Forense Computacional com Software Livre

Apresentação

Luiz Vieira

- Construtor 4Linux
- Consultor de Segurança
- 16 anos de experiência em TI
- Pen-Tester, Perito Forense (CHFI)
- 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

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
- Análise de memória física
- Demo: Análise de tráfego de rede com Xplico
- Demo: Recuperação de senhas Windows com Ophcrack

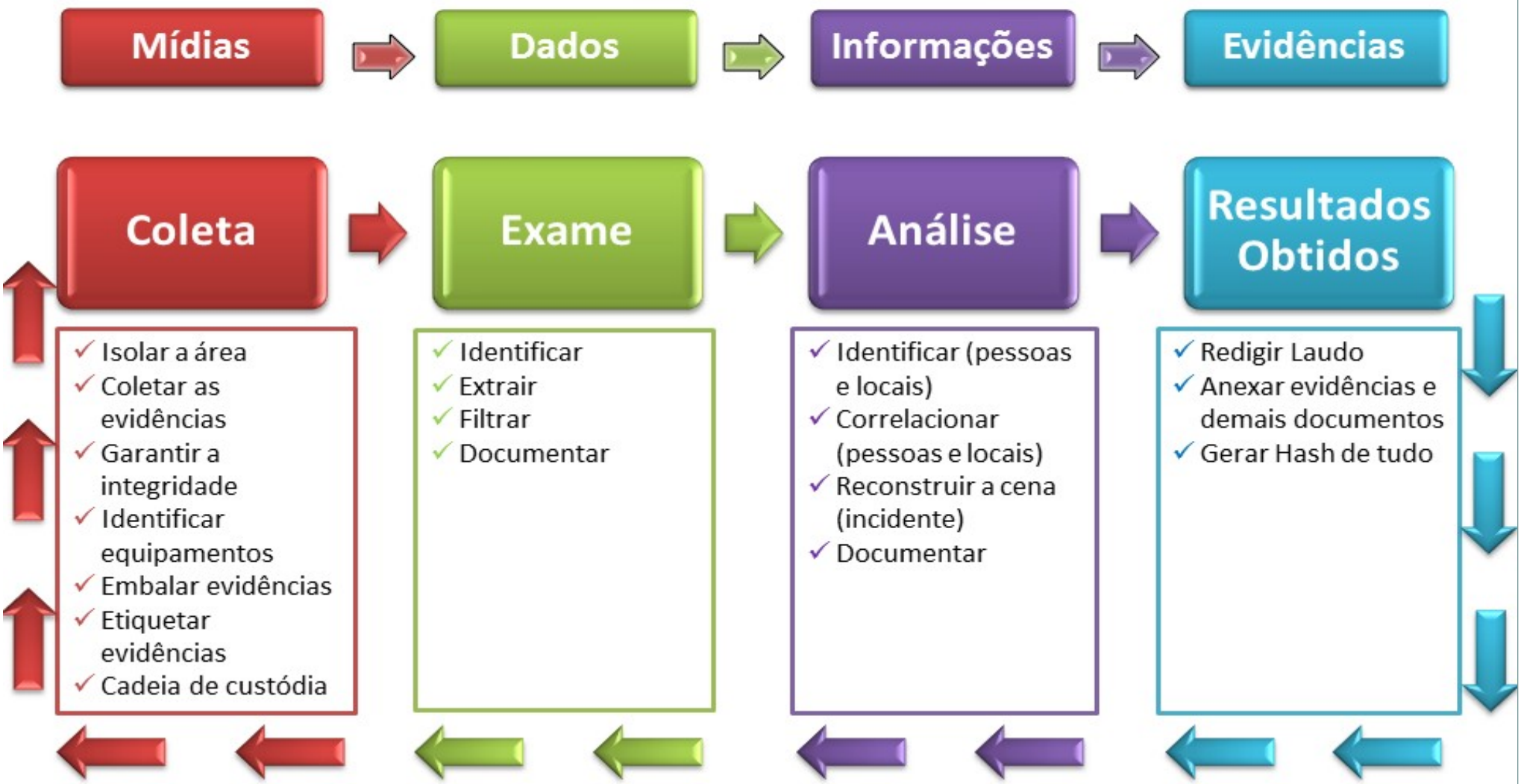
Introdução & Ferramentas

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

Ciclo de uma investigação



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.

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...

4LINUX
FREE SOFTWARE SOLUTIONS

Análise de Memória

Análise Viva e Post Mortem

Dados Voláteis

- São informações 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”.

Análise de memória física

- A análise de memória física baseia-se em fazer um dump da memória física e virtual de um sistema.

- O que podemos conseguir através da memória física?
  - Arquivos com senhas em texto puro
  - Arquivos com variáveis de ambiente ($HISTFILE)
  - O mapas de todos os serviços que se encontram em execução.

- Aplicações de terminal:
  - **memdump** (posix) - http://www.porcupine.org/forensics/memdump-1.0.tar.gz (solaris/bsd/linux)
  - **Configuração de memory dump do windows** (windows)

Dump da memória

- Dump da memória é nome do processo de capturar as informações da memória, e pode ser feito através do comando dd:
  - *#dd < /dev/mem > mem.dump*
  - *#dd < /dev/kmem > kmem.dump*
- O investigador pode realizar buscas por palavras-chave através dos comandos grep e strings:
  - *#strings -a mem.dump | grep palavra-chave*

Diretório /proc

- O diretório /proc é um pseudo-sistema de arquivos usado como uma interface para as estruturas de dados do kernel do sistema operacional.
- A memória pode ser acessada pelo pseudo-arquivo /proc/kcore, que representa a memória física do sistema no formato de um core file.
- Buscando processos vinculados ao firefox:
  - *# strings -a /proc/kcore | grep firefox > kcore_firefox.dump*

Investigando Tráfego de Rede

Ferramentas de coleta de informações de rede

- Ferramentas de coleta de informações em redes são softwares que podem ser usados para obter dados da rede para análise forense.

- Estas ferramentas geralmente oferecem a funcionalidade de um sniffer e um sistema de detecção de intrusão combinadas.

- **Sniffers**
- Os sniffers operam na camada de enlace do modelo OSI. Isso significa que eles não têm que jogar pelas mesmas regras que as aplicações e serviços que residem nas camadas mais acima. Os sniffers podem capturar tudo e gravar para posterior análise. Eles permitem que o usuário analise todos os dados que estão contidos no pacote.

Análise de tráfego de redes

- A partir do tráfego de rede é possível analisar toda a comunicação entre atacante e máquina invadida, estabelecendo uma seqüência de eventos e comparando com as outras evidências encontradas.

- Um dos programas desse gênero mais popular é o tcpdump.

  - # tcpdump -i eth0 host 10.10.0.1

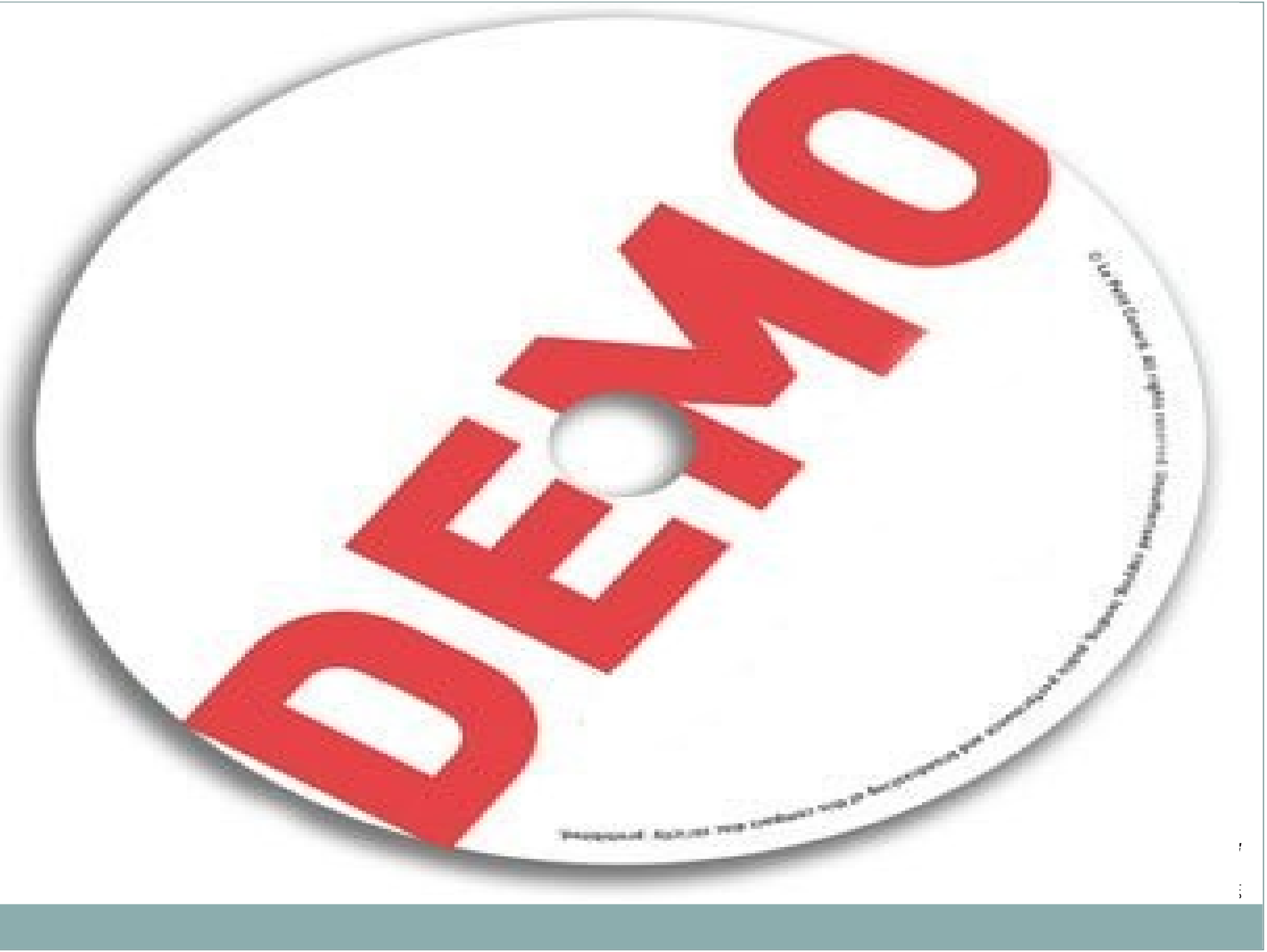
- O parâmetro -w do tcpdump permite armazenar os datagramas capturados em um arquivo binário para posterior análise:
  - # tcpdump -w trafego.dump

Análise de tráfego de redes

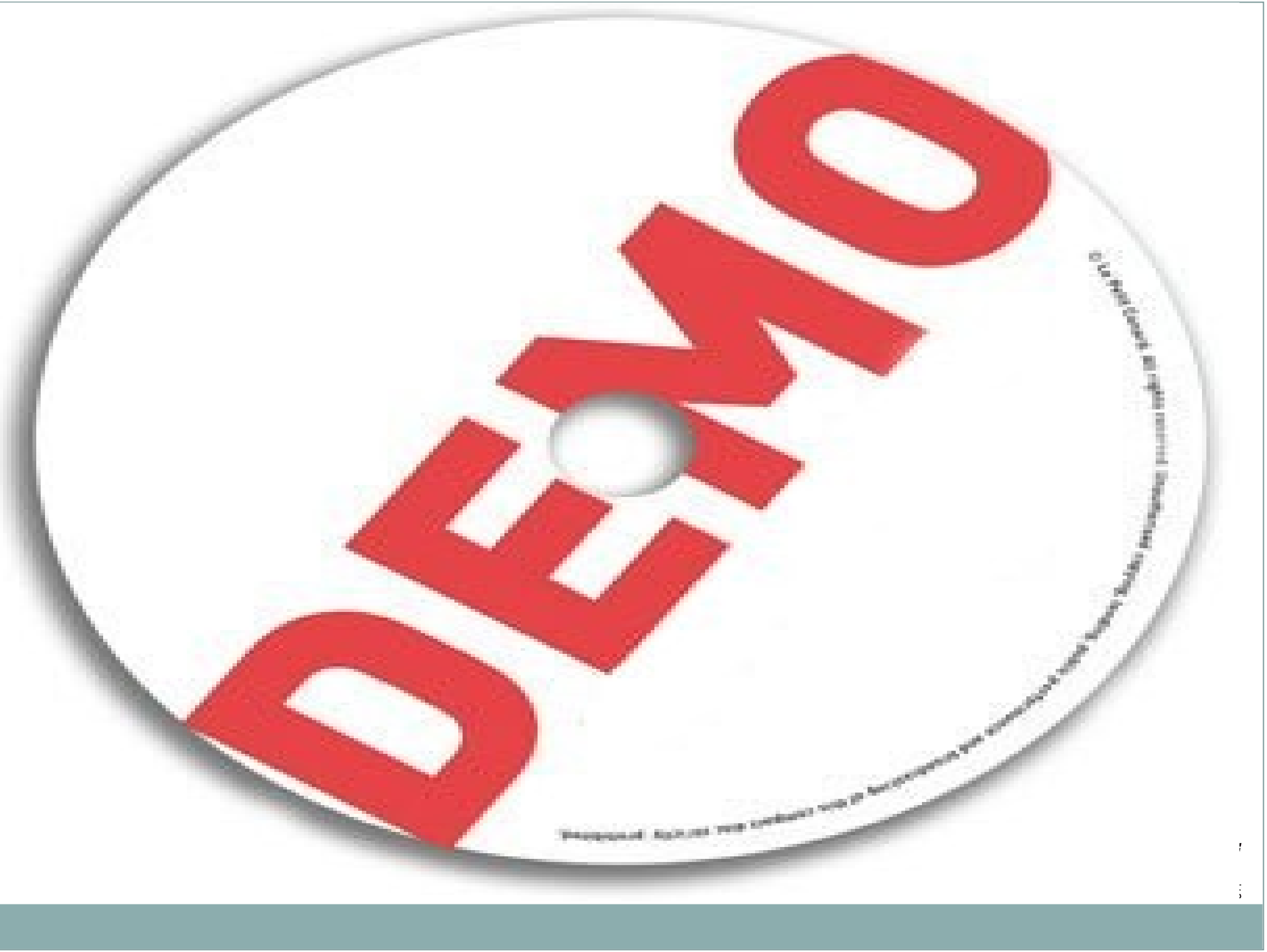
- Com a análise dos datagramas pode-se encontrar evidências como:

  - endereço IP inválido ou suspeito;
  - tráfego em portas desconhecidas;
  - tráfego em serviços ou portas que não deveria estar ocorrendo;
  - datagramas com opções, flags ou tamanhos que não respeitam os padrões do protocolo (Request for Comment - RFC);
  - flood de datagramas na rede;
  - tráfego TCP em portas incomuns.

Captura de tráfego de rede com Xplico

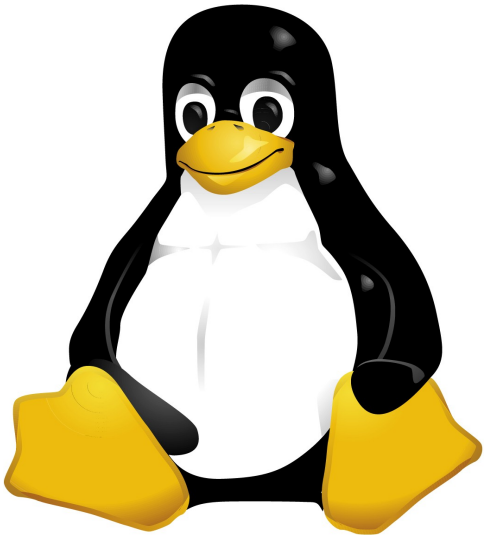

DEMO

Recuperação de senhas de Windows com Ophcrack


DEMO

4LINUX
FREE SOFTWARE SOLUTIONS

Obrigado!!!!



Luiz Vieira
luiz.vieira@4linux.com.br
luizwt@gmail.com

https://groups.google.com/group/exploits-brasil
hackproofing.blogspot.com
www.4linux.com.br

Tel: 55-11-6429-0505

4LINUX
FREE SOFTWARE SOLUTIONS