Manual do Usuário – **TargetRecon**

Autor: Raphael Cavalcanti Banov

Visão Geral

TargetRecon é uma ferramenta de linha de comando (CLI) para reconhecimento de alvos em testes de invasão. Ele integra múltiplas ferramentas essenciais para coleta de informações durante a fase inicial de um pentest.

Requisitos

Antes de utilizar o aplicativo, certifique-se de que as seguintes ferramentas estão instaladas no sistema:

- Python 3.6+
- `whois`
- `nslookup` (já vem por padrão em muitos sistemas)
- `wafw00f`:
  Instale com `pip install wafw00f`
- `dirb`:
  Instale com `sudo apt install dirb`
- `nikto`:
  Instale com `sudo apt install nikto`
- Linux (recomendado)

Execução

Execute o aplicativo via terminal com:

```
python3 main.py
```

Menu Principal

```
Este é TargetRecon, seu aplicativo de reconhecimento de alvos

Selecione uma opção:

0 - Port Scanning
1 - Consulta WHOIS
2 - Detecção de WAF (wafw00f)
3 - Scanner de Diretórios (dirb)
```

```
4 - Varredura de Vulnerabilidades (nikto)
5 - Finalizar
```

Funcionalidades

0 – Port Scanning

- Realiza escaneamento de portas TCP e UDP.
- Pode usar portas conhecidas (well-known) ou personalizadas.
- Inclui visualização de hosts na rede via ARP.

1 – Consulta WHOIS

- Executa uma busca `whois` para IPs ou domínios.
- Útil para descobrir informações do registrante, ASN, etc.

Exemplo:

```
Digite o domínio ou IP para consulta WHOIS: example.com
```

---

2 – Detecção de WAF (wafw00f)

- Verifica se a aplicação web está protegida por um firewall.
- Usa o utilitário `wafw00f`.

Exemplo:

```
Digite a URL ou IP: http://example.com
```

---

3 – Scanner de Diretórios (dirb)

- Executa força bruta para encontrar diretórios ocultos.
- Usa a wordlist padrão `/usr/share/dirb/wordlists/small.txt`.

Exemplo:

```
Digite a URL alvo: http://example.com
```

---

4 – Varredura de Vulnerabilidades (nikto)

- Varre o servidor web em busca de vulnerabilidades conhecidas.
- Usa o `nikto` com o alvo informado.

Exemplo:

```
Digite a URL ou IP: http://example.com
```