4LINUX

FREE SOFTWARE SOLUTIONS

Forense Computacional com Software Livre

Apresentação

Luiz Vieira

- Construtor 4Linux
- Consultor de Segurança
- 16 anos de experiência em TI
- Pen-Tester, Perito Forense
- Articulista sobre Segurança de vários sites: VivaOLinux, SegurançaLinux, Imasters, HackProofing e etc
- Entusiasta do Software Livre
- Filósofo e Psicoterapeuta
- Blog: http://hackproofing.blogspot.com

4LINUX
FREE SOFTWARE SOLUTIONS

Webcast – Agenda

- Análise de Malware com Software Livre - **29/03**
- Análise de Vulnerabilidades em Redes, usando software livre - **31/03**

4LINUX
FREE SOFTWARE SOLUTIONS

Tópicos de hoje

- O que é Forense Computacional?
- Principais desafios da Forense Computacional
- Passos de uma Investigação
- Análise Viva e Post Mortem
- Distribuições Linux para Forense
- Ferramentas Livres e Toolkits para Forense

O que é Forense Computacional?

“Uma série metódica de técnicas e procedimentos para coletar evidências de um sistema computadorizado, de dispositivos de armazenamento ou de mídia digital, que podem ser apresentadas em um fôro de uma forma coerente e de formato inteligível”. - Dr. H. B. Wolf

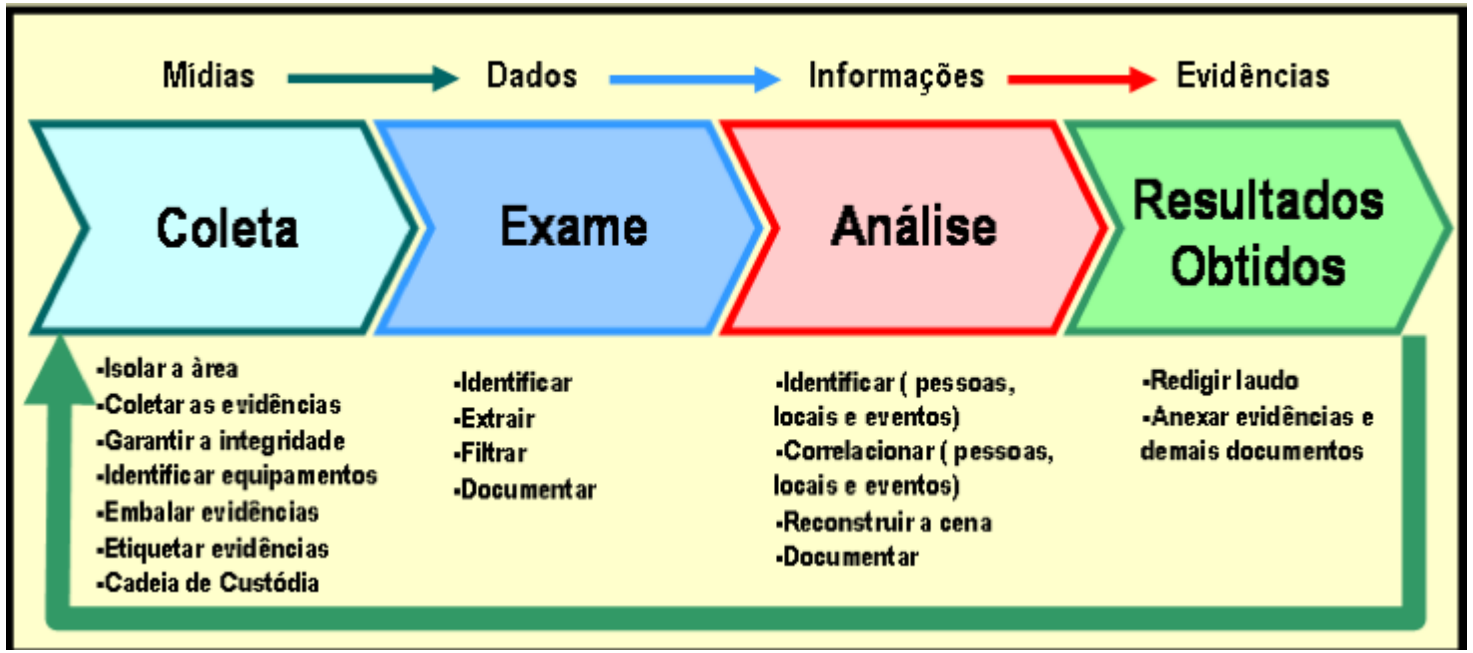
4LINUX
FREE SOFTWARE SOLUTIONS

Principais desafios da Forense Computacional

- Ainda é mais uma arte do que ciência;
- Ainda está em seus estados iniciais de desenvolvimento;
- Há pouco conhecimento teórico sobre o qual as hipóteses empíricas são baseadas;
- Há falta de treinamento apropriado;
- Não há padronização de ferramentas.

Passos de uma Investigação

- 1. Avaliação inicial do caso
- 2. Preparar um projeto detalhado
- 3. Determinação dos recursos necessários
- 4. Identificação dos riscos envolvidos
- 5. Investigação das informações recuperadas
- 6. Preenchimento do relatório do caso
- 7. Conclusão do caso



Análise Viva e Post Mortem

Dados Voláteis

- São infomações que ficam armazenados na memória principal do computador. Isso quer dizer que elas possuem um ciclo de vida curto. Esse tipo de análise é chamada de “Análise Viva”.

Dados não-voláteis

- Dados não voláteis, são dados que podem permanecer na máquina durante longos períodos de tempo e podem ser recuperados mesmo após a mesma ser desligada. As análises baseadas em dados armazenados em mídia de backup, pendrives, Cds, ou memória auxiliar como um HD, são chamadas de “Análise Post-Mortem”.

Distribuições Linux para Forense

- FDTK – Forensic Digital Toolkit
- Helix
- REMnux
- CAINE - Computer Aided INvestigative Environment
- DEFT Linux
- PeriBR
- Backtrack

4LINUX
FREE SOFTWARE SOLUTIONS

Ferramentas Livres e Toolkits para Forense

Toolkits

- Autopsy
- Framework Volatility
- Sleuth Kit
- The Coroner's Toolkit

Ferramentas

- Centenas delas:
- Foremost
- Scalpel
- memdump
- shred
- Pasco
- etc, etc, etc...

Cursos

Presenciais e EaD

- Segurança em Servidores Linux, com a norma ISO 27002
  - http://www.4linux.com.br/cursos/cursos-seguranca.html#curso-415
- Teste de Invasão em Redes Corporativas
  - http://www.4linux.com.br/cursos/cursos-seguranca.html#curso-406
- Forense Computacional
  - http://www.4linux.com.br/cursos/cursos-seguranca.html#curso-427

4LINUX
FREE SOFTWARE SOLUTIONS

Promoções

- **Lançamento curso Investigação Forense à distância - desconto de 50% para a próxima turma com inicio dia 09/05/11.**

Conheça o curso:
http://www.4linux.com.br/cursos/cursos-seguranca.html#curso-427

- **Pacote com 50% de desconto para cursos de Segurança Linux.**

A 4Linux oferece os melhores cursos de segurança com ferramentas livres. Turmas presenciais e à distância. Vagas limitadas e promoção válida até 25/03/11.
http://www.4linux.com.br/cursos/pacote-seguranca-avancada-406415.html

4LINUX
FREE SOFTWARE SOLUTIONS

Soluções oferecidas pela 4Linux

- Auditoria e análise de vulnerabilidades em aplicações WEB
  http://www.4linux.com.br/solucoes/auditoria-analise-vulnerabilidades-aplicacoes-web.html
- Investigação e Forense Digital
- Teste de Invasão em Redes Corporativas
- Implementação de Controles de Segurança
  http://www.4linux.com.br/solucoes/implementacao-controles-seguranca.html

4LINUX
FREE SOFTWARE SOLUTIONS

4LINUX
FREE SOFTWARE SOLUTIONS