Relatório – Roteiro 2: App Reconhecimento do Alvo

Felipe Maia

1. Introdução e Objetivos

Este relatório documenta o desenvolvimento do app_recon, um aplicativo de reconhecimento de alvos para pentests que reúne seis módulos principais (PortScan, WHOIS Lookup, DNS Enumeration, Subdomain Scan, WAF Detection e Vulnerability Scan) em uma interface gráfica em Tkinter. O objetivo é integrar as ferramentas de footprinting e reconnaissance mais utilizadas, de forma modular e extensível, visando atingir nota máxima (9–10).

2. Respostas às Perguntas de Pesquisa

2.1 Ferramentas Adicionais para Reconhecimento

- **`nslookup / dig`**: Descoberta de servidores autoritativos via DNS.

- **`dnsenum`**: Enumeração DNS e brute-force de subdomínios.

- **`theHarvester`**: Coleta de e-mails e subdomínios públicos.

- **`Shodan CLI`**: Busca de dispositivos IoT e gateways industriais.

- **`whois`**: Consulta de registros de domínio e dados de registrante.

2.2 SYN Scan vs TCP Connect Scan

- `SYN Scan (-sS)` : meio-aberto, não completa handshake, mais furtivo (requer root).
- `TCP Connect Scan (-sT)` : completa handshake via connect(), mais detectável, sem root.

2.3 Técnicas para Evitar Detecção por IPS

- Fragmentação de pacotes (-f)

- Controle de taxa (--scan-delay, --max-rate)

- Uso de decoys (-D)

- Randomização de portas e ordem (--source-port, --randomize-hosts)

- Roteamento via VPN, proxies ou Tor

3. Arquitetura e Decisões de Design

O projeto é organizado de forma modular, com cada ferramenta em um módulo separado dentro de `core/`. A GUI foi implementada em Tkinter por ser leve e familiar, reutilizando padrões do Roteiro 1.

Estrutura de pastas:

```
app_recon/
├── core/
│   ├── __init__.py
│   ├── portscan.py
│   ├── whois_lookup.py
│   ├── dns_enum.py
│   ├── subdomain_scan.py
│   ├── waf_detection.py
│   └── vuln_scan.py
├── utils.py
├── gui.py
├── requirements.txt
└── README.md
```

4. Análise das Ferramentas Integradas

- **PortScan**: Varredura TCP/UDP, banner grabbing, well-known ports.

- **WHOIS Lookup**: Consulta WHOIS de domínio.

- **DNS Enumeration**: Consulta NS, MX, A com dnspython.

- **Subdomain Scan**: Descoberta via Sublist3r com tratamento de erro de CSRF.

- **WAF Detection**: Identificação de WAF via subprocess (wafw00f).

- **Vulnerability Scan**: Varredura HTTP com Nikto.

5. Resultados dos Testes

5.1 PortScan

```
Iniciando escaneamento em 172.20.10.4 (TCP) de 20 até 25:
Port 20: closed/filtered (unknown)
Port 21: closed/filtered (SSH)
Port 22: open (SSH) - Banner: SSH-2.0-OpenSSH_7.6p1
Port 23: closed/filtered (unknown)
Port 25: closed/filtered (SMTP)
```

5.2 WHOIS Lookup

```
domain:      ekkopark.com.br
owner:       FAM PARTICIPAÇÕES E EMP. IMOBILIÁRIOS LTDA
ownerid:     03.135.544/0001-59
responsible: Paulo Tasso Amoroso
country:     BR
owner-c:     PATAM13
tech-c:      MAC1362
nserver:     ns558.hostgator.com.br
nsstat:      20250427 AA
nslastaa:    20250427
nserver:     ns559.hostgator.com.br
nsstat:      20250427 AA
nslastaa:    20250427
saci:        yes
created:     20190722 #19919009
changed:     20230627
expires:     20250722
status:      published

nic-hdl-br:  PATAM13
person:      Paulo Tasso Amoroso
e-mail:      paulotasso84@gmail.com
country:     BR
created:     20190722
changed:     20230814

nic-hdl-br:  MAC1362
person:      Marcel Cibim
e-mail:      marcel@cgpropaganda.com.br
country:     BR
created:     20020322
changed:     201912115.3 DNS Enumeration
Name Servers:
ns1.ekkopark.com.br
ns2.ekkopark.com.br

Mail Servers:
mail.ekkopark.com.br

A Records:
203.0.113.10
```

5.4 Subdomain Scan

Carregando subdomínios...
www.ekkopark.com.br
autodiscover.ekkopark.com.br
cpanel.ekkopark.com.br
cpcalendars.ekkopark.com.br
cpcontacts.ekkopark.com.br
jardimbarcelona.ekkopark.com.br
www.jardimbarcelona.ekkopark.com.br
mail.ekkopark.com.br
webdisk.ekkopark.com.br
webmail.ekkopark.com.br

5.5 WAF Detection

```
The Web Application Firewall Fingerprinting Toolkit [0m]
[*] Checking https://ekkopark.com.br
[+] The site [1;94mhttps://ekkopark.com.br [0m is behind
[1;96mModSecurity (SpiderLabs) [0m] WAF.
[~] Number of requests: 2
```

5.6 Vulnerability Scan

```
Carregando vulnerabilidades...
- Nikto v2.1.6
+ Target IP: 192.168.0.10
+ Server: Apache/2.4.41 (Ubuntu)
+ OSVDB-3102: /admin/: Directory indexing found.
```