# Avaliação de Ferramentas OSINT para Integração

Este documento resume a avaliação de ferramentas OSINT gratuitas com foco em integração programática (CLI/API) para o projeto de pentest automatizado.

## Critérios de Avaliação:

* **Gratuidade:** Preferência por ferramentas gratuitas ou com um nível gratuito robusto.
* **Integração Programática:** Suporte a CLI ou API para automação.
* **Abrangência de Fontes:** Quantidade e variedade de fontes de dados que a ferramenta consulta.
* **Tipos de Informação Coletada:** E-mails, subdomínios, IPs, nomes de usuário, tecnologias, vazamentos, etc.
* **Facilidade de Instalação e Uso:** Simplicidade para configurar e executar.
* **Comunidade e Documentação:** Disponibilidade de suporte e documentação clara.
* **Manutenção:** Frequência de atualizações e atividade do projeto.

## Ferramentas OSINT Selecionadas (Principais Candidatas):

Com base na avaliação, as seguintes ferramentas são as principais candidatas para integração inicial, devido à sua gratuidade (ou robusto nível gratuito), capacidade de integração programática e abrangência:

1. **theHarvester:**
   * **Justificativa:** Excelente para enumeração inicial de e-mails, subdomínios, hosts. CLI bem estabelecida, saída parseável. Ampla gama de fontes, embora algumas exijam chaves de API com limites gratuitos.
   * **Foco de Integração:** Coleta de e-mails, subdomínios, IPs associados a um domínio.
2. **SpiderFoot (Versão Open Source):**
   * **Justificativa:** Extremamente abrangente com mais de 200 módulos. Permite uma coleta de dados muito rica e correlação. A integração programática pode ser feita via CLI ou scripts que interajam com seus módulos Python.
   * **Foco de Integração:** Coleta diversificada de informações (DNS, WHOIS, e-mails, redes sociais, vazamentos de dados, etc.), correlação de dados.
3. **Photon:**
   * **Justificativa:** Rastreador web rápido e eficiente para extrair informações de um site específico (URLs, e-mails, arquivos, contas de mídia social). Saída em JSON facilita a integração.
   * **Foco de Integração:** Extração detalhada de informações de websites alvo.
4. **Shodan (API com Chave Gratuita):**
   * **Justificativa:** Essencial para identificar dispositivos conectados à internet, portas abertas, banners de serviços e tecnologias. A API, mesmo com limites no plano gratuito, oferece informações valiosas.
   * **Foco de Integração:** Identificação de serviços expostos, tecnologias e potenciais vulnerabilidades baseadas em banners.

**Outras Ferramentas Consideradas (Para Expansão Futura ou Módulos Específicos):**

* **Recon-ng:** Framework modular poderoso, pode ser considerado para funcionalidades de reconhecimento mais avançadas ou específicas. A complexidade de scriptar todos os módulos pode ser um desafio inicial.
* **Maltego (Versão Comunitária):** Embora a integração programática direta possa ser limitada na versão gratuita, pode inspirar a lógica de correlação e visualização.

## Bibliotecas para Visualização em Grafo Selecionadas:

1. **NetworkX (com Matplotlib ou Graphviz para Renderização):**
   * **Justificativa:** NetworkX é o padrão de fato em Python para manipulação de grafos. É flexível e poderoso. Para a renderização:
     + **Matplotlib:** Boa para visualizações estáticas simples e integração direta com PyQt.
     + **Graphviz:** Excelente para layouts de grafos mais complexos e esteticamente agradáveis. A integração com Python é direta, e as imagens geradas podem ser facilmente exibidas na GUI PyQt.
   * **Foco de Integração:** Criar a estrutura de dados do grafo com NetworkX. Usar Graphviz para gerar as imagens do grafo da "teia de aranha" e exibi-las na interface PyQt. Matplotlib pode ser uma alternativa para grafos mais simples ou interatividade básica se Graphviz apresentar desafios de dependência no ambiente final.
2. **PyQtGraph (Consideração Secundária para Grafos):**
   * **Justificativa:** Se a interatividade direta com o grafo dentro da janela PyQt (zoom, pan, seleção de nós) for um requisito forte e as opções acima se mostrarem limitadas, PyQtGraph pode ser explorado, embora sua especialidade não seja grafos de rede complexos.

## Próximos Passos:

Com estas seleções preliminares, o próximo passo é detalhar a arquitetura de como estas ferramentas e bibliotecas serão integradas no sistema existente. Isso incluirá:

* Como os dados de cada ferramenta OSINT serão chamados, processados e armazenados.
* Como os dados coletados formarão o grafo de investigação.
* Como o grafo será visualizado na interface gráfica.
* Como a lógica de decisão será expandida para usar os dados OSINT e sugerir novas ações.