Fingerprinting - Coleta de dados do alvo

Coleta de dados de Servidores

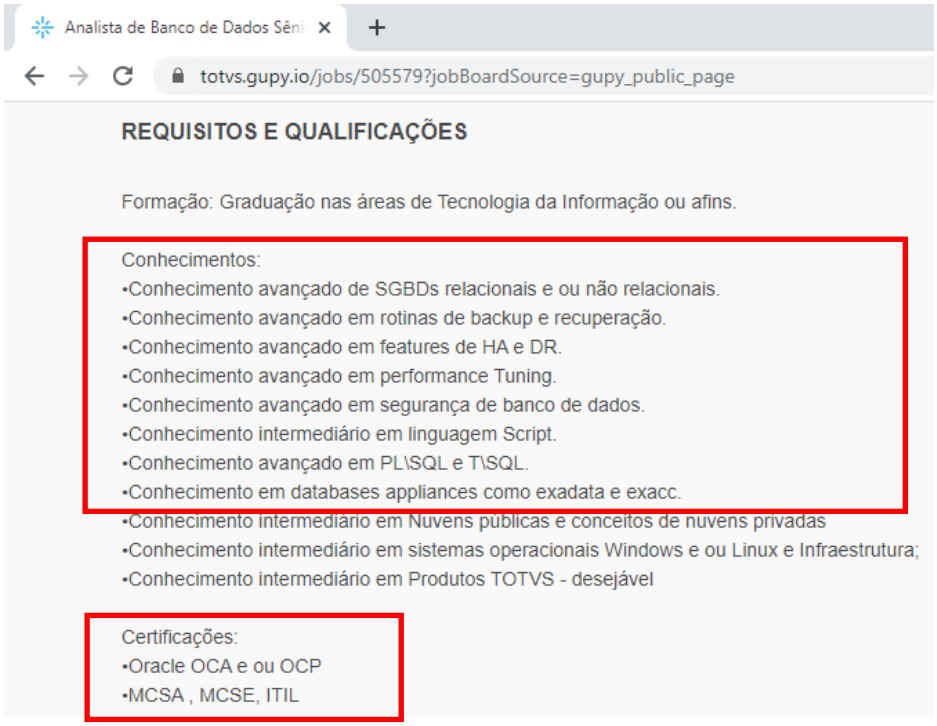
Uma técnica muito utilizada é digitar propositalmente o nome do site para obter informações com a página de erro, caso não esteja tratada devidamente.

Coleta de dados de pessoas

Outra forma de coleta de dado é verificar informações sobre pessoas na empresa, que não deveriam ser reveladas abertamente por se tratarem de informação interna e, dessa forma, possibilitarem ataques do tipo Engenharia Social.

Coleta de dados de tecnologias utilizadas

Pode-se obter também informações sobre sistemas e softwares utilizados pela empresa, que também se classificam como informação interna e que por consequência podem propiciar direcionamentos em ataques específicos de forma a poupar tempo ao atacante.



Coleta de dados usando WHOIS

O WHOIS é um sistema de registros de domínios, IP e sistemas autônomos na internet. O WHOIS pode ser usado para obter informações sobre o proprietário de um domínio.

Os registros de WHOIS são abastecidos pelas empresas de hospedagem e reúnem todas as informações pertencentes a um domínio. No Brasil o WHOIS é indexado pelo CNPJ ou pelo CPF, fornecendo, portanto, informações que não deveriam ser públicas.

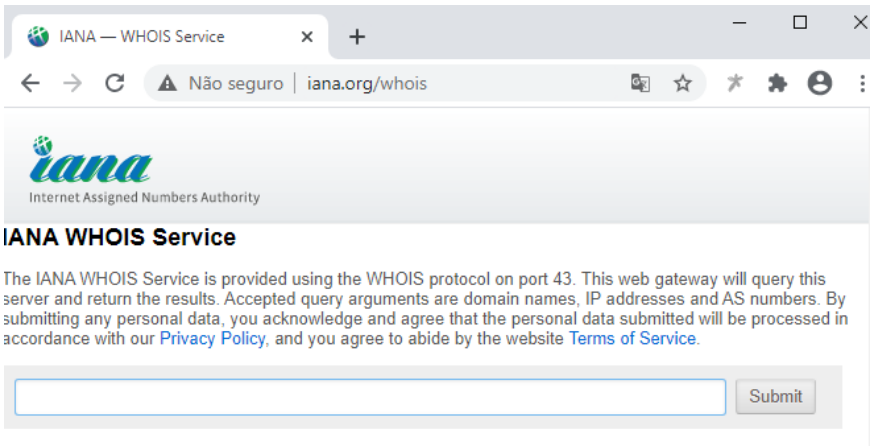
O WHOIS exibe outras informações importantes como: telefones e endereços físicos, além de:

- Contato administrativo;

- Contato técnico;

- Contato de cobrança.

O WHOIS é um comando que vem instalado por padrão nos sistemas Unix/Linux e que pode ser acessado via linha de comando, utilizando ferramentas específicas ou ainda pelo site oficial da IANA () ou ainda no Registro.br (https://registro.br/tecnologia/ferramentas/whois/).



Comando WHOIS no Linux:

whois www.ifms.br -h whois.dns.br

Onde:

-h: conecta a um servidor para realizar a pesquisa.

whois.dns.br: servidor que realizará a consulta (neste caso o Registro.br).

Coleta de dados no archive.org

O archive.org é uma organização responsável por registrar os dados de todos os websites. Foi fundada por Brewster Kahle em 1996 e tem como objetivo disponibilidade destas informações como acervo histórico da Internet.

Inclui diversos informações como:

- Cópias arquivadas de páginas da internet;

- Múltiplas cópias de cada página mostrando a evolução da internet;

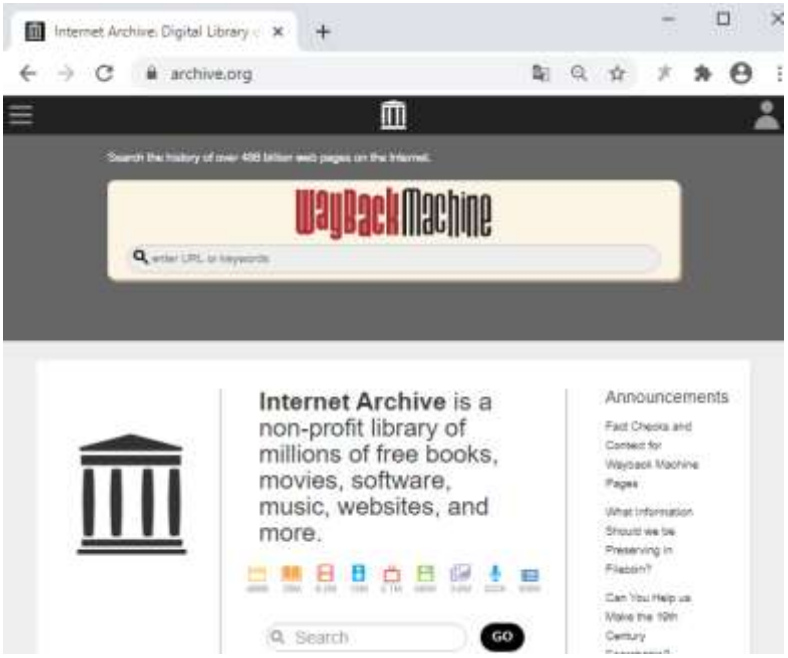
- Softwares;

- Imes;

- Livros;

- Gravações de áudio.

Caso se queira coletar informações do alvo, pode-se passar um tempo navegando em versões anteriores do website no acervo de forma que se possa extrair alguma informação que direcione um determinado tipo de ataque.



Coleta de dados usando DNS

O DNS carrega em seus registros dados importantes como A, AAAA, CNAME, MX, NS, PTR e SOA, que serão vistos com mais detalhes mais adiante, que podem agregar informações importantes na coleta de dados sobre um alvo.

Comandos como nslookup, dig e host possibilitam que as informações nos registros de DNS possam ser visualizados de acordo com a sua utilização.

Exemplo:

$ host www.ifms.edu.br

www.ifms.edu.br is an alias for ifms.edu.br.

ifms.edu.br has address 200.19.32.46

ifms.edu.br mail is handled by 10 alt4.aspmx.l.google.com.

ifms.edu.br mail is handled by 5 alt1.aspmx.l.google.com.

ifms.edu.br mail is handled by 10 alt3.aspmx.l.google.com.

ifms.edu.br mail is handled by 1 aspmx.l.google.com.

ifms.edu.br mail is handled by 5 alt2.aspmx.l.google.com.

$ host -t NS www.ifms.edu.br

www.ifms.edu.br is an alias for ifms.edu.br.

ifms.edu.br name server ns2.ifms.edu.br.

ifms.edu.br name server ns3.ifms.edu.br.

ifms.edu.br name server ns0.ifms.edu.br.

Onde:

-t NS: exibe os endereços dos servidores de nomes (DNS)

$ nslookup www.ifms.edu.br

Server: 10.96.0.10

Address: 10.96.0.10#53

Non-authoritative answer:

www.ifms.edu.br canonical name = ifms.edu.br.

Name: ifms.edu.br

Address: 200.19.32.46

$ dig www.ifms.edu.br

; <<>> DiG 9.16.1-Ubuntu <<>> www.ifms.edu.br

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22952

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;www.ifms.edu.br. IN A

;; ANSWER SECTION:

www.ifms.edu.br. 30 IN CNAME ifms.edu.br.

ifms.edu.br. 30 IN A 200.19.32.46

;; Query time: 184 msec

;; SERVER: 10.96.0.10#53(10.96.0.10)

;; WHEN: Wed Nov 04 19:32:25 UTC 2020

;; MSG SIZE rcvd: 111

Automatizando varreduras

É possível, e recomendável, que sempre que se pode automatize as tarefas para que não seja necessário executar comandos constantemente.

Assim pode-se criar um Script Shell para automatizar a busca de informações de DNS utilizando o comando host.

O Shell Script é uma forma de se programar códigos de forma interpretada, ou seja, cada comando é executado por vez, e utilizando os comandos do Linux, no entanto, a sua força reside no fato de permitir que se use praticamente todos os recursos de programação existentes, como laços condicionais, variáveis, arrays e etc.

$ nano scriptdns.sh

```
#!/bin/bash

for url in $(cat subdominios.txt);

do host $url.$1

done
```

Onde:

#!/bin/bash: carrega os recurso do terminal bash para executar os comandos.

for url in $(cat sub-domains.lst): cria variável que usa as entradas do arquivo subdomínio.txt por ordem e repassa como argumento para o comando que a chamar.

do host $url.$1: o do usa o comando host com os argumentos do arquivo subdomínios.txt exibindo os resultados até todos estes acabarem.

done: finaliza o Shell Script.

A seguir criar o arquivo subdomínios.txt com os tipos de serviços de um subdomínio de servidor:

$ nano subdomínio.txt

```
www

mail

docs

ftp
```

Executando o Shell Script:

$ bash scriptdns.sh ifms.edu.br

www.ifms.edu.br is an alias for ifms.edu.br.

ifms.edu.br has address 200.19.32.46

ifms.edu.br mail is handled by 10 alt3.aspmx.l.google.com.

ifms.edu.br mail is handled by 1 aspmx.l.google.com.

ifms.edu.br mail is handled by 5 alt1.aspmx.l.google.com.

ifms.edu.br mail is handled by 10 alt4.aspmx.l.google.com.

ifms.edu.br mail is handled by 5 alt2.aspmx.l.google.com.

mail.ifms.edu.br is an alias for pop.ifms.edu.br.

pop.ifms.edu.br is an alias for ghs.googlehosted.com.

ghs.googlehosted.com has address 74.125.134.121

ghs.googlehosted.com has IPv6 address 2607:f8b0:400c:c02::79

docs.ifms.edu.br is an alias for ghs.google.com.

ghs.google.com has address 173.194.215.121

ghs.google.com has IPv6 address 2607:f8b0:400c:c0f::79

Host ftp.ifms.edu.br not found: 3(NXDOMAIN)

Coleta de dados DNS-reverso

Da mesma forma que foi feita com a consulta automática no DNS, o reverso também pode ser feito em forma de Shell Script.

O DNS-reverso é justamente o oposto do DNS, que quando digitado um endereço nominal o reverte para o endereço IP do host solicitado, assim o reverso, recebe o endereço IP e o converte em nome.

O DNS-reverso é bastante utilizado para constatar a origem de um endereço como verdadeiro ou falso, por exemplo, caso se receba um e-mail com determinado endereço de servidor mascarado, pode-se, via DNS-reverso, verificar se o IP relacionado ao nome é verdadeiro ou não.

$ nano reverso.sh

```
#!/bin/bash

for ip in $(seq 0 255);

do host $1.$ip

done
```

Onde:

for ip in $(seq 0 255);: cria variável que irá receber a sequência de 0 a 255 como argumento.

do host $1.$ip: enquanto o valor da variável for entre 0 e 255 irá realizar o loop colocando cada valor como argumento do octeto do endereço IP.

Executando o script:

$ bash reverso.sh 200.19.32

…

```
44.32.19.200.in-addr.arpa domain name pointer selecao.ifms.edu.br.

45.32.19.200.in-addr.arpa domain name pointer sistemas.ifms.edu.br.

46.32.19.200.in-addr.arpa domain name pointer ifms.edu.br.

47.32.19.200.in-addr.arpa domain name pointer siga-adm.ifms.edu.br.

48.32.19.200.in-addr.arpa domain name pointer siga-edu.ifms.edu.br.

48.32.19.200.in-addr.arpa domain name pointer siga-edu-teste.ifms.edu.br.

49.32.19.200.in-addr.arpa domain name pointer suap.ifms.edu.br.
```

Transferência de zonas de DNS

Transferência de zoans de DNS ocorrem quando se faz a transferência do servidor DNS de uma base para outra.

Exemplo dessa necessidade são uma realidade em uma internet com tantas demandas, em qeu servidores de DNS balanceiam sua carga com outros servidores distribuídos.

O que um atacante pode fazer é forçar essa transferência natural de zona de DNS de um servidor oficial para um criado para ataque.

O primeiro passo é verificar os servidores de nomes:

$ host -t NS ifms.edu.br

ifms.edu.br name server ns0.ifms.edu.br.

ifms.edu.br name server ns2.ifms.edu.br.

ifms.edu.br name server ns3.ifms.edu.br.

O passo seguinte é forçar a transferência de zona utilizando o comando host com a opção “- l”, que tenta forçar uma transferência de zona para o nome da zona, que transfere a zona exibindo os registros NS, PTR e endereço A/AAAA na tela.

$ host -l ifms.edu.br ns0.ifms.edu.br.

;; Connection to 200.19.32.24#53(200.19.32.24) for ifms.edu.br failed: timed out.

;; connection timed out; no servers could be reached

;; Connection to 200.19.32.24#53(200.19.32.24) for ifms.edu.br failed: timed out.

$ host -l ifms.edu.br ns2.ifms.edu.br.

;; Connection to 200.203.239.199#53(200.203.239.199) for ifms.edu.br failed: timed out.

;; connection timed out; no servers could be reached

;; Connection to 200.203.239.199#53(200.203.239.199) for ifms.edu.br failed: timed out.

$ host -l ifms.edu.br ns3.ifms.edu.br.

;; Connection to 200.19.32.52#53(200.19.32.52) for ifms.edu.br failed: timed out.

;; connection timed out; no servers could be reached

;; Connection to 200.19.32.52#53(200.19.32.52) for ifms.edu.br failed: timed out.

Automatizando a transferência de zonas

Utilizando Shell Script pode-se automatizar o processo de transferência de zonas.

$ nano transferzone.sh

```
#!/bin/bash

for server in $(host -t ns $1 | cut -d "" -f4);

do

host -l $1 $server;

done
```

Enumeração DNS

Ferramentas de enumeração de DNS são utilizados para pesquisar servidores de nomes e domínios. As ferramentas utilizadas são:

- dig;

- nslookup

- e dnsenum.

dig

O dig é uma ferramenta que vem como parte integrante dos principais sistemas operacionais como Unix, Linux e Windows®. O seu acesso se dá pelo terminal (Unix e Linux) ou prompt de comando (Windows®).

$ dig -t NS ifms.edu.br

```
; <<>> DiG 9.16.1-Ubuntu <<>> -t NS ifms.edu.br

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31868

;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
```

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;ifms.edu.br. IN NS

;; ANSWER SECTION:

ifms.edu.br. 30 IN NS ns2.ifms.edu.br.

ifms.edu.br. 30 IN NS ns3.ifms.edu.br.

ifms.edu.br. 30 IN NS ns0.ifms.edu.br.

;; Query time: 148 msec

;; SERVER: 10.96.0.10#53(10.96.0.10)

;; WHEN: Thu Nov 05 22:30:37 UTC 2020

;; MSG SIZE rcvd: 160

Também é possível realizar transferência de zona com o dig:

$ dig -t axfr guardweb.com.br.

; <<>> DiG 9.16.1-Ubuntu <<>> -t axfr ifms.edu.br

;; global options: +cmd

; Transfer failed.

dnsenum

O dnsenum é uma ferramenta que já vem pré-instalada em praticamente todos as versões dos sistemas operacionais Unix e Linux. Para realizar a consulta basta utilizar o comando:

$ dnsenum –enum ifms.edu.br

dnsrecon

O dnsrecon exibe informações gerais sobre o servidor DNS ou domínio.

$ dnsrecon -d ifms.edu.br

Onde:

-d : indica o domínio a ser consultado.

fierce

O fierce é uma ferramenta que também vem pré-instalada na maioria das versões do Unix/Linux. O comando fierce, usado genericamente, apresenta mais informações sobre o domínio do que os outros comandos anteriores.

$ fierce -dns ifms.edu.br

Dependendo da necessidade de determinadas informações pode ser utilizado apenas uma destas ferramentas quanto todas elas. O uso depende, portanto, do retorno da informações que cada ferramenta retorna.