

# Faculdade de Tecnologia Senac Goiás

## Relatório estatístico a partir da coleta de dados durante a realização do ataque de CAM Flood e MITM

Alunos:

Jordan Gladys

Liniker Lettierre

Rony Gabriel

Vinícius Henrique

Goiânia/Dezembro/2015

## Relatório geral de ataque

Segue abaixo as seguintes informações sobre o andamento do ataque:  
Total de hosts envenenados : 1;

Total de hosts afetados pelo ataque: 2;

Lista de endereços MAC afetados:

50e5.49f5.4904  
50e5.49fa.49fb7

Throughput de pacotes ARP do atacante:

[illegible]

Para negar o ataque de ARP spoofing, foi utilizada uma defesa (hardening) a partir da Ferramenta arpON, que monitora a tabela ARP na rede, bloqueando alterações na tabela. Como o Man in the middle utiliza-se de falsificar o endereço do pacote para redirecioná-lo, depois dessa técnica de hardening se torna, o ataque se torna falho, pois o arpON nega a modificação do endereço do pacote. Com isso, impedimos o ataque e conseguimos até ver qual é o atacante.