**Relatório de aplicação para reconhecimento de alvo**

## Principais ferramentas para o reconhecimento do alvo

A fase de reconhecimento de alvo (*reconnaissance*) é considerada a primeira de um ataque cibernético. Diferentes ferramentas são utilizadas com o objetivo de extrair informações referentes a infraestrutura, serviços e tecnologia do alvo. Essas informações levam o invasor a mapear as relações entre os sistemas, para assim identificar vulnerabilidades. As ferramentas a seguir se destacam, nesse relatório, com maior relevância:

1. *The harvester*, uma ferramenta que coleta endereços de e-mail, subdomínios, endereços ip e outras informações públicas que estejam associadas a um domínio alvo.
2. *nslookup*, ferramenta para descobrir os endereços IP dos servidores web principais do alvo. Isso pode indicar onde a infraestrutura web está hospedada e possibilitar investigações pelo ip, como o escaneamento de portas.
3. *PortScan*, uma aplicação que envia um pacote para cada porta disponível na rede e verifica sua resposta para determinar seu estado (categorias aberto, fechado e ocupado).
4. *Nmap*, ferramenta que oferece as funcionalidades de port scanner para um host ou rede, análise de vulnerabilidades e host discovery. Host discovery consiste em enviar uma mensagem a todos os ips da rede e verificar quais deles respondem, possibilitando a comunicação e a descoberta de seu sistema operacional.
5. *Shodan*, um mecanismo de busca dos dispositivos conectados na internet, como dispositivos IoT.
6. *Wappalyzer*, uma ferramenta para identificação das tecnologias utilizadas no back-end de um domínio através do *header HTTP* de suas respostas às requisições.

## Ferramentas adicionadas no código fonte

No código fonte, foram adicionadas as ferramentas *port-scanner*, *nslookup*, *wappalyzer* e, para além das ferramentas descritas acima, foram também acrescidas as ferramentas *wafwoof* e *WHOIS*. A execução deve ocorrer pelo arquivo main.py, que está na raiz do projeto. Esse arquivo apresenta um fluxo amigável de boas vindas com as opções de ferramentas, que devem ser escolhidas pelo usuário. Cada ferramenta possui seu arquivo e código correspondente na pasta tools. Abaixo seguem-se evidências de teste de cada ferramenta.

```
Welcome to Recon-Tools! A group of tools for target recognition
1. Portscan
2. Nslookup
3. Wappalyzer
4. Wafw00f
5. Whois
Type the number of the tool you want to use: 1
Initializing port scanner
What is the scan type? [0 - Host | 1 - Network] 0
Which is the version of protocol to be scanned? [4 | 6]? 4
Insert the IPv4 host adress: 192.168.15.145
Which port the scanner might start at? 20
Which port the scanner might end at? 80
Starting port scan of ip 192.168.15.145 from ports 20 to 80
================================================================================================================================
OS: Windows XP, 7, 8, 2003, 2008 | Port: 20/tcp | Service: ftp-data | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 20/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 21/tcp | Service: ftp | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 21/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 22/tcp | Service: ssh | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 22/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 23/tcp | Service: telnet | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 23/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 24/tcp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 24/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 25/tcp | Service: smtp | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 25/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 26/tcp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 26/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 27/tcp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 27/udp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 28/tcp | Service: unknown | State: Closed
OS: Windows XP, 7, 8, 2003, 2008 | Port: 28/udp | Service: unknown | State: Closed
```

Imagem: teste do *port-scanner*

```
1. Portscan
2. Nslookup
3. Wappalyzer
4. Wafw00f
5. Whois
Type the number of the tool you want to use: 2
Initializing Nslookup
Insert the domain: google.com
Servidor:  menuvivofibra.br
Address:  fe80::860b:bbff:fecf:b670

Nome:    google.com
Addresses:  2800:3f0:4001:815::200e
          172.217.172.174


Ended Nslookup
```

Imagem: teste do *nslookup*

```
Type the number of the tool you want to use: 3
Initializing Wappalyzer
URL to identify technologies: https://www.rodolfoavelino.com.br/
Technologies found:
- reCAPTCHA
- Bootstrap
- Modernizr
- jQuery
- jQuery Migrate
- WordPress
- MySQL
- Google Font API
- PHP
- Cloudflare
- Font Awesome
Ended Wappalyzer
```

Imagem: teste do *wappalyzer*

```
Type the number of the tool you want to use: 4
Initializing Wafw00f
Insert the url to describe if there is WAF: https://www.rodolfoavelino.com.br/


                    ______
                   /      \
                  (  Woof! )
                   \  ____/                    )
                   ,,                        ) (_
               .-. -    _______              ( |__|
              ()``; |==|_______)             .)|__|
              / ('        /|\\               (  |__|
            (  /  )      / | \               . |__|
             \(_)_))    /  |  \                |__|

                    ~ WAFW00F : v2.3.1 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.rodolfoavelino.com.br/
[+] The site https://www.rodolfoavelino.com.br/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

Ended Wafw00f
```

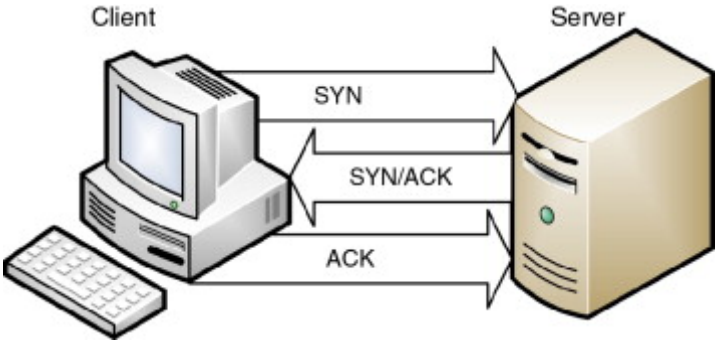
Imagem: teste do *wafwoof*

```
Type the number of the tool you want to use: 5
Initializing Whois
Insert the domain:https://www.rodolfoavelino.com.br/
Domain: rodolfoavelino.com.br
Registered by: None
Creation date: [datetime.datetime(2008, 6, 23, 0, 0), datetime.datetime(2005, 4, 15, 0, 0)]
Expiration date: 2026-06-23 00:00:00
DNS servers: None
Emails: None
Ended Whois
```

Imagem: teste do *whois*

**SYN vs. TCP scan**

A seguir, introduz-se a diferença entre um *port-scanner* de tipo *SYN* e *TCP Connect*. A explicação para isso é baseada no *three-way handshake*, a sequência de pacotes usada para estabelecer uma conexão entre o cliente e o servidor. Conforme visualizado na imagem abaixo, o *SYN* trata-se apenas do primeiro pacote da sequência — que é o único pacote enviado em *port-scanners* de tipo *SYN*. Por outro lado, *port-scanners* do tipo *TCP* realizam toda a sequência e, sendo assim, de fato estabelecem uma conexão com o servidor.




Pacotes envolvidos no *three-way handshake*. Fonte da imagem

O scan SYN é a opção de scan padrão e mais popular, por ser mais rápido e mais discreto que uma conexão TCP completa, portanto é ideal que ele seja escolhido quanto essas características são prioritárias no contexto.

**Técnicas para não ser detectado por sistemas de detecção de intrusão (IPS)**

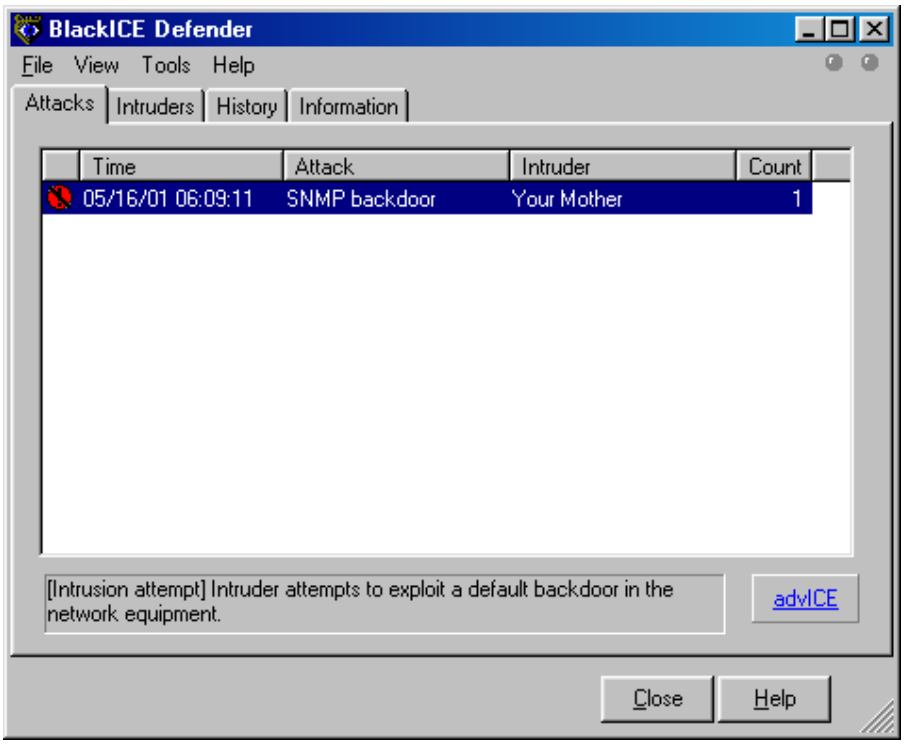
É válido destacar que ambas os tipos de scan citados anteriormente podem ser detectada por IPS. A seguir, menciona-se os principais modos de o invasor ser discreto, contendo 1 exemplo específico para cada modo, quando a empresa possuir IPS:

- Evitar o IDS como se o invasor não estivesse lá

  Uma alternativa é realizar desaceleração da varredura. Isso se baseia nos IPS que detectam atividades maliciosas considerando o intervalo de tempo entre diferentes requisições. Com isso, invasores ativam parâmetros como --scan-delay para evitar tais limites. A consequência direta é que o escaneamento será mais lento.

- Confundir o IDS com dados enganosos

  Uma investigação comumente iniciada por IPSs é o DNS reverso, para obter um domínio associado ao ip do invasor. O problema dessa abordagem ocorre quando o invasor controla o seu próprio DNS, pois assim eles recebem os logs em tempo real e descobrem que foram detectados. A partir disso, eles usam dessa oportunidade para fornecer informações falsas ao IPS solicitante. Uma evidência prática disso pode ser vista na imagem abaixo.




Fornecimento de informações falsas pelo invasor. Fonte da imagem

- Explorar o IDS para obter mais privilégios de rede ou para desligá-lo
  Nos casos em que a detecção de comportamentos anômalos são identificados e comunicados pelo IDS (ao, por exemplo, enviar um pacote RST ao invasor, que indica a detecção de suas atividades). A partir do pacote enviado pelo IDS, o invasor pode inferir seu tipo e explorar as vulnerabilidades do tipo especificado.