

**INSTITUTO  
FEDERAL**

São Paulo

---

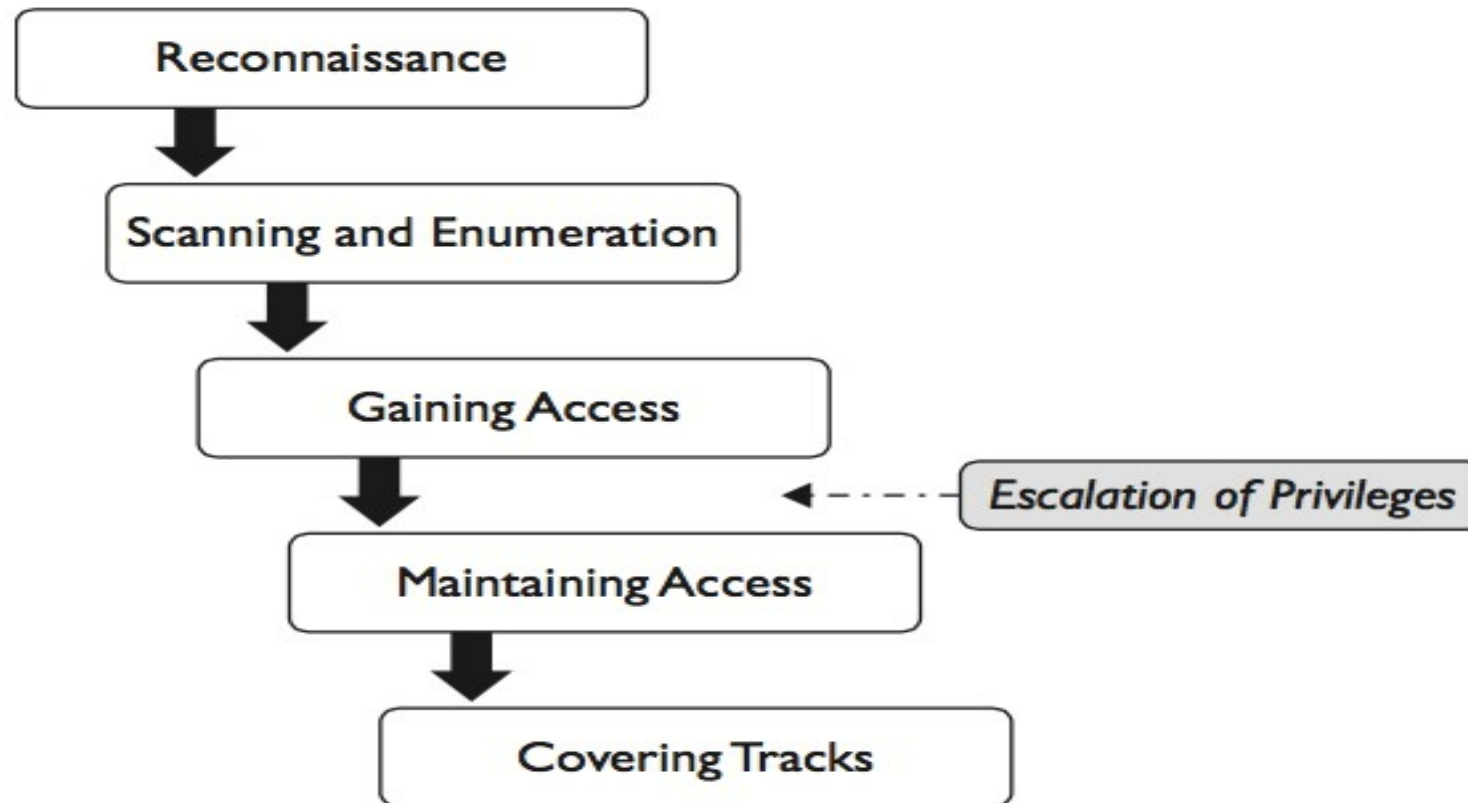
Câmpus  
Barretos

# Segurança da Informação

## Aula 2

**Prof. Lucas**

# Fases - Pen Test



# Tipos de Pen Test

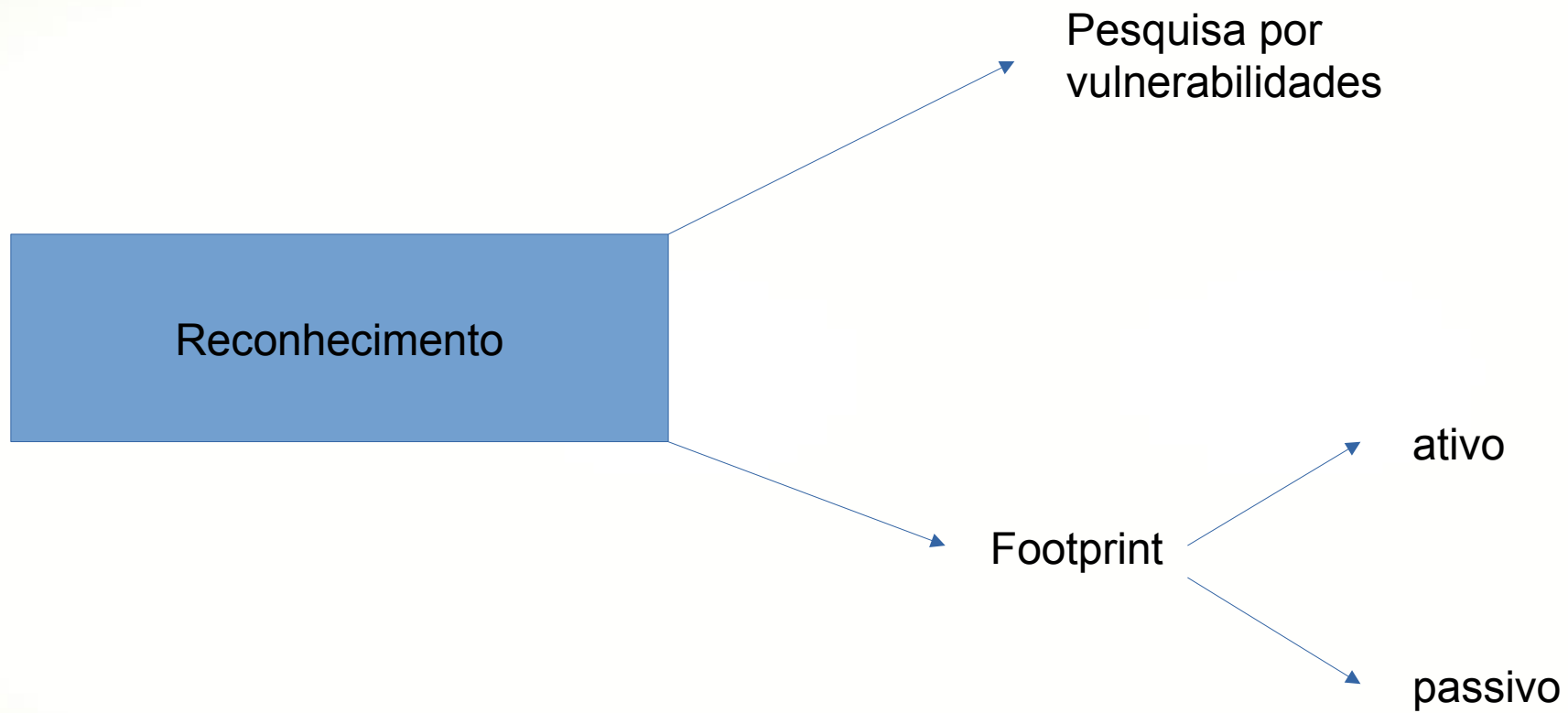
- Conhecido:
  - Trabalha junto com a organização para identificar potenciais brechas de segurança
  - pessoal de TI apresentam-lhe os sistemas
  - tem acesso liberado às informações internas da empresa
  - é mais fácil de fazer (você tem a informação), porém resulta facilmente num trabalho viciado
- Secreto
  - tem a finalidade de simular um ataque real (pega o pessoal de TI de surpresa)
  - testa também o time de segurança da organização
  - testes custosos e mais complexos devido a ausência de informação
  - apaixonados pela área preferem assim

# Outras metodologias de pen test

- Alguns modelos/guias
- PTES: Penetration Testing Execution Standard
  - [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page)
- NIST 800-115
  - <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- OSSTMM: Open source security testing methodology manual
  - <https://www.isecom.org/OSSTMM.3.pdf>
- OWASP: Open web application security project
  - [https://owasp.org/www-project-web-security-testing-guide/latest/3-The\\_OWASP\\_Testing\\_Framework/1-Penetration\\_Testing\\_Methodologies](https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies)
- PCI: Penetration testing guide
  - [https://listings.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1\\_1.pdf](https://listings.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf)

# Introdução

- Não se trata apenas da fase inicial
- Fase que já envolve uma certa habilidade
- Que tipo de informação devemos procurar?
- Como pegá-las?



# Pesquisas de vulnerabilidades

- Conhecer as principais (atuais) vulnerabilidades torna sua vida mais fácil
- Objetiva não executar ferramentas de vulnerabilidades, mas sim obter informações (preocupação principal do analista de segurança)
- Fase vital (extremamente relevante)

# Pesquisas de vulnerabilidades

- Ameaça *zero-day*: Quando os responsáveis desconhecem um ataque que explora alguma vulnerabilidade
- Para descobrir tais vulnerabilidades, é necessário pesquisá-las e verificar quais recomendações estão sendo dadas
- Envolve pesquisas (pró-ativo) para mantê-lo atualizado
  - Uma notícia em um site comum provavelmente já estava disponível há muito tempo em um site de vulnerabilidade!



# Pesquisas de vulnerabilidades

- Sites para manter em seus favoritos:

- <http://www.eccouncil.org/>
- <http://blogs.technet.com/>
- <https://www.exploit-db.com/>
- <https://nvd.nist.gov>
- <http://www.securiteam.com/>
- <http://secunia.com/>
- <http://hackerstorm.co.uk/>
- <http://www.hackerwatch.org/>
- <http://www.securityfocus.com/>
- <http://www.securitymagazine.com/>
- <http://www.scmagazine.com/>
- <http://www.digitalattackmap.com/>
- <http://www.zerodayinitiative.com/>

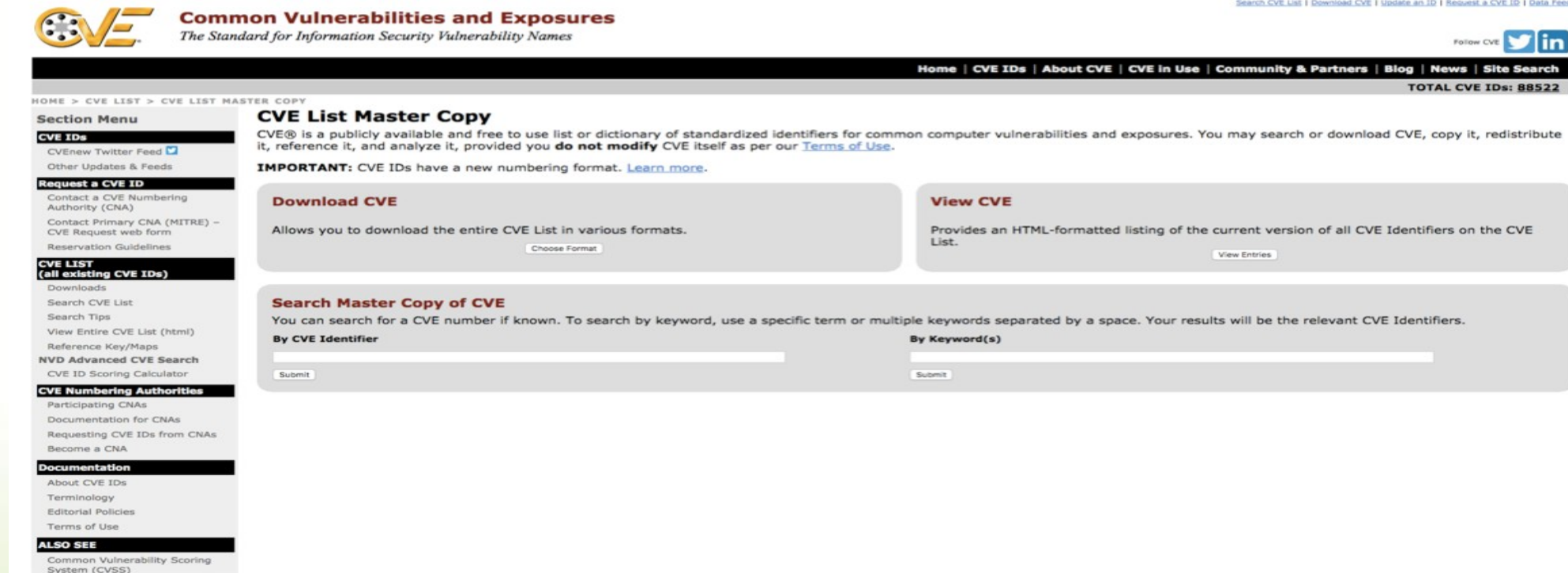
português

\*detalha forma de pagamento caso alguém encontre uma vulnerabilidade

Esta fase não objetiva encontrar vulnerabilidades no seu alvo! Apenas trata de manter uma base sólida de conhecimentos

# Pesquisas de vulnerabilidades

- CVE
- Projeto financiado pelo governo americano e mantido pela empresa MITRE
- Listagem padrão de vulnerabilidades <http://cve.mitre.org/>



The screenshot shows the CVE website interface. At the top, the CVE logo is displayed next to the text "Common Vulnerabilities and Exposures" and "The Standard for Information Security Vulnerability Names". A navigation bar includes links for Home, CVE IDs, About CVE, CVE in Use, Community & Partners, Blog, News, and Site Search. The main content area is titled "CVE List Master Copy" and explains that CVE is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures. It provides instructions on how to search or download CVE, copy it, redistribute it, reference it, and analyze it, provided you do not modify CVE itself as per their Terms of Use. An important note states that CVE IDs have a new numbering format, with a link to learn more. Below this, there are two main sections: "Download CVE" and "View CVE". The "Download CVE" section allows users to download the entire CVE List in various formats, with a "Choose Format" button. The "View CVE" section provides an HTML-formatted listing of the current version of all CVE Identifiers on the CVE List, with a "View Entries" button. At the bottom, there is a "Search Master Copy of CVE" section, which allows users to search for a CVE number if known, or by keyword. It includes input fields for "By CVE Identifier" and "By Keyword(s)", and "Submit" buttons. A sidebar on the left contains a "Section Menu" with links to CVE IDs, Request a CVE ID, CVE LIST (all existing CVE IDs), NVD Advanced CVE Search, CVE Numbering Authorities, Documentation, and ALSO SEE.

# Footprinting

- Qualquer informação do alvo (não importa se grande ou pequena)
- Não necessariamente ser uma informação técnica
- Antes de conhecer a arquitetura de rede, aplicações e web-sites ou segurança física, devemos perguntar:
  - Regras de negócios
  - Objetivo e missão da empresa
- Informações dos próprios empregados

# Definição

*“Footprinting is defined as the process of gathering information on computer systems and networks. It is the first step in information gathering and provides a high-level blueprint of the target system or network. It is all about gathering as much information as possible – usually easy-to-obtain, readily available information.”*

[Walker,2014]

# Footprinting

- Cuidado ao coletar muitos dados!
- Dividido em 2 categorias:
  - *Footprinting* ativo: Significa que o hacker terá que “tocar” nos dispositivos, rede ou recursos
  - *Footprinting* passivo: Coletar informações de fontes públicas

# Footprinting passivo

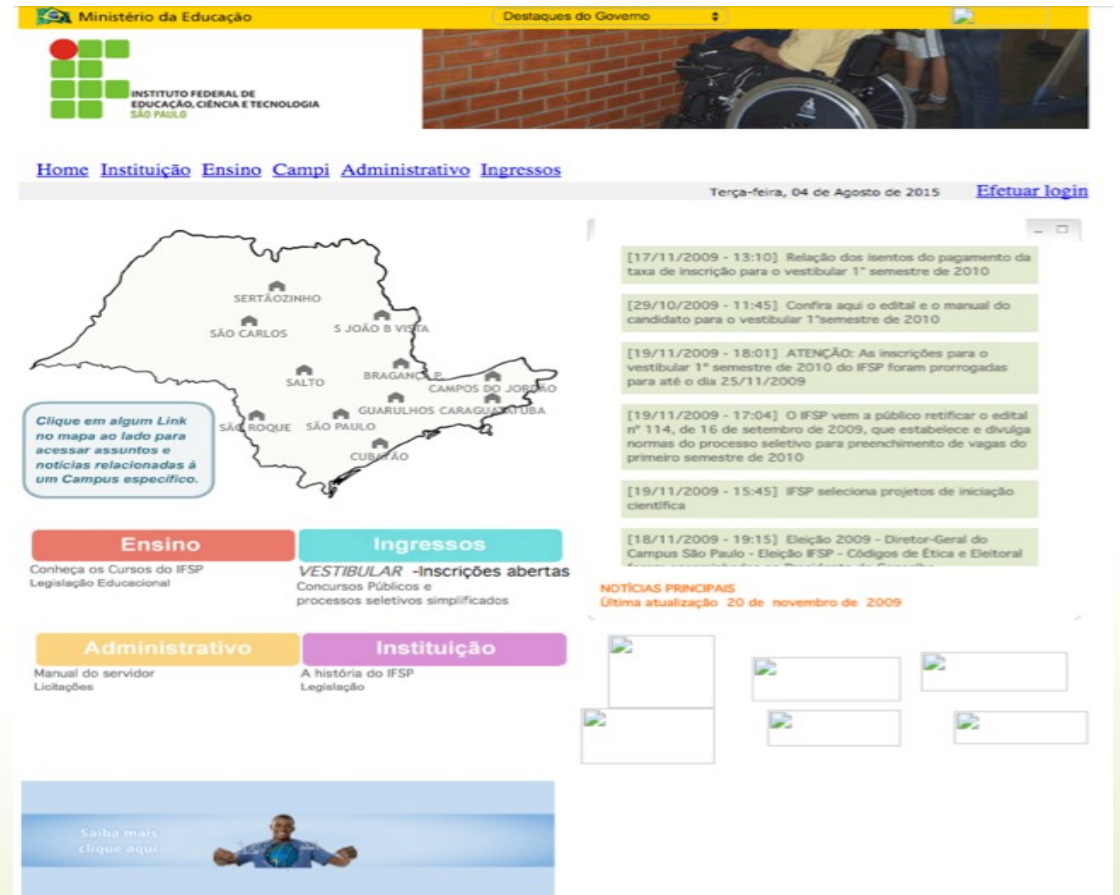
- Requer menos esforço
- Qualquer informação que está acessível publicamente
- Mecanismos de buscas, sites de redes sociais, eventos populares, *range* da rede, informação de DNS, sites de emprego, etc...

# Footprinting passivo

- Web mirroring
  - <http://www.httrack.com/>
  - <http://www.gnu.org/>
  - <http://www.spadixbd.com/>

# Footprinting passivo

- Históricos dos sites
  - [www.archive.org](http://www.archive.org)
- Google cache



The screenshot shows the official website of the Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP). The header includes the logo of the Instituto Federal de Educação, Ciência e Tecnologia de São Paulo and the text "Ministério da Educação" and "Destaque do Governo". The main navigation bar contains links: Home, Instituição, Ensino, Campi, Administrativo, and Ingressos. The date "Terça-feira, 04 de Agosto de 2015" and a login link "Efetuar login" are displayed. The central content area features a map of São Paulo state with markers for various IFSP campuses: Sertãozinho, São Carlos, S. João B. Vieira, Bragança, Campos do Jordão, Salto, Guarulhos, Caraguatatuba, São Roque, São Paulo, and Cubatão. A text box next to the map says: "Clique em algum Link no mapa ao lado para acessar assuntos e notícias relacionadas à um Campus específico." Below the map are four main sections: "Ensino" (Conheça os Cursos do IFSP, Legislação Educacional), "Ingressos" (VESTIBULAR - inscrições abertas, Concursos Públicos e processos seletivos simplificados), "Administrativo" (Manual do servidor, Licitações), and "Instituição" (A história do IFSP, Legislação). On the right side, there is a "NOTÍCIAS PRINCIPAIS" section with a list of recent news items, each with a date and time stamp. At the bottom, there is a banner with the text "Saiba mais clique aqui" and an image of a person.



# Footprinting passivo

- Visualizar códigos HTML das páginas
- Procurar por “hidden” campos
- Cookies
- Informações nos cabeçalhos dos e-mails

Delivered-To: [REDACTED]@gmail.com  
Received: by 10.31.183.200 with SMTP id h191csp53203vkf;  
Tue, 4 Aug 2015 12:19:53 -0700 (PDT)  
X-Received: by 10.170.198.144 with SMTP id pl38mr5605878yke.70.1438715992839;  
Tue, 04 Aug 2015 12:19:52 -0700 (PDT)  
Return-Path: [REDACTED]@ifsp.edu.br  
Received: from email.ifsp.edu.br (email.ifsp.edu.br. [200.133.214.45])  
by mx.google.com with ESMTP id p125si396232ywb.45.2015.08.04.12.19.52  
for [REDACTED]@gmail.com>;  
Tue, 04 Aug 2015 12:19:52 -0700 (PDT)  
Received-SPF: pass (google.com: domain [REDACTED]@ifsp.edu.br designates 200.133.214.45 as permitted sender) client-ip=200.133.214.45;  
Authentication-Results: mx.google.com;  
spf=pass (google.com: domain of [REDACTED]@ifsp.edu.br designates 200.133.214.45 as permitted sender) smtp.mail=ba121496@ifsp.edu.br;  
dkim=pass header.i=@ifsp.edu.br;  
dmarc=pass (p=NONE dis=NONE) header.from=ifsp.edu.br  
Received: from localhost (localhost [127.0.0.1])  
by email.ifsp.edu.br (Postfix) with ESMTP id 6E692166C23  
for [REDACTED]@gmail.com>; Tue, 4 Aug 2015 16:19:51 -0300 (BRT)  
Received: from email.ifsp.edu.br ([127.0.0.1])  
by localhost (email.ifsp.edu.br [127.0.0.1]) (amavisd-new, port 10032)  
with ESMTP id 7HlW\_7LqvPcj for [REDACTED]@gmail.com>;  
Tue, 4 Aug 2015 16:19:46 -0300 (BRT)  
Received: from email.ifsp.edu.br (localhost [127.0.0.1])  
by email.ifsp.edu.br (Postfix) with ESMTP id A198616B1AD  
for [REDACTED]@gmail.com>; Tue, 4 Aug 2015 16:19:46 -0300 (BRT)  
DKIM-Filter: OpenDKIM Filter v2.9.2 email.ifsp.edu.br A198616B1AD  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=ifsp.edu.br;  
s=F67E9BF8-6F46-11E4-B529-30183D1F85CC; t=1438715986;  
bh=RvMwPWDjXEWQILQ4dgiRoSVFPjy7yvayY+TitMh9Dv0=;  
h=Date:From:To:Message-ID:Subject:MIME-Version:Content-Type;  
b=ilriRd27Ob5ki7F1mBjy40xbvYV8BAUDLTCKcMjh03ilgRZwl7AX6M+akitykjhg  
lxsS8QtIYn5XMjVFdfIY8NUWrgIb9Ji2bgutPfYxA/vdEwb0Y7WzztwkfyPiNQW33B  
SnltQEvvhFmThuMKmocBVqUD4oOvyi7YpuXqwgqLo=  
Received: from email.ifsp.edu.br (localhost [127.0.0.1])  
by email.ifsp.edu.br (Postfix) with ESMTP id 9CB9516B152  
for [REDACTED]@gmail.com>; Tue, 4 Aug 2015 16:19:46 -0300 (BRT)  
[REDACTED]@ifsp.edu.br  
[REDACTED]@ifsp.edu.br  
Subject: teste  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
boundary="-----\_Part\_1298245\_994179362.1438715986582"  
X-Originating-IP: [189.79.245.28]  
X-Mailer: Zimbra 8.0.9\_GA\_6191 (ZimbraWebClient - GC44 (Mac)/8.0.9\_GA\_6191)  
Thread-Topic: teste  
Thread-Index: tvHxXceLevo7Py3q5zF6n7vX0gvasA==  
  
-----\_Part\_1298245\_994179362.1438715986582  
Content-Type: text/plain; charset=utf-8  
Content-Transfer-Encoding: 7bit  
  
teste  
  
-----\_Part\_1298245\_994179362.1438715986582  
Content-Type: text/html; charset=utf-8  
Content-Transfer-Encoding: 7bit  
  
<html><body><div style="font-family: times new roman, new york, times, serif; font-size: 12pt; color: #000000"><div>teste</div></div></body></html>  
-----\_Part\_1298245\_994179362.1438715986582--

## Whois

189.79.245.28

CONSULTAR

Versão com informações de contato

% Copyright (c) Nic.br  
% A utilização dos dados abaixo é permitida somente conforme  
% descrito no Termo de Uso em <http://registro.br/termo> , sendo  
% proibida a sua distribuição, comercialização ou reprodução,  
% em particular para fins publicitários ou propósitos  
% similares.  
% 2015-08-04 16:26:03 (BRT -03:00)

inetnum: 189.78/15  
asn: AS27699  
c-abusos: ENRED4  
titular: TELEFÔNICA BRASIL S.A  
documento: 002.558.157/0001-62  
responsável: Diretoria de Planejamento e Tecnologia  
país: BR  
c-titular: ARITE  
c-técnico: ARITE  
inetrev: 189.78/15  
servidor DNS: orion.vivo.com.br  
status DNS: 03/08/2015 AA  
último AA: 03/08/2015  
servidor DNS: lynx.vivo.com.br  
status DNS: 03/08/2015 AA  
último AA: 03/08/2015  
servidor DNS: hercules.vivo.com.br  
status DNS: 03/08/2015 AA  
último AA: 03/08/2015  
servidor DNS: aquarius.vivo.com.br  
status DNS: 03/08/2015 ERR  
último AA: 27/07/2015  
criado: 09/11/2007  
alterado: 07/03/2013

Contato (ID): ARITE  
nome: Administração Rede IP Telesp  
e-mail: dominios-vivo.br@telefonica.com  
criado: 07/04/2008  
alterado: 17/04/2014

Contato (ID): ENRED4  
nome: Engenharia de Redes

# Footprinting passivo

- Ferramentas de e-mail tracking
  - Read Notify
  - WhoReadMe
  - MSGTAG
  - Trace Email
  - Zendio
- Capture o cabeçalho de um e-mail e cole no site <http://www.ip2location.com/free/email-tracer>

# Footprinting passivo

- Outras ferramentas disponíveis:
  - Google Alerts
  - Yahoo Site Explorer
  - SpyFu
  - Quarkbase
  - DomainTools.com
- Ou simplesmente pesquise por **footprint tool** !



# Footprinting passivo - resumo

- Pegue informações que farão sentido posteriormente
- Atividades tipicamente legais (do ponto de vista da lei)

# Exercícios

1-Tente executar a ferramenta Foca e faça o download de todos os documentos pdf de algum site . Em seguida, explore os metadados apresentados.

Envie o print da ferramenta em execução no moodle.

Links:

<https://github.com/ElevenPaths/FOCA>

<https://www.youtube.com/watch?v=Ou4TRvzYpVk>