Hackers do Bem – Fundamental
Prof. Fábio Carneiro de Castro
10/02/2026

Atividade Prática – Módulo 1

Aulas 3 e 4

Gabriel dos Santos Schmitz

Este documento foi criado usando LaTeX
https://github.com/gabrielzschmitz/uni/tree/main/hackers-do-bem/fundamental/aulas3-4.

1 Introdução

Este documento apresenta as evidências práticas das atividades do Módulo 1 (Aulas 3 e 4) do Programa Hackers do Bem – Nível Fundamental, por meio dos prints solicitados, demonstrando a correta execução das tarefas propostas.

Conforme orientações do curso, este documento reúne, em um único arquivo PDF, os seguintes prints obrigatórios: Atividade 1.6 (passo 11), Atividade 1.7 (passo 4), Atividade 1.8 (passo 10), Atividade 1.9 (passo 9) e Atividade 1.10 (passo 8), todos acompanhados de breve descrição explicativa para facilitar a avaliação pelo instrutor.

2 Atividades

Atividade 1.6. Conhecendo a ferramenta de Phishing ShellPhish no Kali Linux

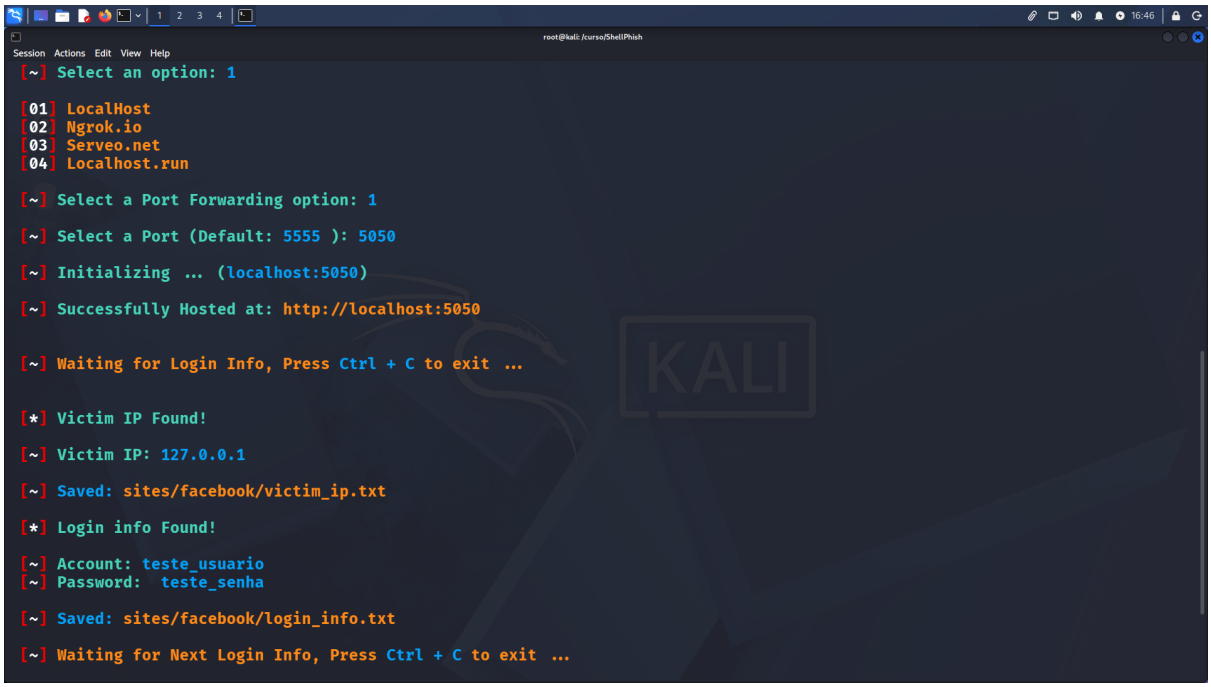

Fig. 1: Simulação de ataque de phishing utilizando a ferramenta ShellPhish no Kali Linux

Sobre:

Nesta atividade, foi utilizada a ferramenta ShellPhish para simular um ataque de phishing em ambiente controlado no Kali Linux. A aplicação foi configurada para hospedar localmente uma página falsa de login do Facebook, permitindo a captura de credenciais inseridas para fins de demonstração.

Após o acesso à página hospedada em `localhost`, as credenciais digitadas foram registradas no terminal, evidenciando o funcionamento da ferramenta e demonstrando, de forma prática, o princípio básico de ataques de phishing voltados à captura de informações sensíveis.

Atividade 1.7. Explorando a Ferramenta WHOIS no Kali Linux

Fig. 2: Consulta de informações públicas de domínios utilizando a ferramenta WHOIS no Kali Linux

Sobre:

Nesta atividade, foi explorada a ferramenta `whois`, nativa do Kali Linux, com o objetivo de coletar informações públicas associadas a registros de domínios na Internet. Após a elevação de privilégios para superusuário (`sudo -i`), foram realizadas consultas aos domínios `rnp.br`, `guanambi.ba.gov.br` e `itapaje.ce.gov.br`.

A análise das respostas permitiu identificar informações relevantes como:

- Nome do domínio registrado (`domain`);
- Entidade proprietária (`owner`);
- Identificador do proprietário no Registro.br (`owner-c`);
- Responsável técnico pelo domínio (`tech-c`);
- Servidores de nomes (DNS) associados (`nserver`);
- Datas de criação, alteração e status do domínio;
- Registros de segurança DNSSEC (`dsrecord` e `dsstatus`).

Observou-se que domínios governamentais estaduais e municipais utilizam infraestruturas centralizadas de TI (como PRODEB e ETICE), evidenciando modelos de gestão tecnológica compartilhada.

Atividade 1.8. Explorando a Ferramenta de Engenharia Social Maltego no Kali Linux

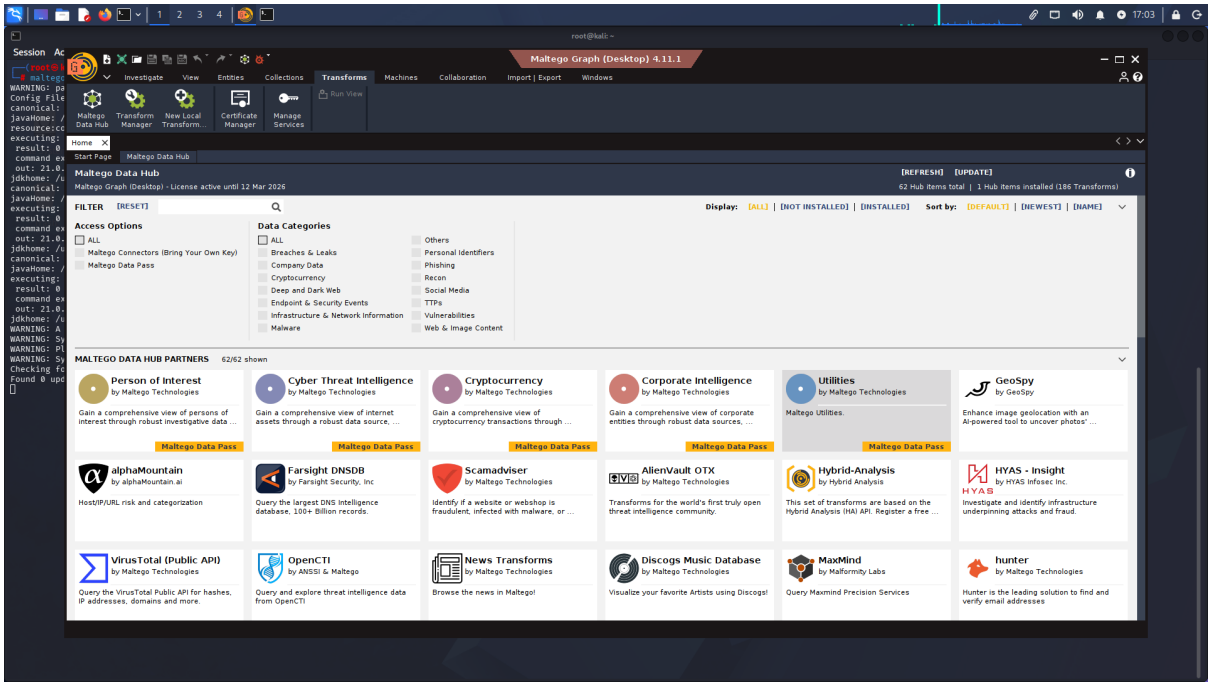

Fig. 3: Configuração inicial e exploração da aba Transforms no Maltego Data Hub

Sobre:

Nesta atividade, foi realizada a configuração inicial e exploração da ferramenta *Maltego*, disponível nativamente no Kali Linux, com foco na utilização de recursos de *OSINT* (Open Source Intelligence).

Inicialmente, foi criada uma conta gratuita no site oficial do Maltego. Em seguida, na máquina virtual Kali Linux, o software foi iniciado pelo terminal com o comando `maltego`. Durante o processo de ativação, foram selecionadas as opções *Maltego ID* e *Online Activation*, realizado o login via navegador (Browser Login) e aceitos os termos de uso (*Data Sources T&Cs*).

Após a conclusão da configuração, o ambiente principal do Maltego foi acessado. Foi então explorada a aba **Transforms** e o **Maltego Data Hub**, onde estão disponíveis diversas integrações e fontes de dados OSINT, utilizadas para coleta e correlação de informações públicas, como domínios, endereços IP, e-mails, organizações e perfis digitais.

Atividade 1.9. Reconhecimento Passivo OSINT com Maltego no Kali Linux

Fig. 4: Execução de Transforms no domínio ufc.br e identificação de servidores MX

Sobre:

Nesta atividade, foi realizado reconhecimento passivo utilizando a ferramenta *Maltego*, com foco em técnicas de *OSINT* (Open Source Intelligence) aplicadas a um domínio institucional.

Após iniciar o Maltego no Kali Linux, foi criada uma nova análise (*New*) e adicionada a entidade **Website**, disponível no grupo *Infrastructure*. O domínio configurado foi `ufc.br`, pertencente à Universidade Federal do Ceará.

Foram executadas diversas *Transforms* para extração de informações públicas associadas ao domínio:

- **To Domains [within Properties]**: identificação do domínio relacionado;
- **To DNSNames [within Properties]**: levantamento de registros DNS associados;
- **To Person [PGP]**: identificação de possíveis pessoas vinculadas ao domínio;
- **To Email Addresses [PGP]**: coleta de endereços de e-mail institucionais expostos;
- **To DNS Name – MX (mail server)**: identificação dos servidores de e-mail utilizados pela instituição.

Como resultado, foi possível observar a associação do domínio `ufc.br` a diversos registros DNS, endereços de e-mail institucionais e servidores de e-mail (MX), identificando a utilização de infraestrutura de serviços do Google para correio eletrônico.

Atividade 1.10. Conhecendo Ataques Contra Aprendizagem de Máquinas (Adversarial Machine Learning)

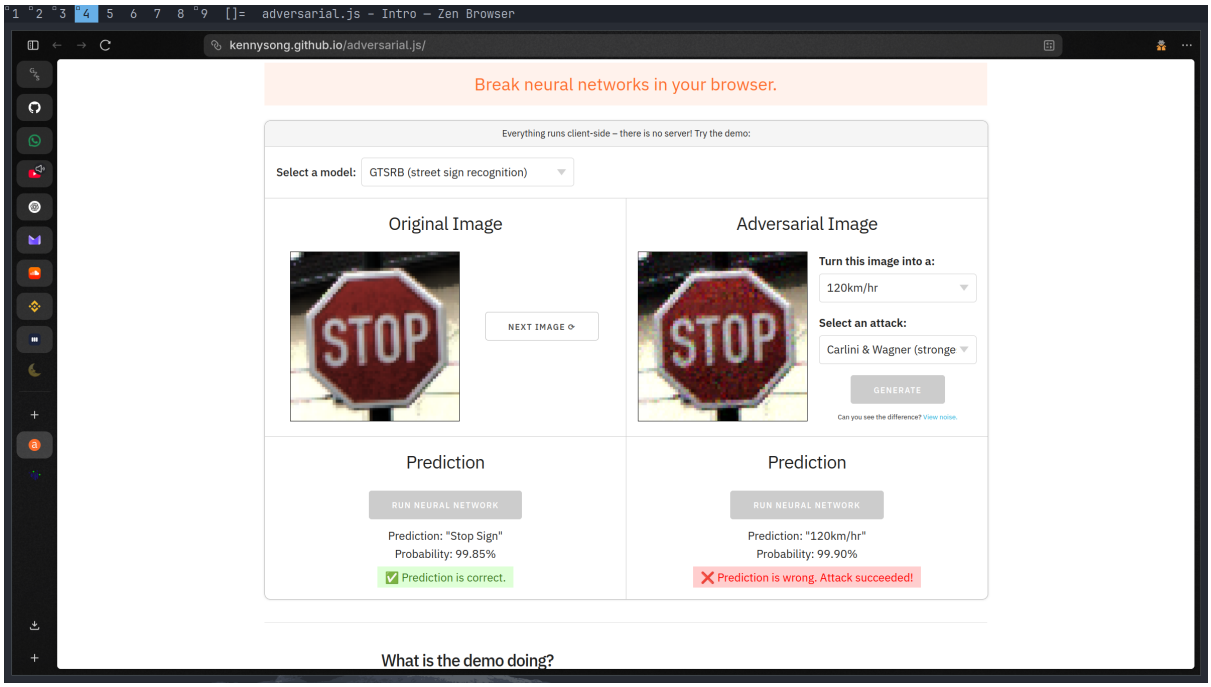

Fig. 5: Execução de ataque adversarial no modelo GTSRB e erro de classificação após perturbação

Sobre:

Nesta atividade, foi explorado o conceito de *Adversarial Machine Learning*, que estuda vulnerabilidades em modelos de aprendizado de máquina quando submetidos a entradas maliciosamente manipuladas.

Foi utilizada a plataforma interativa `adversarial.js`, acessada via navegador, permitindo visualizar o comportamento de uma rede neural treinada para reconhecimento de placas de trânsito (**GTSRB – German Traffic Sign Recognition Benchmark**).

Inicialmente, foi selecionado o modelo **GTSRB (street sign recognition)**. Na seção *Original Image*, ao executar a opção **RUN NEURAL NETWORK**, observou-se que a imagem da placa de trânsito "STOP" foi corretamente classificada pelo modelo, com alta confiança na predição.

Em seguida, na seção *Adversarial Image*, foi acionada a opção **GENERATE**, que aplicou pequenas perturbações matematicamente calculadas à imagem original. Essas alterações são praticamente imperceptíveis ao olho humano, porém são suficientes para modificar os padrões de ativação interna da rede neural.

Após executar novamente a opção **RUN NEURAL NETWORK** na imagem adversarial, verificou-se que o modelo passou a classificar a imagem incorretamente, demonstrando que o sistema foi enganado com sucesso.

Esse experimento evidencia que modelos de aprendizado de máquina, especialmente redes neurais profundas, podem ser altamente sensíveis a pequenas perturbações nos dados de entrada. Em contextos críticos, como veículos autônomos, sistemas biométricos ou diagnósticos médicos, essas vulnerabilidades podem representar riscos significativos.