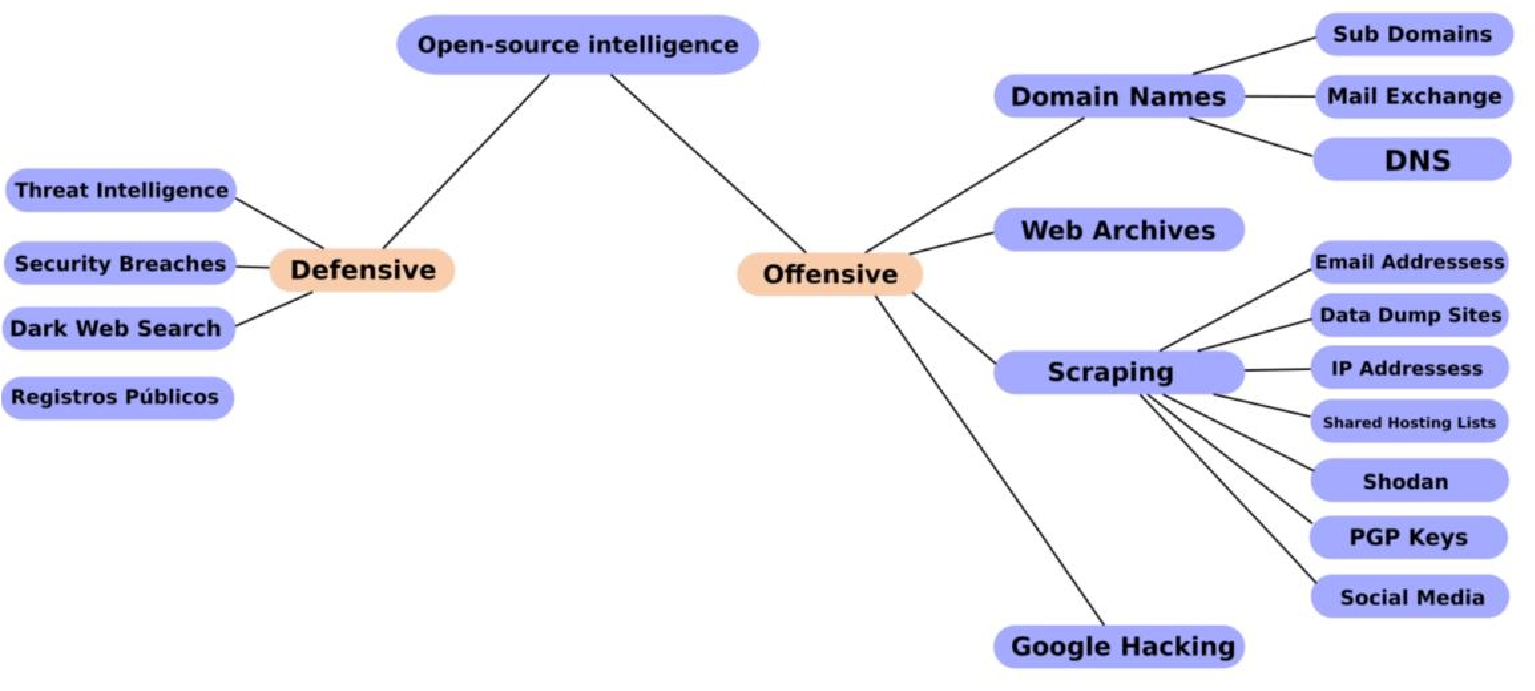
|  |
| --- |
| UC – SISTEMAS COMPUTACIONAIS E SEGURANÇA |
| **Título**: Pratica nº 11 – SCSHACLAB03A – **Estudo Dirigido 1**  **Data: NOV/2023**  **Grupo de no Máximo de 2 até 3 alunos**  ***Tema:*** *Análise e Coleta e Organização de Informações* ***Objetivo:*** *Apresentação dos Softwares e Principais Interfaces*  ***Roteiro:*** *Formar grupos e desenvolver as atividades propostas.* |

# **1. OSINT**

OSINT é um conjunto de atividades para coletar, armazenar e analisar as informações de fontes públicas — basicamente, qualquer dado sobre uma empresa ou pessoa que possa ser encontrado por meio de ferramentas da Internet ou OSINT framework, como os buscadores. Práticas de OSINT são usadas especificamente para a segurança cibernética.



## 1.1. História

O conceito de OSINT tem sua origem na espionagem, precisamente, na década 1930, quando o serviço norte-americano FBIS (*Foreign Broadcast Information Service*) utilizou a estratégia pela primeira vez. A instituição pretendia obter informações de noticiários internacionais na Segunda Guerra Mundial e na Guerra Fria. Ela captava, por rádio, as informações oficiais relacionadas aos inimigos dos Estados Unidos na época, como a União Soviética.

Após o fim da Guerra Fria, o FBIS diminui consideravelmente suas ações, voltando apenas em 2001, nos ataques ao World Trade Center e ao Pentágono. Nessa época, os Estados Unidos voltaram a utilizar fontes abertas para obter informações.

## 1.2. Objetivo

As práticas de OSINT podem ser feitas por profissionais de TI, hackers e até agentes do Estado. Além disso, boa parte das empresas têm alguma estrutura para lidar com esse tipo de informação, não só para a produção e a divulgação, como também para a coleta e o armazenamento.

As práticas de OSINT podem ser divididas em **três principais funções**:

## a) Descobrir canais públicos

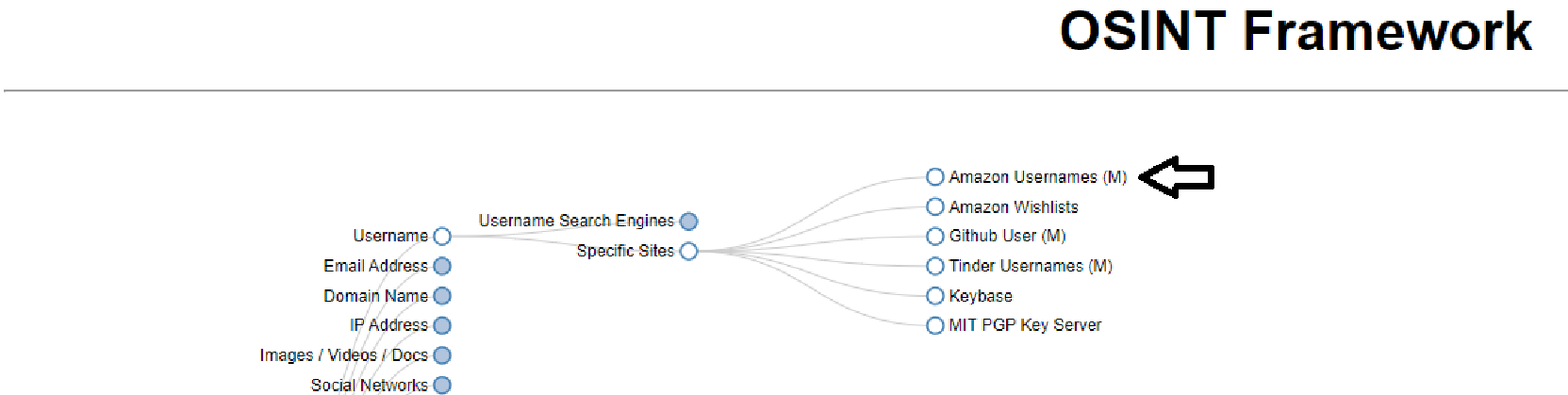
A OSINT ajuda profissionais de TI a encontrar canais de informações voltados ao público que contêm dados sobre a empresa, não apenas os oficiais, mas aqueles que pertencem a outros usuários ou empresas que citam a companhia.

## b) Descobrir dados relevantes fora da organização

Ajuda a encontrar dados relevantes que estão fora do ecossistema *online* da empresa. Dizemos relevantes porque não são informações básicas, como o endereço de uma sede ou o nome da companhia.

## c) Juntar ou agrupar informações e torná-las acessíveis

Com a OSINT, é possível juntar os dados e agrupá-los, para serem facilmente acessados. Algumas ferramentas não só são capazes de realizar a função de captura, elas conseguem fazer a organização desses dados, facilitando o acesso a informações específicas.



d) ( Exercício rápido ) Acessar o OSINT FRAMEWORK e testar o “Amazon Usernames”:

Sintaxe : site:amazon.com <username><https://osintframework.com/>

**1.3. Aplicação das práticas de OSINT**

Práticas de OSINT são usadas especificamente para a segurança cibernética.

## a) Identificação pontos fracos

* vazamento de dados;
* portas ou dispositivos inseguros conectados à Internet; 
* códigos disponíveis das páginas da empresa.

## b) Identificar ameaças externas

É muito comum que o trabalho dos profissionais de segurança fique um pouco sobrecarregado, já que é preciso lidar com todos os aspectos da [**cibersegurança**](https://blogbr.clear.sale/ciberseguranca) da empresa.O grande problema é que há uma extensa quantidade de dados na Internet. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Atividade 1**:

1. (**Pesquisa**) Escolher e testar **2 (duas) fontes** relevantes do OSINT FRAMEWORK destacando o item de pesquisa e as informações que podem ser coletadas. Após selecionar, **comente a aplicação de cada uma das suas escolhas.**

**SHODAN:**

1. **Domínio:** <https://www.shodan.io>
2. **Função principal:** Busca por hosts e exibe as portas abertas com base em uma pesquisa feita pelo usuário.
3. **Informações retornadas:** Nomes de domínio, portas abertas, serviços oferecidos pelas portas abertas, protocolos das portas, nome de ISP’s do host encontrado, equipamentos e suas configurações públicas do host, hostnames.
4. **Aplicação:** Pode ser usado para obter informações de um endereço de host como portas abertas descobertas pela internet, adquirido por meio de ferramentas como o ping, tracert e engenharia social.

**Global Terrorism Database:**

1. **Domínio:** <https://www.start.umd.edu/gtd/>
2. **Função principal:** Busca por incidentes classificados no escopo do terrorismo, ele armazena dados desses incidentes e permite usuários buscar por estes através de um campo de pesquisa.
3. **Informações retornadas:** Informações estatísticas de terrorismos e seus casos isolados, incluindo neste último informações como: organização responsável, tipo de ataque, quem realizou o ataque, número de vítimas, número de condenados pelo ataque, localidade e detalhes do ocorrido.
4. **Aplicação:** Investigações jornalísticas, trabalhos acadêmicos, políticas públicas de segurança, entre outros.
5. (**Pesquisa**) Analisar as caracteristicas da arquitetura do framework [**ThreatX**](https://br.clear.sale/threatx) e destacar **duas** aplicações desta solução para monitoramento em sistemas computacionais, comparando com o **Shodan.**  <https://www.threatx.com/documentation/using-threatx/getting-started/> https://www.shodan.io/

**Características do framework ThreatX:**

O ThreatX é uma ferramenta para análise de endpoints de API e aplicações baseadas em web. Ele tem sensores que coletam dados e exibem esses dados em um dashboard para que equipes de TI possam, posteriormente, analisá-los e definir futuras políticas com bases nessas notificações de cyberthreats (ameaças cibernéticas), tudo isso em tempo real. Ele pode detectar, rastrear e bloquear possíveis requisições consideradas maliciosas.

Ele pode ser usado em aplicativos que façam requisições por meio de uma API à um servidor de alguma organização. Analisando essas requisições e realizando o trabalho de notificar, bloquear ou rastrear essas requisições. Um exemplo seria uma API que realize a solicitação de login.

Outro exemplo interessante, seria a proteção de web sites. Ele pode monitorar o acesso a esses web sites e detectar quais acessos estão se comportando de maneira maliciosa.

**Características de framework Shodan:**

Ele é um serviço de busca pela internet, seu foco é mostrar resultados de portas abertas e seus serviços que estão disponíveis na internet. Ele é capaz de oferecer a uma equipe de Ti, uma noção, de como os seus serviços estão sendo disponibilizados pela internet e quais informações eles estão transmitindo quando solicitados.

**Comparação entre os dois Frameworks:**  
Enquanto o ThreatX é uma ferramenta para monitoramento de uma aplicação web ou API o SHODAN é uma ferramenta para buscar por resultados relacionados aos serviços que estão sendo ofertados pelas portas de um servidor, bem como quais as configurações e algumas informações referentes a localização, ISP, entre outras. De maneira resumida, o Shodan oferece uma forma de buscar por possíveis portas que representem uma ameaça e estão disponíveis pela internet, enquanto o ThreatX analisa diretamente as requisições dessa API. O ThreatX pode ser definido como um IDS (Intrusion Detection System).

1. (**Pesquisa**) Por meio da aplicação do OSINT FRAMEWORK identifique **UMA** ferramenta que pode ser aplicada de modo equivalente ao [**ThreatX**](https://br.clear.sale/threatx) **(Diferente do Shodan). Compare** as duas soluções e realize **uma análise financeira** identificando qual a solução que poderá atender melhor uma empresa no contexto da cibersegurança.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## 1.4. Ética

Com toda essa manutenção de dados que as ferramentas OSINT podem fornecer, pode ser muito fácil entrar em áreas mais complexas do trato de informações, mas boa parte das práticas são legais. Se há alguma ilegalidade, está mais relacionada ao tipo de uso do que exatamente ao que a ferramenta faz.

Estrategicamente, antes de utilizar ou definir uma estratégia voltada para OSINT, é recomendado determinar um código de conduta para orientar os profissionais tanto na captura quanto no manuseio desses dados.

# **2. Enumeração de Serviços**

A Enumeração de Serviços é uma etapa da metodologia *Pentest* que diz respeito a exploração de informações detalhadas sobre o servidor. O objetivo é recolher o máximo de informações de um determinado alvo. As informações esperadas nesta fase incluem, mas não de modo exclusivo, dados sobre: quais serviços estão presentes, quais portas se encontram abertas ou fechadas, se existe um *firewall* sendo executado dentre outros serviços.

## 2.1. Enumeração DNS

Todo site possui um IP válido na rede e existem diversos tipos diferentes de registros DNS disponíveis que são responsáveis por realizar a tradução de nome para IP e vice-versa. Com a ferramenta apropriada poderemos levantar as seguintes informações através de um determinado alvo:

* IP pelo qual o alvo responde.
* Os ns do alvo.
* Os mx do alvo

## 2.2. Tipos de registros DNS

Abaixo será mostrado apenas o que significam os mais comuns de serem encontrados durante o gerenciamento de um domínio:

* **A** – também conhecido por hostname, é o registro central de um DNS, ele vincula um domínio ou subdomínio a um endereço IP direto.
* AAAA – Executa a mesma função de A, porém, para um endereço IPv6.
* **NS** – Name Server (Servidor de Domínio), especifica servidores DNS para o domínio ou subdomínio. Pelo menos, dois registros NS devem ser definidos para cada domínio. Geralmente, um principal e outro secundário.
* CNAME – Significa Canonical NAME. Especifica um apelido (alias) para o hostname (A). É uma forma de redirecionamento.
* **MX** – Sigla para *Mail eXchanger*. Aponta o servidor de e-mails. Pode-se especificar mais de um endereço, formando-se assim uma lista em ordem de prioridade para que haja alternativas no caso de algum e-mail não puder ser entregue.
* PTR – PoinTeR, aponta o domínio reverso a partir de um endereço IP.
* SOA – *Start Of Authority*. Indica o responsável por respostas a um domínio, ou seja, o responsável pelo domínio. Também indica outras informações úteis como número serial da zona, replicação.
* TXT – Refere-se a TeXT, o qual permite incluir um texto curto em um hostname. Técnica usada para implementar o SPF.
* SPF – *Sender Policy Framework*, é uma tentativa de controle de falsos e-mails. Permite ao administrador de um domínio definir os endereços das máquinas autorizadas a enviar mensagens neste domínio.
* SRV – *Abreviação de SeRVice*, permite definir localização de serviços disponíveis em um domínio, inclusive seus protocolos e portas.

## 2.3. Enumeração de serviços no Kali

1. O principal objetivo do Dnsenum é reunir o máximo de informações possível sobre um domínio.

Acesse o **modo root** do kali eexecute o comando aplicando a um site aleatório inexistente. Podemos ainda utilizar a variante do comando **dnsenum** para visualisar outras possibilidades de verificações.

dnsenum --enum teste.com.br **\*** dnsenum –h **(variações)** dnsrecon –d [teste.com.br](http://www.teste.com.br/)**(detalhado)**

1. Outra forma de testar o dns está associado ao comando **Fierce** :

fierce --domain teste.com **\*** fierce -dns teste.com.br -wordlist hosts.txt -file /tmp/output.txt

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Atividade 2:**

1. Enumerar é uma das principais etapas do teste de intrusão, explorando informações mais detalhadas do servidor.No *prompt* root do kali utilize o comando de enumeração (item **2.3**) aplicando a um site real [(google.com.br)](http://www.google.com.br/) e analise os resultados encontrados. **Identifique e explique** o que representa os resultados relacionados aos tipos de registro MX e CNAME contidos nos resultados.

1. Escolher **1** (**UM**) site na internet, aplicar o Dnsenum e identificar quais as informações que podem ser coletadas no que se refere aos **tipos de registros (A) e (AAAA)**. Após aplique o Dnsenum em sintegra.gov.br e compare com os resultados do site escolhido **destacando as diferenças.**

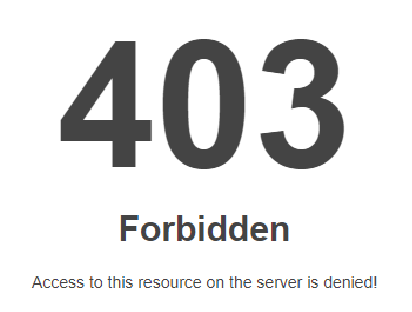
1. ( **Pesquisa** ) Ao executar o Dnsenum em facebook.com podemos encontrar *wilcards* notificando que subdomínios apontarão para o mesmo endereço IP. Executando o mesmo procedimento de enumeração em twi**t**er.com.br, também encontramos *wilcards* desempenhando a mesma função. Após análise dos resultados anteriores, aplique o Dnsenum em twi**tt**er.com e compare com os os resultados encontrados. Interpretando todos os testes conceitue o que são os *wilcards* e **explique se há indícios de vulnerabilidade nos servidores analisados.** *( Atenção: Mantenha seu antivirus atualizado antes da execução.*

*)*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## 2.4. Invervalos de Rede

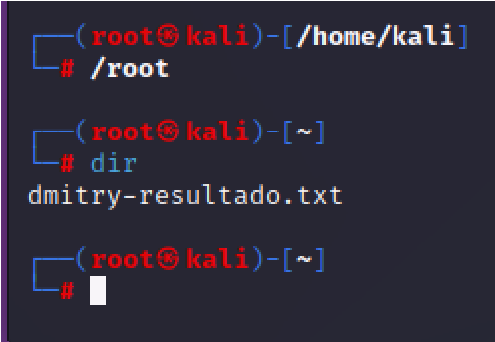
O DMitry (*Deepmagic Information Gathering Tool*) é uma aplicação *Open Source* de linha de comandos que nos permite coletar diversos tipos de informações sobre um host em uma rede. A ferramenta, que é codificada em linguagem C, é capaz de coletar dados sobre subdomínios, endereços de e-mail, efetuar escaneamento de portas TCP (*port scan*), *whois* dentre outras funções.



[http://teste.com.br](http://teste.com.br/)

1. Iniciar o Kali Linux em *prompt* de comando no modo root e informe em linha de comando cada código abaixo:

dmitry –wnspb teste.com.br -o /root/dmitry-resultado **\*** cat /root/dmitry-resultado.txt **(relatório)**



**Local do arquivo**

1. (Exercício rápido) Identifique um OUTRO domínio ou site na internet, aplique o comando ***dmitry*** e analise os resultados encontrados. Compare os resultados com o servidor [www.teste.com.br,](http://www.teste.com.br/) gere o relatório e arquive em seus documentos.

**Scapy** é um programa interativo de manipulação de pacotes com a capacidade de criar pacotes customizáveis, especificando as diferentes camadas e protocolos de rede, bem como alterar cada um dos campo dos cabeçalhos destes pacotes. Com a função *rdpcap* em que é possível ler arquivos de gravação de tráfego (.pcap), arquivos estes que podem ser gerados em capturas de ferramentas como Tcpdump e **Wireshark**.

>>>ls() (protocolos suportados)

>>>lsc()(comandos básicos)

a) Eventualmente torna-se necessário avaliar a **enumeração por rota dos pacotes** desde a origem

até o destino e desta forma utilizaremos, via *prompt* do terminal, o ***scapy****.* Dentro da aplicação, para retornar ao *prompt* utilize “**exit**”.

# ans,unans=sr(IP(dst="www.targethost.com/30",ttl=(1,6))/TCP()) ans,unans=sr(IP(dst="www.google.com.br/30",ttl=(1,6))/TCP())

1. Após, para identificar os roteadores que pertencem a conexão entre o analista e o alvo, pode ser verificado e acordo com a seguinte linha de comando:

ans.make\_table( lambda s,r:(s.dst,s.ttl,r.src))

1. Podemos ainda testar outros domínios ou sites aplicando um ***traceroute*.**

res,unas=traceroute(["www.google.com"],dport=[80,443],maxttl=20,retry=-2)

|  |  |
| --- | --- |
| res,unans=traceroute(["www.google.com","www.kali.org","www.targethost.com" | |
| ],dport=[80,443],maxttl=20,retry=-2) |  |

## *Atenção: exemplo avaliando um site nas portas 80 e 443*

d) Para se realizar uma análise mais técnica, podemos utilizar o *traceroute* a ferramentas gráficas para visualizar o teste realizado no **item C**. Desta forma, podemos gerar um gráfico da pesquisa e salvar em um arquivo **.svg.** Para visualizar os resultados, procurar pela pasta **/tmp** e o arquivo salvo**.**

res.graph(target="> /tmp/graph.svg")

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Atividade 3:**

1. (**Pesquisa**) Dmitry significa *DeepMagic Information Gathering Tool* e é uma ferramenta de linha de comando usada para coletar informações sobre o alvo podendo ser usadas para ataques de engenharia social. A ferramenta Dmitry pode ser usada com o serviço *whois* para obter as informações de destino, como **domínio registrado**, **nome**, **endereço** e as **informações** de **contato** da pessoa que o registrou. Realize testes de enumeração no domínio facebook.com por meio do comando **fierce** e após, compare com o ***dmitry*.**

fierce --domain teste.com

dmitry –wnspb teste.com.br

O que representa o *wilcard* identificado no relatório de análise? Identifique quais as principais diferenças entre a enumeração realizada pelo comando **fierce** e o comando **dmitry**. Realize testes em um navegador de sua preferência com os IP’s rastreados e **explique** o que representam os subdomínios encontrados na pesquisa. Utilize também como referência o site: [https://ipinfo.io.](https://ipinfo.io/)

(Exemplo : <https://ipinfo.io/173.252.95.252>)



1. (**Pesquisa**) O Scapy fornece uma interface Python para a libpcap , (WinPCap / Npcap no Windows), de maneira similar àquela em que o **Wireshark** fornece uma visão e captura da GUI . Ele pode interagir com uma série de outros programas para fornecer visualização incluindo Wireshark para pacotes de decodificação, gnuplot para fornecer gráficos, graphviz ou VPython para visualização. Realize testes por meio do scapy, gere o gráfico e analise as interações servidor. Explique e comente os resultados encontrados.

|  |  |
| --- | --- |
| res,unans=traceroute(["www.facebook.com","www.instagram.com"],dport=[80,443], | |
| maxttl=20,retry=-2) |  |

res.graph(target="> /tmp/graph2.svg")

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## 3. ORIENTAÇÕES GERAIS

* O trabalho deverá ser feito em grupos de 5 a 10 alunos;
* Será avaliada a análise dos resultados e o trabalho final em equipe.

###  A processo de avaliação será feita da seguinte forma: o Entregáveis : Atividades 1,2 e 3 *(conforme template)* o Submissão Online da ACCLAB-10 (formato .pdf) (no Drive/U-Life). o Data da entrega : 04/12/2023