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

O QUE É OSINT?

- **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 DO OSINT

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 Princenton. 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 OSINT?

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.

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

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.

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.

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 signais sem-fio da marinha russa, destinados para a mobilização dos navios da esquadra; esta foi a primeira vez que algo do tipo ocorreu

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.

SIGINT: HISTÓRIA

- Cada vez mais a SIGINT vem se tornado 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.

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.

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

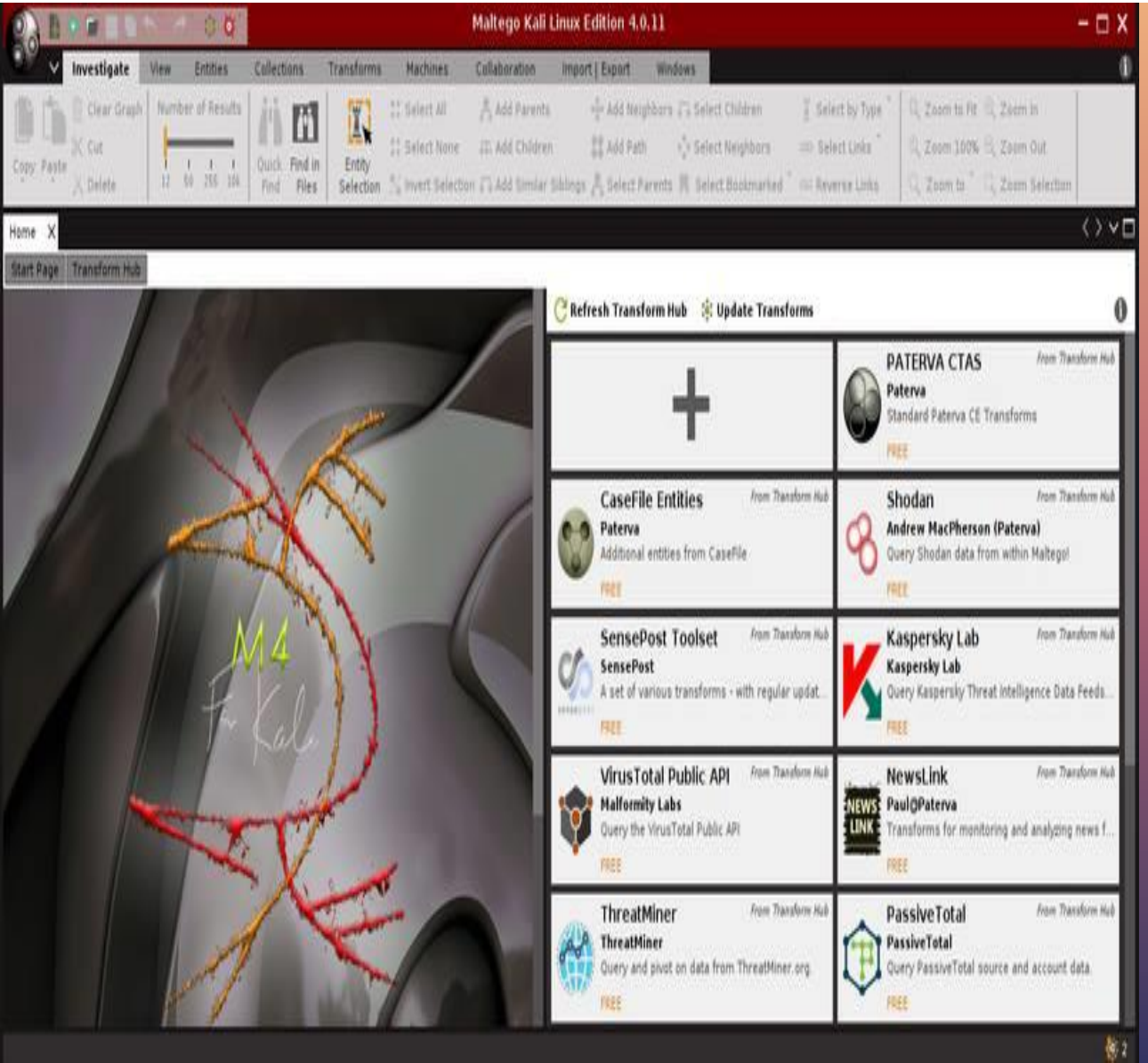
FERRAMENTAS OSINT

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/datasploit
- https://github.com/s-rah/onionscan
- https://osintframework.com/
- https://inteltechniques.com/menu.html
- http://www.misp-project.org/

MALTEGO

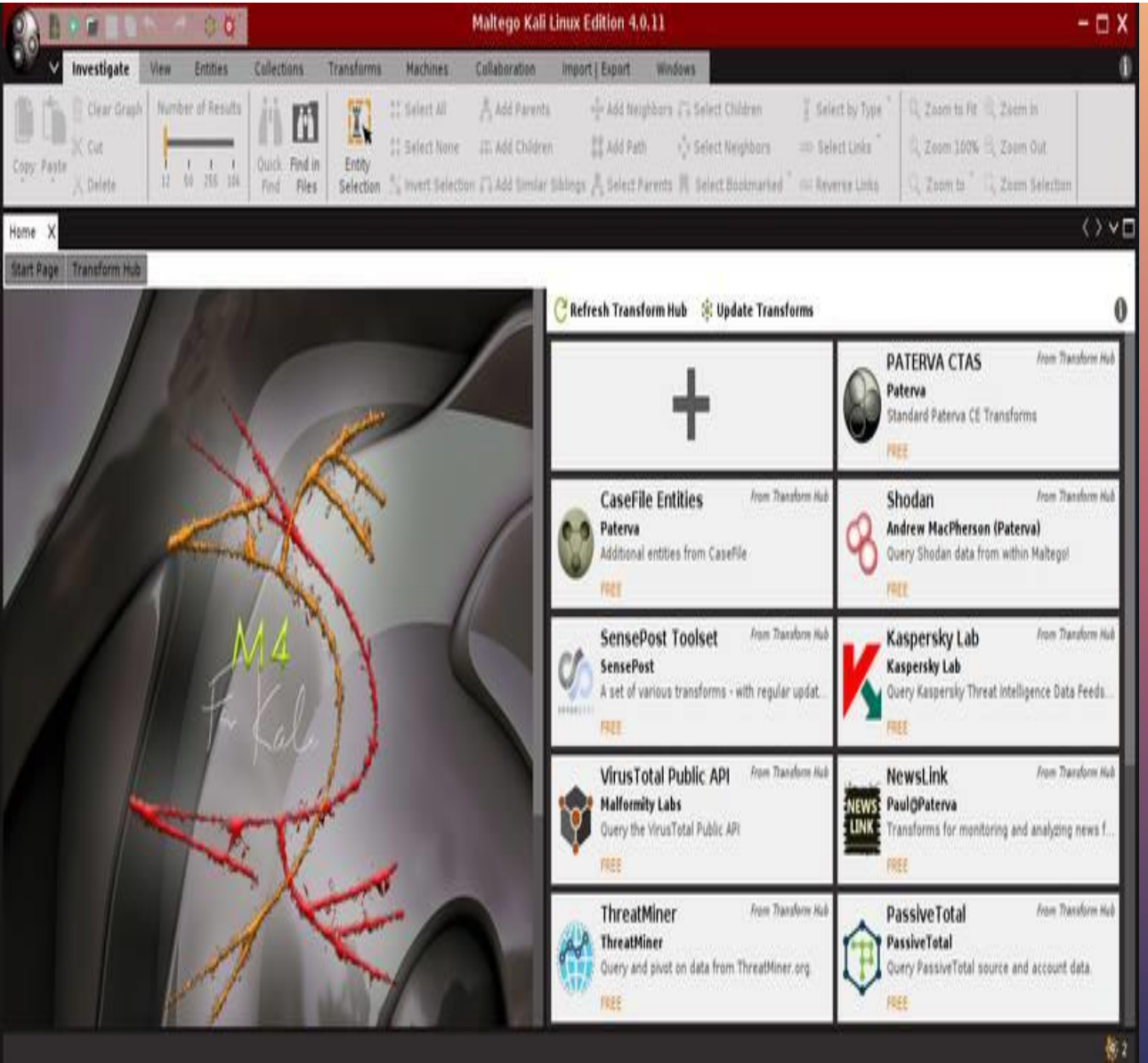
FERRAMENTAS OSINT: MALTEGO



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

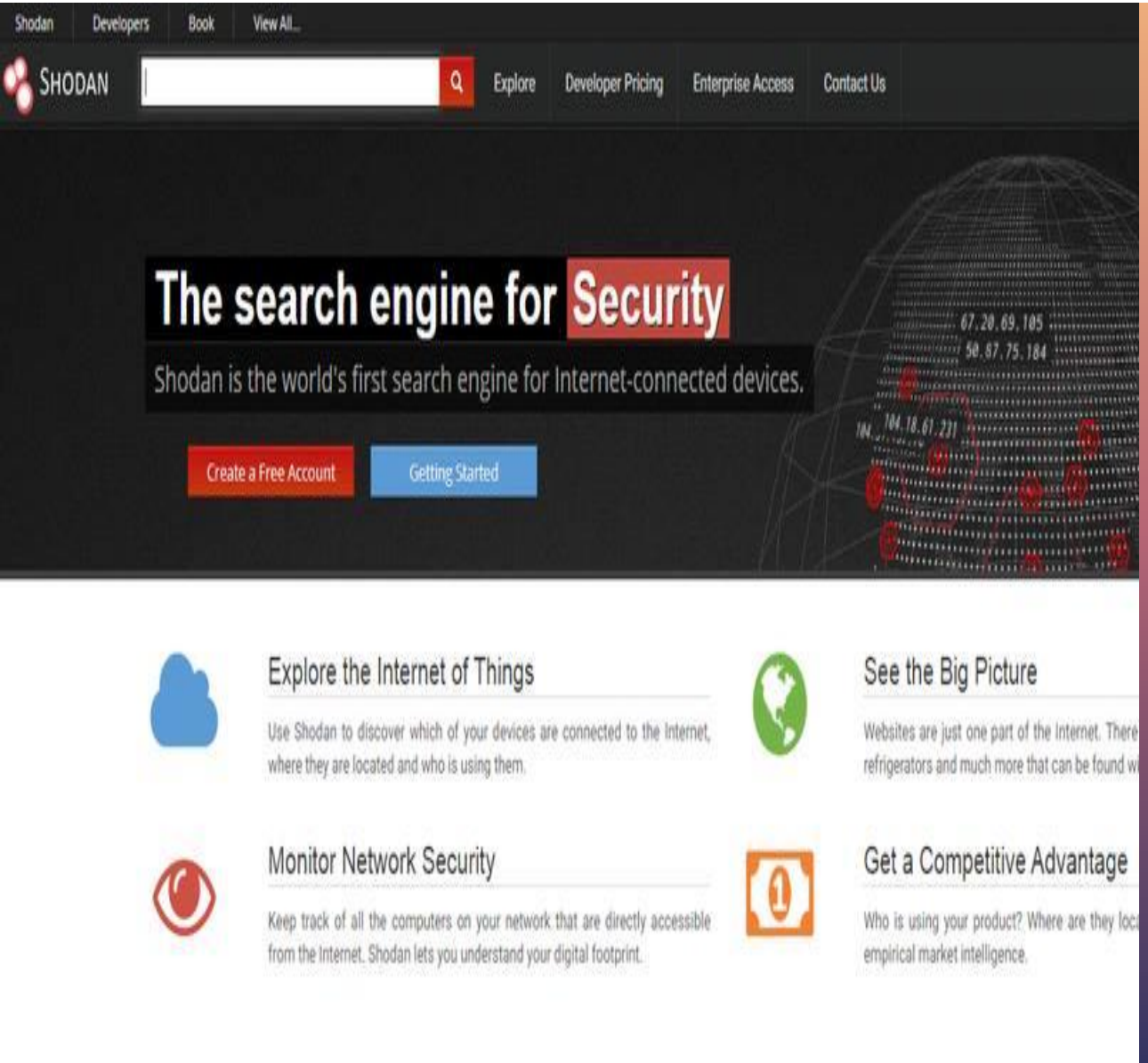


MATERIAL PARA ESTUDO

- https://www.youtube.com/watch?v=oSJCUfEcgT0
- https://pt.slideshare.net/cassioaramos/tutorial-maltego
- https://www.youtube.com/watch?v=sP-Pl_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

SHODAN

FERRAMENTAS OSINT: SHODAN



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

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 aquivos 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”.

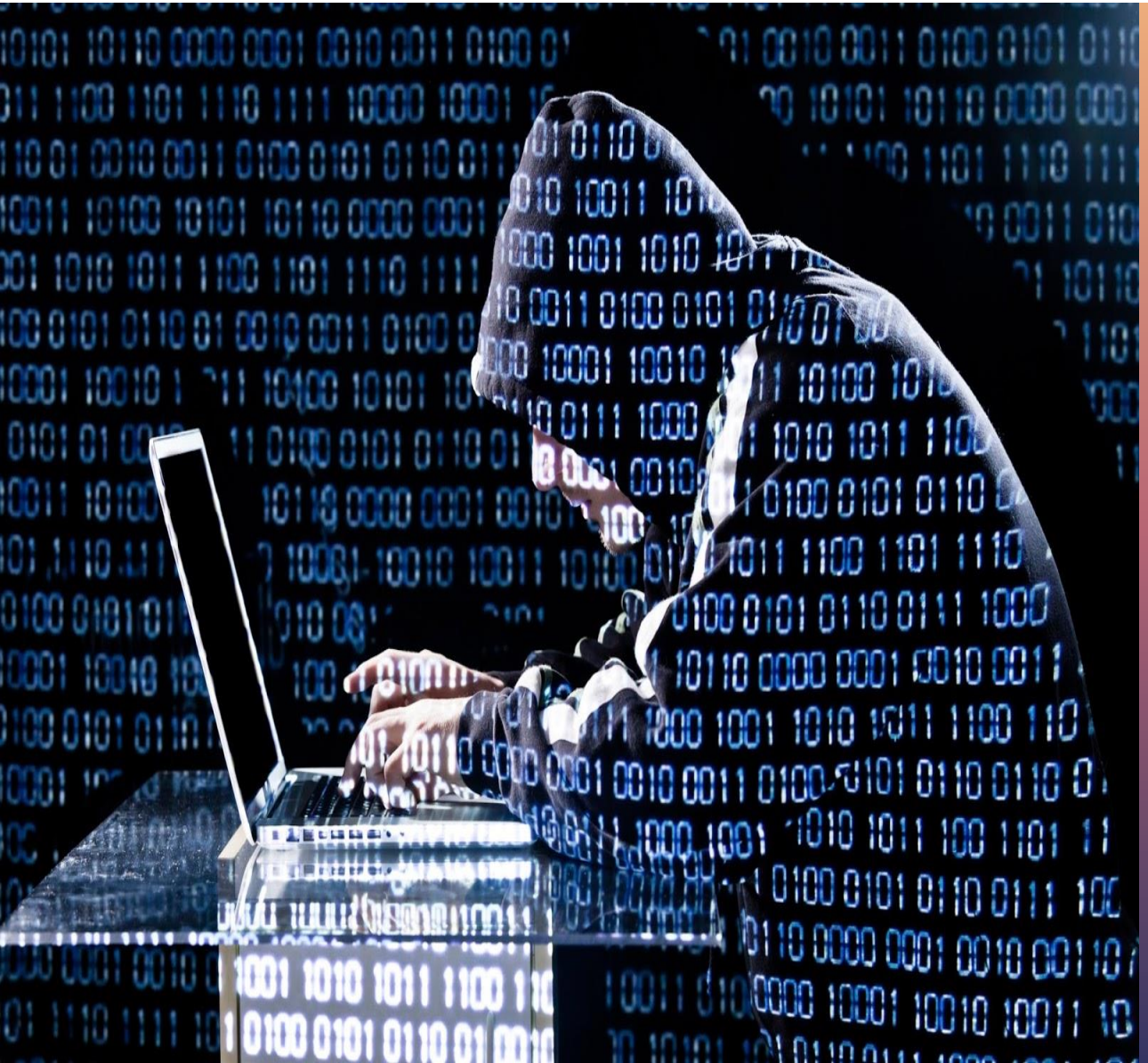
FERRAMENTAS OSINT: GOOGLE HACKING

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=d3NzsrmVrlw

SOCIAL NETWORK

FERRAMENTAS OSINT: SOCIAL NETWORK

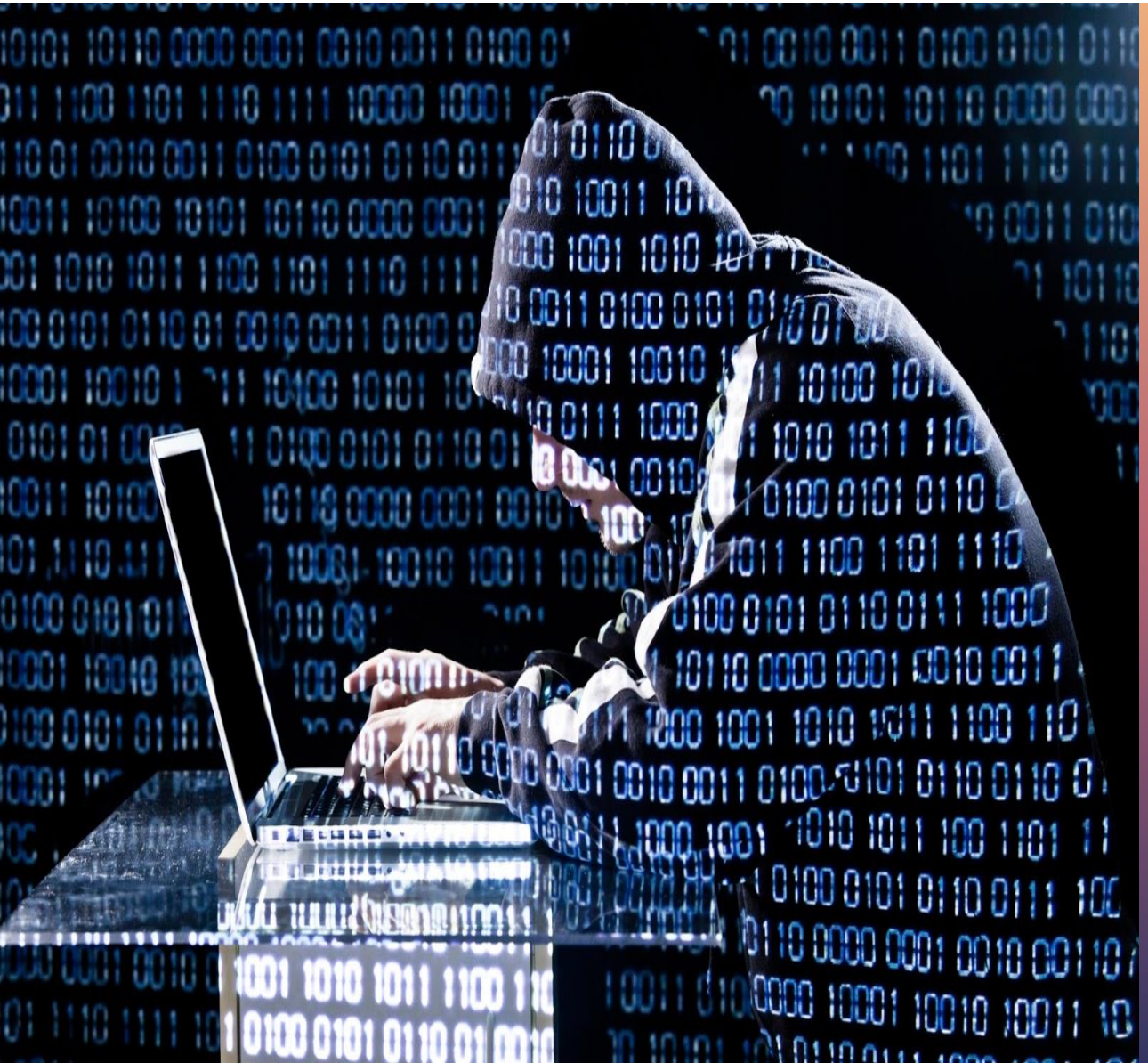


MATERIAL PARA ESTUDO

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

CHECK USERNAME

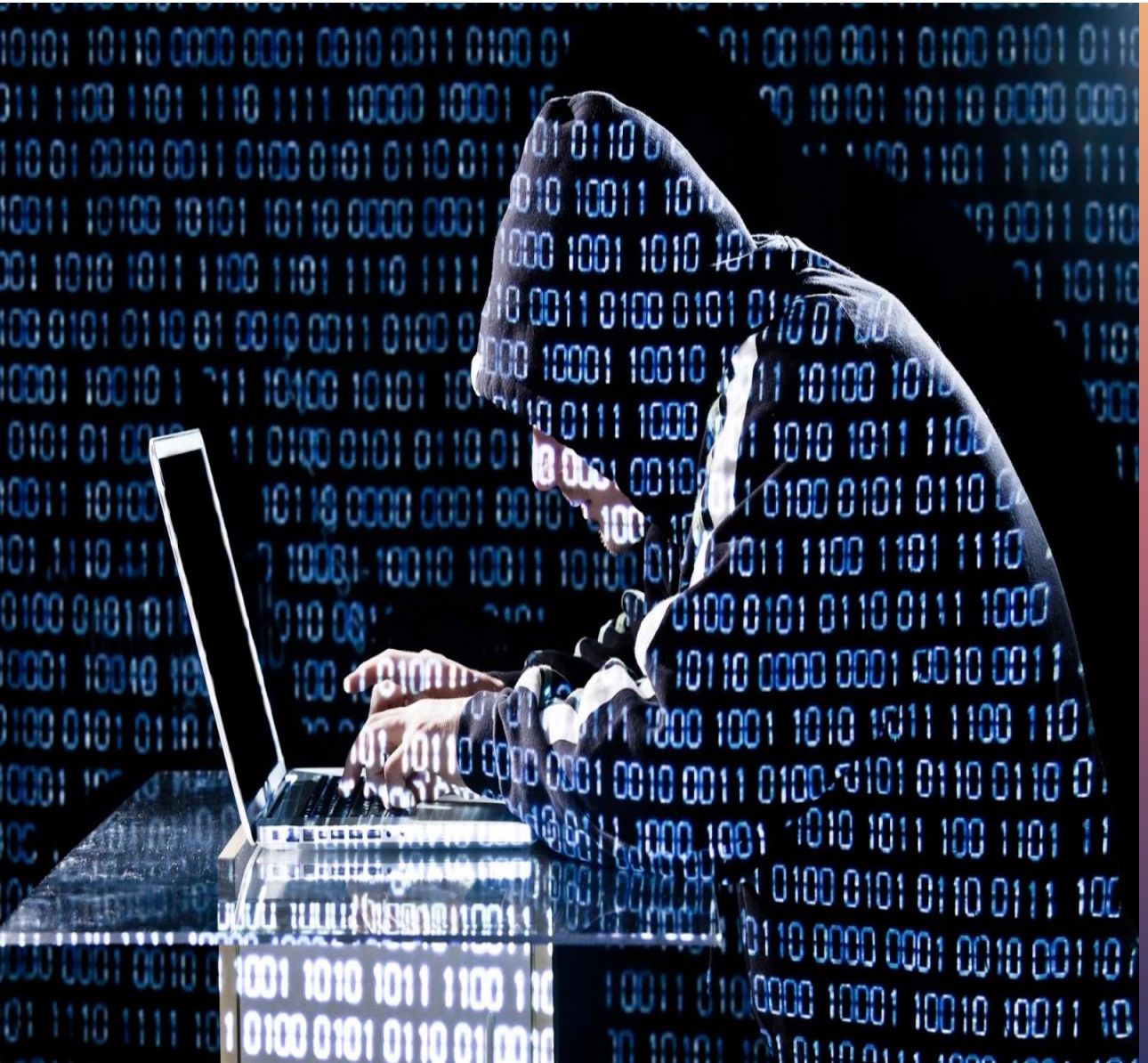
FERRAMENTAS OSINT: SOCIAL NETWORK



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

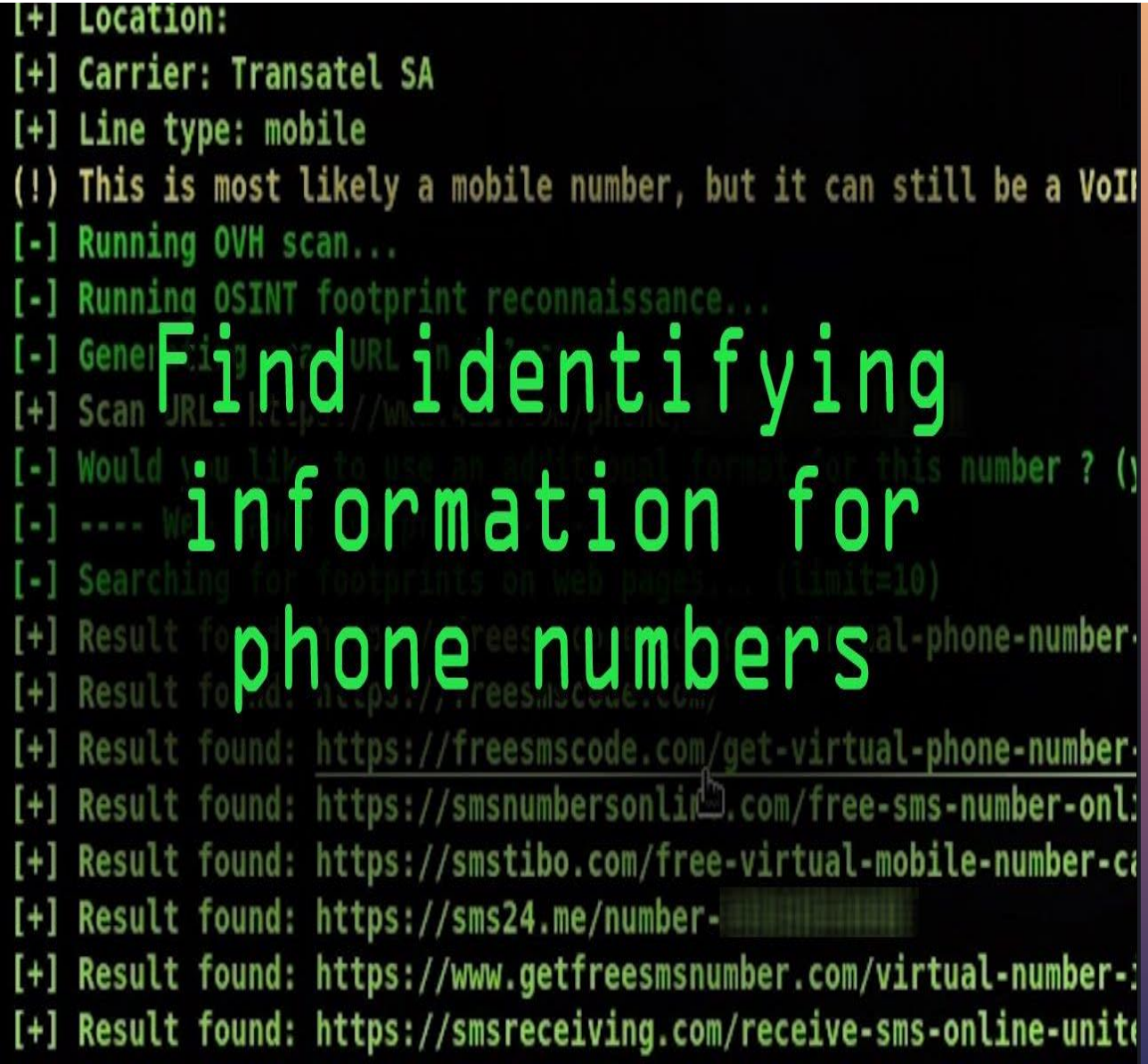


MATERIAL PARA ESTUDO

- 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

NUMERO DE TELEFONE

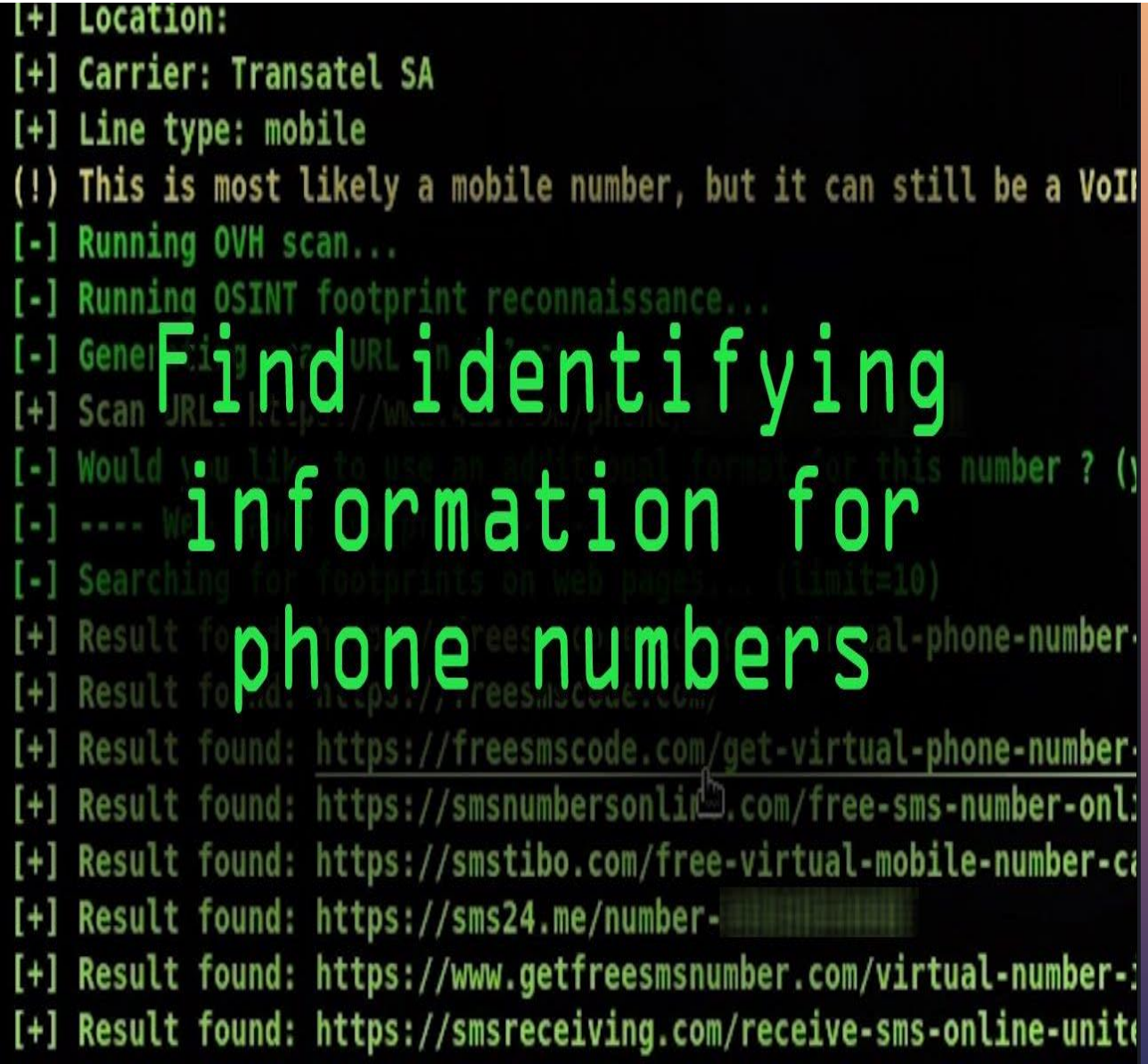
FERRAMENTAS OSINT: NUMERO DE TELEFONE



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

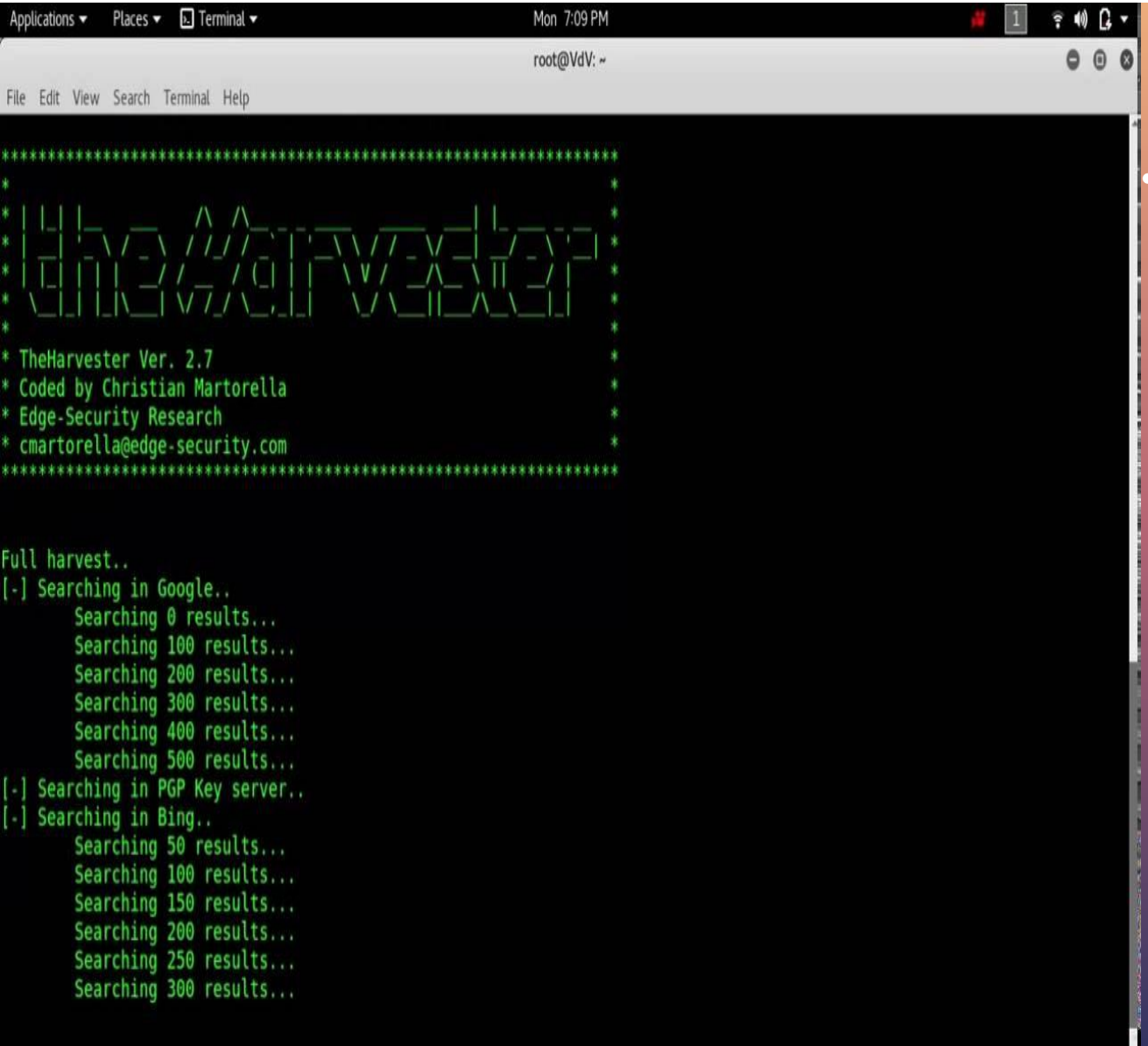


MATERIAL PARA ESTUDO

- 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

THE HARVERSTER

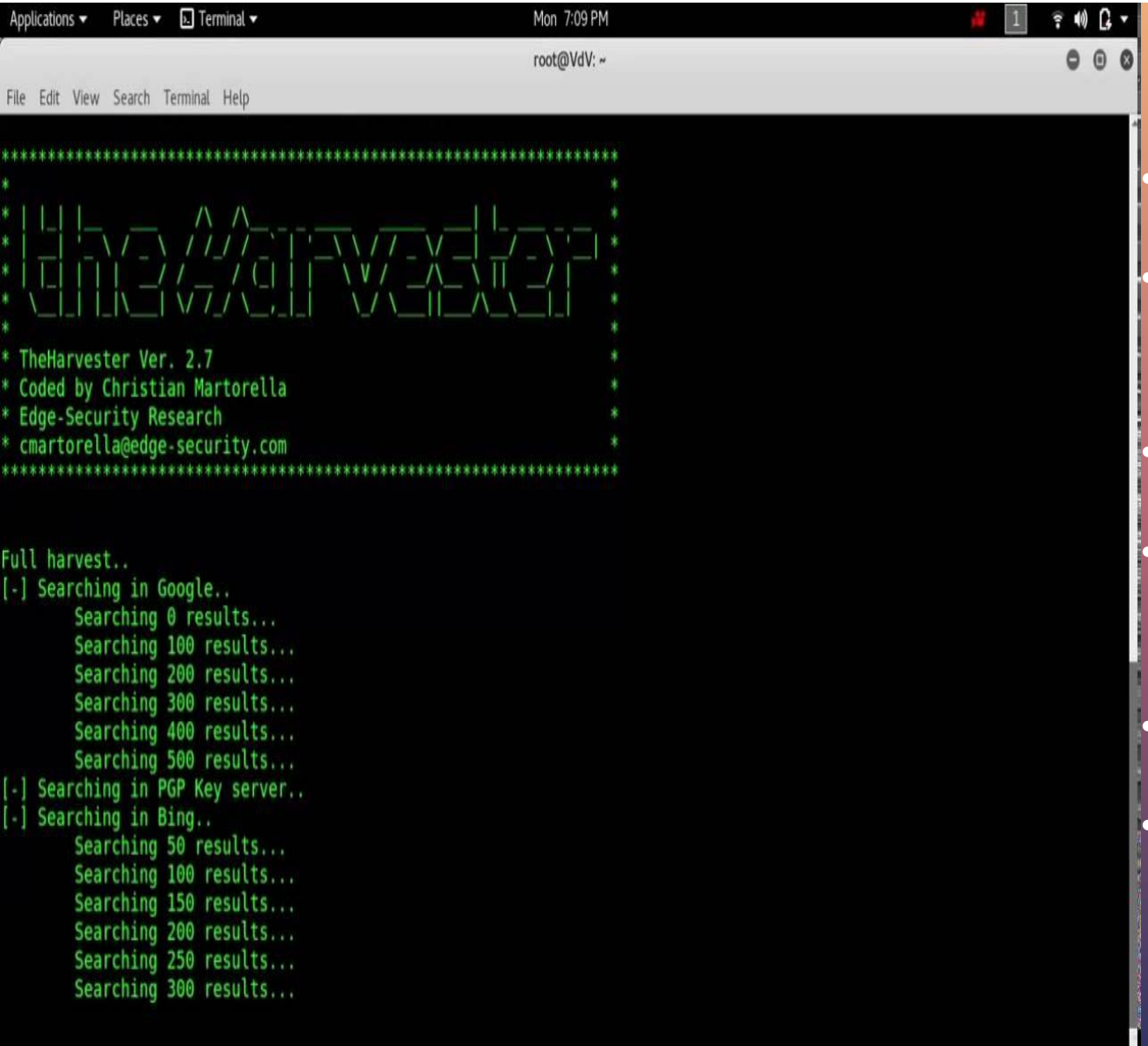
FERRAMENTAS OSINT: THE HARVESTER



SOBRE

- theHarvester é uma ferramenta muito simples, mas eficaz, projetada para ser usada nos estágios iniciais de um teste de penetração. Use-o para coleta de inteligência de código aberto e para ajudar a determinar o cenário de ameaças externas de uma empresa na Internet. A ferramenta reúne e-mails, nomes, subdomínios, IPs e URLs usando várias fontes de dados públicos

FERRAMENTAS OSINT: THE HARVESTER



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/

METAGOOFIL

FERRAMENTAS OSINT: METAGOOFIL

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.

FERRAMENTAS OSINT: METAGOOFIL

MATERIAL PARA ESTUDO

- https://www.100security.com.br/metagoofil/
- https://github.com/laramies/metagoofil
- https://www.youtube.com/watch?v=bZSYkh92xmM
- https://www.youtube.com/watch?v=nhnqScoyo_s
- https://www.youtube.com/watch?v=4hHPhCw5a-4
- https://www.youtube.com/watch?v=jgu_guhz_Ag

TINEYE

FERRAMENTAS OSINT: TINIEYE

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

MATERIAL PARA ESTUDO

- https://www.tineye.com/
- https://www.youtube.com/watch?v=5qkbsI9zi8Y
- https://www.youtube.com/watch?v=sufLXYuLL9M

WEB SCRAPING

FERRAMENTAS OSINT: 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.

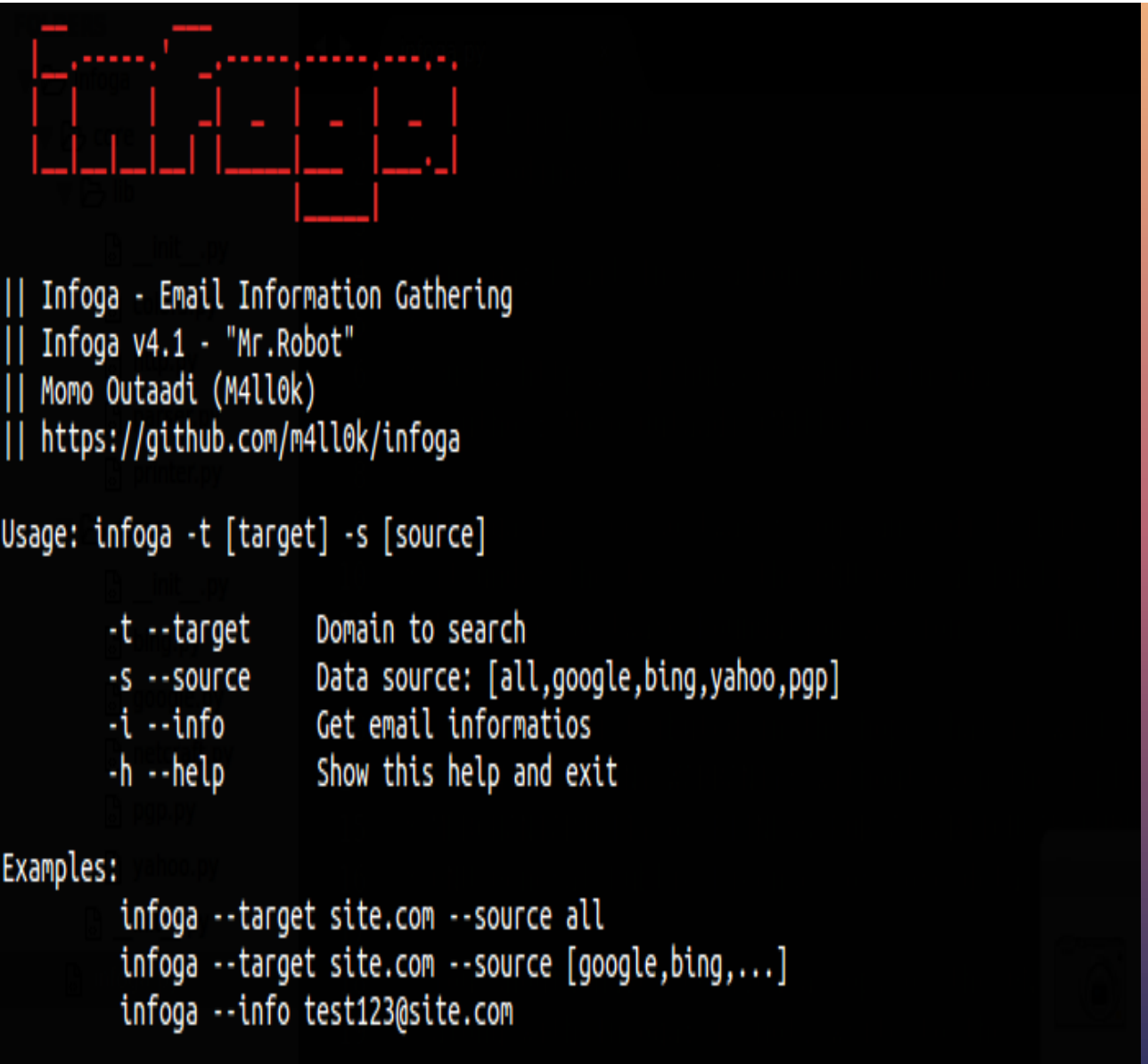
FERRAMENTAS OSINT: WEB SCRAPING

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/

INFOGA

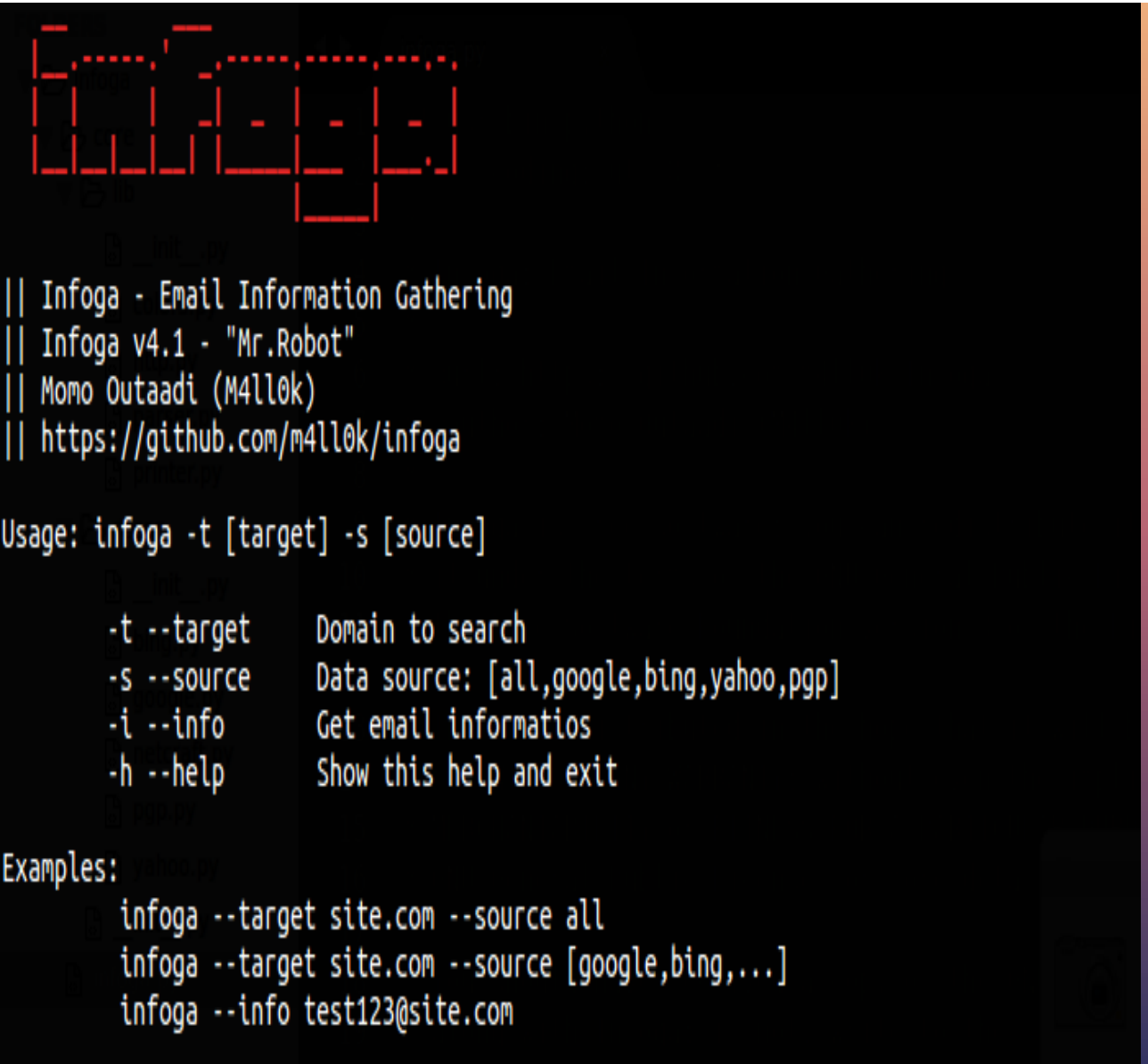
FERRAMENTAS OSINT: INFOGA



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

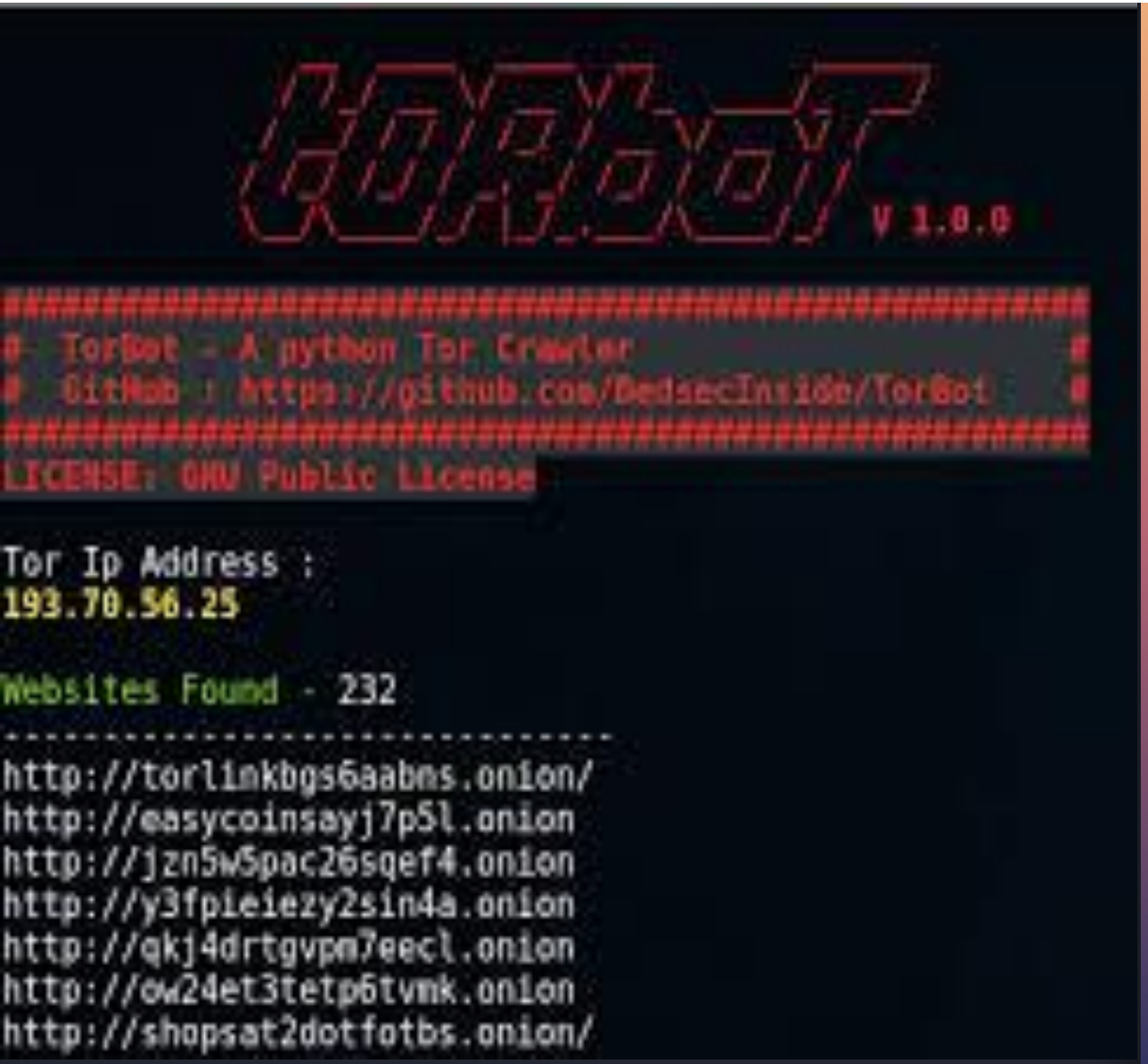


MATERIAL PARA ESTUDO

- https://github.com/m4ll0k/Infoga
- https://www.youtube.com/watch?v=KItbNlyA9IY
- 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

TORBOT

FERRAMENTAS OSINT: TORBOT



MATERIAL PARA ESTUDO

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

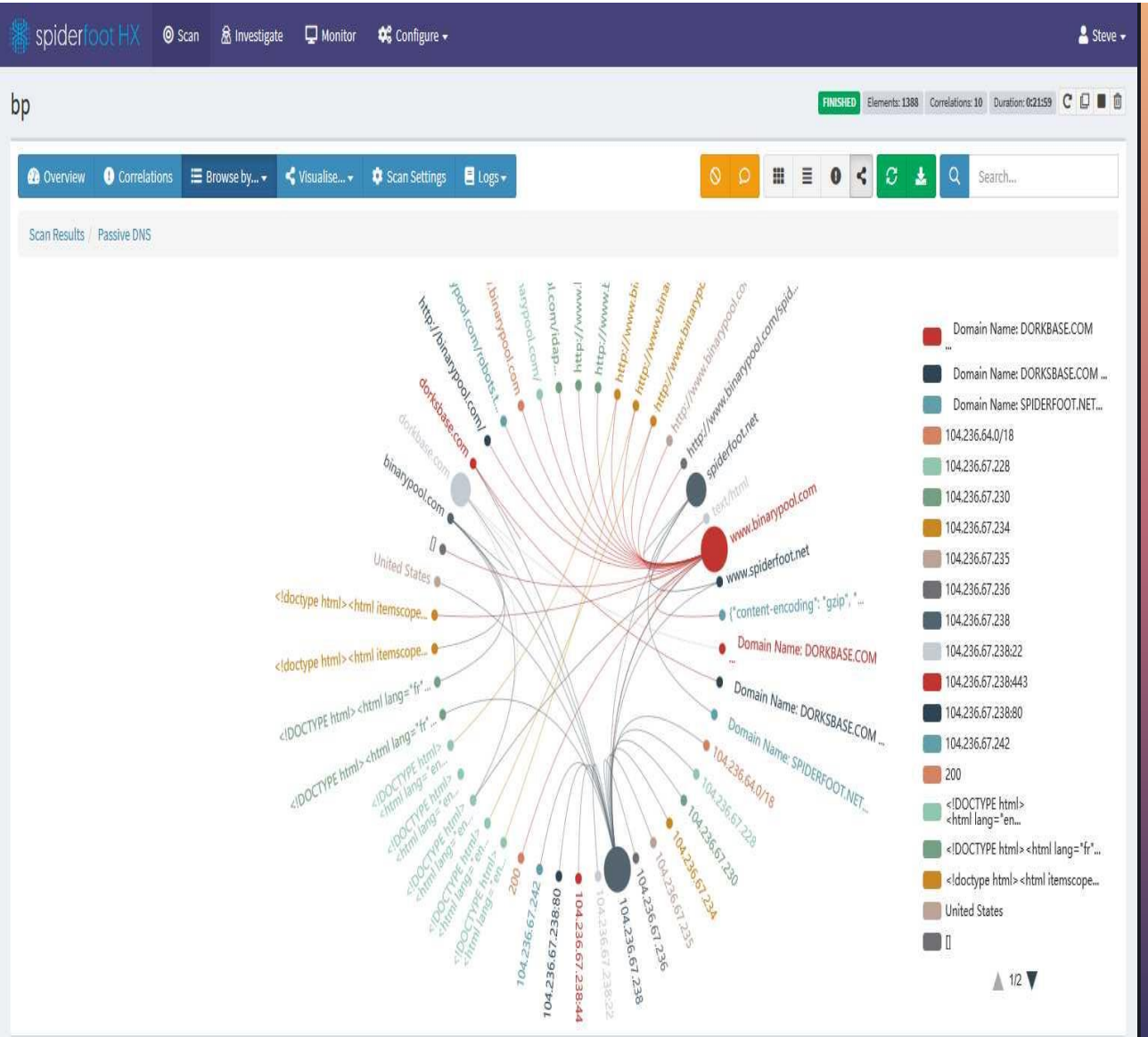
SPIDERFOOT

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

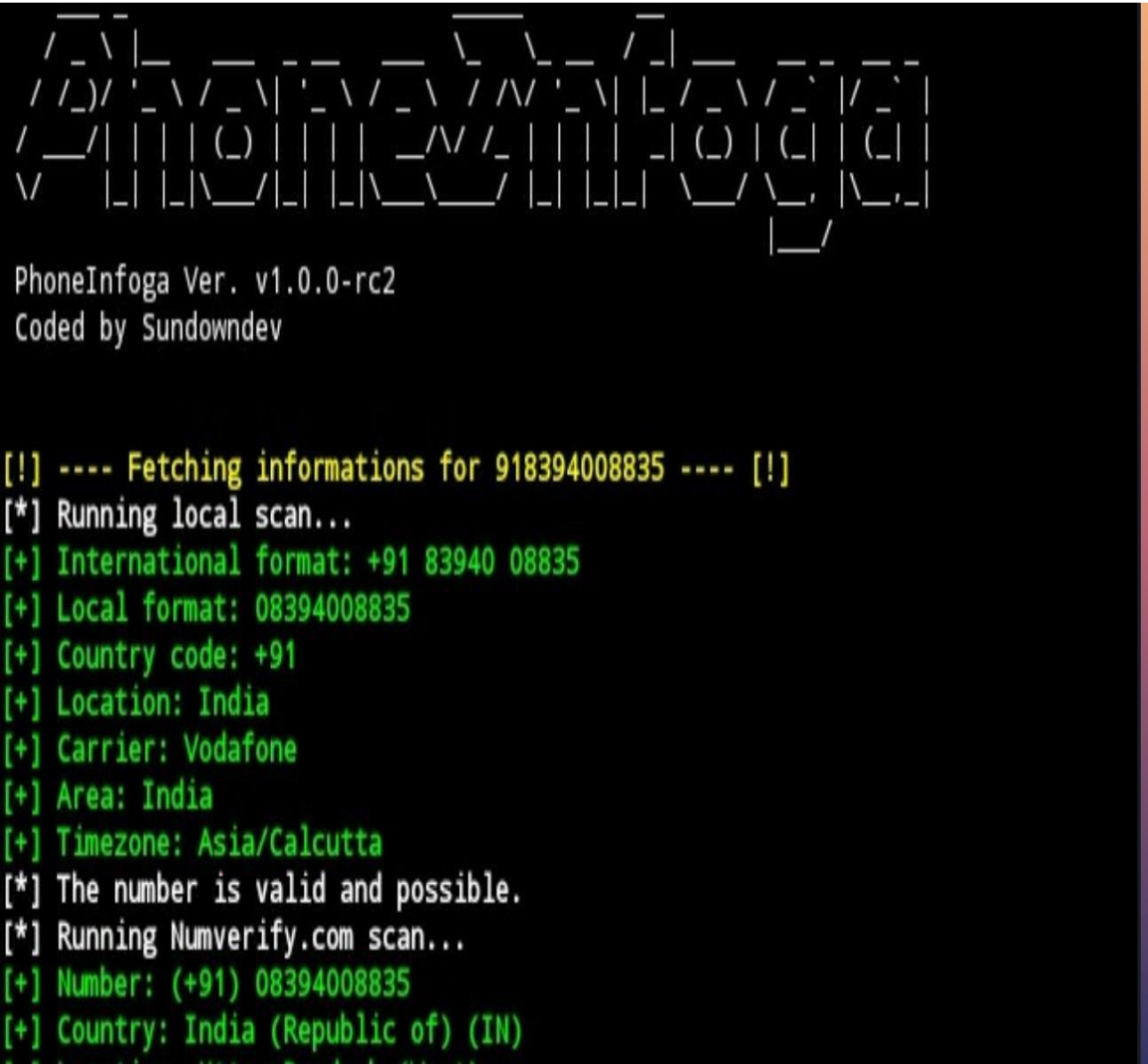


MATERIAL PARA ESTUDO

- 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/

PHONEINFOGA

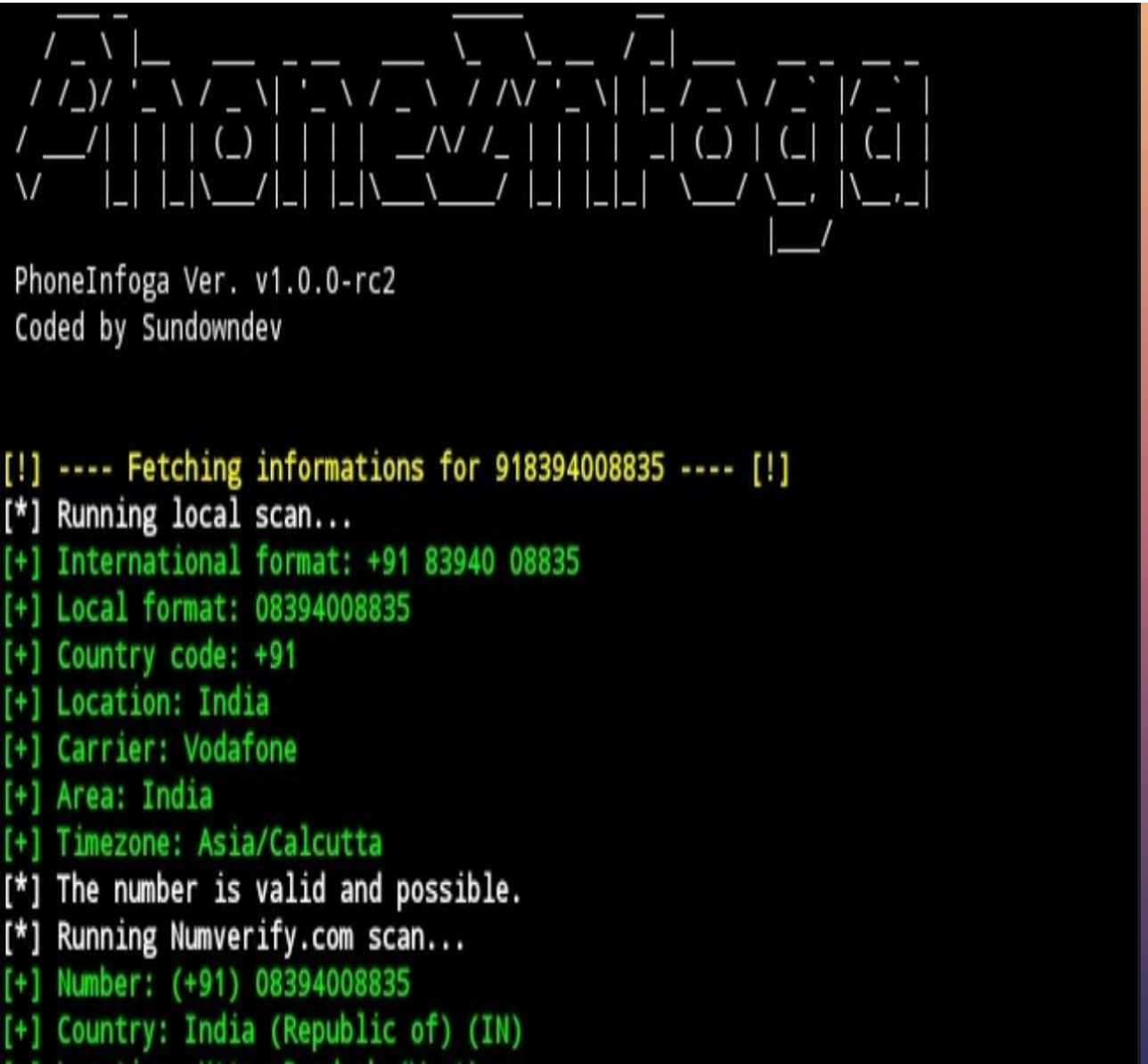
FERRAMENTAS OSINT: PHONEINFOGA



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

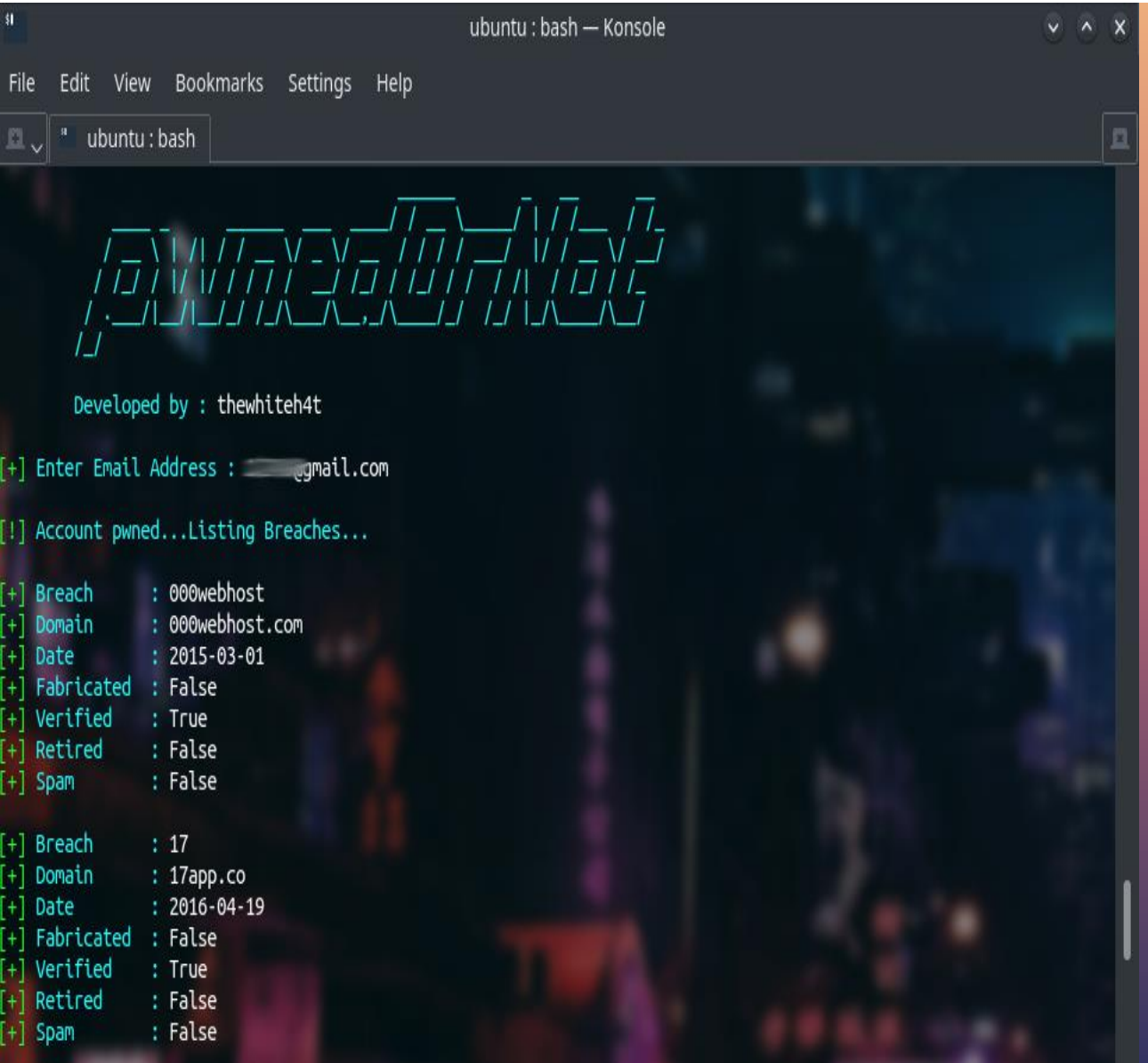


MATERIAL PARA ESTUDO

- 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

PWNEDORNOT

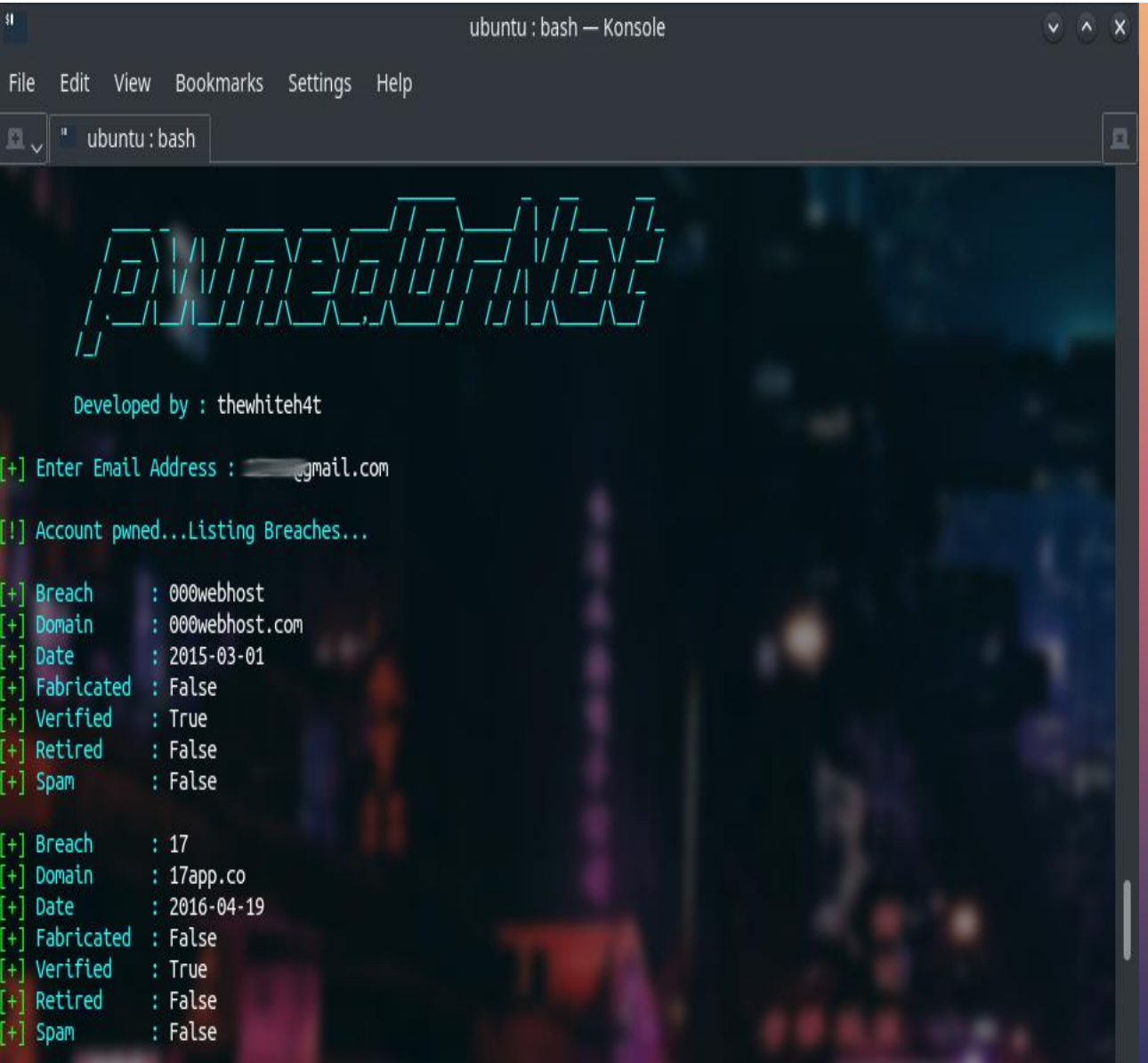
FERRAMENTAS OSINT: PWNEDORNOT



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

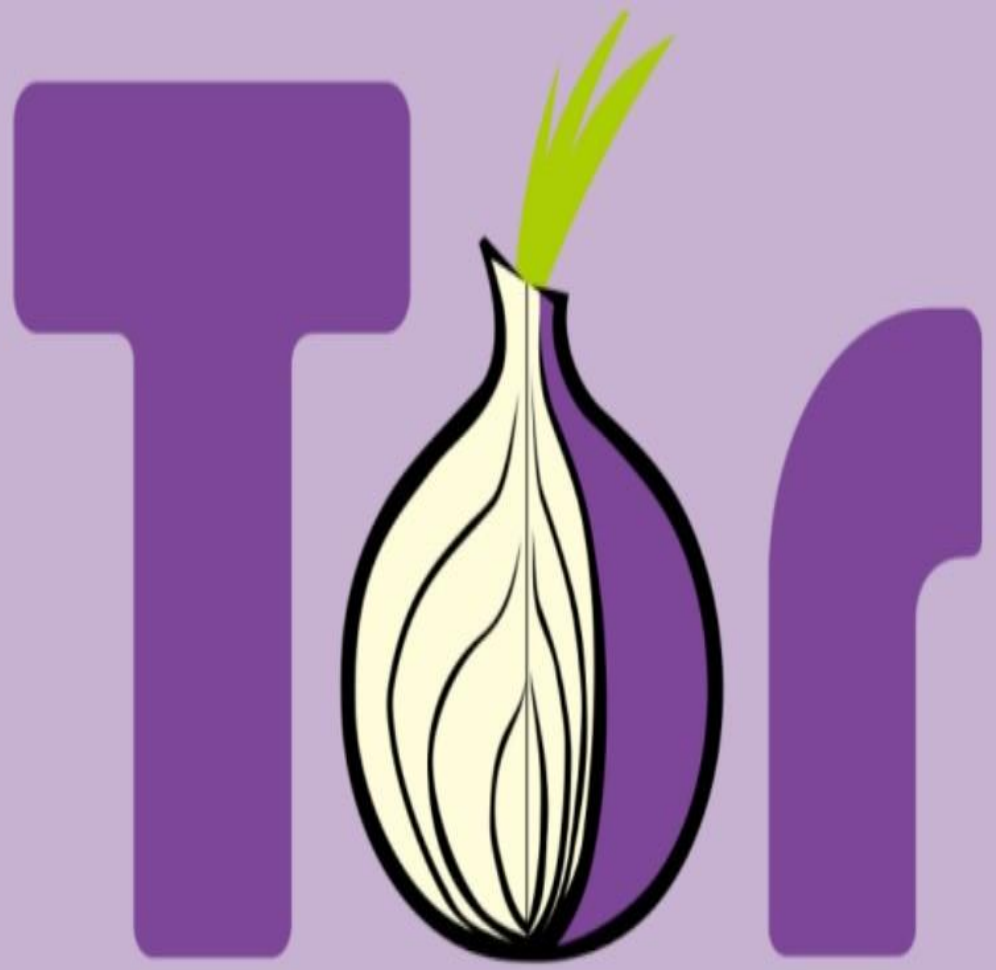


MATERIAL PARA ESTUDO

- https://github.com/thewhiteh4t/pwnedOrNot
- https://www.youtube.com/watch?v=BdJZhrkrpUI
- https://www.youtube.com/watch?v=cen0xC-MzZ8

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

SKYPE OSINT

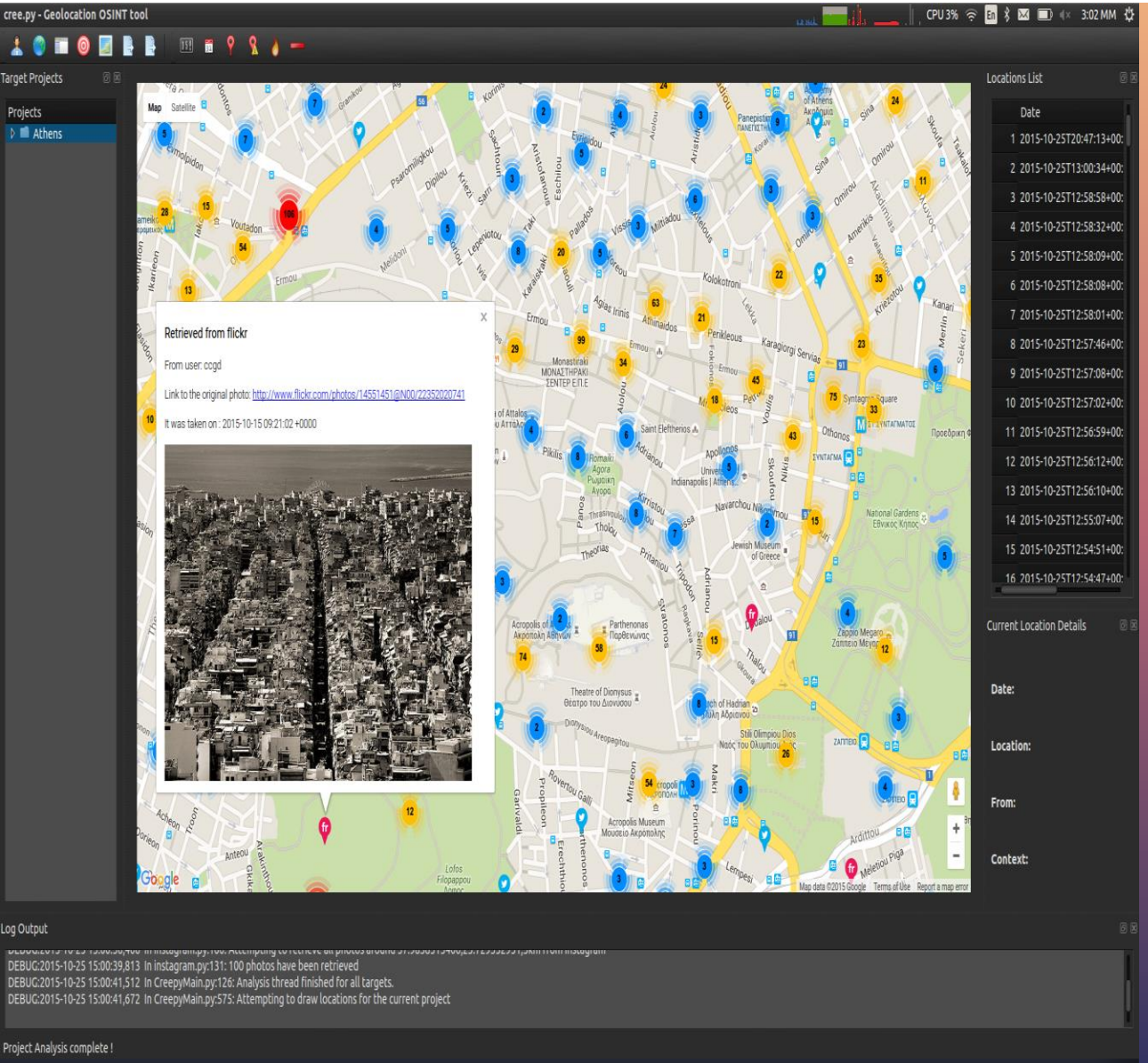
FERRAMENTAS OSINT: SKYPE

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

CREEPY

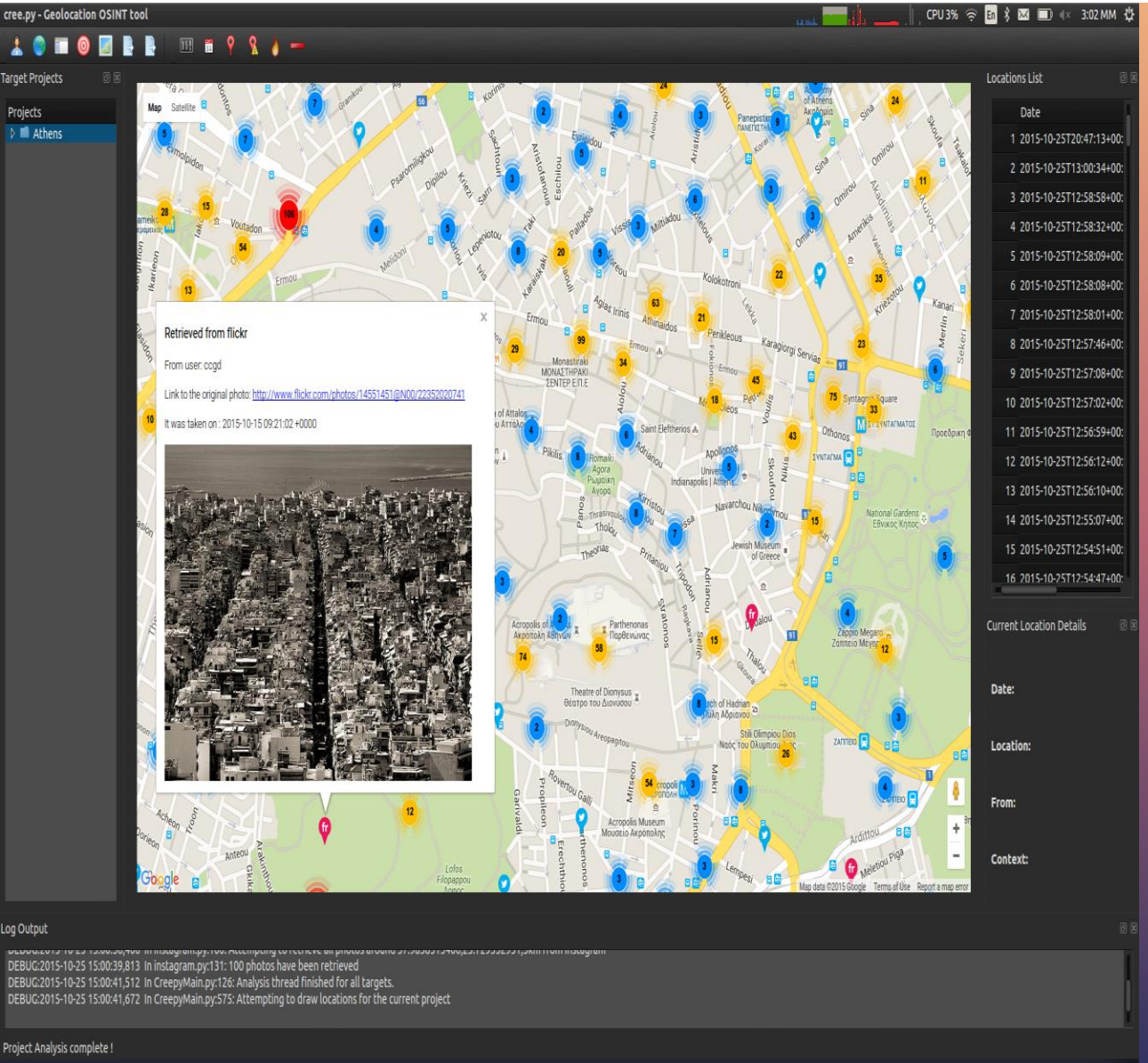
FERRAMENTAS OSINT: CREEPY



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

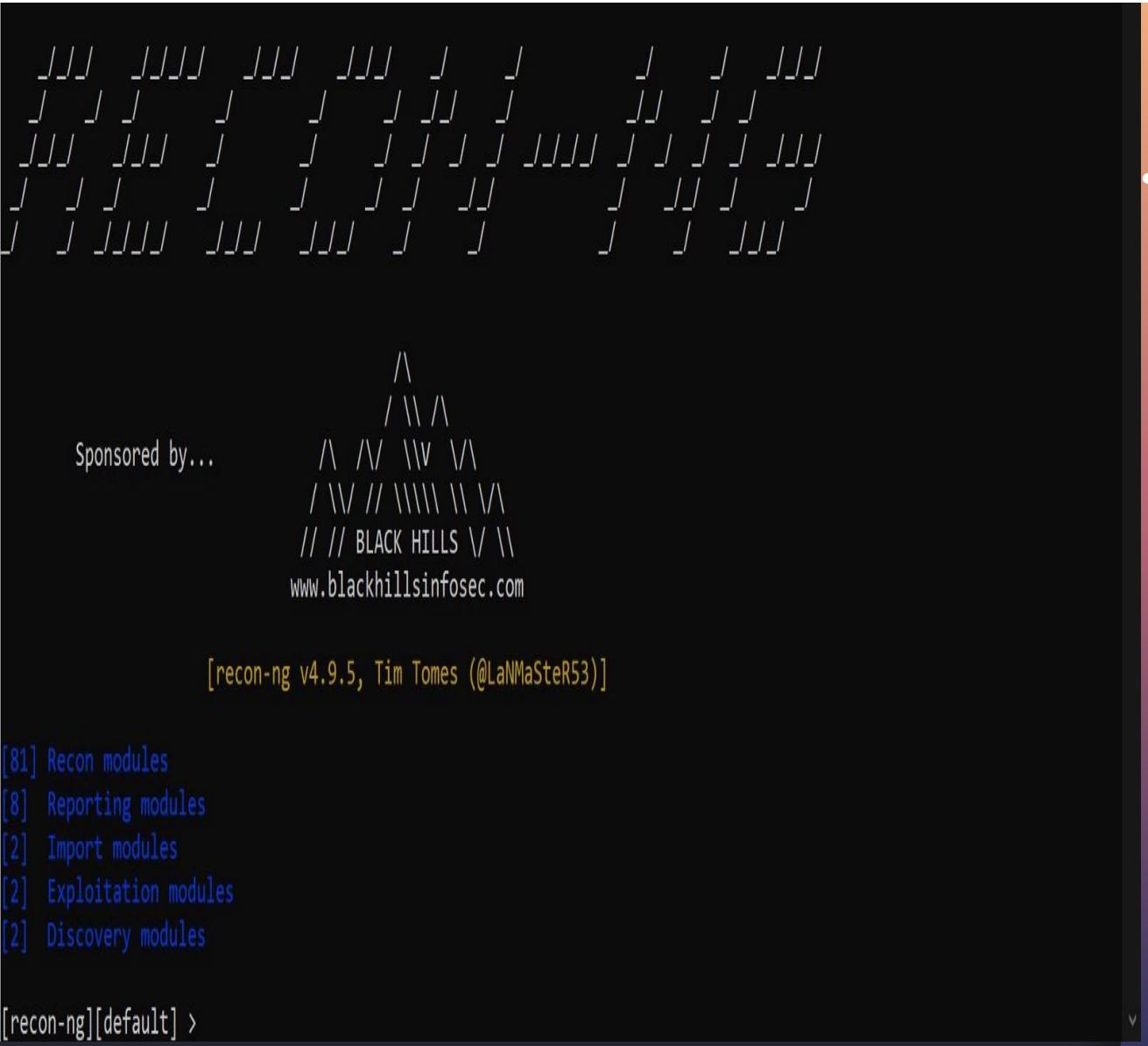


MATERIAL PARA ESTUDO

- https://github.com/ilektrojohn/creepy
- https://www.youtube.com/watch?v=JqJ4zaDIVAs
- https://www.youtube.com/watch?v=H4INyjrsRNA

RECON-NG

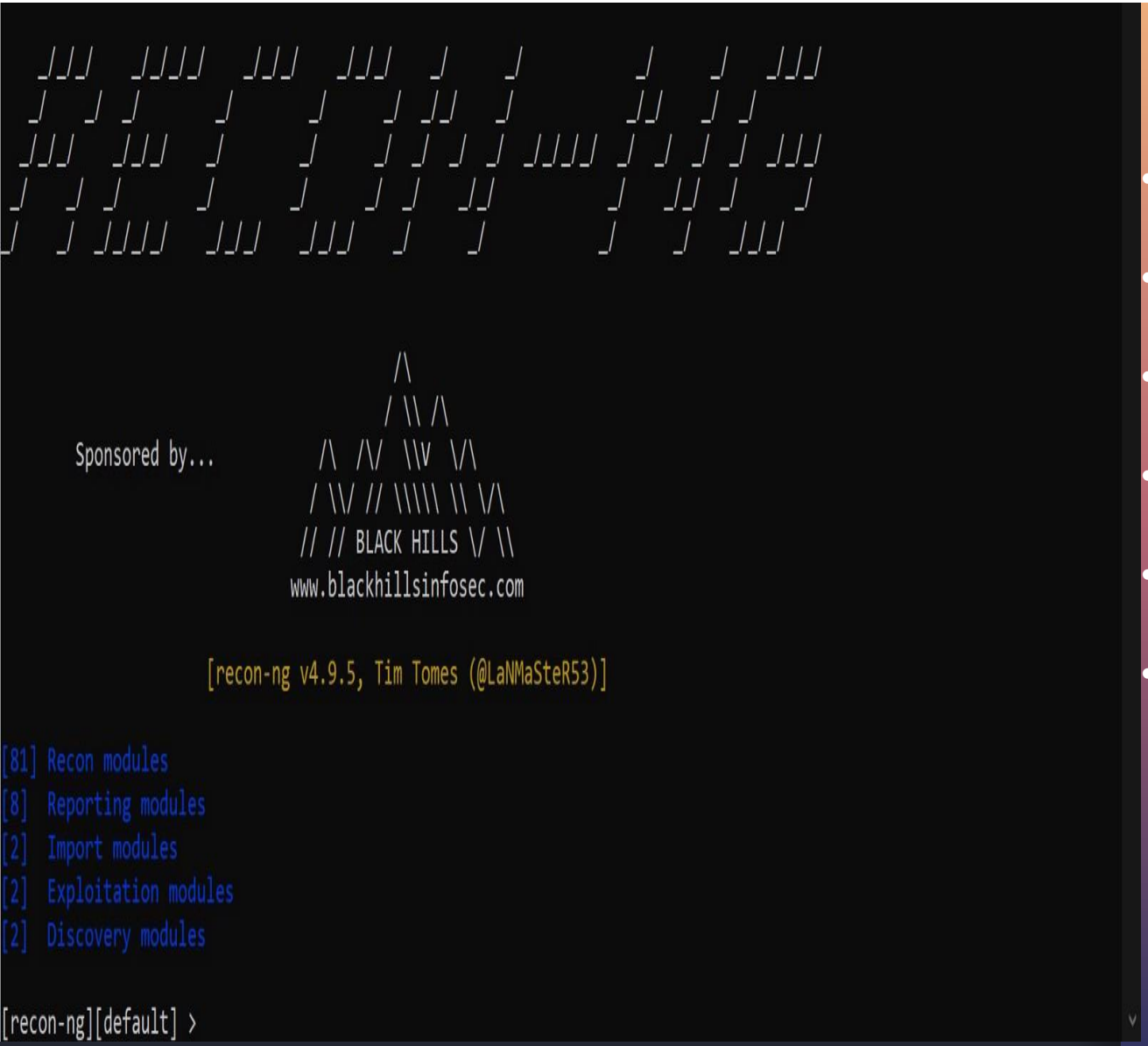
FERRAMENTAS OSINT: RECON-NG



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

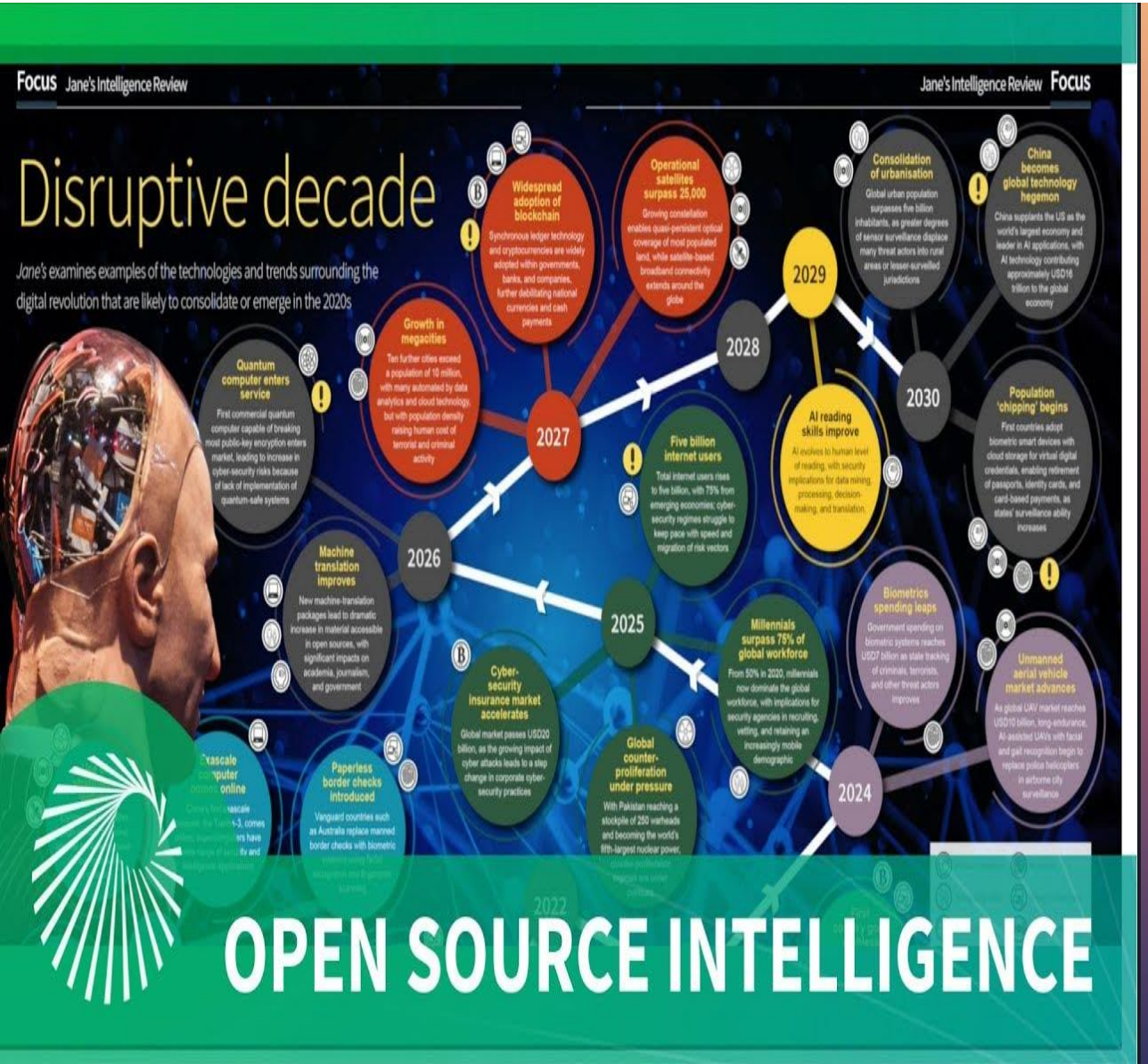


MATERIAL PARA ESTUDO

- 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

BEST TOOLS SEARCH

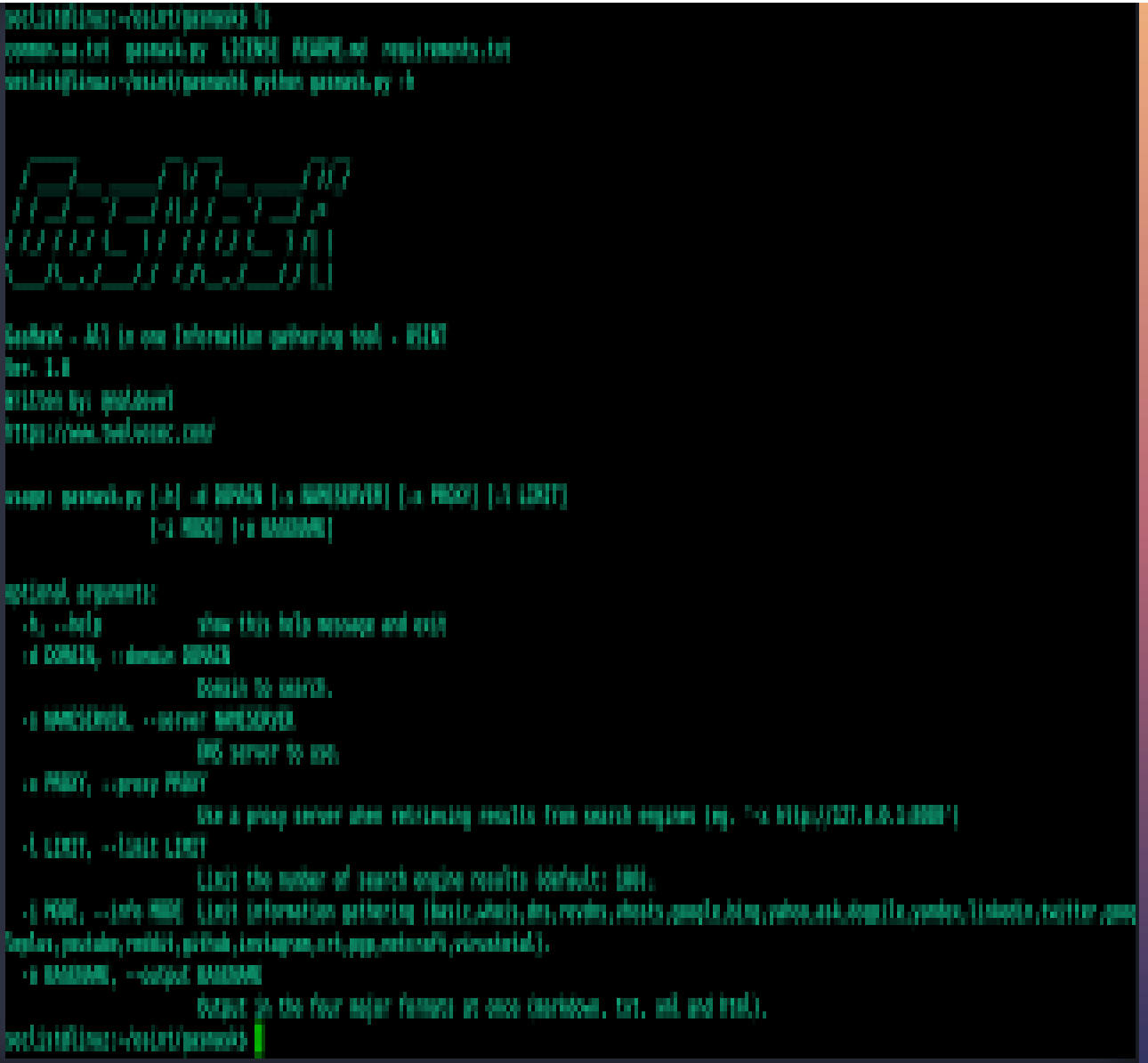
FERRAMENTAS OSINT: BEST TOOLS SEARCH



- https://www.intelligencefusion.co.uk/blog/the-best-open-source-intelligence-osint-tools-and-techniques

GASMAK

FERRAMENTAS OSINT: GASMAK



MATERIAL PARA ESTUDO

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

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=nvdsQlT9_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