http://shopsat2dotfotbs.onion/

```

MATERIAL PARA ESTUDO

- <https://github.com/DedSecInside/TorBot>
- https://www.youtube.com/watch?v=3iuw_5emVW0

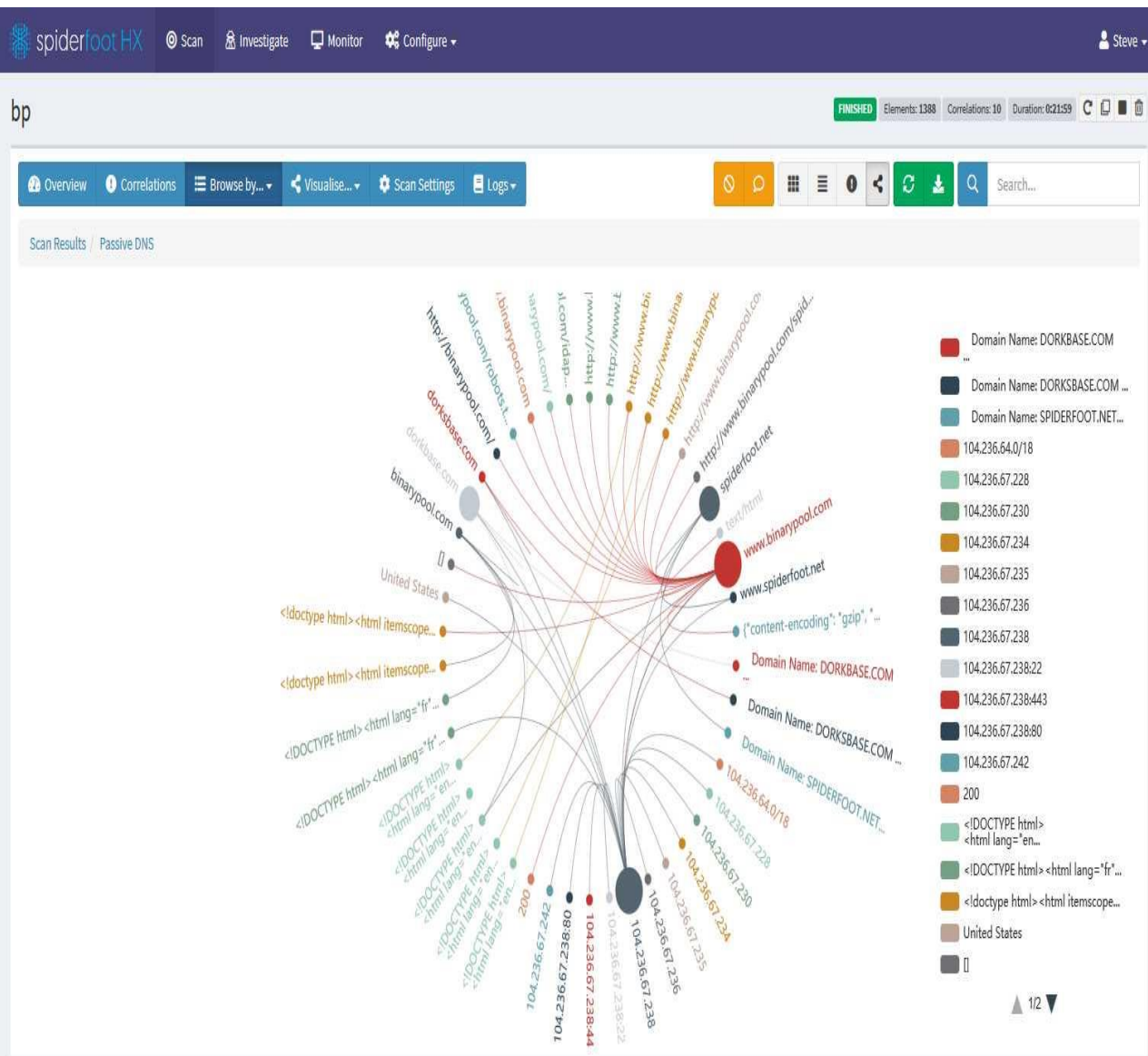
FERRAMENTAS OSINT: SPIDERFOOT



SOBRE

- O SpiderFoot é uma ferramenta de automação de inteligência de fonte aberta (OSINT). Seu objetivo é automatizar o processo de coleta de informações sobre um determinado alvo, que pode ser um endereço IP, nome de domínio, nome de host, sub-rede, ASN, endereço de e-mail ou nome da pessoa.
- O SpiderFoot pode ser usado ofensivamente, ou seja, como parte de um teste de penetração de caixa preta para coletar informações sobre o alvo ou defensivamente para identificar quais informações sua organização está fornecendo para os invasores usarem contra você. gratuitamente

FERRAMENTAS OSINT: SPIDERFOOT



MATERIAL PARA ESTUDO

- <https://github.com/smicallef/spiderfoot>
- <https://www.spiderfoot.net/>
- <https://www.youtube.com/watch?v=dUQl0jPiSFw>
- <https://www.youtube.com/watch?v=CNPaG6ixf9Q>
- <https://www.youtube.com/watch?v=jD2rgooP2T0>
- <https://osintbrasil.blogspot.com/2017/06/spiderfoot.html>
- <https://securitytrails.com/blog/spiderfoot-osint-automation-tool>
- <https://www.100security.com.br/spiderfoot/>

FERRAMENTAS OSINT: PHONEINFOGA

```
PhoneInfoga Ver. v1.0.0-rc2
Coded by Sundowndev

[!] ---- Fetching informations for 918394008835 ---- [!]
[*] Running local scan...
[+] International format: +91 83940 08835
[+] Local format: 08394008835
[+] Country code: +91
[+] Location: India
[+] Carrier: Vodafone
[+] Area: India
[+] Timezone: Asia/Calcutta
[*] The number is valid and possible.
[*] Running Numverify.com scan...
[+] Number: (+91) 08394008835
[+] Country: India (Republic of) (IN)
```

SOBRE

- O PhoneInfoga é uma das ferramentas mais avançadas para escanear números de telefone usando apenas recursos gratuitos. O objetivo é primeiro coletar informações padrão como país, área, operadora e tipo de linha em qualquer número de telefone internacional com uma precisão muito boa. Em seguida, pesquise pegadas nos mecanismos de pesquisa para tentar localizar o provedor de VoIP ou identificar o proprietário.

FERRAMENTAS OSINT: PHONEINFOGA

```
PhoneInfoga Ver. v1.0.0-rc2
Coded by Sundowndev

[!] ---- Fetching informations for 918394008835 ---- [!]
[*] Running local scan...
[+] International format: +91 83940 08835
[+] Local format: 08394008835
[+] Country code: +91
[+] Location: India
[+] Carrier: Vodafone
[+] Area: India
[+] Timezone: Asia/Calcutta
[*] The number is valid and possible.
[*] Running Numverify.com scan...
[+] Number: (+91) 08394008835
[+] Country: India (Republic of) (IN)
```

MATERIAL PARA ESTUDO

- <https://github.com/sundowndev/PhoneInfoga>
- <https://github.com/sundowndev/PhoneInfoga/wiki>
- <https://www.youtube.com/watch?v=AX30uLvc9tU>
- <https://www.youtube.com/watch?v=jkZoV80WJnM>
- <https://www.youtube.com/watch?v=QzGb9SG5SL8>

FERRAMENTAS OSINT: PWNEDORNOT

```
ubuntu : bash — Konsole
File Edit View Bookmarks Settings Help
ubuntu : bash

  PWNEDORNOT

Developed by : thewhite4t

[+] Enter Email Address : [REDACTED]@gmail.com

[!] Account pwned...Listing Breaches...

[+] Breach      : 000webhost
[+] Domain     : 000webhost.com
[+] Date       : 2015-03-01
[+] Fabricated  : False
[+] Verified   : True
[+] Retired    : False
[+] Spam       : False

[+] Breach      : 17
[+] Domain     : 17app.co
[+] Date       : 2016-04-19
[+] Fabricated  : False
[+] Verified   : True
[+] Retired    : False
[+] Spam       : False
```

SOBRE

- pwnedOrNot usa a API vib do v2 de haveibeenpwned para testar contas de e-mail e tenta encontrar a **senha no Pastebin Dumps** .

FERRAMENTAS OSINT: PWNEDORNOT

```
ubuntu : bash — Konsole
File Edit View Bookmarks Settings Help
ubuntu : bash

Developed by : thewhite4t

[+] Enter Email Address : [REDACTED]@gmail.com
[!] Account pwned...Listing Breaches...

[+] Breach      : 000webhost
[+] Domain     : 000webhost.com
[+] Date       : 2015-03-01
[+] Fabricated  : False
[+] Verified   : True
[+] Retired    : False
[+] Spam       : False

[+] Breach      : 17
[+] Domain     : 17app.co
[+] Date       : 2016-04-19
[+] Fabricated  : False
[+] Verified   : True
[+] Retired    : False
[+] Spam       : False
```

MATERIAL PARA ESTUDO

- <https://github.com/thewhite4t/pwnedOrNot>
- <https://www.youtube.com/watch?v=BdJZhrkrpUI>
- <https://www.youtube.com/watch?v=cen0xC-MzZ8>

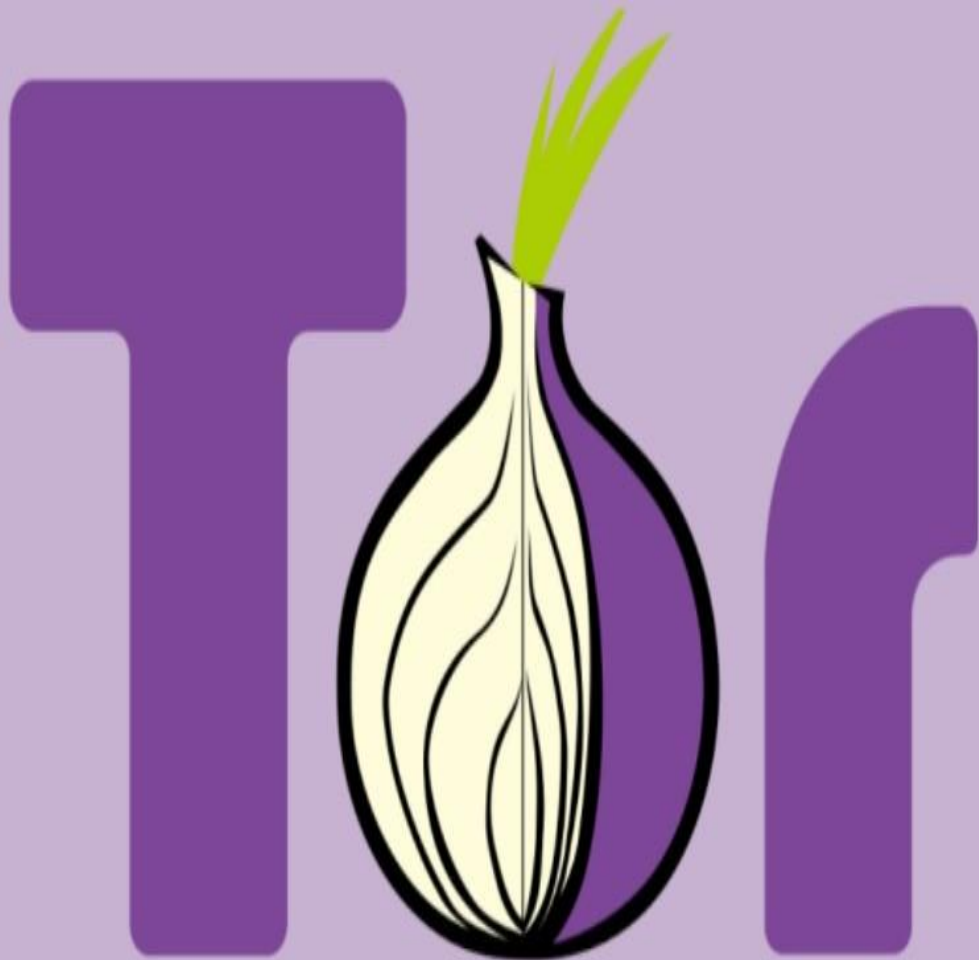
```
language_attributes(); ?>>
charset="<?php bloginfo( 'charset' ); ?>" />
name="viewport" content="width=device-width" />
rel="profile" href="http://gmpg.org/xfn/11" />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($responsive_menu_type);
```

TOR OSINT

FERRAMENTAS OSINT: TOR

MATERIAL PARA ESTUDO

- <https://jakecreps.com/2019/05/16/osint-tools-for-the-dark-web/>
- <https://medium.com/@IanBarwise/the-osint-ification-of-isis-on-the-dark-web-19644ec90253>
- <http://www.automatingosint.com/blog/2016/07/dark-web-osint-with-python-and-onionscan-part-one/>
- <https://github.com/pielco11/DOT>



FERRAMENTAS OSINT: SKYPE

MATERIAL PARA ESTUDO

- <https://github.com/PaulSec/skype-osint>
- <http://www.automatingosint.com/blog/2016/05/expanding-skype-forensics-with-osint-email-accounts/>
- <http://seclist.us/skype-osint-python-osint-tool-to-retrieve-information-from-skype.html>


```
charset="<?php bloginfo( 'charset' ); ?>" />  
name="viewport" content="width=device-width" />  
<?php wp_title( '|', true, 'right' ); ?>  
rel="profile" href="http://gmpg.org/xfn/11" />  
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />  
fruitful_get_favicon(); ?>  
wp_head(); ?>  
<?php body_class();?>  
<div id="page-header" class="hfeed site">  
<?php  
$theme_options = fruitful_get_theme_options();  
$logo_pos = $menu_pos = '';  
if (isset($theme_options['logo_position']))  
$logo_pos = esc_attr($theme_options['logo_position']);  
if (isset($theme_options['menu_position']))  
$menu_pos = esc_attr($theme_options['menu_position']);  
$logo_pos_class = fruitful_get_class($logo_pos);  
$menu_pos_class = fruitful_get_class($menu_pos);  
$responsive_menu_type = fruitful_get_class($theme_options['responsive_menu_type']);  
$responsive_menu_class = fruitful_get_class($responsive_menu_type);  
$responsive_menu_id = fruitful_get_class($responsive_menu_id);  
$responsive_menu_attr = fruitful_get_class($responsive_menu_attr);  
</div>
```

CREEPY

FERRAMENTAS OSINT: CREEPY

The screenshot displays the 'cree.py - Geolocation OSINT tool' interface. The main window shows a map of Athens, Greece, with numerous blue and yellow location markers. A pop-up window titled 'Retrieved from flickr' is open, showing a photo of a dense urban area. The photo is attributed to user 'ccgd' and was taken on '2015-10-15 09:21:02 +0000'. The original photo link is <http://www.flickr.com/photos/14551451@N00/22352020741>. The interface also includes a 'Locations List' on the right, a 'Current Location Details' section, and a 'Log Output' at the bottom.

Retrieved from flickr

From user: ccgd

Link to the original photo: <http://www.flickr.com/photos/14551451@N00/22352020741>

It was taken on: 2015-10-15 09:21:02 +0000

Locations List

Date
1 2015-10-25T20:47:13+00:
2 2015-10-25T13:00:34+00:
3 2015-10-25T12:58:58+00:
4 2015-10-25T12:58:32+00:
5 2015-10-25T12:58:09+00:
6 2015-10-25T12:58:08+00:
7 2015-10-25T12:58:01+00:
8 2015-10-25T12:57:46+00:
9 2015-10-25T12:57:08+00:
10 2015-10-25T12:57:02+00:
11 2015-10-25T12:56:59+00:
12 2015-10-25T12:56:12+00:
13 2015-10-25T12:56:10+00:
14 2015-10-25T12:55:07+00:
15 2015-10-25T12:54:51+00:
16 2015-10-25T12:54:47+00:

Current Location Details

Date:

Location:

From:

Context:

Log Output

```
DEBUG:2015-10-25 15:00:39,813 In Instagram.py:131: 100 photos have been retrieved
DEBUG:2015-10-25 15:00:41,512 In CreepyMain.py:126: Analysis thread finished for all targets.
DEBUG:2015-10-25 15:00:41,672 In CreepyMain.py:573: Attempting to draw locations for the current project
```

Project Analysis complete!

SOBRE

- Assustador é uma ferramenta OSINT de geolocalização. Reúne informações relacionadas à geolocalização de fontes on-line e permite a apresentação no mapa, a filtragem de pesquisa com base no local e / ou na data exata, a exportação no formato csv ou kml para análise posterior no Google Maps.

FERRAMENTAS OSINT: CREEPY

The screenshot displays the 'cree.py - Geolocation OSINT tool' interface. The main window shows a Google Map of Athens, Greece, with numerous blue and yellow location markers. A pop-up window titled 'Retrieved from flickr' is open, showing a photo of the Acropolis of Athens. The photo is attributed to user 'ccgd' and was taken on 2015-10-15 at 09:21:02 +0000. The link to the original photo is <http://www.flickr.com/photos/14551451@N00/22352020741>. The interface also includes a 'Locations List' on the right side, a 'Current Location Details' section, and a 'Log Output' at the bottom. The log output shows the following messages:

```
DEBUG:2015-10-25 15:00:39,813 In instagram.py:131: 100 photos have been retrieved
DEBUG:2015-10-25 15:00:41,512 In CreepyMain.py:126: Analysis thread finished for all targets.
DEBUG:2015-10-25 15:00:41,672 In CreepyMain.py:575: Attempting to draw locations for the current project
```

Project Analysis complete!

MATERIAL PARA ESTUDO

- <https://github.com/ilektrjohn/creepy>
- <https://www.youtube.com/watch?v=JqJ4zaDIVAs>
- <https://www.youtube.com/watch?v=H4INyjrRNA>


```
language_attributes(); ?>>
charset="<?php bloginfo( 'charset' ); ?>"
name="viewport" content="width=device-width"
rel="profile" href="http://gmpg.org/xfn/11"
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>"
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
```

RECON-NG

FERRAMENTAS OSINT: RECON-NG

```

  \\\  \\\  \\\  \\\  \  \  \  \  \\\  \  \  \  \\\
 \  \  \  \  \  \  \  \  \  \  \  \  \  \  \  \
 \\\  \\\  \\\  \\\  \  \  \  \  \\\  \  \  \  \\\
 \  \  \  \  \  \  \  \  \  \  \  \  \  \  \  \

      ^
     / \ \ /
Sponsored by...  \ /  \ \  \ \  \ \
                  \ \  \ \  \ \  \ \
                  / \ \ // \ \ \ \ \ \ \ \ \ \
                  // // BLACK HILLS \ \ \ \
                  www.blackhillsinfosec.com

[recon-ng v4.9.5, Tim Tomes (@LaNMaSteR53)]

[81] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] >
```

SOBRE

- Recon-ng é uma ferramenta de reconhecimento com uma interface semelhante ao Metasploit. Ao executar a reconexão a partir da linha de comandos, você entra em um ambiente semelhante a shell, no qual é possível configurar opções, executar resultados de reconhecimento e saída para diferentes tipos de relatórios.

FERRAMENTAS OSINT: RECON-NG

```
///  ///  ///  ///  /  /  /  /  ///
/  /  /  /  /  /  /  /  /  /  /  /  /
///  ///  /  /  /  /  /  /  /  /  /
/  /  /  /  /  /  /  /  /  /  /  /

      ^
     /\
    /\  \
   /\  \ \
  /\  \ \ \
 /  \ \ \ \ \ \ \
//  // BLACK HILLS \ \
www.blackhillsinfosec.com

[recon-ng v4.9.5, Tim Tomes (@LaNMaSteR53)]

[81] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] >
```

MATERIAL PARA ESTUDO

- <https://hackertarget.com/recon-ng-tutorial/>
- <https://github.com/lanmaster53/recon-ng>
- <https://itharley.com/osint-com-o-recon-ng-parte-1-de-3/>
- <https://www.youtube.com/watch?v=0J6Auz88iTY>
- <https://www.youtube.com/watch?v=x80wy7XQCoU>
- <https://www.youtube.com/watch?v=ueWeucZMdmk>


```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?> />
rel="profile" href="http://gmpg.org/xfn/11" />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_class = fruitful_get_class($menu_pos);
```

GASMAK

FERRAMENTAS OSINT: GASMAK

```
welsh@kali:~/osint/gasmak$ ls
README.md  gasmask.py  LICENSE  README.md  requirements.txt
wslsh@kali:~/osint/gasmak$ python3 gasmask.py

  _____
 |  _  _  _  |
 |  _  _  _  |
 |  _  _  _  |
 |  _  _  _  |

Gasmak - OSINT is an information gathering tool - OSINT
Ver. 1.0
Written by @tw0lsec
Github: https://github.com/twelvesec/gasmak

usage: gasmask.py [-h] [-d DOMAIN] [-s SERVER] [-p PROXY] [-l LIMIT]
                 [-i PROXY] [-o OUTPUT]

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        DOMAIN to search.
  -s SERVER, --server SERVER
                        DNS server to use.
  -p PROXY, --proxy PROXY
                        Use a proxy server when retrieving results from search engines (eg. '-p http://127.0.0.1:8080')
  -l LIMIT, --limit LIMIT
                        Limit the number of search engine results (default: 100).
  -i PROXY, --input PROXY
                        Limit information gathering (has: whois, dns, reverse, whois, google,bing, yahoo,ask,duck (ie: yandex),linkedin,twitter,amazon,
                        legals,publicdns,reddit,github,instagram,rt,qq,wechat,videochat).
  -o OUTPUT, --output OUTPUT
                        Output in the four major formats at once (darkroom, txt, xml and html).

wslsh@kali:~/osint/gasmak$
```

MATERIAL PARA ESTUDO

- <https://github.com/twelvesec/gasmak>
- <https://www.youtube.com/watch?v=dVEP5rHZEAw>
- <https://www.youtube.com/watch?v=jwTFmLcZBNs>

```
charset="<?php bloginfo( 'charset' ); ?>" />
<?php wp_title( '|', true, 'right' ); ?> />
rel="profile" href="http://gmpg.org/xfn/11" />
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>" />
fruitful_get_favicon(); ?>
wp_head(); ?>
<?php body_class();?>
<div id="page-header" class="hfeed site">
<?php
    $theme_options = fruitful_get_theme_options();
    $logo_pos = $menu_pos = '';
    if (isset($theme_options['logo_position']))
        $logo_pos = esc_attr($theme_options['logo_position']);
    if (isset($theme_options['menu_position']))
        $menu_pos = esc_attr($theme_options['menu_position']);
    $logo_pos_class = fruitful_get_class($logo_pos);
    $menu_pos_class = fruitful_get_class($menu_pos);
    $responsive_menu_type = fruitful_get_class($menu_pos);
    $responsive_menu_class = fruitful_get_class($menu_pos);
```

RESOURCES

FERRAMENTAS OSINT: RESOURCE



MATERIAL PARA ESTUDO

- <https://medium.com/@micallst/osint-resources-for-2019-b15d55187c3f>

CONCLUSÃO

“O OSINT É UMA DAS ARMAS MAIS PERIGOSAS UTILIZADAS POR HACKERS, POIS TENDO CONHECIMENTOS EM OSINT, FICA MAIS FÁCIL PARA REALIZAR ATAQUES DE ENGENHARIA SOCIAL OU INTRUSIVOS EM UMA EMPRESA, ALÉM DE COLETAR INFORMAÇÕES DE UMA PESSOA OU ORGANIZAÇÃO”

AGRADECIMENTO

Obrigado por ler esse livro

<https://www.facebook.com/cybersecup>

<https://www.facebook.com/Expersec/>

<https://www.facebook.com/exchangesec/>

<https://www.facebook.com/como.hackear.curso/>

PALESTRAS

https://www.youtube.com/watch?v=nvdsQIT9_xY

<https://www.youtube.com/watch?v=IDEd4tXdEjc>

<https://www.youtube.com/watch?v=46st98FUf8s>

<https://www.youtube.com/watch?v=I5OYDN5PwU4>

<https://www.youtube.com/watch?v=qH1p-N0AzYk>

REFERÊNCIAS

<https://pt.wikipedia.org/wiki/OSINT>

<https://pt.wikipedia.org/wiki/HUMINT>

<https://pt.wikipedia.org/wiki/IMINT>

<https://pt.wikipedia.org/wiki/MASINT>

<https://pt.wikipedia.org/wiki/SIGINT>

<https://pt.wikipedia.org/wiki/ELINT>

<https://pt.wikipedia.org/wiki/FISINT>

<https://pt.wikipedia.org/wiki/SIGINT>

<https://osintbrasil.blogspot.com/2017/08/ferramentas-osint-e-como-voce-aprende.html>

<https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools>