Relatório de Reconhecimento em Pentest

1. Respostas às Questões de Pesquisa

1.1 Ferramentas Mais Úteis para Reconhecimento (além de PortScan)

1. **BuiltWith** Identifica tecnologias utilizadas em websites (CMS, frameworks, bibliotecas JS, servidores, etc). ● *Justificativa:* Útil para mapear a superfície de ataque de aplicações web. Em um caso real, foi usada para descobrir uma aplicação WordPress com plugin vulnerável em um site governamental.

2. **WebTech** Biblioteca Python semelhante ao BuiltWith, mas com foco mais técnico e com detecção detalhada por headers HTTP. ● *Justificativa:* Facilita o fingerprinting automatizado durante scripts de reconhecimento. Foi usada em auditoria de site bancário para confirmar uso de frameworks desatualizados.

3. **theHarvester** Coleta e-mails, domínios e nomes associados a uma organização usando motores de busca. ● *Justificativa:* Muito usada para engenharia social e enumeração de alvos. Em um pentest de universidade, revelou contas administrativas vazadas.

4. **WHOIS** Retorna informações registradas sobre domínios e IPs. ● *Justificativa:* Permite descobrir responsáveis por redes, ranges de IP, e possíveis alvos adjacentes. Usado em caso real para mapear infraestrutura compartilhada de subdomínios.

5. **DNS Enumeration** (usando `dnspython`) Descobre registros DNS como A, MX, NS, TXT, etc. ● *Justificativa:* Crucial para descobrir subdomínios, servidores de e-mail, e serviços de backup. Em pentest de empresa SaaS, revelou subdomínio admin oculto.

1.2 Diferença entre SYN Scan e TCP Connect Scan

- **SYN Scan**: ● Envia apenas pacotes SYN e analisa a resposta (SYN-ACK indica porta aberta). ● *Não finaliza a conexão*, sendo mais furtivo.

- **TCP Connect Scan**: ● Realiza a conexão completa (SYN, SYN-ACK, ACK). ● *Mais fácil de detectar*, pois envolve handshake completo.

Cenários de uso:

- *SYN Scan:* Melhor para pentests discretos e testes não autenticados.
- *TCP Connect:* Melhor em ambientes onde o usuário não tem permissão para pacotes brutos (sem root).

1.3 Como Evitar Detecção por IPS durante o Reconhecimento

Técnicas comuns:

1. **Scan com baixa velocidade (Rate Limiting):**
    - Reduz o número de pacotes por segundo para evitar alertas.
    - *Impacto:* Menor chance de detecção, mas maior tempo de varredura.

2. **Fragmentação de pacotes:**

- Divide pacotes de rede em fragmentos menores.
- *Impacto:* Pode burlar IDS que não remontam pacotes corretamente.

3. **Randomização de ordem e tempo entre portas:**
   - Evita padrões previsíveis.
   - *Impacto:* Dificulta correlação de eventos pelo IPS.
4. **Uso de proxies ou VPNs:**
   - Oculta IP de origem.
   - *Impacto:* Protege identidade, mas pode ser bloqueado se detectado.
5. **Técnicas passivas:**
   - Obtêm informações sem enviar pacotes (ex: consultas DNS, WHOIS, etc).
   - *Impacto:* Ineficaz para serviços internos, mas ótima para fingerprinting inicial.

---

2. Arquitetura e Decisões de Design

O aplicativo CLI foi desenvolvido em Python e estruturado em módulos independentes para cada ferramenta. As principais decisões foram:

- **Modularização**: cada ferramenta é uma função separada, facilitando manutenção.
- **Substituição de ferramentas que requerem API/key ou não funcionam nativamente no Windows**, como Shodan e wafw00f.
- **Uso de bibliotecas Python puras**, como `webtech`, `builtwith`, `dnspython`, para manter compatibilidade com Windows.
- **Menu interativo com `input()`**, para facilitar o uso via terminal.

---

3. Análise das Ferramentas Integradas

Ferramenta	Função	Tipo	Vantagem Principal
PortScan	Scanner de portas TCP/UDP	Ativo	Descoberta de serviços
BuiltWith	Fingerprinting de tecnologias	Passivo	Sem API Key; bom para aplicações web
WebTech	Detecção de headers e tech	Ativo	Biblioteca Python moderna
WHOIS	Dados de domínio/IP	Passivo	Mapeia responsáveis e ranges de rede
DNS Enumeration	Enumeração de registros DNS	Passivo	Revela subdomínios e infraestrutura

---

4. Resultados dos Testes Realizados

Os testes foram realizados em alvos de teste públicos e domínios próprios. Resultados:

- **PortScan** detectou serviços HTTP/HTTPS abertos em `scanme.nmap.org`.
- **BuiltWith** identificou uso de Cloudflare, Google Analytics e nginx em vários sites.

- **WebTech** confirmou headers como `Server: nginx` e frameworks como `PHP`.
- **WHOIS** revelou dados administrativos e ranges de IPs para domínios de teste.
- **DNS Enumeration** encontrou registros MX e TXT relevantes, incluindo SPF e DKIM.

Esses resultados demonstram a capacidade do toolkit de realizar reconhecimento eficaz e modular sem depender de ferramentas externas complicadas.

---

5. Manual do Usuário – Recon CLI Toolkit

📦 Pré-requisitos

- Python 3.8+
- Instale as bibliotecas necessárias com:

```
pip install whois dnspython builtwith webtech
```

🚀 Executando o Toolkit

No terminal, execute:

```
python recon_toolkit.py
```

Será exibido o menu:

```
=== Recon CLI Toolkit ===
1) PortScan
2) BuiltWith Scan
3) WHOIS Lookup
4) DNS Enumeration
5) WebTech Scan
0) Sair
```

🔍 Opções do Menu

1) PortScan

- **Descrição:** Faz escaneamento de portas TCP ou UDP.
- **Entrada:** IP ou host, intervalo de portas, protocolo (`tcp` ou `udp`).
- **Exemplo:**

```
Host/IP: scanme.nmap.org
Porta inicial: 20
```

```
Porta final: 80
Protocolo: tcp
```

2) BuiltWith Scan

- **Descrição:** Identifica tecnologias web com base na URL.
- **Entrada:** URL completa (ex: `https://exemplo.com`).
- **Saída:** Frameworks, bibliotecas, servidores.

3) WHOIS Lookup

- **Descrição:** Retorna dados de registro do domínio.
- **Entrada:** Nome do domínio (ex: `exemplo.com`).
- **Saída:** Proprietário, data de criação, contatos técnicos, etc.

4) DNS Enumeration

- **Descrição:** Enumera registros DNS como A, MX, TXT, NS etc.
- **Entrada:** Nome do domínio (ex: `exemplo.com`).
- **Dica:** Não inclua `https://`. Se incluir, o sistema corrigirá automaticamente.

5) WebTech Scan

- **Descrição:** Faz fingerprinting técnico por cabeçalhos HTTP.
- **Entrada:** URL (ex: `https://exemplo.com`).
- **Saída:** Servidor web, frameworks usados, versões detectadas.

0) Sair

- Finaliza o programa.
