Pentest (Teste de penetração) - básico para administração de servidores de rede

Professor Anderson Alves de Albuquerque

IFRJ campus Arraial do Cabo

- Bacharelados:
  - Engenharia Industrial Elétrica Eletrotécnica;
  - Engenharia Industrial Elétrica de Telecomunicações;
  - Ciência da Computação.
- Mestrado:
  - Informática.
- Pós Graduações:
  - Análise e Projeto de Sistema;
  - Gestão em Tecnologia da Informação e Comunicação;
  - Docência na educação profissional de nível técnico.

10/10/2020

Experiências

CEFET/RJ

CBPF
Centro Brasileiro de Pesquisas Físicas

Rede Rio 2

RNP
REDE NACIONAL DE ENSINO E PESQUISA

NCE UFRJ
Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

RIO PREFEITURA
IPLANRIO

UFRJ

UFRJ TIC

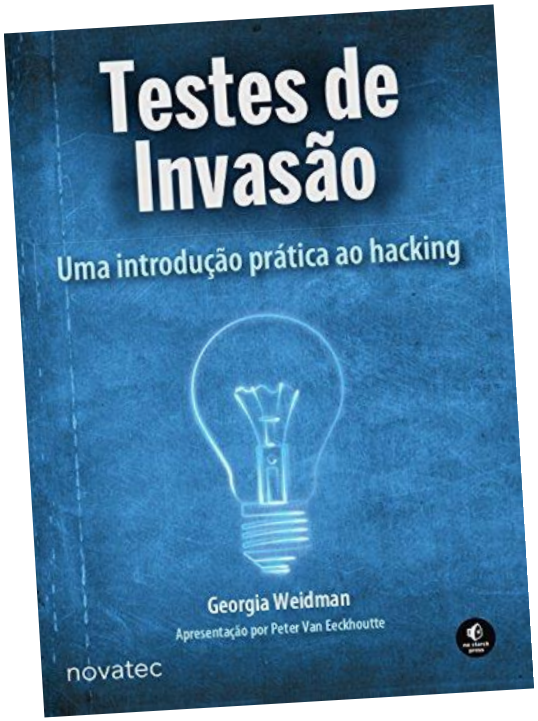
INSTITUTO FEDERAL
Rio de Janeiro
Campus Arraial do Cabo

solaris

QNX, VMS, Irix, NetBSD e AIX

Referências Bibliográficas Principais

Referências Bibliográficas Principais



Objetivo da palestras

- **Visão geral sobre Pentest (Teste de Penetração):**
  - Foco em servidores de rede (Linux);
  - Perceber a importância de verificar o ambiente computacional.

- **Observação:**
  - Pentest não é para ser utilizado para invasões, crimes, etc;
  - Pentest é para avaliar e medir a segurança de um ambiente, sendo utilizada para aumentar a segurança e sanar os problemas encontrados;
  - Previamente, sempre adquira autorização;
  - Siga as leis, normas e qualquer legislação vigente.

- **Público alvo:**
  - Administradores de rede ou servidores;
  - Desenvolvedores que precisam avaliar o ambiente.

Antes de começar

- **Lei 12.737 de novembro/2012:**

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

- **Qualquer teste precisa ser autorizado:**
  - Documento com permissão: assinado seguindo as exigências legais do setor da empresa.

Antes de começar

- **Outras Leis:**
  - **LGPD (Lei Geral de Proteção de Dados Pessoais);**
  - **Lei de acesso à informação:**
    - Lei nº 12.527 de novembro de 2011.
  - **Marco civil da Internet;**
  - **Leis pertinentes ao poder público e seus órgãos.**

- **Curiosidade:**
  - **Glossário:** https://www.in.gov.br/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663

Motivação

- **Conhecer os riscos do negócio e mitigá-los;**

- **Minimizar preventivamente os impactos aos 3 pilares da segurança da informação:**
  - Confidencialidade;
  - Integridade;
  - Disponibilidade.

Dificuldade

Linux para PenTest

- **Kali Linux**

- **Pentoo Linux;**
- **Parrot Security OS;**
- **Back Box;**
- **BlackArch;**
- **Cyborg Hawk;**
- **DHstrike;**
- **Live Hacking OSEFT Linux;**

- **Lista com várias distros:**
  - https://terminalroot.com.br/2019/12/as-22-melhores-distros-linux-para-hackers-pentesting.html
  - https://diolinux.com.br/2015/05/melhores-distros-linux-para-pentest.html

Teste de invasão

- **Procedimento de análise do nível de segurança de um sistema ou rede usando a perspectiva de um infrator.**

- **Nunca realize testes sem a devida autorização:**
  - Falta de ética;
  - Implicações penais.

- **Tipos de Pentest:**
  - ***Blind:*** auditor não recebe informações do alvo, mas o alvo sabe que será atacado e sabe o que será feito;

  - ***Double Blind:*** o auditor não recebe informações do alvo, o alvo também não sabe que será atacado;

Teste de invasão

- **Tipos de Pentest:**
  - ***Gray Box:*** o auditor tem conhecimento parcial do alvo. O alvo sabe que será atacado, mas pode saber os testes que serão feitos;
  - ***Double Gray Box:*** similar ao Gray Box, mas o alvo não sabe os teste que serão realizados;
  - ***Tandem* (caixa de cristal):** o auditor sabe muito do alvo. O alvo sabe que será atacado e sabe o que será realizado nos teste;
  - ***Reversal* (equipe de resposta de incidente):** o auditor sabe muito do alvo. O alvo não sabe que será atacado.

Fases do teste de invasão

1. Levantamento de informações;
2. Coleta / Varredura;
3. Conquistar o acesso;
4. Continuar acessando;
5. Apagar os rastros.

Fases do teste de invasão

1. **Levantamento de informações;**
2. **Coleta / Varredura;**
3. **Conquistar o acesso;**
4. ~~**Continuar acessando**~~**;**
5. ~~**Apagar os rastros**~~**.**

Adaptação para um caso fictício.
Impacto nulo na prática.

Motivo:

- Impacto ao bem protegido pode ser nocivo/perigoso.

Esses itens serão mencionados, mas não serão mostrados na prática.

Motivo:

- Impacto ao bem protegido pode ser nocivo/perigoso.

Fases do teste de invasão

- **Foram listadas 5 fases no teste de invasão:**

- **Até que ponto devo ir?**
  - Tudo precisa acordado com a alta gestão;
  - Tudo precisa ser documentado e assinado;
  - Efeitos colaterais podem surgir: faça um plano de contingência, *backups*, medidas de recuperação e tudo mais que for possível;
  - Cuidado com alguns setores por ter legislação especial: médicos, bancários, poder judiciário, etc.

1. Levantamento de informações

- **As informações obtidas são utilizadas no planejamento.**
- **Neste caso, as informações podem ser obtidas:**
  - Google e redes sociais;
  - Serviços como *Whois*, repositório de sites web, etc;
  - Lixo;
  - Sondar pessoas, familiares, comerciantes próximos, etc;
  - Observação.

- **Informações:**
  - Nomes das pessoas e cargos;
  - Rotinas;
  - Sites e sistemas utilizados;
  - Empresas parcerias, terceirizadas e concorrentes;
  - Outras informações.

1. Levantamento de informações

- **Sites com testes de rede (alguns são considerados na fase de varredura):**
  - https://ipok.com.br/.
- **Serviço Whois:**
  - https://whois.domaintools.com;
  - https://registro.br/tecnologia/ferramentas/whois;
  - https://uolhost.uol.com.br/consulta-whois.html.
- **Base de dados com os sites no decorrer do tempo:**
  - https://archive.org/web/.
- Verifique se os e-mail importantes estão em sites de vazamento de senhas:
  - Em caso de problema com alguma conta é importante => solicitar a troca periódica e forçar senhas segura. Avise as pessoas afetadas porque as vezes as mesmas senhas são utilizadas em outros locais;
  - Exemplos de e-mails (tanto coorporativos como os funcionais e pessoais): diretoria, presidência, gerencias, suporte, ouvidoria, administração de sistemas e setores, etc.
  - [redacted]
  - [redacted]

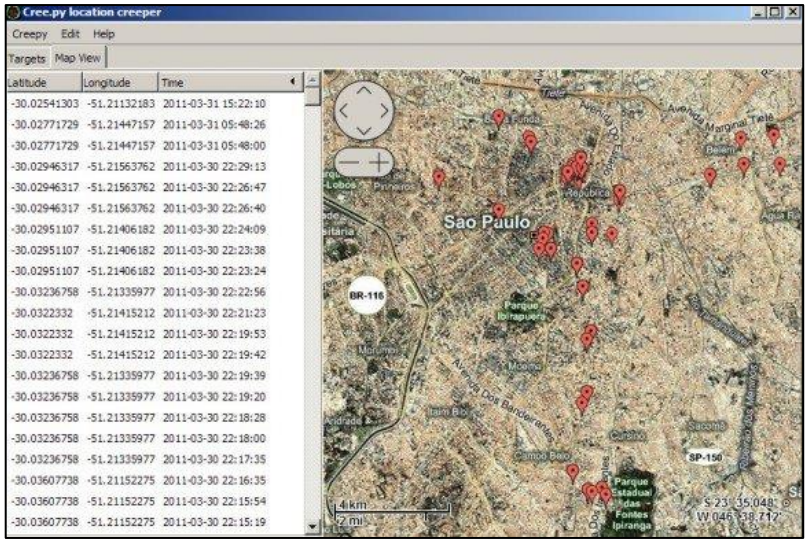
1. Levantamento de informações

- **NetWork Connect Log:**
  - https://www.nirsoft.net/utils/network_connect_log.html

- **Levantamento de informações (*Social Media Resources*):**
  - https://www.osinttechniques.com/osint-tools.html

1. Levantamento de informações

- **Geolocalização:**
  - Creepy (foi descontinuado).
  - As redes sociais evoluem e sofrem mudanças internas, o que faz essas ferramentas ficarem descontinuadas.



- **Maxmind (Geolocalizador):**
  - https://www.maxmind.com/

- **Outras para Geolocalização:**
  - https://ipinfo.io/200.20.0.0
  - www.ipaddress.my
  - www.ipfingerprints.com

2. Coleta / Varredura

- **Coletar informações mais detalhadas (forma ativa ou passiva):**
  - Quais os sistemas operacionais?
  - Quais os serviços utilizados? quais estão disponíveis ou e quais não estão?
  - Quais as versões dos serviços e sistemas operacionais?
  - Existem mecanismos de proteção (IDS, logs, *backup* e *Firewall*)?
  - Se precisar localizar uma pessoa ou local por fotos para levantamento de informações, utilize sites de busca via URL ou arquivo de imagem:

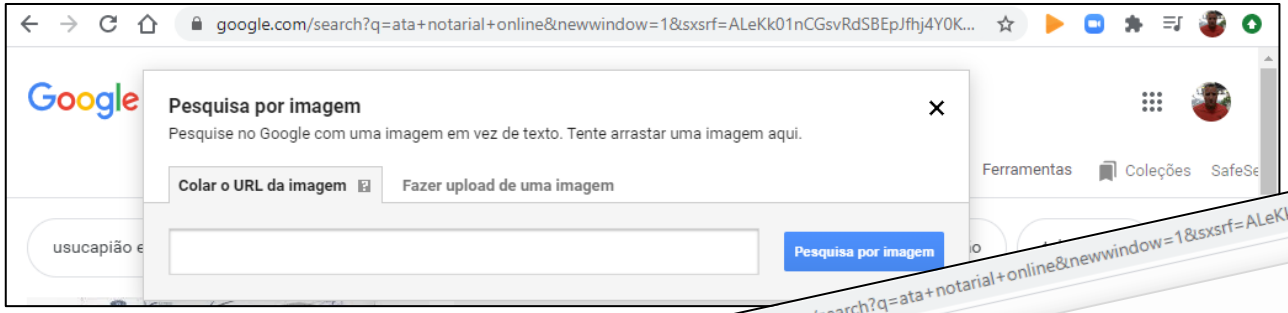


Figura 01: via URL

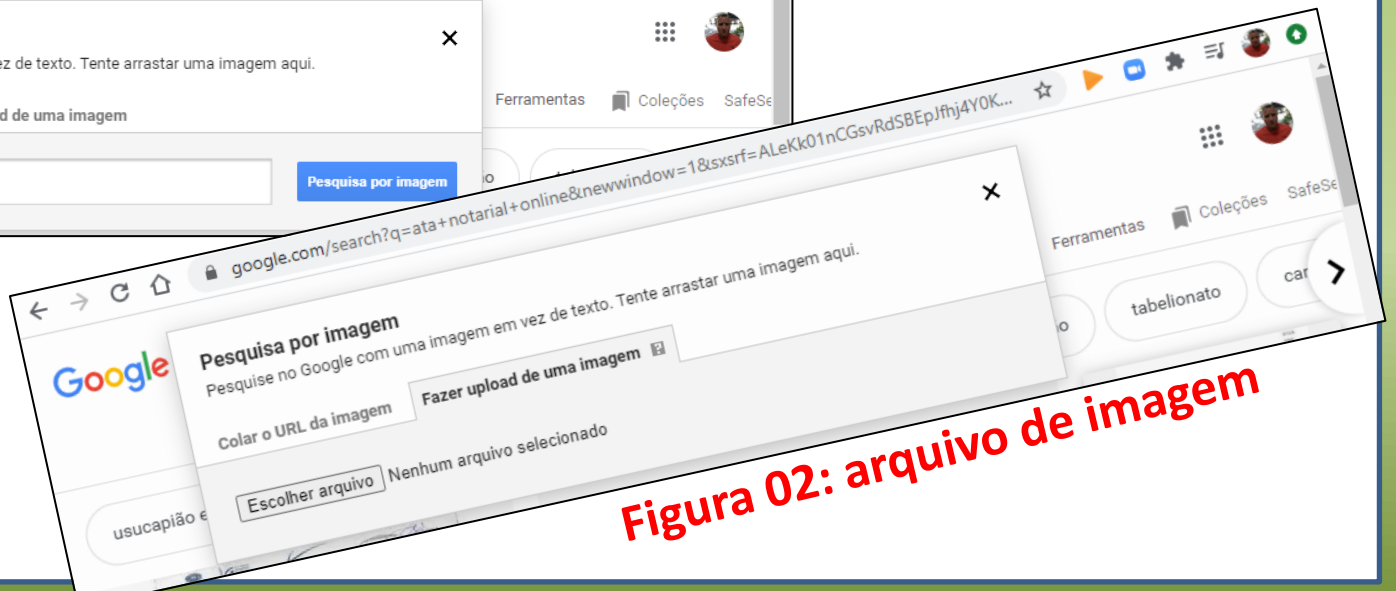


Figura 02: arquivo de imagem

2. Coleta / Varredura

- **Obter informações dos servidores contendo serviços e nomes registrados no DNS:**
  - https://ipinfo.io/200.20.0.0.
- **Sites com testes de rede (alguns são considerados na fase de varredura):**
  - https://ipok.com.br/.
- **verificar se site eh malicioso:**
  - http://virustotal.com/.
- **Verificar se o servidor de e-mail está em *blacklist*:**
  - https://mxtoolbox.com/.
- **Caso tenha acesso aos *browsers* teste a segurança:**
  - http://panopticlick.eff.org;
  - **Pode ser interessante instalar extensões para bloquear rastreamento via browser: https://privacybadger.org/.**

2. Coleta / Varredura

- Portscan (**nmap**, **Nessus** e outros);
- Verificar serviços ativos (**nmap, Zenmap** e **nping**);
- Fingerprint (**nmap**, xprobe2 e **amap**);
- **Maltego:**
  - Ferramenta de busca de informação na web, redes sociais, DNS, etc;
  - Coleta e avaliação de ameaças:
    - A ferramenta *Maltego* não será mostrada por ser mais incisiva e falta de tempo disponível.
- **DNSenum** (obter informações de DNS);
- Ferramentas existentes no Linux para administração de servidores e rede:
  - dig, nslookup, whois, telnet, netcat, etc;
- **Dmitry** (determinar ranges da rede).

2. Coleta / Varredura

- **Winaudit: https://www.parmavex.co.uk/winaudit.html**
  - Auditoria de computadores Windows
  - Pode ser interessante para levantar informações locais do Windows (acesso a perfis de redes sociais, registros do *Windows*, *history* de *browser*, *softwares* acessados, etc).

- **Pode fazer escopo da coleta:**
  - Ter acesso aos sistemas, neste caso verifique se as licenças estão em dia. Lembre que muitos *software* "*crackeados*" tem embutido em seu código comportamentos nocivos: *backdoor*, vírus, *spyware*, cavalos de troia ou qualquer outro *malware*;

    "Da mesma forma que o crime não compensa, a pirataria não compensa"

  - Rode *antimalware* e antivírus;

  - Verifique se existe *software* automático para verificar *hash* de arquivos, caso não tenha um *software* como este sugira isto no relatório. Exemplos: **cfv, Tripwire, AIDE, Labrador**, etc.

2. Coleta / Varredura

- **Caixa de areia para acessar sites e obter informações:**
  - http://urlscan.io

- **Ajudar a saber se o site é mal intencionado (mostra se sites estão com suspeitas de *phishing*, fraudes, etc):**
  - http://dnstwister.report

- **Ler cabeçalho de e-mail de forma automatizada:**
  - Útil para achar e-mails fraudulentos;
  - https://mxtoolbox.com/EmailHeaders.aspx

2. Coleta / Varredura
Avaliação das vulnerabilidades

- **Pode ser feita manualmente:**
  - Dependendo da quantidade e variedade dos sistemas, a verificação manual pode ser improdutiva e não ser eficiente.
- **Nessus;**
- **OpenVAS**.
- **Existe o V3n0M Scanner (originado do Baltazar scanner):**
  - Não recomendo usar (tenha cuidado);
  - É um programa experimental;
  - Pode sair do controle e “atacar” sites e sistemas achados no Google;

3. Conquistar o acesso

- **Nesta fase cuidado para não causar danos;**

- **Exemplos de ferramentas:**
  - *Nmap NSE (Nmap Script Engine);*
  - *Hydra;*
  - *Metasploit*;
  - *Mastering Amistage*.

- **Sniffers podem ser utilizados para escalonar acessos (pode ser utilizado na fase 01):**
  - *Neste momento podemos localizar inclusive problemas de configuração;*
  - *Lembre que grampo não é permitido, verifique as questões legais. A ideia aqui é analisar tráfego, ou seja, não é para fazer grampo ou qualquer ação ilegal;*
  - *TCPDump ou TShark;*
  - *Network Traffic View:*
    - *https://www.nirsoft.net/utils/network_traffic_view.html*
  - ***Wireshark: www.wireshark.org**.*
  - *Se tiver acesso e permissão: lembre de "sniffar" a rede wifi ou BlueTooth, muitas informações podem aparecer.*

3. Conquistar o acesso

- **Exemplos:**
  - Ataque na autenticação de serviços:
    - Banco de dados;
    - POP3 (*Post Office Protocol*);
    - SSH (Secure Shell).

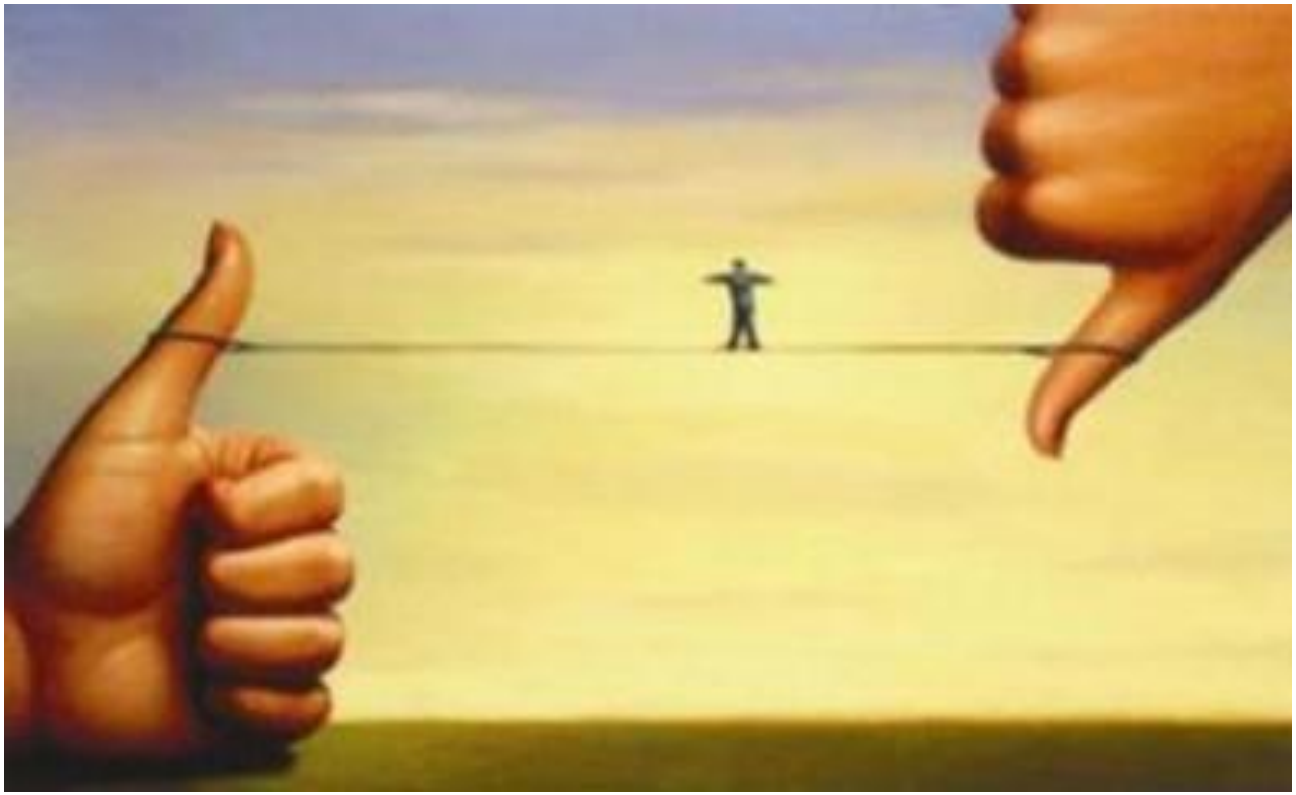
3. Conquistar o acesso

- **Outros exemplos que podem ser realizados em laboratório:**
  - Man-in-the-middle (homem do Meio);
  - Overflow;
  - Exploits;
  - SQL injecton (tipo de exploit);
  - DoS (Denial Of service);
  - DDoS (DOS Distribuído);
  - Servidores de e-mail, banco de dados e DNS mal configurado.

- Consultar os ataques mais recentes e os mais frequentes:
  - OWASP;
  - Grupos de resposta de incidentes ou Cert do seu país ou região, exemplo: CERT-BR ou NIC .br;

Corda bamba: Fases 4 e 5

- **Se for mau utilizado:**
  - A divisão entre o bem e o mal;
  - Pode causar sérios danos;
  - Na literatura muitas vezes não estão no Pentest.



4. Continuar acessando e 5. Apagar os rastros

- **Em muitos casos (talvez a maioria) não é considerado parte de um Pentest:**
  - Deve ser considerado como ações de *blackhat*.

- **Em quais casos esta fase pode ser solicitada pelo cliente:**
  - Alguns sistemas possuem permissões extras que impedem ações do invasor e escalonar poderes/acessos, mesmo com a conquista do acesso.
  - Exemplos: SeLinux e alguns Unix BSDs.

Relatório

- **Exemplos de relatório:**
  - https://anubis.website/docs/report_access_pentest_anbistrade.pdf

- **Várias ferramentas que podem ajudar no PenTest:**
  - https://minutodaseguranca.blog.br/lista-completa-de-ferramentas-de-teste-de-penetracao-e-hacking/.

Dicas: outras ferramentas (pode ser útil em vários momentos)

- **HashMyfiles:** www.nirsoft.net/utils/hash_my_files.html
  - Pode ser útil em algum momento para criar ou comparar *Hash*.
- **Outras opções de Hash no Linux/Unix:**
  - Exemplos mais comuns de utilitários: md5 (ou md5sum em alguns Linux) e o sha1 (ou sha1sum em alguns Linux);
  - Prefira, dependendo da finalidade versus impacto de desempenho, os utilitários *hash* com mais de 128 bits na *string* de *hash*.
- **Forense das fotos:**
  - http://fotoforensics.com;
  - https://tineye.com/.
- **Cofre de senhas:**
  - http://keepassxc.org;
  - http://teampass.net.
- **Ata notarial:**
  - Opção 01: Registro em cartório;
  - Opção 02: https://www.verifact.com.br/.

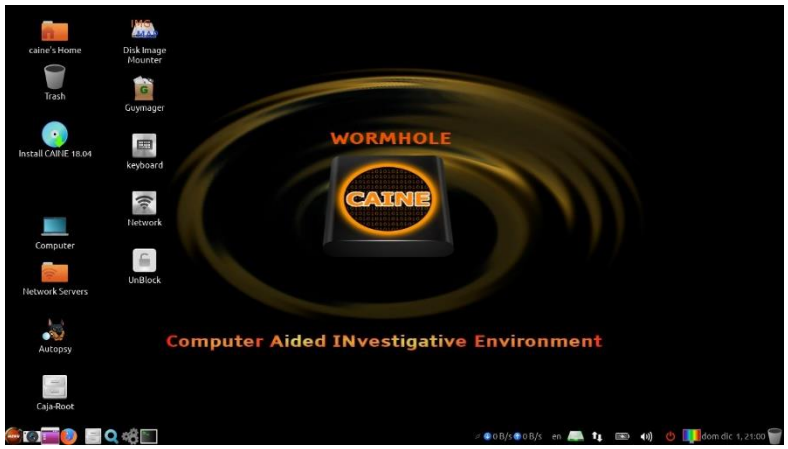
Dicas de S.O.: Linux para Forense

Os Linux abaixo são para forense, mas podem ser úteis para Pentest em alguns casos:

- http://www.caine-live.net;
- http:// digital-forensics.sans.org:
  - https://digital-forensics.sans.org/community/downloads
- http://lubuntu.me/deft-linux-7/.

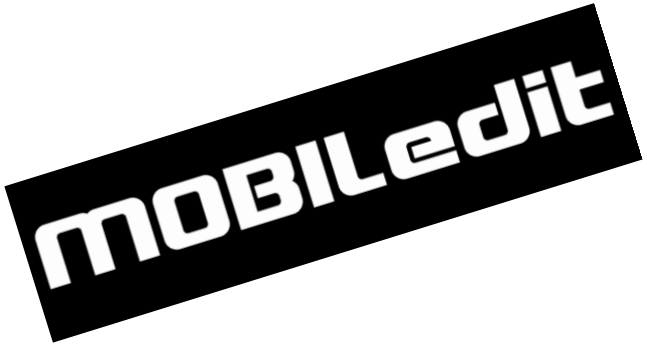
SANS

SIFT



Dicas de S.O.: Forense em smartphone

- http://santoku-linux.com
- www.mobiledit.com/mobiledit-forensic
- www.oxygen-forensic.com
- forensicdesk.com



Dicas: outras ferramentas (pode ser útil em vários momentos)

- **Forense Tool Kit:**
  - IPED: https://servicos.dpf.gov.br/ferramentas/.
  - EnCase (utilizados por policias federais em vários países);
  - UFED Touch (empresa israelense – utilizados por policias federais em vários países e serviços de inteligência);
  - DFF (investigação forense);
- **FTK Imager:**
  - Análise de mídias.
- **Autopsy do kali Linux;**
- **Caine;**
- **Site com varias ferramentas periciais:**
  - https://www.nirsoft.net/.

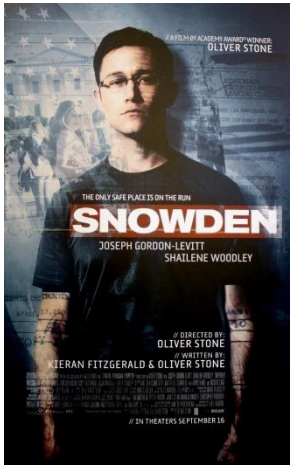
Dicas: outras ferramentas

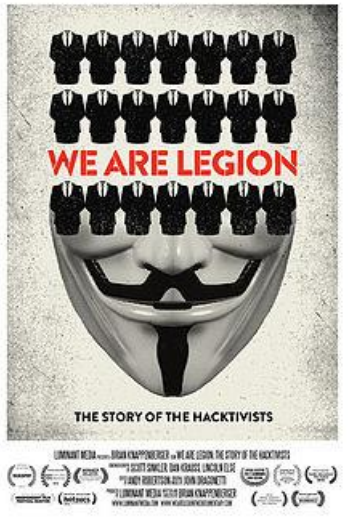
- **Encurtar URL (pode ser utilizado na fase 01 no levantamento de informações):**
  - Pode ser usado para capturar informações dos usuários;
  - Pode ser utilizado também para engenharia social;
  - https://iplogger.org/;
  - https://bitly.com/.

- IP Net Info - Ferramenta para Localização de IP:
  - https://www.nirsoft.net/utils/ipnetinfo.html.

Dicas de filme e documentários

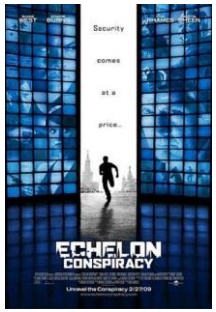
- Snowden: Herói ou Traidor;
- DeepWeb;
- Steve Jobs (2015);
- O Jogo da imitação;
- The Wikileaks Documentary;
- We Are Legion: The Story of the Hacktivists;
- O Quinto Poder (Julian Assange);
- A Origem dos Hackers – Documentário (histórico);
- Os estagiários (sobre a seleção de profissionais no Google);
- Piratas do Vale do Silício (histórico).





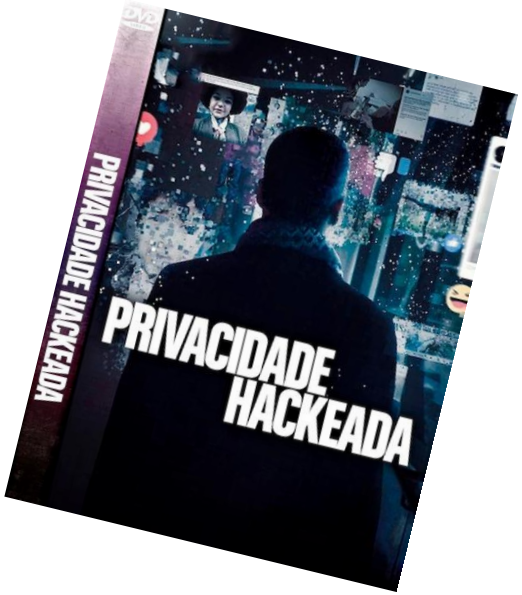
Dicas de filmes e documentários alternativos - Abrir os olhos

- O Círculo (Julho 2017);
- Matrix (trilogia);
- Invasores - Nenhum Sistema Está à Salvo (2015);
- Mr. Robot;
- Todo Crime Tem Um Início (HACKER) (2017);
- ALGORITHM: The Hacker Movie;
- A chamada - Echelon Conspiracy (2009);
- Invasão de Privacidade;
- Hackers 3 Antrust;
- Filme Cyberbully.



Filmes/documentários Atuais

- *DarkNet* – Rede Sombria;
- Privacidade Hackeada (*The Great Hack*);
- O dilema das redes.



Fim

Dúvidas

Obrigado

FIM

Obrigado a todos!

Estou a disposição para dúvidas.