GT-CIRD
Caracterização e Identificação Remota de Dispositivos

João Paulo de Souza Medeiros

Universidade Federal do Rio Grande do Norte

19º WRNP
Workshop RNP
7 | 8 MAIO
Campos do Jordão | SP

RNP

GT-CIRD: Caracterização e Identificação Remota de Dispositivos

WRNP 2018 – Programa de Internet Avançada

João Paulo de Souza Medeiros (DCT/UFRN, coordenador)
Agostinho de Medeiros Brito Júnior (DCA/UFRN, coordenador adjunto)
Antonio Alfredo Ferreira Loureiro (DCC/UFMG, coordenador adjunto)
Rommel Wladimir de Lima (DI/UERN, coordenador adjunto)

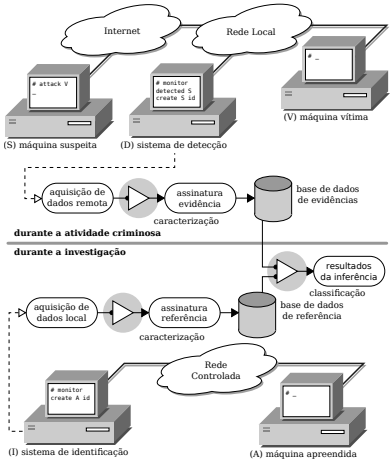
Laboratório de Elementos do Processamento da Informação – LabEPI
Departamento de Computação e Tecnologia – DCT
Universidade Federal do Rio Grande do Norte – UFRN

07 de maio de 2018

Proposta do Protótipo

GT-CIRD

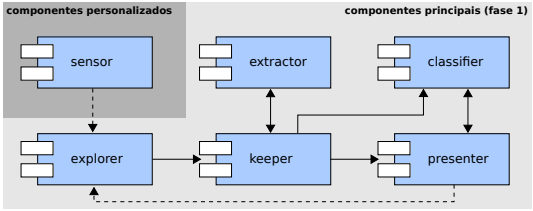
- **Objetivo**: criação de assinaturas para caracterização e identificação de máquinas remotas.
- **Caracterização**: busca por características que possam ser utilizadas para representar de forma eficaz algum componente de uma máquina remota.
- **Identificação**: utilização de métricas e métodos de comparação de assinaturas com o objetivo de classificar máquinas remotas.

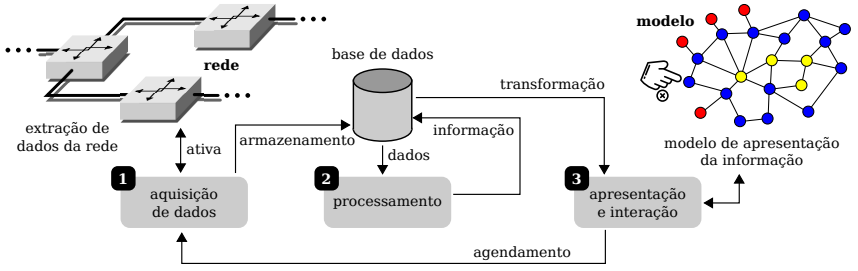


Arquitetura do Protótipo

Componentes e tecnologias desenvolvidas

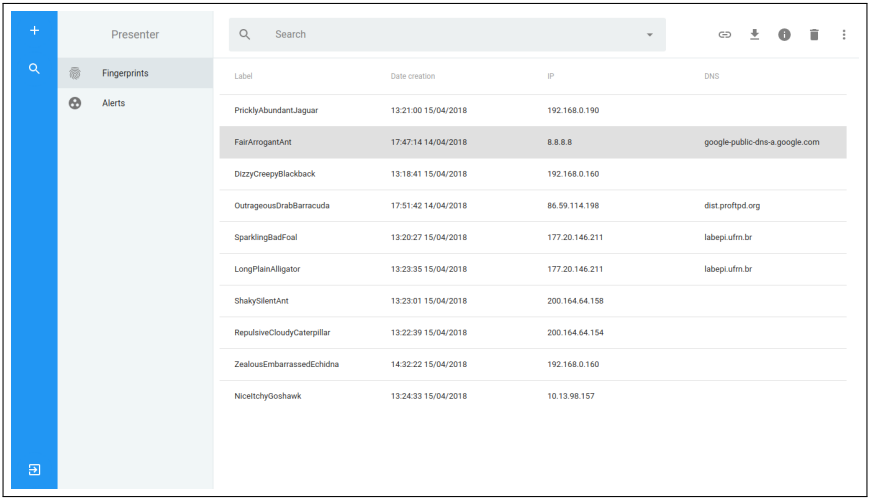
- Infraestrutura (Rotas, RTT e Serviços)
- Relógios (TCP e ICMP)
- Sistema Operacional (TCP ISN e IP ID)
- Camada de Aplicação
  (HTTP, SSH, DNS e FTP)
- Integração com IDS (Suricata)



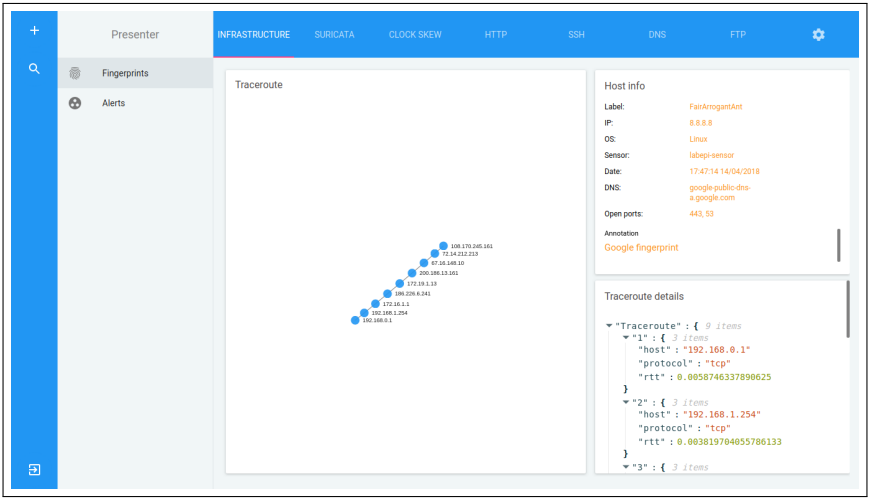


Resultados do Protótipo

Utilização dos resultados (`presenter`)



Utilização dos resultados (infraestrutura)

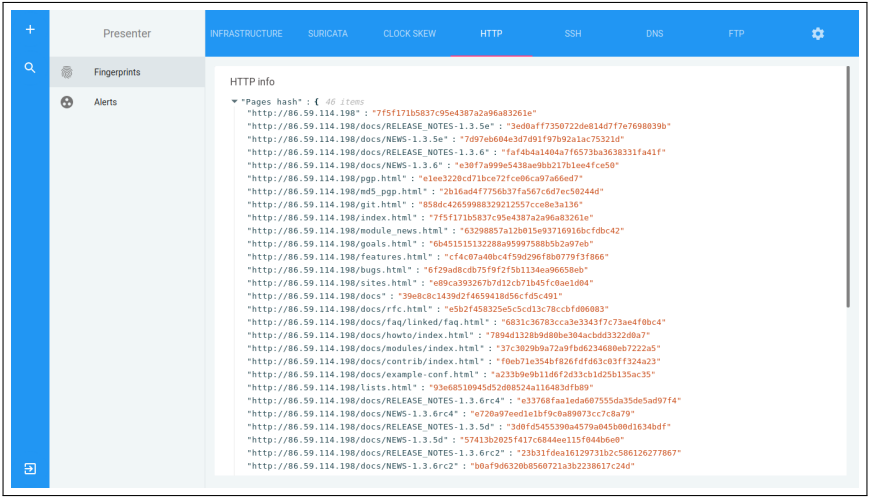


Resultados do Protótipo

Utilização dos resultados (Relógio)

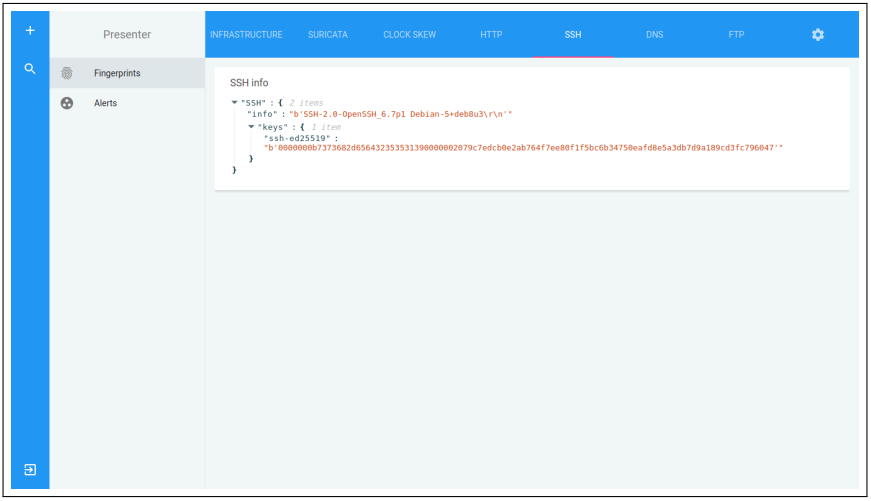
Resultados do Protótipo

Utilização dos resultados (HTTP)



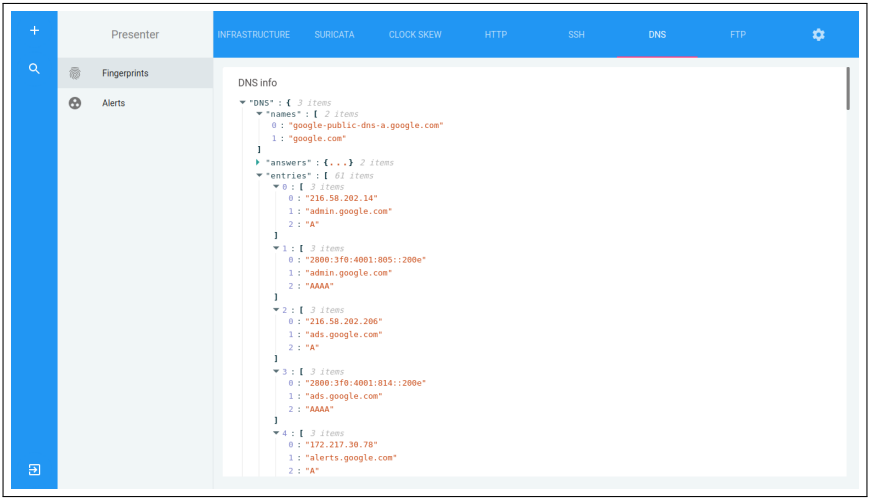
Resultados do Protótipo

Utilização dos resultados (SSH)



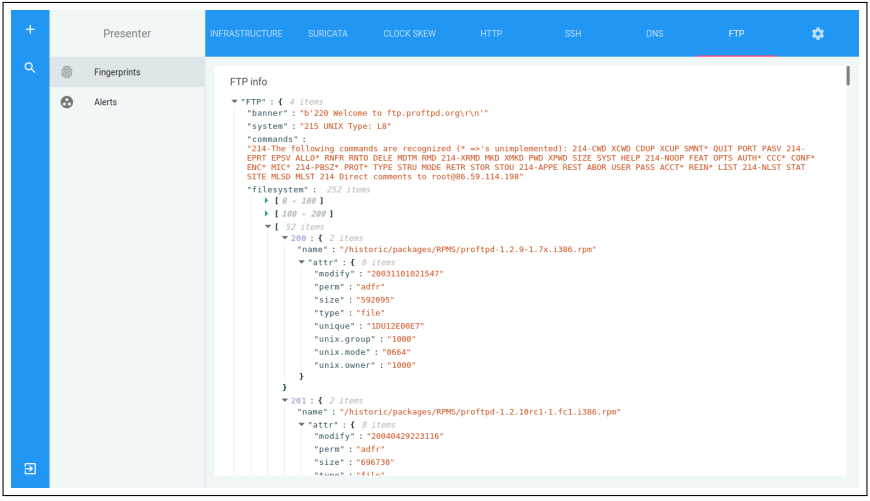
Resultados do Protótipo

Utilização dos resultados (DNS)

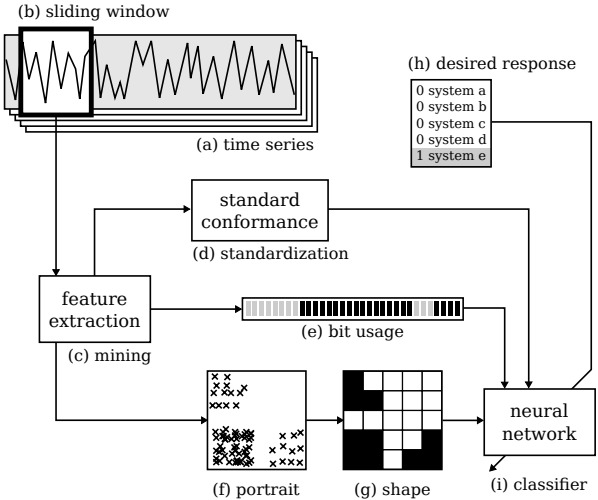


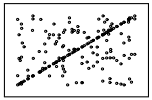
Resultados do Protótipo

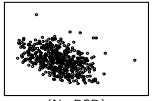
Utilização dos resultados (FTP)

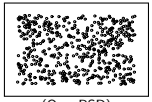


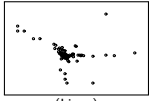
Utilização dos resultados (Sistema Operacional)







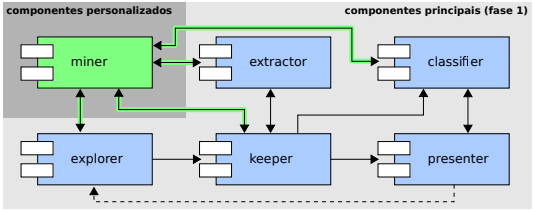


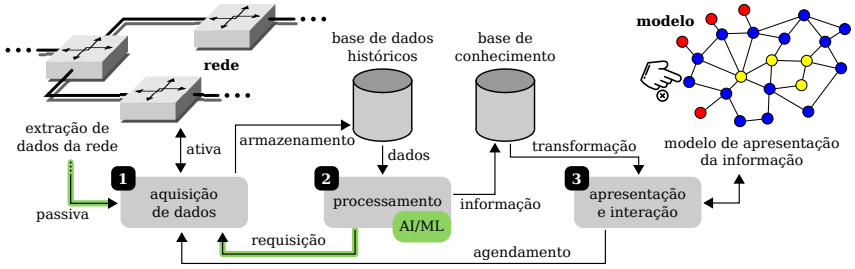


Proposta para Fase Piloto

Visão para próxima fase

- Caracterização passiva
- Caracterizar infraestrutura
- Alertar atividade suspeita
- Confiabilidade da identificação
- Base de dados e transmissão segura





19º WRNP
Workshop RNP
7 | 8 MAIO
Campos do Jordão | SP

Obrigado

João Paulo de Souza Medeiros

jpsm@dct.ufrn.br