

## **MTD para Proteção de Redes SDN**

**Cristian Souza (IFRN)**

Túlio Pascoal (Université du Luxembourg)

Emídio Neto (IFRN)

Francisco Sales (IFRN)

Felipe Dantas (IFRN)

---



# Agenda

1. Conceitos básicos;
2. Motivação e proposta;
3. Avaliação e resultados;
4. Conclusão e trabalhos futuros.



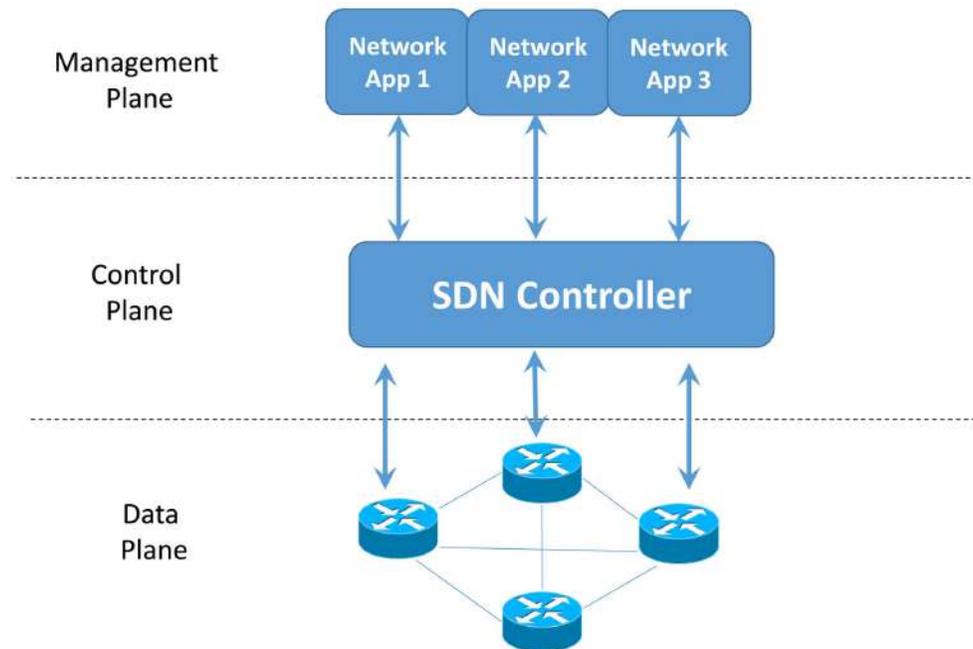
# Conceitos básicos

---



# Conceitos básicos: SDN

- Software-Defined Networking



Fonte: <https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3990>



# Conceitos básicos: Network fingerprinting

- Etapa essencial para a execução de ataques mais sofisticados
- O atacante realiza um levantamento preciso da rede
  - Hosts ativos, portas abertas, sistemas operacionais, serviços vulneráveis, etc.
- Ferramentas para varredura automática:
  - nmap (<https://nmap.org>)
  - Angry IP Scanner (<https://angryip.org>)
  - Zmap (<https://zmap.io>)
- Portanto, é necessário fazer uso de ferramentas para minimizar a superfície de ataque



# Conceitos básicos: MTD

- **M**oving **T**arget **D**efense
- Técnicas para prevenção de diferentes ataques
- Consiste em randomizar os atributos da rede ou sistema com o objetivo de diminuir a superfície de ataque
- Não é restrito ao domínio das redes de computadores
- *IP randomization*



# Motivação e proposta

---



# Motivação e proposta

- MTD para proteção de SDN
- Utilizar a alta programabilidade de redes SDN para melhorar a segurança das mesmas
- Aplicar **IP *randomization*** para dificultar a execução de ataques de fingerprinting



# Descrição da solução

- O algoritmo aloca IPs virtuais aos dispositivos
- Todo o tráfego gerado para os IPs reais é bloqueado
- A randomização ocorre em intervalos predefinidos (**exemplo: 60s**)
- Resiliência em redes de diferentes tamanhos
- Alta velocidade (**0.038s no pior cenário considerado**)



# Avaliação e resultados

---



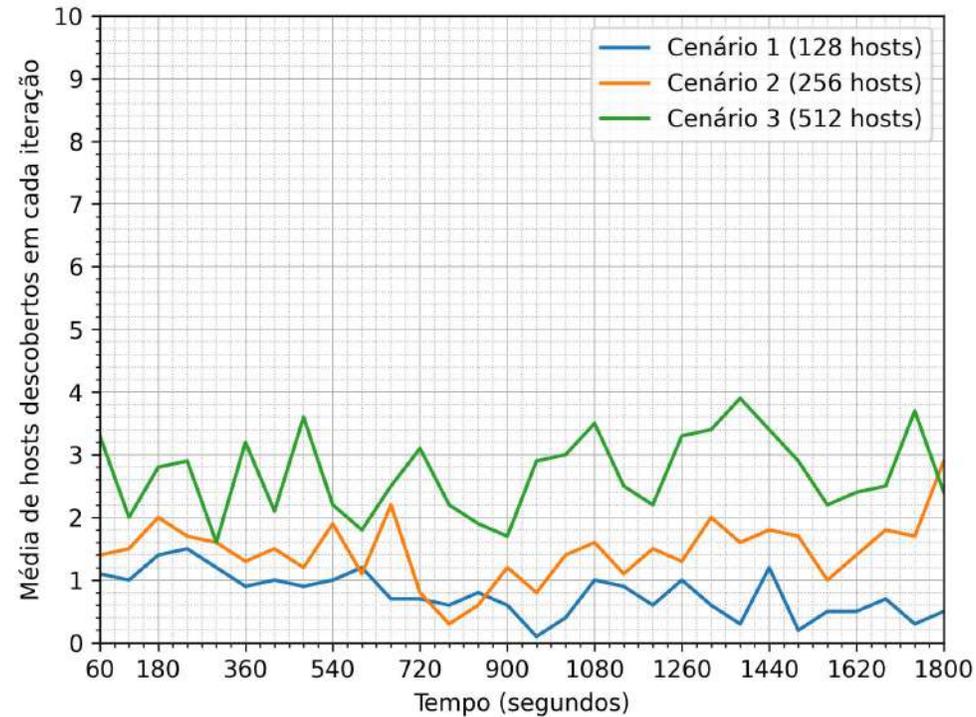
# Avaliação e resultados

- Modelo de ameaça:
  - ◆ Um atacante faz o *scan* da rede com o Nmap (**fingerprinting**)
  - ◆ Para acelerar a análise, o mesmo utiliza os parâmetros máximos de paralelismo
  - ◆ Para uma comparação justa, o Nmap é configurado para realizar a varredura em faixas aleatórias
  
- Ambiente de testes:
  - ◆ Dell Inspiron I14-5457-A30
  - ◆ 2.40 GHz Intel Corei7-6500U
  - ◆ 8GB RAM
  - ◆ Ambiente virtualizado com Docker
  - ◆ Mininet e Ryu
  - ◆ Redes consideradas: 128, 256 e 512 *hosts*.



# Avaliação e resultados

- Resultados alcançados:





# Avaliação e resultados

- Quantitativamente:
  - O atacante foi capaz de reconhecer apenas 0.78% dos endereços válidos no primeiro cenário, 1.46% no segundo e 2.7% no terceiro.
  - O conhecimento do atacante é limitado e válido apenas durante um período de 60s



# Conclusão e trabalhos futuros

---



# Conclusão e trabalhos futuros

- Foi apresentada uma proposta para proteção de SDN contra ataques de *fingerprinting*
- A ferramenta obteve sucesso em dificultar a coleta de informações por parte do atacante
  
- Trabalhos futuros:
  - Formalização de uma métrica para a definição do parâmetro de randomização
  - Avaliar o impacto da ferramenta na Qualidade de Serviço (QoS)
  - Avaliar a efetividade da ferramenta em cenários com múltiplos atacantes



# Agradecimentos

Os autores agradecem ao CNPq e ao IFRN pelo fomento ao desenvolvimento do presente trabalho.

## **MTD para Proteção de Redes SDN**

**Cristian Souza (IFRN)**

Túlio Pascoal (Université du Luxembourg)

Emídio Neto (IFRN)

Francisco Sales (IFRN)

Felipe Dantas (IFRN)

---