INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 03: Levantamento de Informações com Maltego

Olá turma, hoje iremos conhecer uma ferramenta que podem nos auxiliar a obtermos informações no levantamento de informações. Essa ferramenta é o Maltego. Vamos lá preparados??

Maltego

O Maltego é uma ferramenta para *data mining* (mineração de dados), projetada para visualizar o resultado da coleta de dados de inteligência de fontes abertas. Entretanto, ele também é utilizado para coleta de informações no teste de penetração. O Maltego tem uma versão comercial quanto uma versão gratuita. A versão gratuita, que usaremos nesta disciplina, possui alguns limites porém ela pode ser usada para coletar uma boa quantidade de informações interessantes na rede.

O Maltego utiliza informações que estão publicamente disponíveis na Internet, portanto efetuar o reconhecimento em qualquer entidade é perfeitamente legal.

Entre as informações, temos: usuários do domínio, pessoas relacionadas a empresa, sobre a empresas, sites, domínios e subdomínios, endereços IP, documentos e arquivos.

Informações e tutoriais sobre o Maltego podem ser encontrados em http://www.paterva.com/. Invista um tempo utilizando as transformações do Maltego para descobrir informações interessantes sobre a empresa.

Para a instalação digite num terminal:

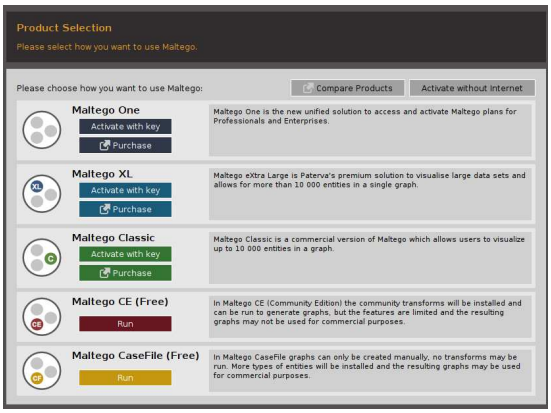
```
sudo apt update

sudo apt install maltego
```

Para utilizarmos precisamos realizar um cadastro no site: `https://www.maltego.com/ce-registration`. Nele será solicitado sobre o nome, e-mail e instituição de ensino. Você receberá um e-mail para validação. Cuidado pois o e-mail poderá estar na pasta de spam. Após o cadastro, abra a ferramenta. Para isso digite no terminal:

```
sudo maltego
```

A primeira tela mostrará a página de seleção de produtos, onde podemos visualizar as várias versões do Maltego. Iremos utilizar a edição comunitária do Maltego que é gratuita para todos, então selecione "Maltego CE (Free)" e clique em "Run".



Na sequência iniciar as configuração do Maltego. Primeiro, precisamos aceitar os termos e condições da Maltego. Para isso, clique em "Aceept" e clique em "Next".

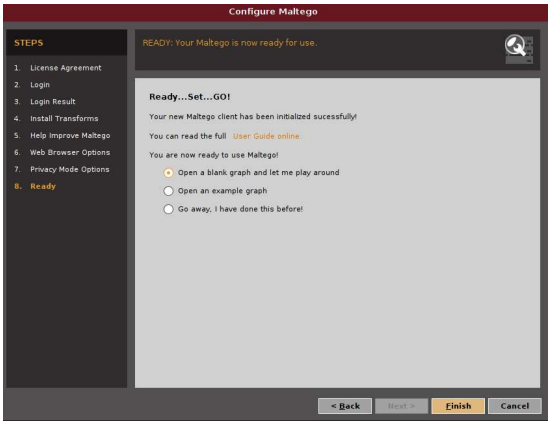
Posteriormente, aparecerá a tela de login. Insira as informações que você colocou no cadastro de registro.

Após o login, os usuários serão solicitados a escolher seu modo de privacidade preferido, são eles:

- Modo Normal: projetado para fornecer aos usuários a experiência mais rica. Durante uma investigação, este modo permite que o Maltego busque certos tipos de dados diretamente da Internet.

- Modo Stealth: restringe completamente o software de baixar quaisquer dados ou informações diretamente da Internet. Isso significa que a busca de uma imagem de Entidade ou sobreposição de site será bloqueada. Ele será usado sob rígidas práticas de confidencialidade, ou os usuários estiverem simplesmente preocupados em expor seu IP.

Iremos utilizar o modo Normal. Por último, selecione “Open a blank graph and let me play around” (Abra um grafo em branco e deixe-me brincar) e, em seguida, clique em “Finish” (Finalizar).

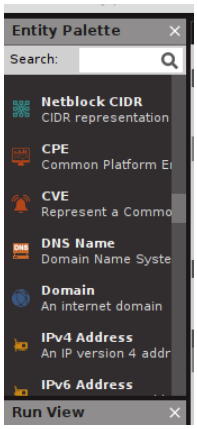


A Maltego fornece uma interface gráfica que torna a visualização das informações facilitadas. O Maltego define três estruturas, são eles:

- *Entities*: são objetos com os quais é possível interação, por exemplo, domínio, endereço de e-mail, registro MX, etc.
- *Transforms*: são operações que pode ocorrer com os objetos. Ele executam tarefas e constroem gráficos, por exemplo, resolver endereço IP de host, encontrar responsável por um endereço IP ou obter informações sobre um servidor de e-mail.
- *Machines*: são conjuntos de transforms que automatizam algumas tarefas repetitivas, por exemplo, consultas de informações em diferentes níveis.

Iremos acrescenter uma entidade do tipo domínio. Para isso, selecione a opção Palette (Paleta) na borda esquerda. Como você pode ver, podemos coletar informações sobre todo tipo de entidades. Vamos começar com o domínio ifrn.edu.br.

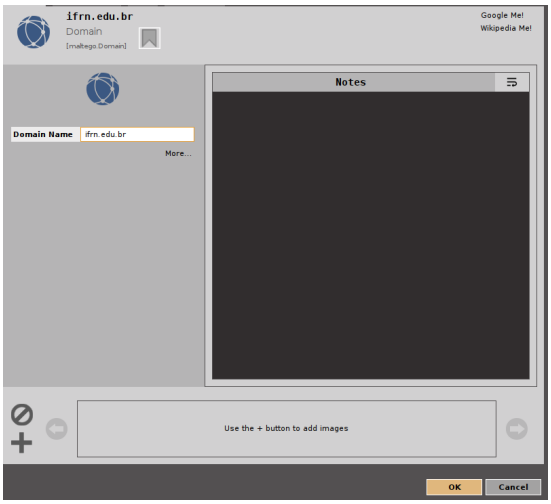
Expanda a opção Infrastructure (Infraestrutura) em Palette (à esquerda da janela do Maltego) e arraste uma entidade Domain (Domínio) de Palette para o novo grafo. Por padrão, o domínio é paterva.com.



Coletando Informações do IFRN

Agora iremos coletar informações sobre a rede ifrn.edu.br. Para isso, no Maltego insira um domínio de internet.

Para alterá-lo dê um clique duplo no texto ou altere o campo de texto do lado direito da tela.



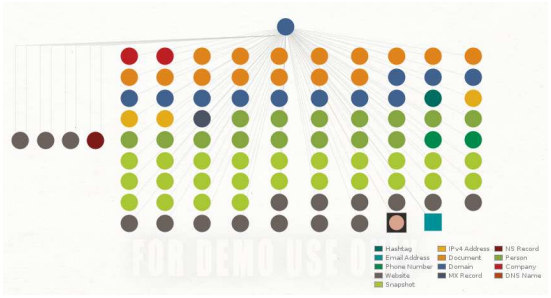
As tarefas no Maltego são nomeadas como transformações. As transformações vêm embutidas na ferramenta e são definidas como scripts de código que executam tarefas específicas. Existem também vários plugins disponíveis no Maltego, como o conjunto de ferramentas SensePost, Shodan, VirusTotal, ThreatMiner e assim por diante.

Depois que o domínio estiver definido, iremos executar uma transformação (consultas). As transformações poderão ser do tipo: DNS do domínio, Dados do proprietário do domínio, Endereços de e-mail do domínio, Arquivos e documentos do domínio, Pessoa, Números de Telefone e Site.

Para definir as transformações clique com o botão direito do mouse no ícone de domínio. Iremos utilizar o “All Transform”.

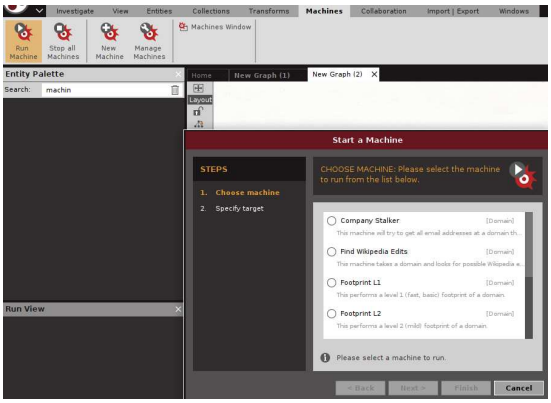
Será questionado o período que deseja realizar a busca. Por exemplo, iremos especificar os últimos dois anos.

A consulta retornará um grafo com os servidores web, de e-mail endereços IPs, arquivos, backups existentes dos sites, usuários, telefones de contato, subdomínios DNS, entre outras informações.



Coletando Informações do Google

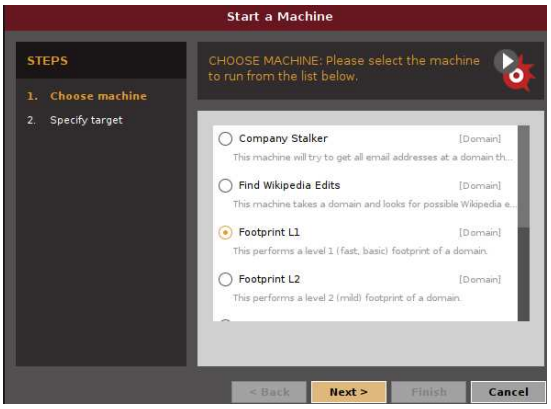
Crie um novo gráfo. Na sequência em menu procure "Machines" e clique em "Run Machine".



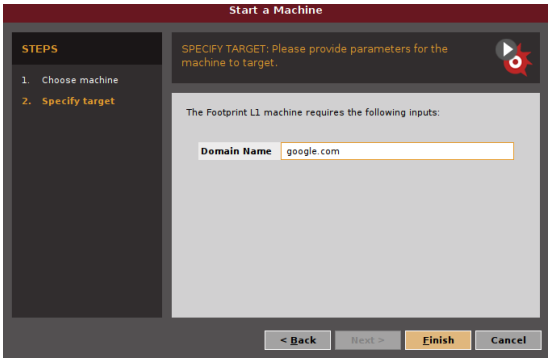
Depois disso, obtivemos uma lista de opções disponíveis nas máquinas públicas Maltego, são elas:

- Company Stalker: obter todos os endereços de e-mail de um domínio e descobrir quais deles são utilizados nas redes sociais. Também baixa e extrai metadados dos documentos publicados na internet.
- Find Wikipedia Edits: procura o domínio na Wikipedia e pesquisa o mesmo em todas as plataformas de mídia social.
- Footprint L1: executa os footprints básicos de um domínio.
- Footprint L2: executa footprints de nível médio de um domínio.
- footprint L3: realiza um busca mais minuciosa de um domínio, normalmente leva tempo e consome muitos recursos da máquina.
- Footprint XXL: Isso funciona em grandes alvos, como uma empresa que hospeda seus próprios data centers, e tenta obter a pegada examinando os registros da estrutura de política do remetente (SPF) esperando por netblocks, bem como DNS delegado reverso para seus servidores de nomes.
- Person - Email Address: obtem o endereço de e-mail de pessoas em um domínio.
- URL to Network and Domain Information: identificará se o domínio é utilizado em outros TLDs. Por exemplo, se fornecermos www.google.com, ele identificará se o mesmo é utilziado nos domínios www.google.us, google.co.in e assim por diante.

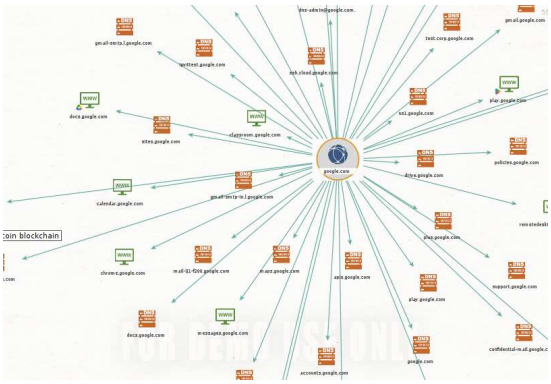
Iremos utilizar o "Footprint L1" para obter uma compreensão básica do domínio, subdomínios e endereços IPs.



Uma vez que a máquina é selecionada, precisamos clicar em "Next" e especificar um domínio. Digite: google.com.



Como resultado, o Maltego apresentará as informações que ele conseguiu obter do domínio google.com.



Atividade

1. Instale e execute o Maltego e obtenha o máximo de informações sobre o domínio ifrn.edu.br.