SOLYD OFFENSIVE SECURITY

Dennis Lopes da Silva

Projeto para a Certificação SYH2

São Paulo - SP

2025

Sumário

1. Proposta do Projeto:

Objetivo do Projeto:

Este projeto tem como objetivo desenvolver uma interface web para facilitar a execução de comandos relacionados à rede e ao sistema em dispositivos como o Raspberry Pi. A ferramenta foi projetada como um implante para equipes Red Team que buscam flexibilidade na exploração da rede e de vulnerabilidades, oferecendo um ambiente acessível e intuitivo para operações avançadas, como:

- Configuração e gerenciamento de redes Wi-Fi, permitindo controle total sobre conexões sem fio;
- Execução remota de comandos de shell diretamente pelo navegador, otimizando ações ofensivas;
- Criação e administração de hotspots Wi-Fi para movimentação lateral e persistência na rede;
- Escaneamento de portas para identificação de serviços expostos e vetores de ataque;
- Enumeração de hosts na rede local para mapeamento detalhado de alvos;
- Estabelecimento de uma shell reversa para acessos remotos discretos e persistentes;
- Simulação de comandos de teclado no estilo Rubber Ducky, viabilizando automação de ataques.

A ferramenta atende profissionais de segurança ofensiva, permitindo uma abordagem eficiente para comprometer e explorar redes de forma controlada, dentro de cenários de testes de intrusão e auditorias de segurança.

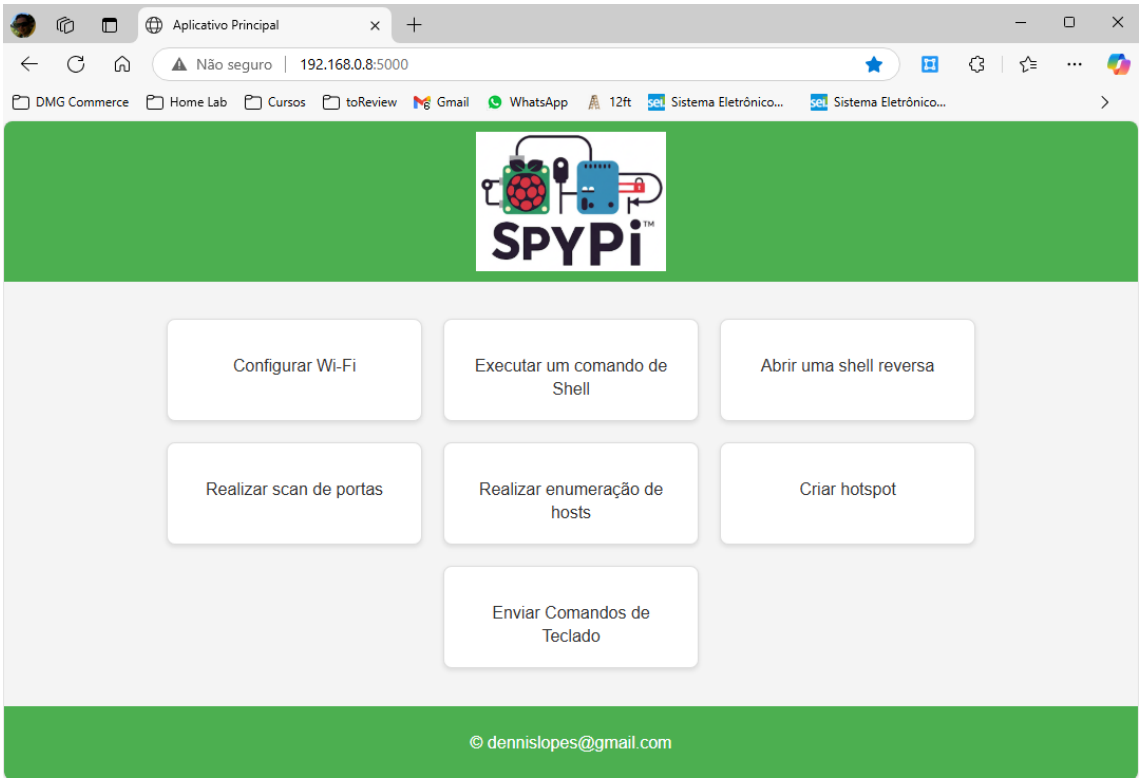
Relevância do Projeto:

A força deste projeto está na sua capacidade de centralizar e automatizar operações essenciais, proporcionando uma interface acessível via navegador para a execução remota de comandos e o gerenciamento de redes. Ao eliminar a necessidade de interação direta com o terminal, a ferramenta reduz a complexidade operacional e aumenta a agilidade das ações, permitindo que especialistas em segurança ofensiva foquem na exploração e análise de vulnerabilidades com mais eficiência.

Desenvolvida para equipes Red Team, a solução possibilita a implantação estratégica de dispositivos na rede, seja por conexões cabeadas ou Wi-Fi,

permitindo acesso remoto a ambientes específicos para testes de penetração, auditorias de segurança e movimentação lateral. Com recursos como escaneamento de portas, enumeração de hosts e estabelecimento de shells reversas, a ferramenta viabiliza operações furtivas e adaptáveis a diferentes cenários.

Além disso, sua flexibilidade permite aplicações que vão desde redes domésticas até infraestruturas corporativas complexas. A integração de automação de comandos no estilo Rubber Ducky adiciona uma camada extra de versatilidade, facilitando interações pré-programadas em sistemas-alvo para testes de segurança e desenvolvimento de novas técnicas ofensivas.
Com essa abordagem, o projeto se consolida como uma peça fundamental no arsenal de profissionais que buscam maior controle e eficiência em ambientes tecnológicos dinâmicos, tornando-se uma solução indispensável para operações de segurança ofensiva avançada



Funcionalidades da Interface Web

A interface web foi projetada para oferecer um conjunto robusto de funcionalidades que simplificam a administração de redes e a execução de comandos no sistema. A seguir, detalhamos cada uma dessas funcionalidades:

1. Configuração de Redes Wi-Fi

A ferramenta permite a busca e conexão com redes Wi-Fi disponíveis utilizando o nmcli. O usuário pode visualizar redes próximas, selecionar uma delas e fornecer credenciais para conexão. Essa funcionalidade é útil tanto para configuração inicial do dispositivo quanto para mudanças dinâmicas de rede.

2. Execução de Comandos de Shell

Com esta funcionalidade, é possível enviar comandos diretamente para o sistema operacional do dispositivo e visualizar a saída em tempo real. Isso permite executar diagnósticos, gerenciar serviços, modificar arquivos de configuração e realizar outras operações sem precisar acessar fisicamente o terminal do dispositivo.

3. Shell Reversa

A interface oferece a possibilidade de estabelecer uma conexão reversa para um IP e porta especificados. Esse recurso permite que um usuário remoto assuma o controle do dispositivo, possibilitando a execução de comandos como se estivesse presente fisicamente. Essa funcionalidade é particularmente útil para testes de segurança, administração remota e auditorias de redes.

4. Escaneamento de Portas

Utilizando o nmap, a ferramenta permite escanear portas abertas de um host especificado, identificando serviços ativos e suas respectivas versões. Os resultados são apresentados diretamente na interface web, permitindo análises rápidas de segurança e diagnósticos de acessibilidade de serviços na rede.

5. Enumeração de Hosts

Essa funcionalidade realiza a identificação de dispositivos ativos dentro de uma rede local utilizando nmap. O usuário pode mapear quais dispositivos estão

conectados, seus endereços IP e outras informações relevantes, facilitando a administração e segurança da rede.

6. Criação de Hotspot Wi-Fi

A ferramenta permite transformar o dispositivo em um ponto de acesso sem fio, utilizando o nmcli para gerenciar interfaces de rede e configurar um hotspot com segurança WPA2. Isso possibilita, por exemplo, o compartilhamento de conexão de internet ou a criação de redes isoladas para testes e desenvolvimento.

7. Envio de Comandos de Teclado (Rubber Ducky)

A interface inclui suporte ao envio de comandos de teclado para um PC conectado ao dispositivo via Arduino configurado como HID (Human Interface Device). Essa funcionalidade permite a automação de tarefas e a execução de scripts simulando a digitação de comandos, seguindo a sintaxe do Rubber Ducky.

Os comandos atualmente suportados incluem:

- STRING <texto> – Digita o texto especificado caractere por caractere.
- ENTER – Pressiona a tecla Enter.
- GUI r – Simula a combinação Windows + R (Abrir Executar no Windows).
- CTRL ALT DEL – Simula a combinação Ctrl + Alt + Del.
- CTRL SHIFT ENTER – Simula a combinação Ctrl + Shift + Enter (Executar como Administrador).
- LEFT – Pressiona a tecla Seta para a Esquerda.
- ALT F4 – Simula a combinação Alt + F4 (Fechar janelas).
- DELAY <tempo> – Aguarda o tempo especificado (em milissegundos) antes de continuar a execução dos comandos.

Essa funcionalidade é especialmente útil para demonstrações de segurança, automação de processos repetitivos e testes de intrusão em sistemas protegidos.

2. Plano de Montagem

Hardware Necessário

- Raspberry Pi 3 ou superior;
- Adaptador Wi-Fi (seria interessante um com suporte a "hotspot" (modos de operação de ponto de acesso, pois futuramente serão disponibilizados comandos para intrusão em rede Wi-Fi);
- Conexão de rede com acesso à internet;
- Arduino Pro Micro;

Passo a Passo para Montagem

Configuração do Raspberry Pi:

Prepare o Raspberry Pi com o sistema operacional Raspbian (agora chamado Raspberry Pi OS). Certifique-se de que o Raspberry Pi esteja conectado à rede local ou à internet.

Instalação das Dependências:

Conecte-se ao Raspberry Pi via SSH ou diretamente. Instale as ferramentas necessárias:

```
sudo apt-get update
sudo apt-get install python3-pip nmap network-manager
pip3 install flask
```

Preparação do Servidor Web:

Faça o download do projeto Flask no GitHub do projeto. O servidor Flask vai rodar na porta 5000 por padrão, acessível através de http://<ip_do_raspberry>:5000.

Configuração de Rede e Hotspot:

Certifique-se de que o adaptador Wi-Fi (ex. wlan0) seja configurado corretamente para o seu Raspberry Pi. Teste a criação de hotspot via nmcli.

Conexão entre Dispositivos

Raspberry Pi - UART

O Raspberry Pi deve ser conectado a arduino via UART pelos pinos de GPIO. A conexão é feita da seguinte forma:

- **TX (Raspberry Pi) -> RX (Arduino)**
- **RX (Raspberry Pi) -> TX (Arduino)**
- **GND -> GND**

Execução da Aplicação:

Navegue até o diretório do projeto e execute:

sudo python3 app.py

Acesse a interface web no navegador através de http://<ip_do_raspberry>:5000.

3. Código Fonte

O código fonte do projeto está disponível em:

https://github.com/dennislopes/spyPi

4. Trabalhos Futuros

Para expandir as funcionalidades da ferramenta, pretende-se implementar novos comandos que ampliem as capacidades de exploração e automação, permitindo maior controle sobre redes e dispositivos-alvo. Algumas das melhorias previstas incluem aprimoramentos na detecção de vulnerabilidades, otimização do gerenciamento de conexões sem fio e integração de novos métodos de persistência e movimentação lateral.

Além disso, um dos principais desenvolvimentos futuros será um **fork** do projeto voltado exclusivamente para a automação de ataques no estilo **Rubber Ducky**. A ideia é criar uma versão mais enxuta e portátil, utilizando o **Raspberry Pi Zero** ou o **Orange Pi Zero**, com preferência pelo Orange Pi devido ao seu custo reduzido. Essa abordagem tornaria o dispositivo mais discreto e acessível, facilitando implantações em cenários diversos.

Um dos desafios técnicos desse fork será a alimentação dos dispositivos. Tanto o Raspberry Pi Zero quanto o Orange Pi Zero operam a **3.3V**, enquanto o **Arduino Pro Micro**, utilizado na simulação de teclado, exige **5V** para funcionamento correto. Será necessário estudar soluções eficientes para conversão de tensão e gerenciamento de energia, garantindo compatibilidade entre os componentes sem comprometer a estabilidade do sistema.

Com essas evoluções, o projeto poderá atender a um espectro ainda maior de aplicações, desde testes de intrusão altamente portáteis até implantações estratégicas para auditorias de segurança mais abrangentes.

REFERÊNCIAS

SMART KITS. Arduino Micro Pinout - Guia Básico de GPIOs. Disponível em: https://blog.smartkits.com.br/arduino-micro-pinout-guia-basico-de-gpios/. Acesso em: Janeiro de 2025.

Documentação do Arduino. Disponível em: https://www.arduino.cc/reference/en/. Acesso em: Janeiro de 2025.

Biblioteca Arduino para sensores. Disponível em: https://www.arduino.cc/reference/en/. Acesso em: Fevereiro de 2025.

Documentação do Flask. Disponível em: https://flask.palletsprojects.com/en/2.0.x/. Acesso em: Fevereiro de 2025.

NetworkManager. Manual do nmcli. Disponível em: https://developer.gnome.org/NetworkManager/stable/nmcli.html.pt. Acesso em: Março de 2025.

Nmap. Manual oficial. Disponível em: https://nmap.org/book/. Acesso em: Março de 2025.

SOLYD. Curso de Hardware Hacking. Disponível em: https://www.solyd.com.br/curso-hardware-hacking. Acesso em: Março de 2025.

SOLYD. Curso de Pentest. Disponível em: https://www.solyd.com.br/curso-pentest. Acesso em: Março de 2025.