Avaliando o impacto de ataques simultâneos em sistemas computacionais: Uma abordagem baseada em modelo de árvore de ataque

Ronierison de Souza Maciel
Orientador: Prof. Dr. Paulo Romero Martins Maciel

rsm4@cin.ufpe.br
http://cin.ufpe.br/~rsm4/

Universidade Federal de Pernambuco - UFPE
Centro de Informática - CIn

Agenda

MoDCS Group

Centro de Informática UFPE

Motivação

- Um número crescente de ataques **Distributed Denial-of-Service (DDoS)** em infraestruturas **computacionais**.
- Este crescimento é solidificado pela **fragilidade das infraestruturas** de **Computação**:
  - Estima-se um **crescimento de anual de 44% na taxa de ataque DDoS** (Arbor Networks, 2017).
- Em contrapartida com o avanço da **Internet of Things (IoT)**, há uma preocupação, cresce a utilização desses dispositivos para criação de redes **zumbi** ou **botnet** ro**bot** e **net**work para realização de **ataques DDoS**.

MoDCS Group Centro de Informática UFPE

Objetivo geral

- O propósito desta pesquisa é avaliar um **conjunto de ameaças** e o impacto de suas ações maliciosas em uma infraestrutura **computacional**.

Objetivos específicos

- Propor modelos de **Attack Tree (AT)** para infraestruturas **computacionais**, considerando **diversas vulnerabilidades** que possam ocorrer no ambiente;
- Identificar os **diferentes tipos impactos** causados pelas ameaças;
- Propor uma **avaliação** dos **agentes de ameaças** para melhor solucionar as atividades hostis.
- Apresentar **soluções** para mitigar as **atividades maliciosas**.

Objetivos específicos

- Propor modelos de **Attack Tree (AT)** para infraestruturas **computacionais**, considerando **diversas vulnerabilidades** que possam ocorrer no ambiente;
- Identificar os **diferentes tipos impactos** causados pelas ameaças;
- Propor uma **avaliação** dos **agentes de ameaças** para melhor solucionar as atividades hostis.
- Apresentar **soluções** para mitigar as **atividades maliciosas**.

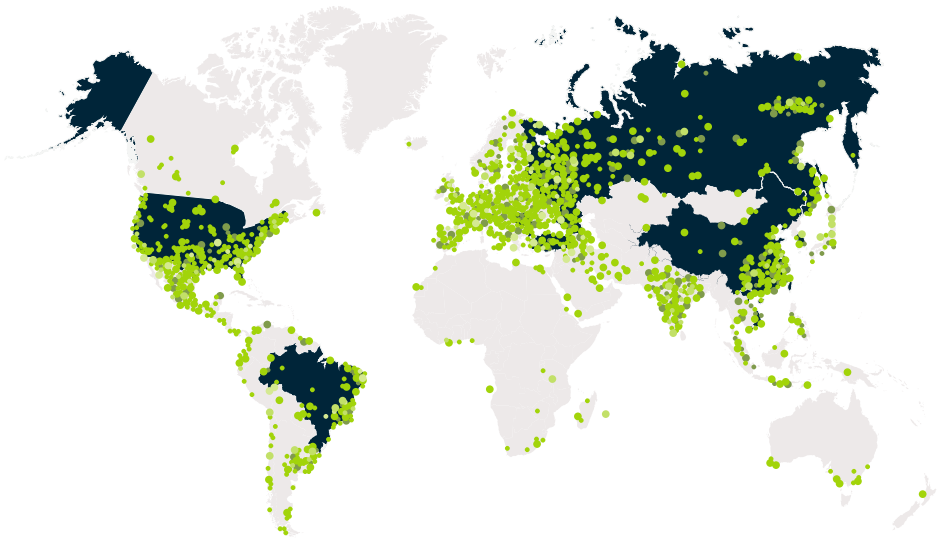
Objetivos específicos

- Propor modelos de **Attack Tree (AT)** para infraestruturas **computacionais**, considerando **diversas vulnerabilidades** que possam ocorrer no ambiente;
- Identificar os **diferentes tipos impactos** causados pelas ameaças;
- Propor uma **avaliação** dos **agentes de ameaças** para melhor solucionar as atividades hostis.
- Apresentar **soluções** para mitigar as **atividades maliciosas**.

Objetivos específicos

- Propor modelos de **Attack Tree (AT)** para infraestruturas **computacionais**, considerando **diversas vulnerabilidades** que possam ocorrer no ambiente;
- Identificar os **diferentes tipos impactos** causados pelas ameaças;
- Propor uma **avaliação** dos **agentes de ameaças** para melhor solucionar as atividades hostis.
- Apresentar **soluções** para mitigar as **atividades maliciosas**.

Países utilizando DDoS



Top Origin Countries for Login Attempts

COUNTRY	NUMBER OF ATTEMPTS
China	102,975
Vietnam	26,573
Republic of Korea	19,465
United States	17,062
Brazil	16,609
Russia	13,378
Taiwan	11,697
Hong Kong	11,200
Turkey	10,190
Romania	9,856

Figure: Países com origem DDoS

MoDCS Group

Países utilizando DDoS

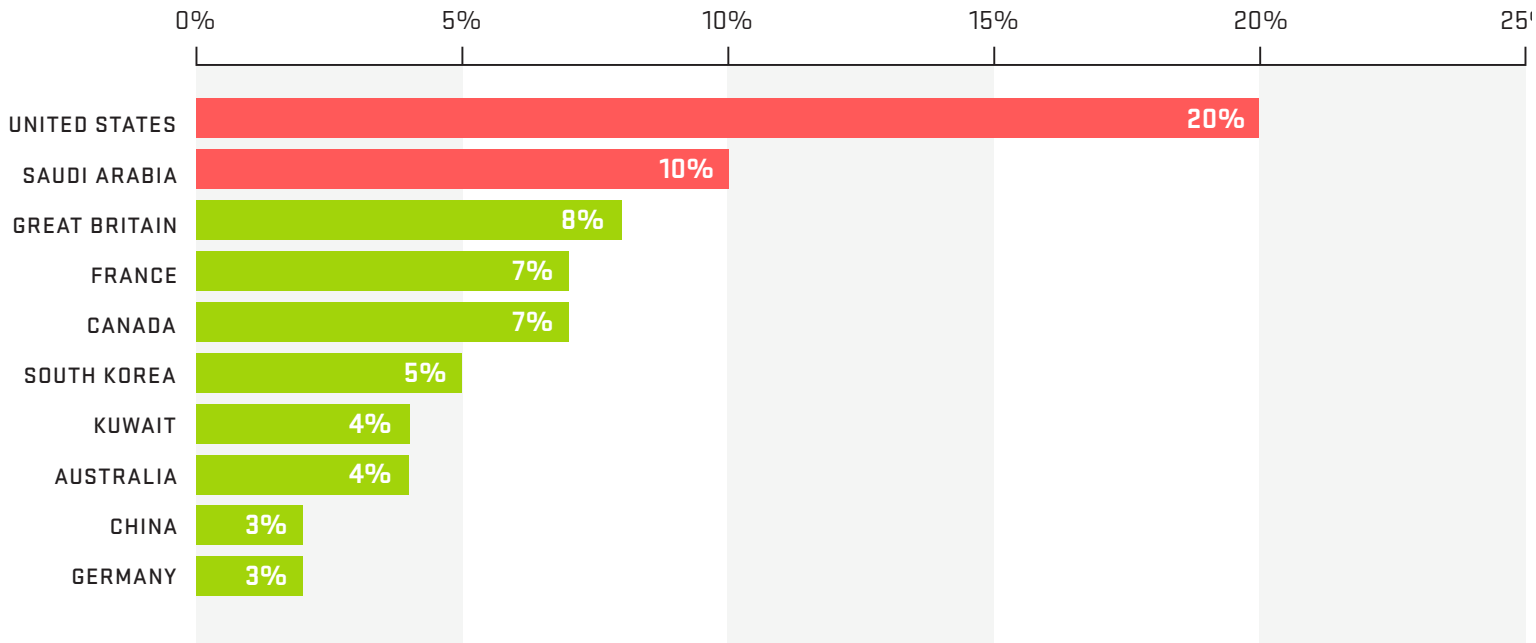


Figure: Principais países que utilizaram ataque acima de 10Gbps

MoDCS Group

Árvore de probabilidade - Left to right

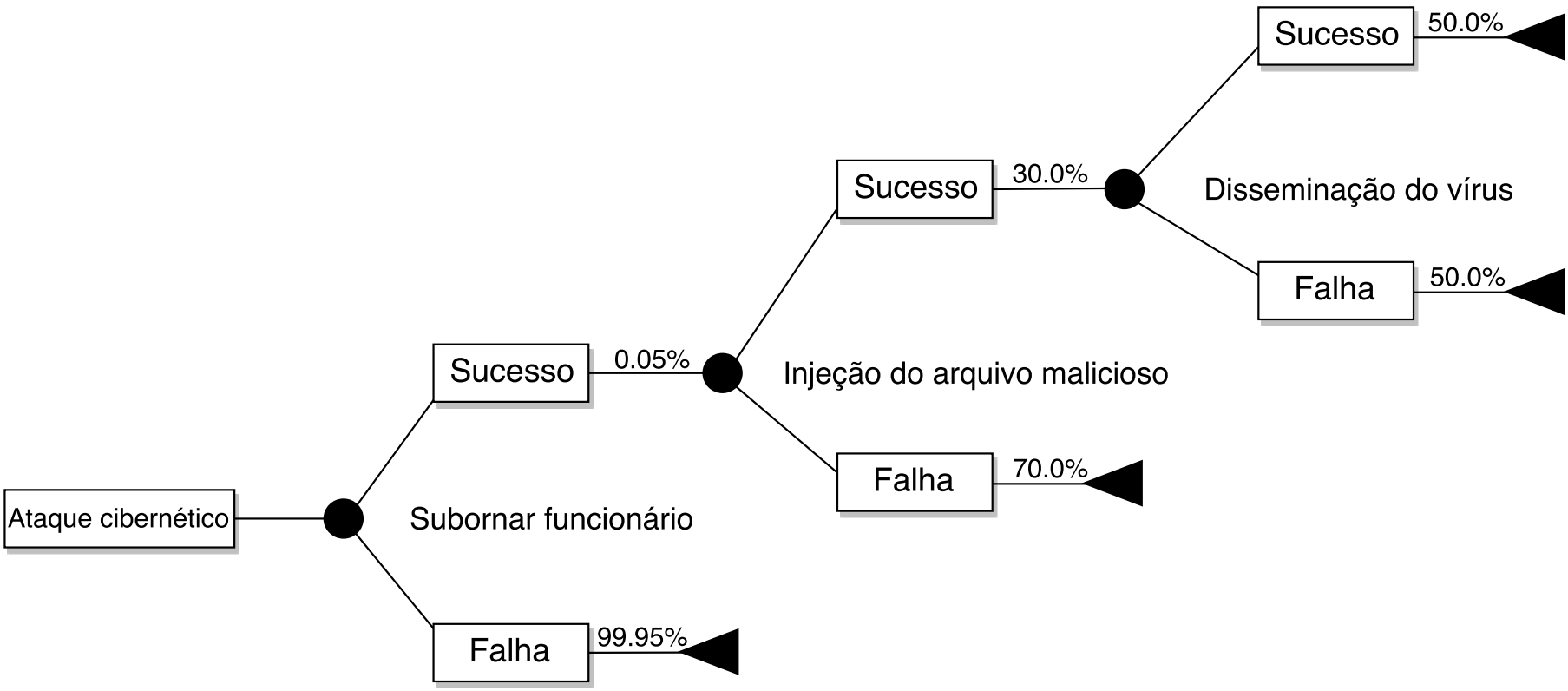


Figure: Árvore de probabilidade

Árvore de decisão - Left to right

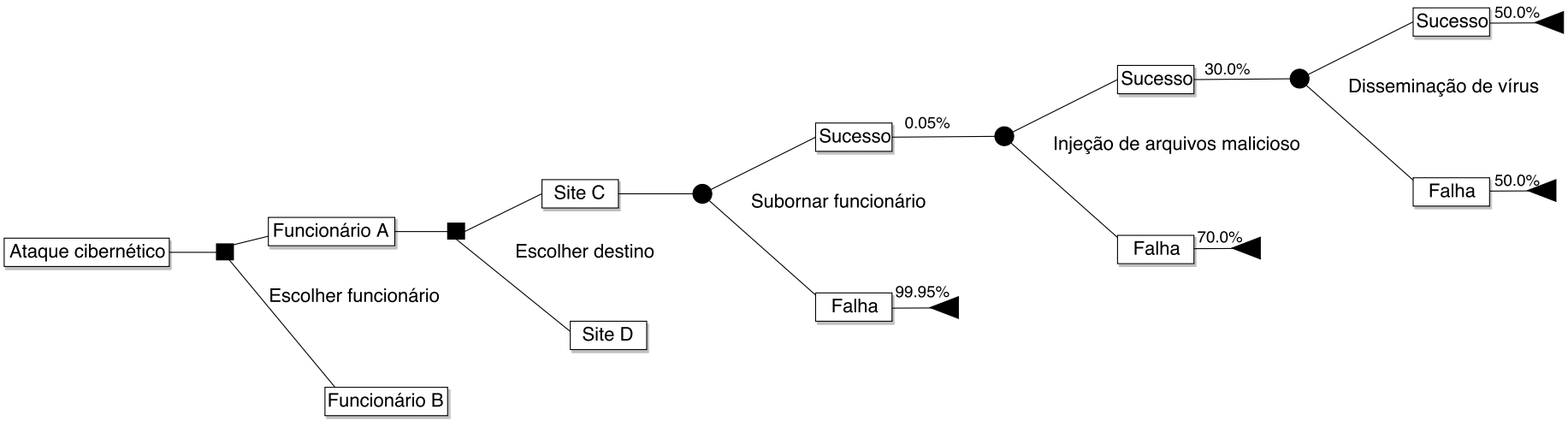


Figure: Árvore de decisão

Metodologia: Visão Geral

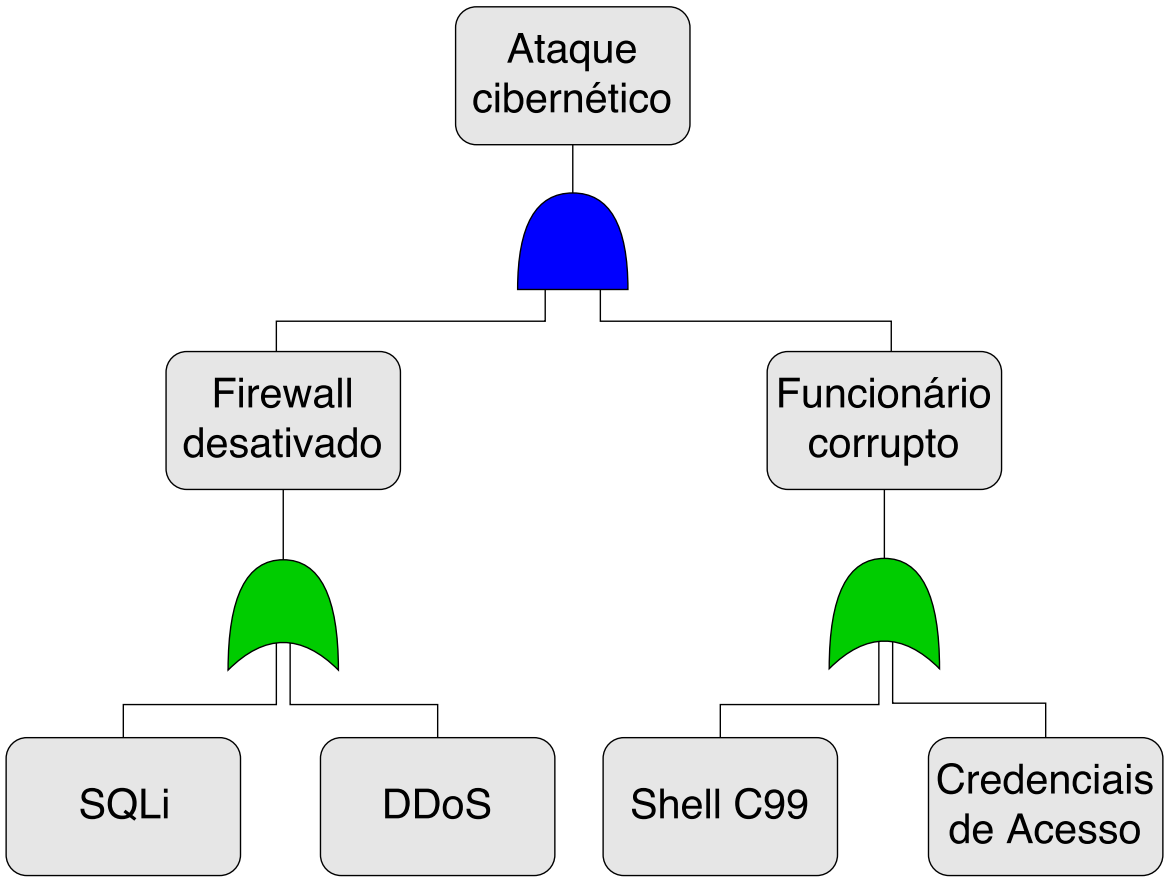


Figure: Exemplo árvore de ataque

Arquitetura DDoS

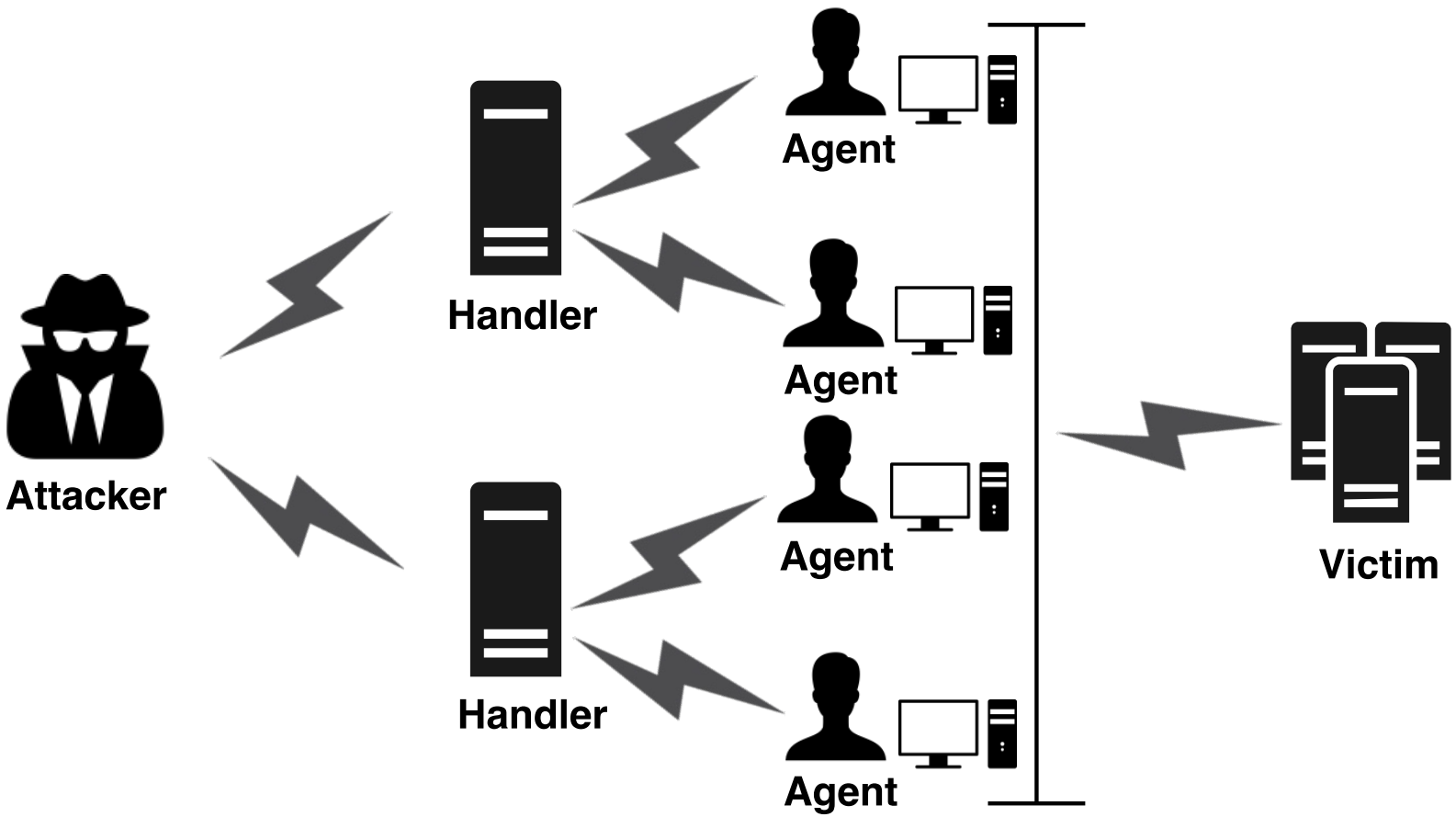


Figure: Arquitetura base

Cenários de conectividade

(a) Cenário #Vítima

(b) Cenário #Atacante

Mapa do modelo base

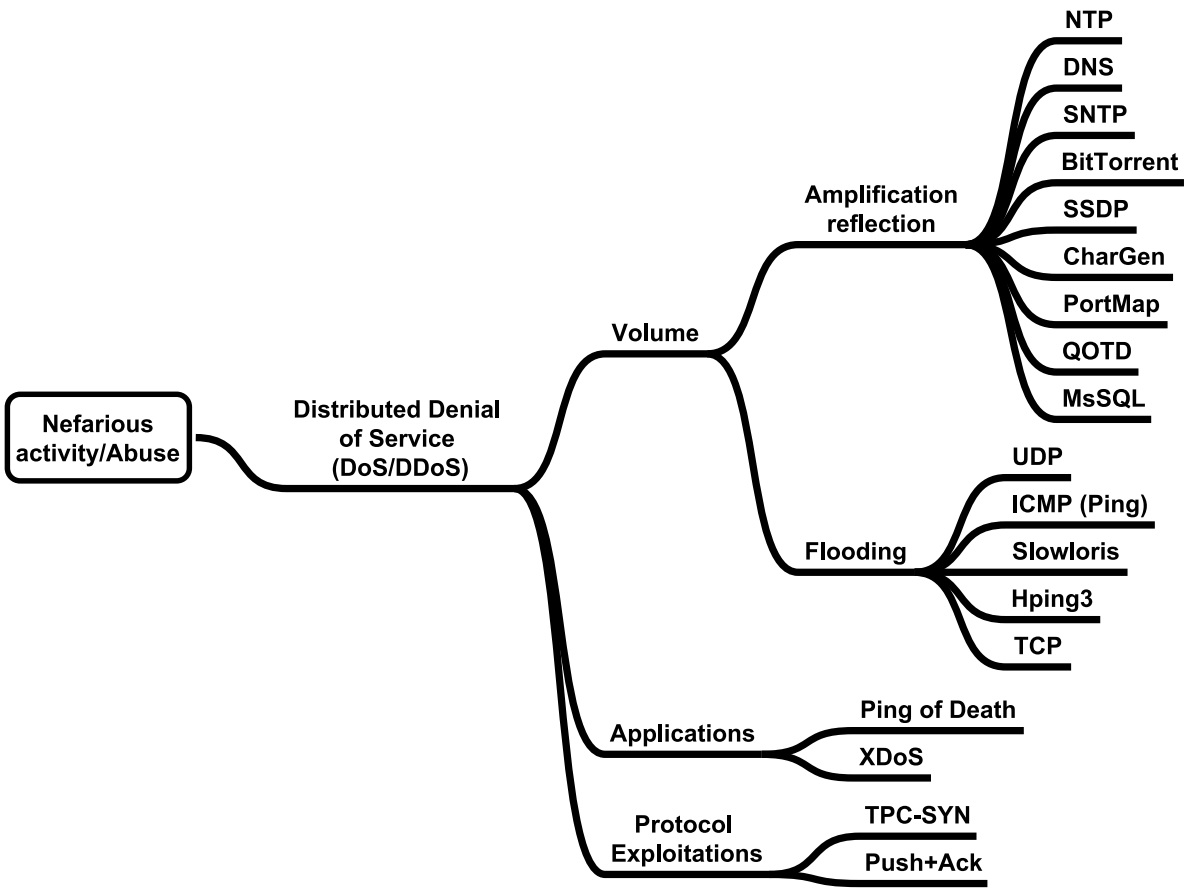


Figure: Mapa de ameaças

Modelo Base

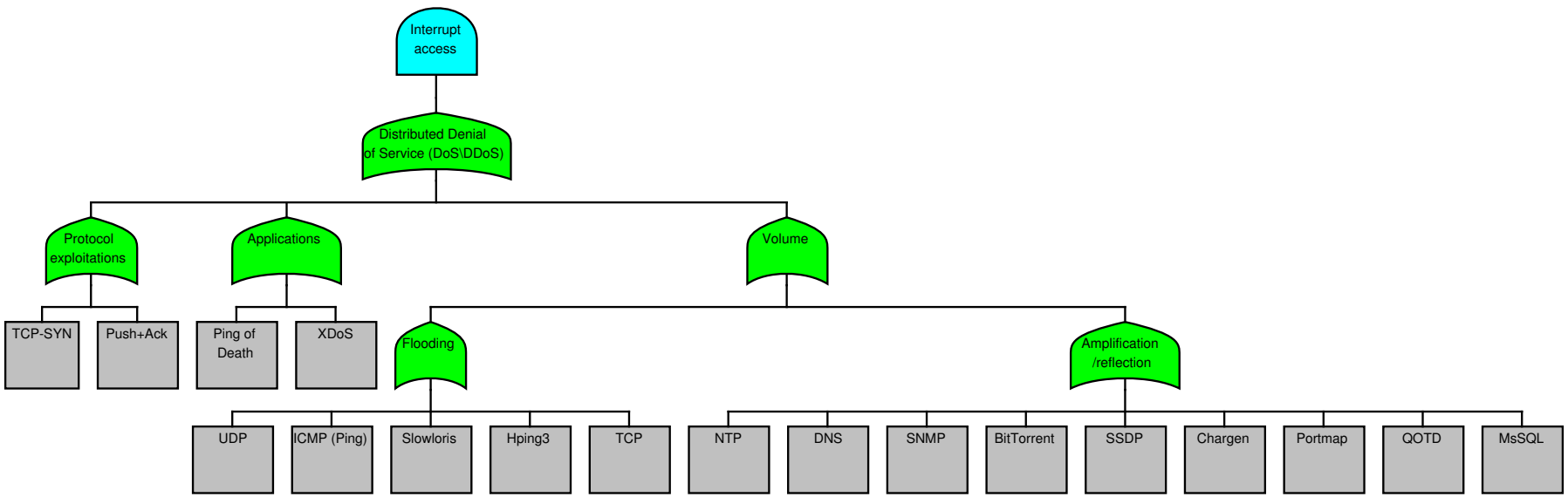
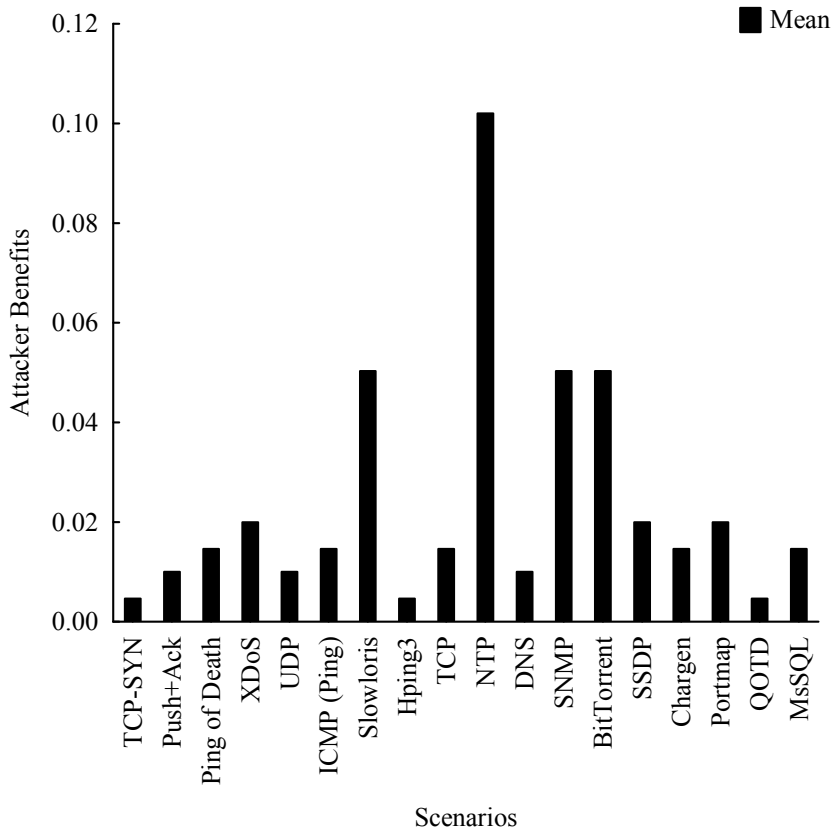


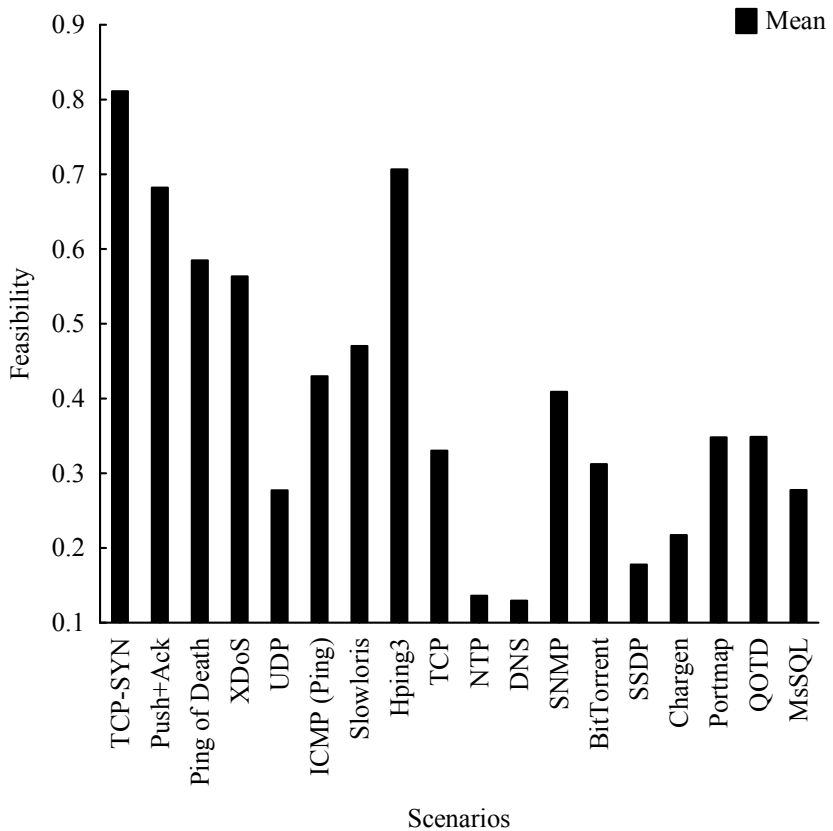
Figure: Árvore de Ataque - Base

Resultados



(a) Benefícios com ataque

Resultados



(b) Facilidade do Ataque

Segundo Modelo

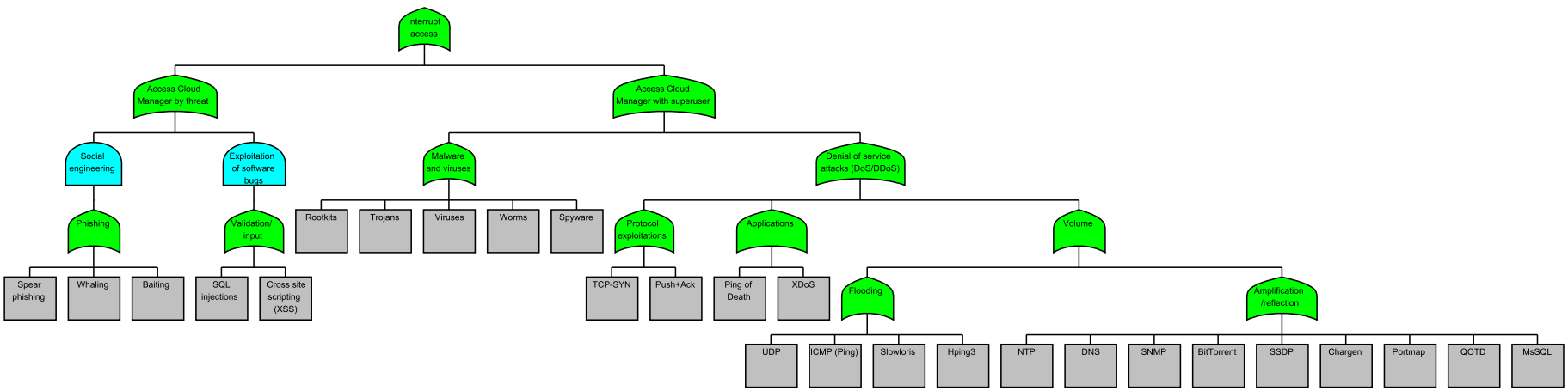


Figure: AT - Diversas ameaças

Segundo Modelo

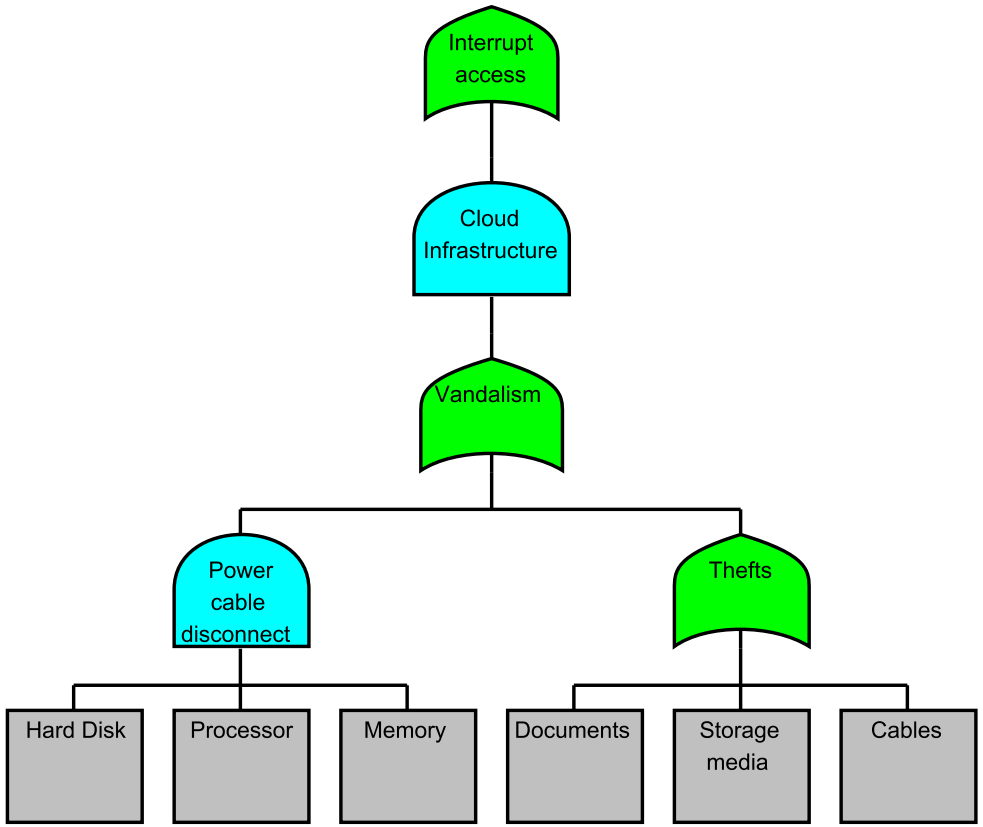


Figure: AT - Ataque físico

Dúvidas?

MoDCS Group

Centro de Informática UFPE