Manual do Usuário do Phishing Manager

Bem-vindo ao Manual do Usuário do Phishing Manager! Este guia abrangente foi criado para ajudá-lo a instalar, configurar e utilizar todas as funcionalidades desta poderosa ferramenta de gerenciamento de campanhas de phishing. Seja você um profissional de segurança, um testador de penetração ou um entusiasta, este manual fornecerá as informações necessárias para maximizar o potencial do Phishing Manager.

1. Introdução ao Phishing Manager

O Phishing Manager é uma plataforma robusta e intuitiva projetada para simular e gerenciar campanhas de phishing de forma controlada e ética. Ele permite que você crie e personalize e-mails de phishing, páginas de destino falsas, rastreie interações de vítimas e analise resultados, tudo em um ambiente seguro e controlado. O objetivo principal é ajudar organizações a testar a resiliência de seus funcionários contra ataques de engenharia social e aprimorar suas defesas.

1.1. Recursos Principais

- **Gerenciamento de Usuários e Permissões**: Controle de acesso baseado em papéis (administrador e usuário comum) com autenticação segura, incluindo 2FA.
- **Campanhas de Phishing Personalizáveis**: Crie e gerencie campanhas com e-mails e páginas de destino customizáveis.
- **Rastreamento Detalhado**: Monitore aberturas de e-mail, cliques em links, submissões de credenciais e outras interações de vítimas.
- **Análise de Resultados**: Obtenha insights sobre o comportamento dos usuários e a eficácia das campanhas através de relatórios e estatísticas.
- **Gerenciamento de Domínios e Scripts**: Organize e reutilize domínios e scripts de phishing para diferentes campanhas.

- **Segurança Integrada**: Proteções contra ataques comuns como XSS, SQL Injection, CSRF e força bruta.
- **Instalador Simplificado**: Instalação fácil em diversos ambientes (manual, Docker, SystemD).
- **Notificações**: Receba alertas em tempo real sobre eventos importantes via Telegram.

1.2. Casos de Uso

- **Treinamento de Conscientização em Segurança**: Simule ataques de phishing para educar funcionários sobre os perigos da engenharia social.
- **Testes de Penetração**: Avalie a vulnerabilidade de uma organização a ataques de phishing.
- **Pesquisa de Segurança**: Estude o comportamento de usuários e a eficácia de diferentes táticas de phishing.
- **Auditorias de Segurança**: Verifique a conformidade com políticas de segurança e identifique pontos fracos.

2. Instalação

O Phishing Manager oferece um instalador aprimorado que simplifica o processo de configuração em diferentes sistemas operacionais Linux. Recomenda-se utilizar o instalador para garantir que todas as dependências sejam configuradas corretamente.

2.1. Pré-requisitos

Antes de iniciar a instalação, certifique-se de que seu sistema atende aos seguintes requisitos:

- **Sistema Operacional**: Distribuição Linux (Ubuntu, Debian, CentOS, Fedora, Arch Linux, etc.).
- **Python 3.8+**: Necessário para o backend Flask.
- **Node.js 14+ e npm/yarn**: Necessário para o frontend React.
- **Git**: Para clonar o repositório.

- **Docker e Docker Compose** (Opcional, mas recomendado para o modo Docker).
- **Acesso à Internet**: Para baixar dependências e pacotes.
- **Privilégios de Administrador (sudo)**: Necessário para instalar pacotes do sistema.

2.2. Utilizando o Instalador Aprimorado

O instalador aprimorado (`install_phishing_manager_v2.py`) oferece uma interface interativa e várias opções de instalação. Siga os passos abaixo:

1. **Clone o Repositório (se ainda não o fez)**: `bash git clone https://github.com/Dedeg0/phishing-manager.git cd phishing-manager`
2. **Execute o Instalador**: `bash sudo python3 install_phishing_manager_v2.py` O instalador irá guiá-lo através do processo, detectando automaticamente as dependências e oferecendo opções de instalação.

2.3. Modos de Instalação

O instalador oferece três modos principais de instalação:

2.3.1. Instalação Manual (Recomendado para Desenvolvimento)

Este modo instala o Phishing Manager diretamente no seu sistema, utilizando um ambiente virtual Python. É ideal para desenvolvedores que desejam modificar o código-fonte.

- **Passos**: O instalador irá:
- Verificar e instalar dependências do sistema (Python, pip, Node.js, npm/yarn).
- Criar um ambiente virtual Python.
- Instalar as dependências Python do backend.
- Instalar as dependências Node.js do frontend.
- Configurar o banco de dados (SQLite por padrão).
- Criar um usuário administrador inicial.
- **Execução**: Após a instalação, você poderá iniciar o backend e o frontend separadamente.

- Backend: `cd phishing-manager/phishing-manager && source venv/bin/activate && flask run`
- Frontend: `cd phishing-manager/phishing-manager-frontend && npm start`

2.3.2. Instalação com Docker (Recomendado para Produção e Facilidade)

Este modo utiliza Docker e Docker Compose para containerizar o Phishing Manager, proporcionando um ambiente isolado e portátil. É ideal para produção devido à sua facilidade de implantação e gerenciamento.

- **Passos**: O instalador irá:
- Verificar e instalar Docker e Docker Compose.
- Construir as imagens Docker do backend e frontend.
- Configurar o Docker Compose para iniciar os serviços.
- **Execução**: Após a instalação, você pode iniciar/parar a aplicação com: `bash cd phishing-manager docker-compose up -d # Inicia em segundo plano docker-compose down # Para a aplicação`

2.3.3. Instalação como Serviço SystemD (Recomendado para Produção em Servidores)

Este modo configura o Phishing Manager como um serviço SystemD, garantindo que a aplicação inicie automaticamente com o sistema e seja gerenciada como um serviço padrão do Linux. Requer Docker.

- **Passos**: O instalador irá:
- Realizar a instalação Docker (se ainda não o fez).
- Criar um usuário de sistema dedicado para o serviço.
- Gerar e configurar os arquivos de serviço SystemD.
- Habilitar e iniciar o serviço.
- **Execução**: Após a instalação, você pode gerenciar o serviço com: `bash sudo systemctl start phishing-manager sudo systemctl stop phishing-manager sudo systemctl status phishing-manager`

2.4. Opções de Linha de Comando do Instalador

O instalador pode ser executado com diversas opções para automação ou depuração:

- `--mode <manual|docker|systemd>`: Define o modo de instalação (padrão: interativo).
- `--username <nome>`: Define o nome de usuário do administrador inicial.
- `--email <email>`: Define o e-mail do administrador inicial.
- `--password <senha>`: Define a senha do administrador inicial.
- `--no-interaction`: Executa o instalador sem prompts interativos (requer `--mode` e credenciais).
- `--check-deps`: Apenas verifica as dependências do sistema.
- `--uninstall`: Desinstala o Phishing Manager.
- `--help`: Exibe a ajuda do instalador.

Exemplo de instalação não interativa:

```
sudo python3 install_phishing_manager_v2.py --mode docker --username admin --email admin@example.com --password MinhaSenhaSegura123! --no-interaction
```

3. Configuração Pós-Instalação

Após a instalação, algumas configurações podem ser ajustadas para otimizar o Phishing Manager para suas necessidades.

3.1. Variáveis de Ambiente

O Phishing Manager utiliza variáveis de ambiente para configurações sensíveis e específicas do ambiente. Um arquivo `.env.example` é fornecido na raiz do projeto. Copie-o para `.env` e ajuste os valores:

```
cp .env.example .env
```

Edite o arquivo `.env` com um editor de texto:

```
SECRET_KEY=sua_chave_secreta_aqui # MUITO IMPORTANTE: Gerar uma chave forte e
única
DATABASE_URL=sqlite:///instance/phishing_manager.db # Ou sua URL de banco de
dados (PostgreSQL, MySQL)
DEBUG=False # Mudar para True apenas em desenvolvimento
TELEGRAM_BOT_TOKEN=seu_token_do_bot_telegram # Opcional: para notificações via
Telegram
TELEGRAM_ADMIN_CHAT_ID=seu_chat_id_admin # Opcional: para notificações de admin
```

Importante: Sempre gere uma `SECRET_KEY` forte e única para cada implantação em produção. Você pode usar o instalador para gerar uma automaticamente ou usar um gerador de senhas.

3.2. Configuração do Banco de Dados

Por padrão, o Phishing Manager utiliza SQLite. Para ambientes de produção, é altamente recomendável usar PostgreSQL ou MySQL. Altere a variável `DATABASE_URL` no arquivo `.env` para apontar para seu banco de dados externo.

Exemplo para PostgreSQL:

```
DATABASE_URL=postgresql://user:password@host:port/database_name
```

Após alterar a URL do banco de dados, você precisará inicializar o esquema no novo banco de dados. Se estiver usando o modo manual, execute:

```
cd phishing-manager/phishing-manager
source venv/bin/activate
flask db upgrade
```

Se estiver usando Docker, o `docker-compose.yml` pode precisar de ajustes para incluir o serviço de banco de dados e as migrações.

3.3. Configuração de Email (SMTP)

Para o envio de e-mails de phishing, você precisará configurar um servidor SMTP. As configurações geralmente são feitas via variáveis de ambiente:

```
SMTP_SERVER=smtp.example.com
SMTP_PORT=587
SMTP_USERNAME=seu_email@example.com
SMTP_PASSWORD=sua_senha_de_email
SMTP_USE_TLS=True
SMTP_USE_SSL=False
```

4. Gerenciamento de Usuários e Autenticação

4.1. Criando Usuários

O instalador cria um usuário administrador inicial. Você pode criar usuários adicionais através da interface administrativa do Phishing Manager ou via linha de comando (apenas para o backend):

```
# No diretório phishing-manager/phishing-manager com ambiente virtual ativado
flask create-user --username novo_usuario --email user@example.com --password SenhaForte123!
```

Para criar um administrador:

```
flask create-admin --username novo_admin --email admin@example.com --password SenhaAdminForte123!
```

4.2. Autenticação de Dois Fatores (2FA)

Para administradores, o 2FA é obrigatório. Para usuários comuns, é opcional, mas altamente recomendado. Para configurar o 2FA:

1. Faça login no Phishing Manager.
2. Navegue até as configurações do seu perfil.
3. Siga as instruções para ativar o 2FA, que geralmente envolve escanear um QR code com um aplicativo autenticador (e.g., Google Authenticator, Authy).

4.3. Recuperação de Senha

Em caso de esquecimento de senha, o administrador pode redefinir a senha de qualquer usuário. Para usuários comuns, um fluxo de recuperação de senha via e-mail pode ser implementado (se configurado).

5. Gerenciando Campanhas de Phishing

Esta seção detalha como criar, executar e monitorar suas campanhas de phishing.

5.1. Visão Geral do Dashboard

O dashboard fornece uma visão geral das suas campanhas ativas, estatísticas de e-mails enviados, cliques, credenciais capturadas e outras métricas importantes.

5.2. Gerenciamento de Domínios

Antes de criar uma campanha, você precisará configurar os domínios que serão utilizados. Estes são os domínios que aparecerão nos links de phishing e nos e-mails.

- **Adicionar Domínio**: Adicione novos domínios ao sistema.
- **Configurar DNS**: Certifique-se de que os registros DNS (A, CNAME, MX, etc.) do seu domínio estejam apontando corretamente para o servidor do Phishing Manager.
- **Gerenciamento Automático de DNS**: Se configurado, o Phishing Manager pode interagir com seu provedor DNS para gerenciar registros automaticamente.

5.3. Criação de Templates (Modelos)

Templates são modelos reutilizáveis para e-mails de phishing e páginas de destino. Eles podem ser criados do zero ou importados.

- **E-mail Templates**: Crie o corpo do e-mail, assunto, remetente e outros detalhes.
- **Landing Page Templates**: Crie páginas HTML que simulam páginas de login ou outras páginas web.
- **Variáveis Dinâmicas**: Utilize variáveis como `{{username}}`, `{{link}}` para personalizar e-mails e páginas para cada vítima.

5.4. Lançando uma Campanha

1. **Definir Alvos**: Importe uma lista de endereços de e-mail dos seus alvos.
2. **Selecionar Template**: Escolha o template de e-mail e/ou landing page a ser utilizado.

3. **Configurar Domínio**: Selecione o domínio que será usado para os links de phishing.
4. **Agendar/Iniciar**: Inicie a campanha imediatamente ou agende-a para uma data/hora futura.
5. **Configurações Avançadas**: Defina opções como proteção anti-bot, redirecionamento após a submissão, etc.

5.5. Monitoramento e Análise de Resultados

Após o lançamento da campanha, o Phishing Manager fornecerá métricas em tempo real:

- **E-mails Enviados**: Quantidade total de e-mails enviados.
- **E-mails Abertos**: Quantidade de e-mails que foram abertos pelos alvos.
- **Cliques em Links**: Quantidade de cliques nos links de phishing.
- **Credenciais Capturadas**: Quantidade de credenciais submetidas nas páginas falsas.
- **Visitantes Únicos**: Número de IPs únicos que acessaram as URLs.
- **Logs Detalhados**: Registros de cada interação, incluindo IP, User-Agent, data/hora.

Utilize esses dados para analisar a eficácia da sua campanha e identificar áreas de melhoria para o treinamento de conscientização em segurança.

6. Funcionalidades Administrativas

Usuários com privilégios de administrador têm acesso a funcionalidades adicionais para gerenciar o sistema e outros usuários.

6.1. Gerenciamento de Usuários

- **Listar Usuários**: Visualize todos os usuários do sistema.
- **Criar/Editar Usuários**: Adicione novos usuários ou modifique os existentes (username, email, senha, privilégios de admin, créditos).

- **Banir/Desbanir Usuários**: Bloqueie ou desbloqueie o acesso de usuários ao sistema.
- **Gerenciar Créditos**: Atribua ou remova créditos dos usuários.

6.2. Logs do Sistema

Acesse logs detalhados de todas as atividades do sistema, incluindo logins, ações administrativas, erros e eventos de segurança. Os logs podem ser filtrados por nível, usuário, tipo de evento e período.

6.3. Estatísticas do Sistema

Visualize estatísticas gerais sobre o uso do Phishing Manager, como o número total de usuários, campanhas ativas, e-mails enviados, credenciais capturadas e uso de armazenamento.

6.4. Configurações do Sistema

Ajuste configurações globais do Phishing Manager, como chaves de API, configurações de notificação, limites de rate limiting e outras opções de segurança.

7. Solução de Problemas (Troubleshooting)

Esta seção aborda problemas comuns que você pode encontrar e como resolvê-los.

7.1. Problemas de Instalação

- **Dependências Ausentes**: O instalador tentará instalar automaticamente. Se falhar, verifique as mensagens de erro e instale manualmente os pacotes ausentes (e.g., `python3-dev`, `build-essential`).
- **Permissões**: Certifique-se de executar o instalador com `sudo` para ter as permissões necessárias.
- **Erros de Rede**: Verifique sua conexão com a internet se o instalador não conseguir baixar pacotes.

7.2. Problemas de Acesso à Aplicação

- **Backend não Iniciado**: Verifique se o processo do Flask está em execução. Se estiver usando o modo manual, certifique-se de ter ativado o ambiente virtual e executado `flask run`.
- **Frontend não Iniciado**: Verifique se o processo do React está em execução. Se estiver usando o modo manual, certifique-se de ter executado `npm start`.
- **Portas em Uso**: Se as portas padrão (5000 para backend, 3000 para frontend) já estiverem em uso, você pode precisar configurá-las para usar portas diferentes.
- **Firewall**: Verifique se o firewall do seu sistema está bloqueando o acesso às portas da aplicação. Permita o tráfego nas portas 5000 e 3000 (ou as portas configuradas).

7.3. Problemas de Autenticação

- **Credenciais Inválidas**: Verifique seu nome de usuário e senha. Se esqueceu a senha, um administrador pode redefini-la.
- **2FA**: Se o 2FA estiver ativado, certifique-se de que o código TOTP do seu aplicativo autenticador está correto e não expirou.
- **Conta Bloqueada**: Após várias tentativas de login falhas, sua conta pode ser bloqueada temporariamente. Aguarde o tempo especificado ou entre em contato com um administrador.

7.4. Problemas de Campanha/Email

- **E-mails não Enviados**: Verifique as configurações SMTP no seu arquivo `.env`. Certifique-se de que o servidor SMTP está acessível e as credenciais estão corretas.
- **Links não Funcionam**: Verifique se os registros DNS do seu domínio estão configurados corretamente para apontar para o servidor do Phishing Manager.
- **Páginas em Branco**: Verifique se os caminhos dos seus templates estão corretos e se os arquivos HTML/e-mail estão bem formatados.

8. Suporte e Contato

Se você encontrar problemas que não podem ser resolvidos com este manual ou tiver dúvidas, por favor, utilize os seguintes canais:

- **Issues do GitHub**: Para relatar bugs ou sugerir funcionalidades: https://github.com/Dedeg0/phishing-manager/issues
- **Documentação Adicional**: Consulte a documentação técnica para desenvolvedores e o guia de arquitetura para informações mais aprofundadas.

Autor: Manus AI **Data:** 28 de Junho de 2025

Referências:

[1] GitHub Repository: https://github.com/Dedeg0/phishing-manager [2] Docker Documentation: https://docs.docker.com/ [3] Systemd Documentation: https://www.freedesktop.org/wiki/Software/systemd/ [4] Flask Documentation: https://flask.palletsprojects.com/en/latest/ [5] React Documentation: https://react.dev/