BlackBox TestBox: uma ferramenta baseada em virtualização para testes de caixa-preta

Carlos A M S Teles
E-mail: carlos.teles@eic.cefet-rj.br

Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
CEFET/RJ - Programa de Pós - Graduação em Ciência da Computação

Sumário

- Introdução
- Conceitos Fundamentais
- Trabalhos Relacionados
- Proposta
- Implementação
- Resultados
- Conclusão

Introdução

- Tecnologia da Informação e de Comunicações (TIC)
  - Conjugação da tecnologia computacional com a tecnologia das telecomunicações

- Ativos de TIC
  - Todo o tipo de hardware e software capaz de executar processamento computacional e que esteja envolvido em atividades de TIC

Introdução

- Comportamento de Ativos de TIC
  - Em conformidade
  - Não-conformidade

- Comprometimento de Ativos de TIC
  - Incidentes de segurança

Introdução

- Volkswagen - Dieselgate
- 2009 à 2015

http://autoetecnica.band.uol.com.br/wp-content/uploads/2018/01/Volkswagen-DieselGate-Beetle-Emitting-Black-Smoke-from-Exhaust.jpg

Introdução

- Câmeras IP

https://images.techhive.com/images/idge/imported/article/nww/2013/01/pital_trendnet_ip_cam_security_vulnerability_0-100274351-orig.jpg

Introdução

Introdução

Introdução

- Contribuições

1. Desenvolvimento de uma ferramenta de testes de ativos de TIC baseado em virtualização

2. Construção de uma base de dados de referência para o estudo de ataques a ativos de TIC a partir do tráfego capturado nos experimentos

Conceitos Fundamentais

- Segurança da Informação
- Virtualização
- Testes Black Box / White Box

Conceitos Fundamentais

- Segurança da Informação
  - Assegurar a proteção dos sistemas de informação e aos dados, além de diminuir os danos causados ao prevenir e minimizar o impacto de incidentes de segurança sobre os ativos de TIC.
  - Propriedades:
    - Confidencialidade, Integridade e Disponibilidade.

- Desempenho
  - Refere-se ao monitoramento e à medição de métricas de relevantes para avaliar o desempenho dos ativos de TIC.
    - Memória, CPU, Tráfego de rede, Tráfego de pacotes

Conceitos Fundamentais

- Virtualização - Inicio dos anos 1960 - IBM
- Tipos de Virtualização
  - Virtualização completa
  - Virtualização assistida por *Hardware*
  - Paravirtualização
  - Virtualização parcial
  - Virtualização híbrida
  - Virtualização em nível de Sistema Operacional

Conceitos Fundamentais - Testes

Black Box	***White Box***
Sem acesso a todas as informações técnicas	Precisa ter acesso a todas as informações técnicas
Utilização de menos pessoas	Utiliza mais pessoas
Mais rápido	Mais demorado
Menor custo	Maior custo

Trabalhos Relacionados

- Taheri, Zomaya, e Kassler 2017 - BlackBox e Virtualização
- Bauer, Heseding e Flittner 2017 - EarlyDrop - Black-Box, Segurança da Informação e monitoramento
- Ibidunmoye, Lakew e Elmroth 2017 - Segurança da Informação e monitoramento
- Perrone e Romano 2017 - Docker Security Playground

Proposta

- Ambiente de Monitoração
- Ambiente de Virtualização

Implementação

- Ambiente de Monitoração
  - Segurança
    - Suricata (IDS, IPS e NSM)
    - Evebox
  - Desempenho
    - Grafana
    - Telegraf e Influxdb

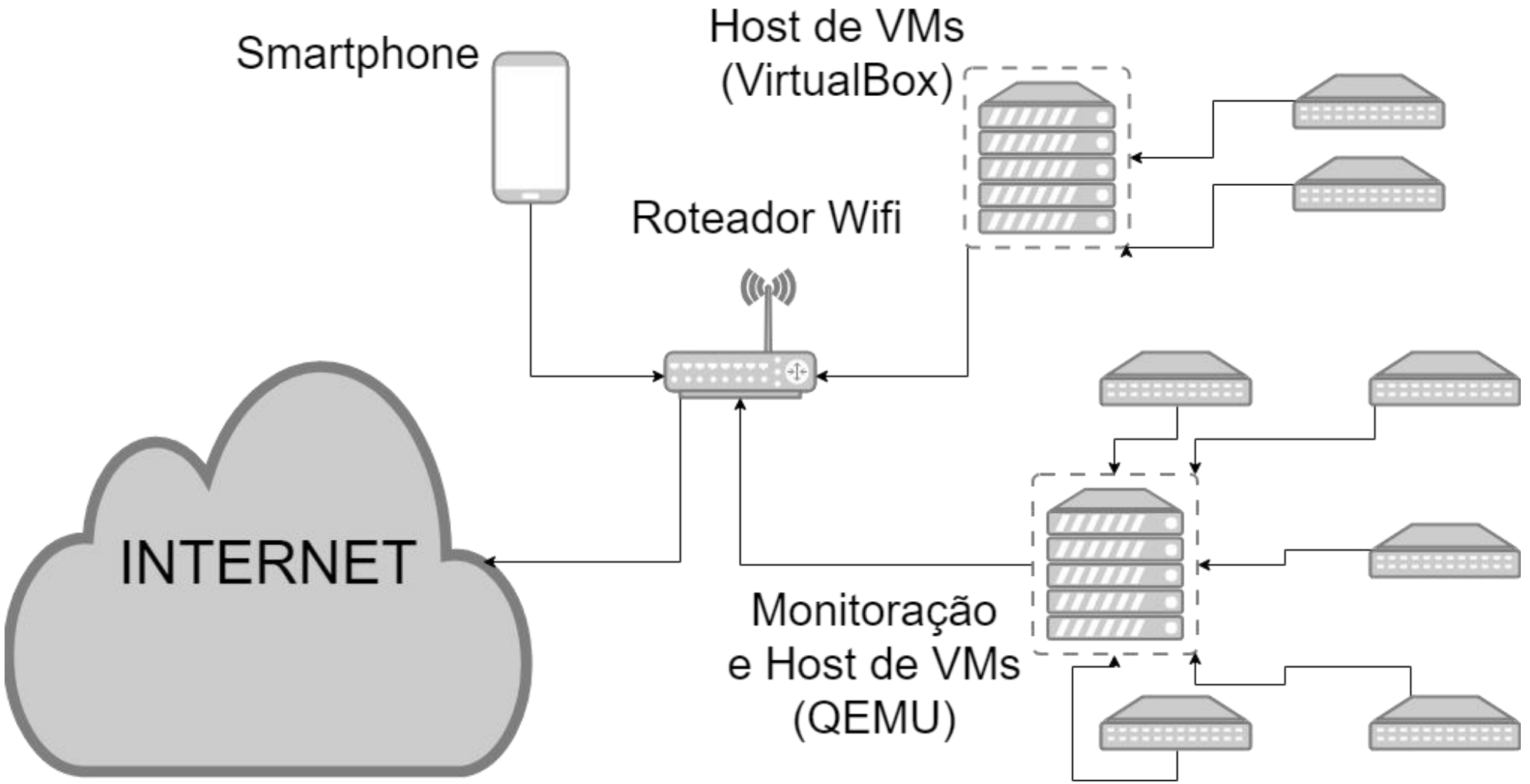
Implementação

- Ambiente de Virtualização para Ensaios
  - Virtualização completa hospedada
    - Oracle VirtualBox
      - x86 e x86_64
    - QEMU
      - Emulador de CPU
      - Emulador de dispositivos
      - Dispositivos genéricos
      - Debugger
      - Interface gráfica
      - Multi arquitetura (x86, x86-64, mips, arm, entre outros)

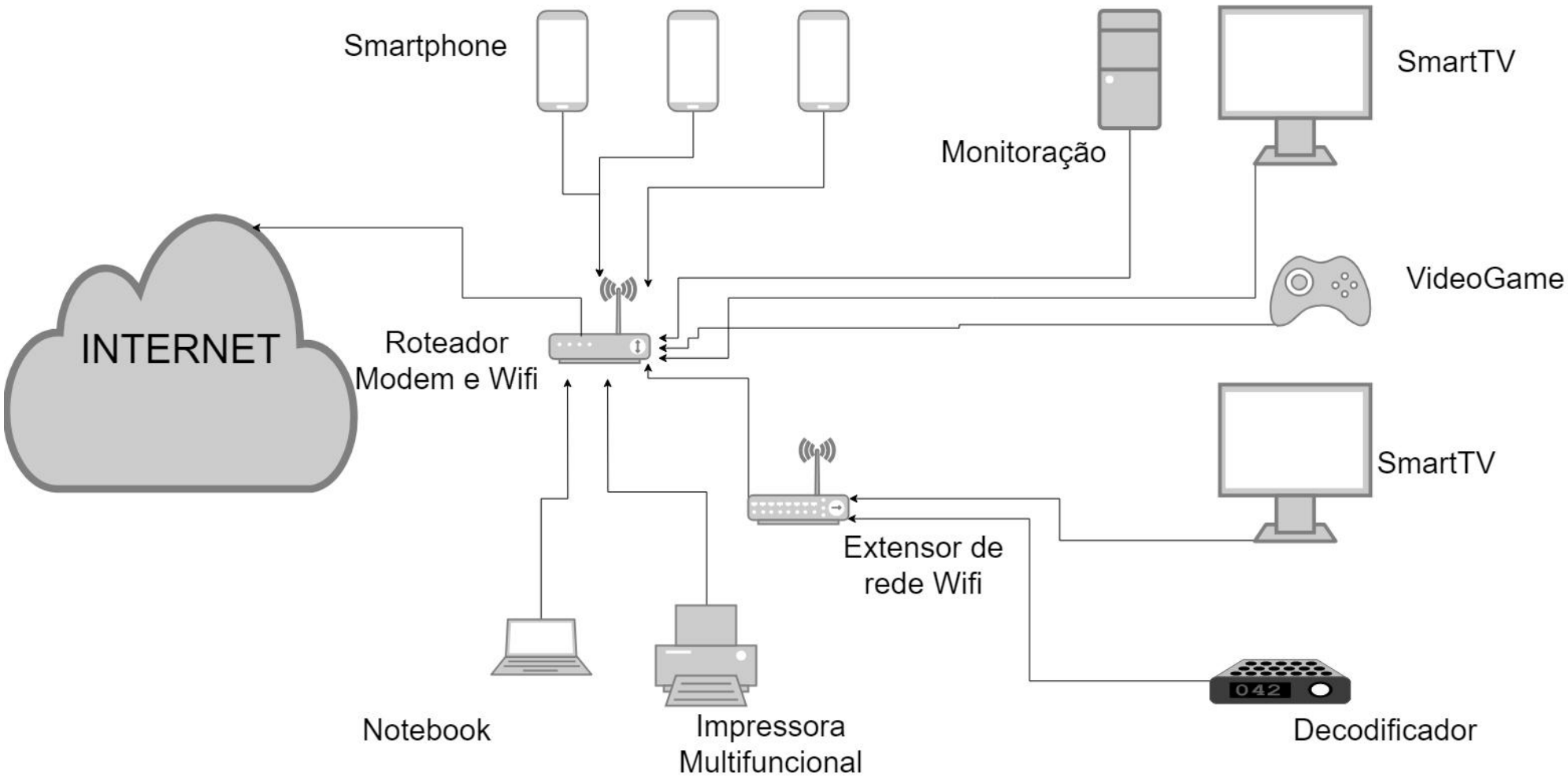
Estudo de caso

- Três cenários
  - Internet
  - Interno
  - Escritório em casa

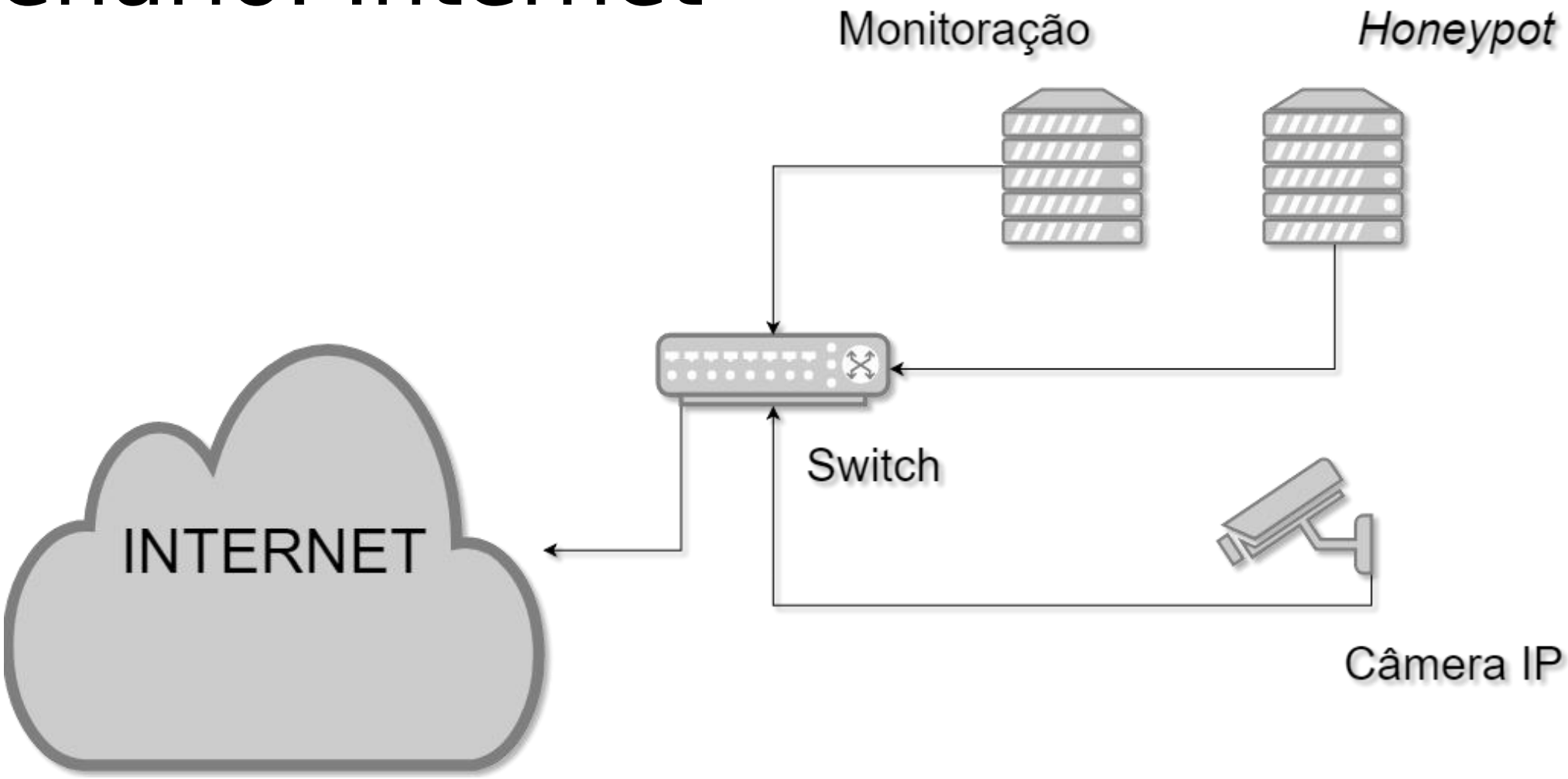
Cenário: Interno



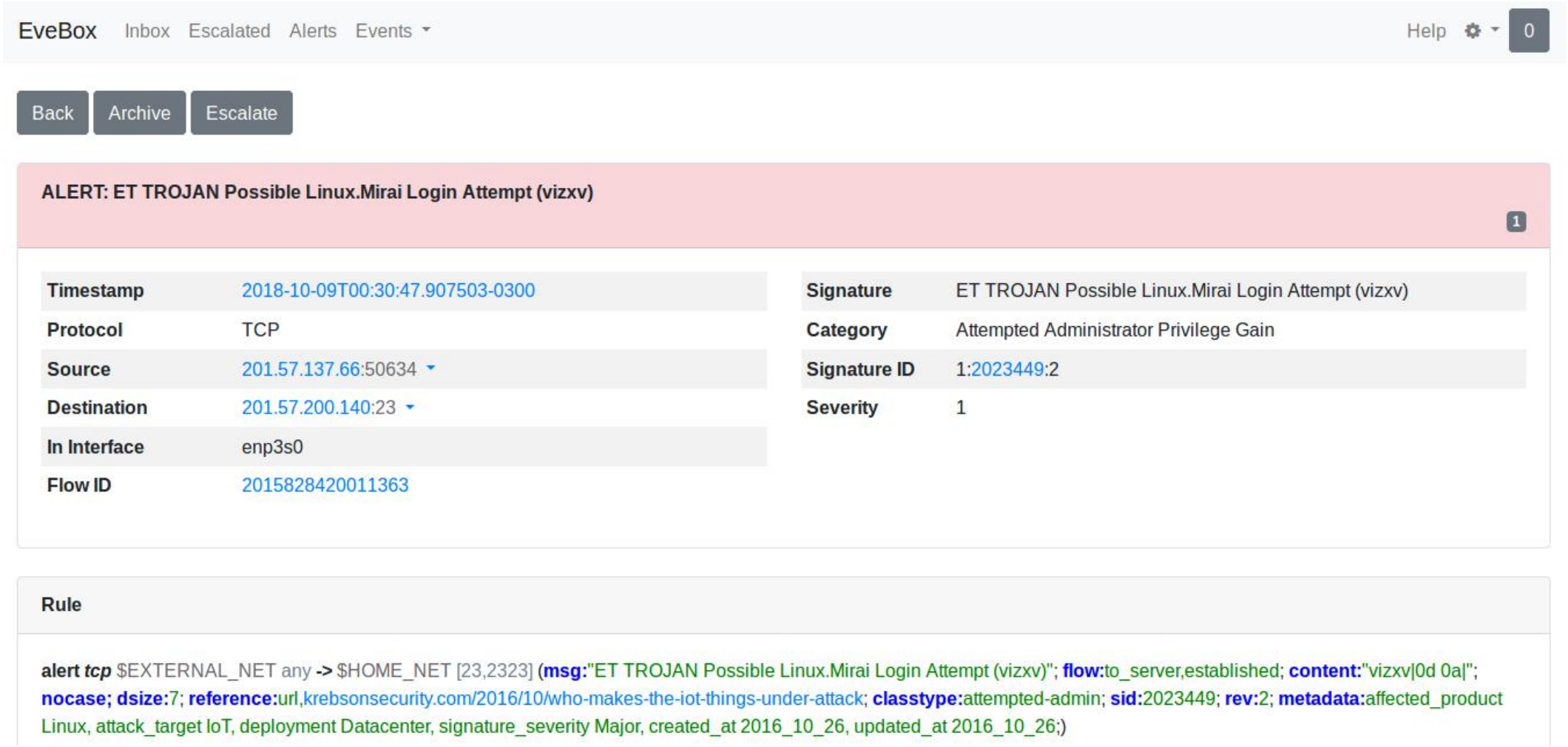
Cenário: Escritório em Casa



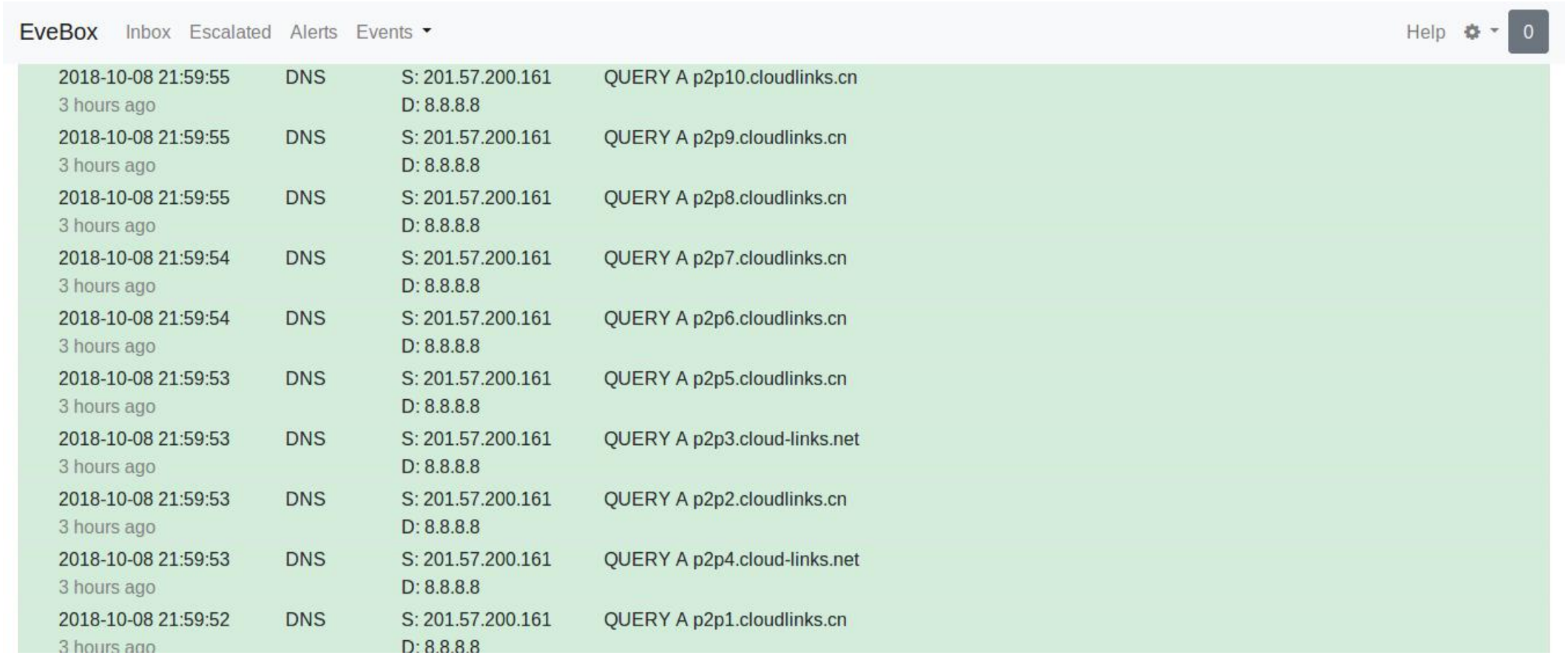
Cenário: Internet



Resultados - Internet



Resultados - Internet



Resultados - Internet

Conclusões

- Os resultados obtidos por meio do monitoramento de dispositivos nos três cenários, nos permitiu demonstrar a viabilidade do BlackBox TestBox à realização de ensaios de segurança baseados em testes de caixa-preta
- Ainda que não tenhamos identificado falhas e vulnerabilidades "novas", identificamos comportamentos "suspeitos" por parte de ativos de TIC

BlackBox TestBox: uma ferramenta baseada em virtualização para testes de caixa-preta

Código-fonte: https://github.com/carlos-teles/etsg

Carlos A M S Teles
E-mail: carlos.teles@eic.cefet-rj.br

Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
CEFET/RJ - Programa de Pós - Graduação em Ciência da Computação