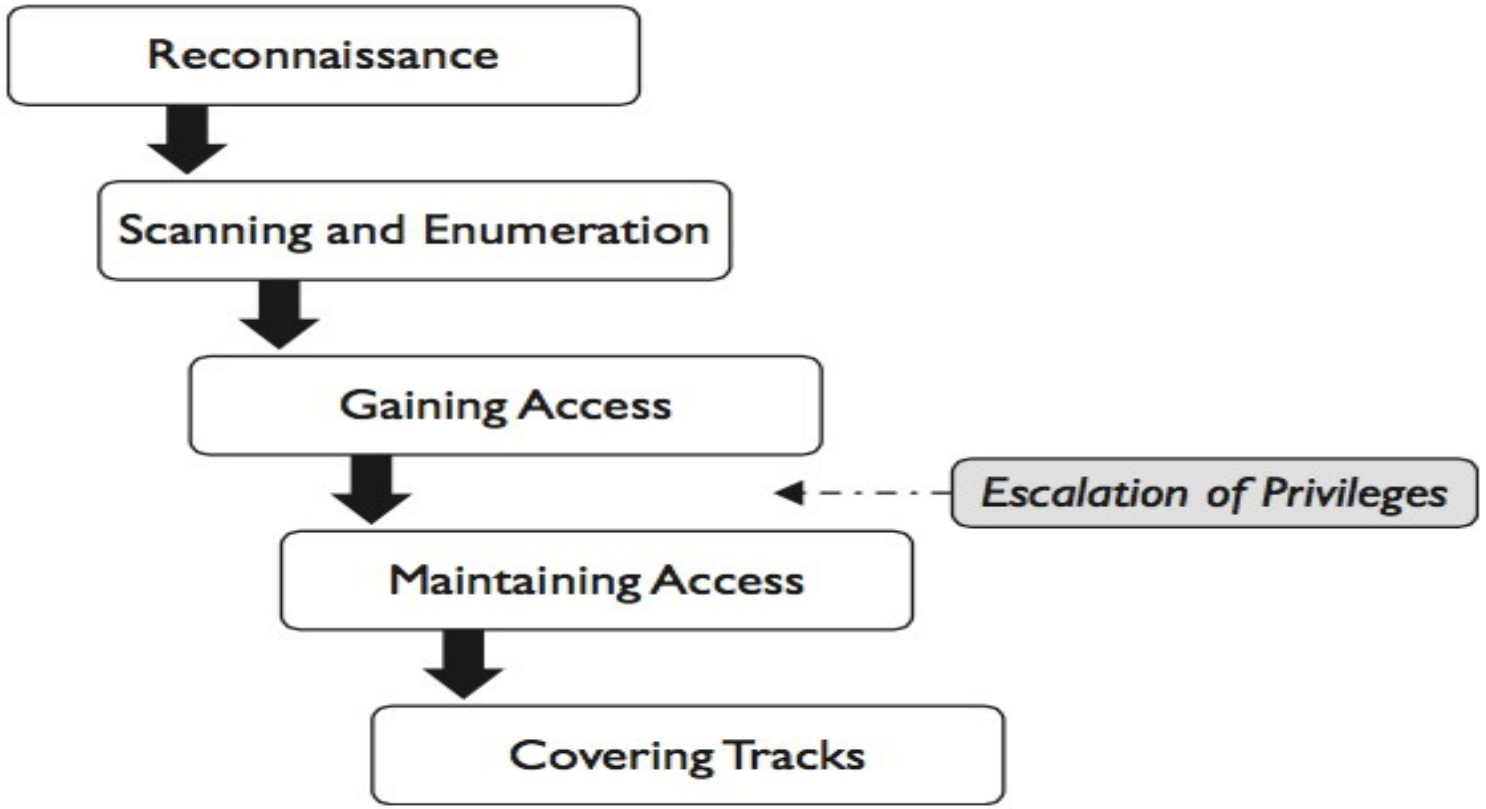
INSTITUTO FEDERAL
São Paulo
Câmpus Barretos

Segurança da Informação

Aula 3

Prof. Lucas

Fases



[Walker, 2014]

Introdução

- Fase que basicamente envolve interação humana e engenharia social

- Engenharia social objetiva convencer pessoas a revelarem informações confidenciais (em alguns casos sem elas perceberem)
- É a prática utilizada para obter acesso a informações importantes/sigilosas em organizações por meio da enganação ou exploração da confiança da pessoa
- Normalmente não tem consciência do valor da informação
- Elemento mais vulnerável é o ser humano: possui traços comportamentais e psicológicos que o torna suscetível a ataques

Dns footprinting

- *Domain Name System*
- DNS faz o mapeamento de um nome para um IP
- Faciliar a navegação

Tipos de Servidores

- Servidor Autoritativo
  - Recebe requisições, responde o endereço caso possua, uma referência caso conheça o caminho da resolução ou uma negação caso não conheça

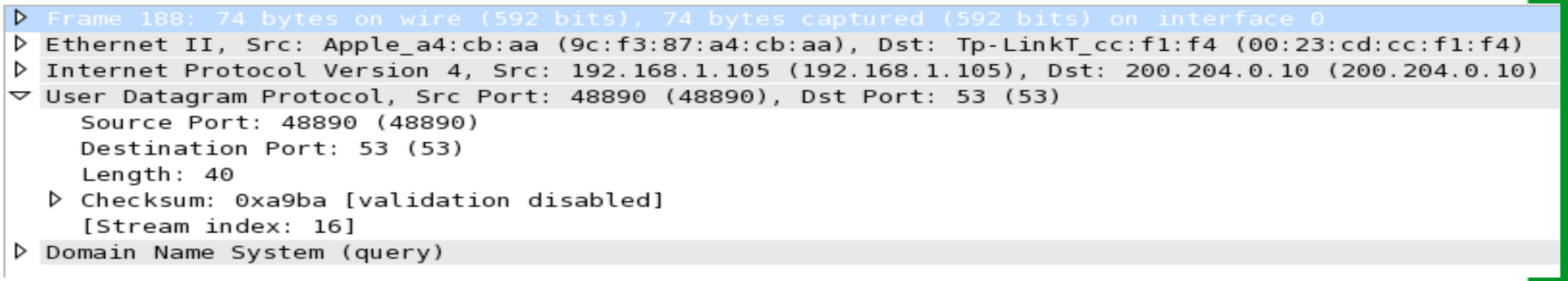
- Servidor Recursivo
  - Recebe requisições e encaminha para os servidores autoritativos e conforme resposta continua a realizar requisições para outros servidores autoritativos até obter resposta satisfatória

Revisão dns

- Composto por vários servidores ao redor do mundo
- Cada servidor mantém e gerencia registros de cada parte do mundo – conhecido como um *namespace*
- Alguns destes registros contém endereços IPs para sistemas individuais, outros contém endereços para servidores de e-mails e outros possuem ponteiros para outros servidores DNS

Revisão Dns

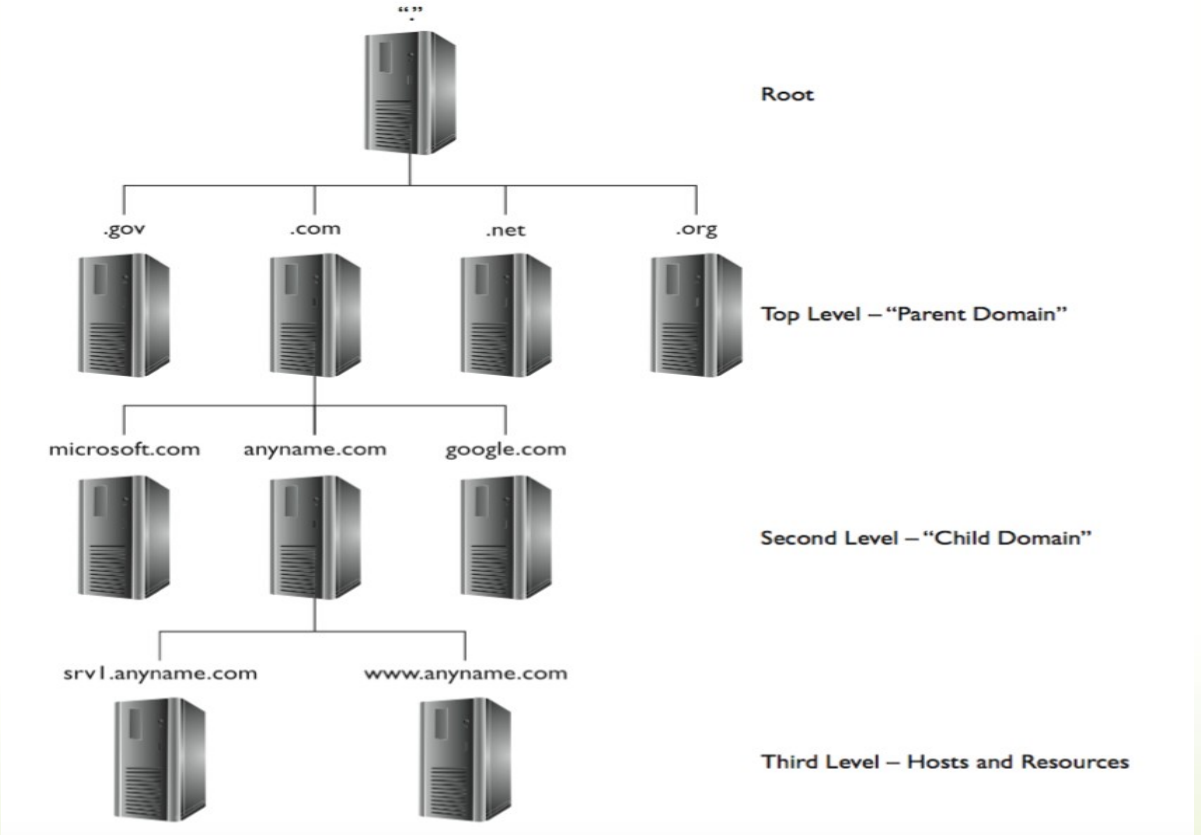
- Utiliza o protocolo UDP porta 53
- Para transferência de zonas é utilizado o TCP



Revisão Dns

- Cada servidor DNS deve preocupar-se apenas com os registros relacionados a sua própria porção do namespace e conhecer como contatar os servidores um nível abaixo

- Estrutura em árvore



[Walker, 2014]

Dns

- É importante (como hacker) conhecer em qual servidor estão os registros de DNS?
- Onde os servidores de e-mail estão?
- Onde os sites estão hospedados?

- Basta analisar os tipos de registros de DNS

Dns

- Tais registros são mantidos e gerenciados por servidores autoritativos (authoritative server) para os *namespaces* (SOA) o qual compartilha as informações com outros servidores DNS

- Tal processo de replicar estes registros é conhecido como transferência de zona (*zona transfer*)

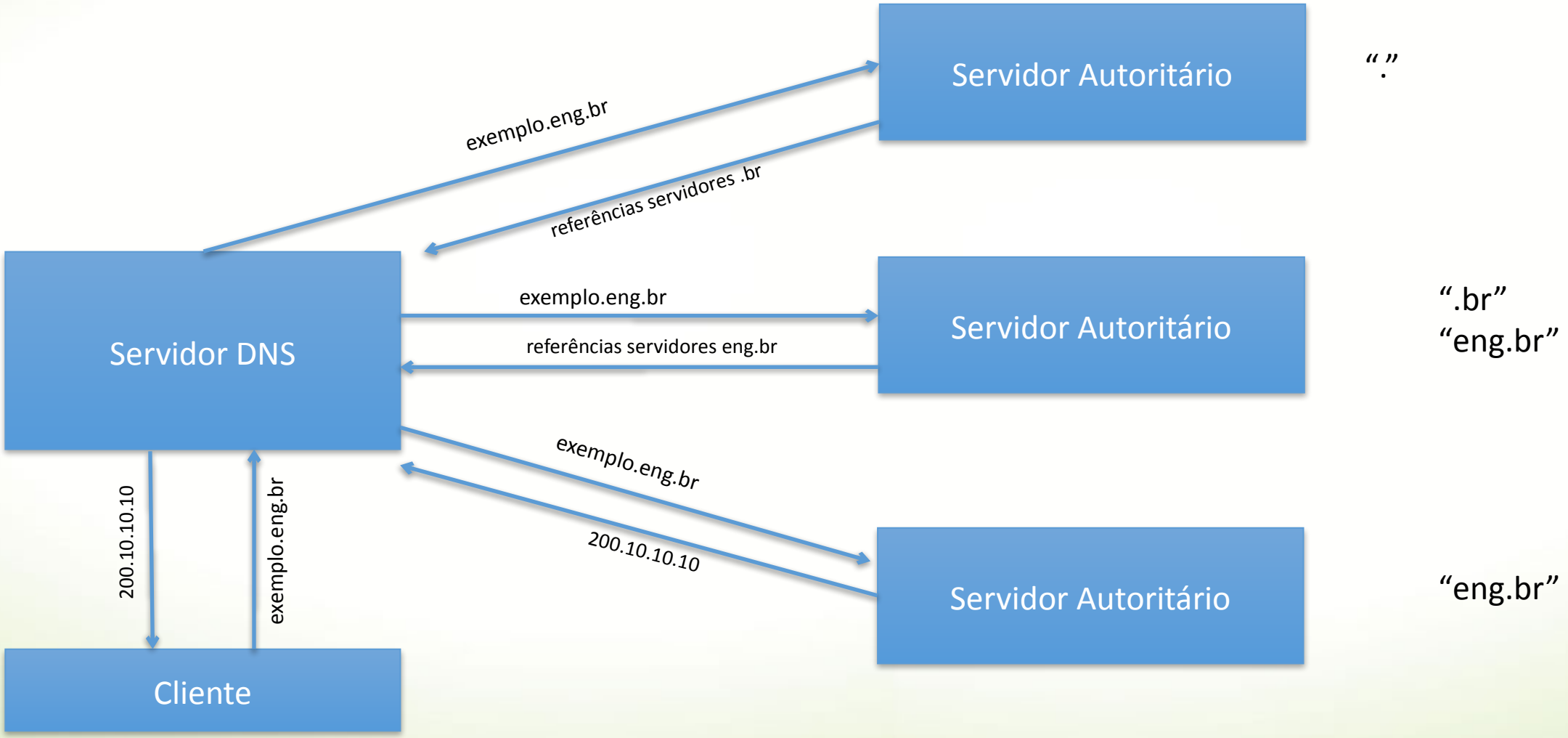
Dns

- Mapeamento estático: C:\Windows\System32\drivers\etc\hosts
- Mapeamento dinâmico: DNS

Tipos de dados

- **SOA** Indica onde começa a autoridade da zona
- **NS** Indica um servidor de nomes para a zona
- **A** Mapeamento de nome a endereço (IPv4)
- **AAAA** Mapeamento de nome a endereço (IPv6)
- **MX** Indica um mail exchanger para um nome (servidor de e-mail)
- **CNAME** Mapeia um nome alternativo
- **TXT** Campo de texto livre

Exemplo de uma consulta



Estrutura

- Servidores raiz (13 no mundo)
- Domínios de primeiro nível (TDL – *Top level domain*)
- Domínios de segundo nível (fácil de conseguir)

- http://www.root-servers.org/

Forma de Proteção

- DNSSEC: **D**omain **N**ame **S**ystem **SEC**urity extensions

- Estende a tecnologia DNS
- Reduz o risco de manipulação de dados
- Baseado na tecnologia de criptografia de chaves públicas

Simulação de um ataque

- DNS poisoning
- Antes da consulta externa, o SO consulta seu cache local e o arquivo hosts
- O exercício é alterar este arquivo hosts e acessar o site
- Comandos:
  - ipconfig /displaydns
  - ipconfig /flushdns

RIRs

[Walker, 2014]

Ferramentas

- Smartwhois
- http://www.geektools.com/whois.php
- www.dnsstuff.com

- E o que e contato da pessoa pode ajudar?
  - www.spoofcard.com

INSTITUTO FEDERAL
São Paulo

Ferramentas

- Comando `nslookup`

```
nslookup [-options] {hostname | [-server]}
```

- Pode ser executado em modo interativo
- Por exemplo:

```
nslookup
set query=MX
<domínio>
```

Tal comando procura por registros de servidores de e-mail

Outro exemplo

```
nslookup
server <ip_address>
set type=any
ls –d domainname.com
```

Se receber um erro, o administrador configurou corretamente!

Outra ferramenta

- Comando dig
- `dig @server name type`
- `server` é o nome ou IP do servidor DNS
- `name` é o nome do recurso que está procurando
- `type` é o tipo de registro

INSTITUTO FEDERAL
São Paulo

traceroute

- `traceroute (tracert) <IP>`

- Ou ferramentas visuais
  - Neotrace
  - Trout
  - VisualRoute

Google hacking

- Popularizou-se em 2004 com Johnny Long
- Buscas utilizando operadores do próprio site
- Pesquisas envolvem descobrir sistemas com acesso remoto ou históricos de páginas com o MySQL, entre outros
- Envolve manipular string de busca para encontrar vulnerabilidades

Google hacking

Operator	Syntax	Description
cache	**cache**:*URL [string]*	Searches through Google's cache for information on a specific site (version) or for returns on a specific word or phrase (optional string). For example, the following will display Google's cache version of the page: `cache:www.mcgraw-hill.com`
filetype	**filetype:***type*	Searches only for files of a specific type (DOC, XLS, and so on). For example, the following will return all Microsoft Word documents: `filetype:doc`
index of	**index of** */string*	Displays pages with directory browsing enabled, usually used with another operator. For example, the following will display pages that show directory listings containing *passwd*: `"intitle:index of" passwd`
info	**info:***string*	Displays information Google stores about the page itself: `info:www.anycomp.com`

intitle	**intitle**:*string*	Searches for pages that contain the string in the title. For example, the following will return pages with the word *login* in the title:
		`intitle: login`
		For multiple string searches, you can use the allintitle operator. Here's an example:
		`allintitle:login password`

inurl	**inurl**:*string*	Displays pages with the string in the URL. For example, the following will display all pages with the word *passwd* in the URL:
		`inurl:passwd`
		For multiple string searches, use allinurl. Here's an example:
		`allinurl:etc passwd`

link	**link**:*string*	Displays linked pages based on a search term.
related	**related:***webpagename*	Shows web pages similar to *webpagename*.
site	**site:***domain or web page string*	Displays pages for a specific website or domain holding the search term. For example, the following will display all pages with the text *passwds* in the site anywhere.com: site:anywhere.com passwds

INSTITUTO FEDERAL
São Paulo

Google hacking

- Exemplos:
  - `site:gov.br ext:sql` — Busca por arquivos de base de dados em sites do governo
  - `inurl:e-mail filetype: mdb` — Arquivos de e-mail em formato .mdb
  - `intitle:VNC inurl:5800 intitle:VNC` — Encontrando VNC
  - `”Active Webcam Page” inurl:8080` — Encontrando webcam ativa
  - etc

INSTITUTO FEDERAL
São Paulo

Google hacking

- https://www.exploit-db.com/google-hacking-database

- http://www.hackersforcharity.org/ghdb/

- Tente a seguinte pesquisa no google:
  - allinurl:tsweb/default.htm

  - Procura páginas com o acesso remoto habilitado

Google hacking

- http://it.toolbox.com/blogs/managing-infosec/google-hacking-master-list-28302
- “intitle:index of” musica.mp3
- “intitle:Nessus Scan Report” “This file was generated by Nessus”

Exemplo Web Cam

- intitle:"WEBCAM 7 " -inurl:/admin.html
- intitle:"webcamXP 5" inurl:8080 'Live’
- etc

INSTITUTO FEDERAL
São Paulo

IP logger

- https://iplogger.org/
- https://blasze.com/
- Informações das pessoas que acessarem determinado link

- Pode ofuscar depois pelo https://bitly.com/

- Crie um URL para www.google.com

INSTITUTO FEDERAL
São Paulo

The harvester

- ”colheita”
- Digitar `theharvester options`
- `theharvester -d www.ifsp.edu.br -l 200 -b all`

INSTITUTO FEDERAL
São Paulo

Maltego – interface gráfica

- Digitar `maltego`
- Versão paga e gratuita (limita os resultados)
- Deve registrar primeiro

- Ferramenta de mineração de dados
- Para pentest é necessário a versão paga!

Whatweb

- Identifica no website plataformas e serviços
- Digitar `whatweb <site>`

INSTITUTO FEDERAL
São Paulo

dmitry

- *Deepmagic Information Gathering Tool*
- Ferramenta escrita em C
- Engloba várias funções
- https://mor-pah.net/
- Digitar `dmitry`
- Exemplos:
- `dmitry -w <site>`

urlcrazy

- Traz urls que parecem com o original
- Digitar: `urlcrazy google.com`

INSTITUTO FEDERAL
São Paulo

hping3

- Digitar `hping3 –h`
- Exemplos:
- `hping3 –S <IP> -p 80`
- `hping3 --tcp-timestamp –S <site> -p 80`
- -S ativa a flag syncronize
-
- Pode usar o tcpdump em outro terminal para acompanhar as respostas:
- `tcpdump -i <interface> host IP`

dnsmap

- Descobrir subdomínios
- Digitar `dnsmap google.com`

INSTITUTO FEDERAL
São Paulo

shodan

- shodan.io
- Motor de busca. Procura por banners de serviços.
- Ajuda a encontrar: roteadores, desktops, switches, webcam, etc
- Exemplos:
- `webcam country:BR`
- `apache hostname:.gov.br`
- `apache 2.2.3 hostname:.gov.br`
- `country:BR OS:xp`
- `country:BR port:5900`

- Obs.: Explore a ferramenta censys

INSTITUTO FEDERAL
São Paulo

Exercícios

1. Explore as ferramentas: `maltego`, `shodan` e `hping3`. Teste alguma opção não apresentada na aula.

   Enviar o print no moodle!

INSTITUTO FEDERAL
São Paulo