Título:

Classificação e Mitigação de Ataques DDoS de Inundação em Servidores Web utilizando Contadores de Desempenho de Hardware.

Aluno: Pablo Philipe Pessoa (ppp2@cin.ufpe.br)
Orientador: Prof. Dr. Paulo Maciel

Centro de Informática UFPE

Universidade Federal de Pernambuco

MoDCS Research Group

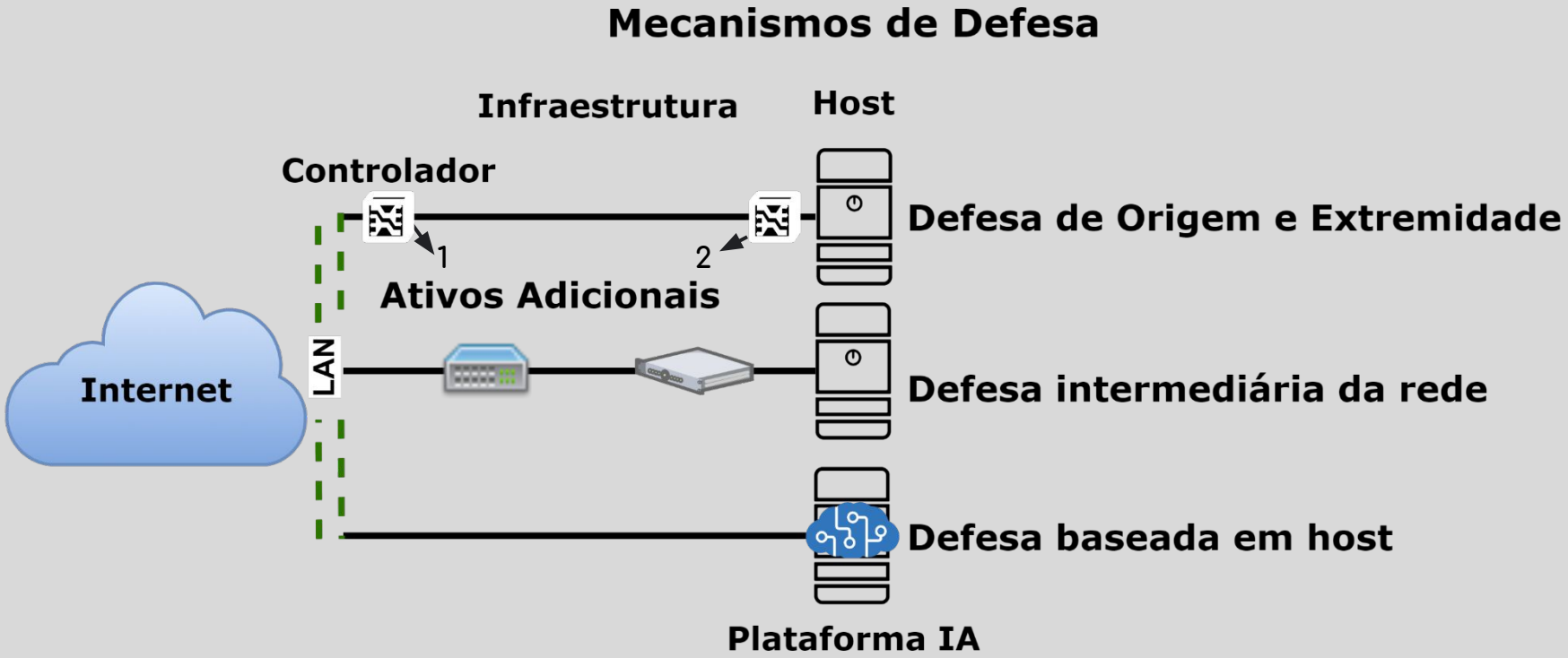
Agenda

- Contextualização
- Justificativa
- Objetivos
- Solução Proposta
- Estudo de Caso
- Contribuições
- Conclusões e Trabalhos Futuros

Contextualização

A **segurança da informação** é o processo de **controle** que envolve várias medidas necessárias para **manter** e **preservar** a **informação** de um determinado conjunto, sendo esse conjunto uma **organização** ou um **ativo**. Proteção essa contra **agentes maliciosos**, que ameaçam de forma **direta** ou **indireta** os **ativos** detentores de informações **sensíveis** e **não sensíveis** (SOLMS; NIEKERK, 2013).

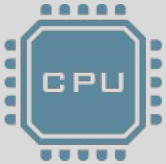
Contextualização



Contextualização

Hardware Performance Counters (**HPCs**) / Contadores de Desempenho de Hardware

São parte de uma unidade especial e dedicada pertencente a estrutura da **CPU**, chamada **Unidade de Monitoramento de Desempenho** (PMU), que pode acessar informações detalhadas sobre as execuções dos processos no sistema.



- Depuração de Hardware;
- Coleta limitada;
- Tipo e o número de eventos disponíveis variam;
- São cumulativos e medidos ao longo do tempo entre intervalos;
- Fornecem informações detalhadas sobre desempenho.

Contextualização

```
perf list

List of pre-defined events (to be used in -e):

cpu-cycles OR cycles                              [Hardware event]
instructions                                      [Hardware event]
cache-references                                  [Hardware event]
cache-misses                                      [Hardware event]
branch-instructions OR branches                   [Hardware event]
branch-misses                                     [Hardware event]
bus-cycles                                        [Hardware event]

L1-dcache-loads                                   [Hardware cache event]
L1-dcache-load-misses                             [Hardware cache event]
L1-dcache-stores                                  [Hardware cache event]
L1-dcache-store-misses                            [Hardware cache event]
L1-dcache-prefetches                              [Hardware cache event]
L1-dcache-prefetch-misses                         [Hardware cache event]
L1-icache-loads                                   [Hardware cache event]
L1-icache-load-misses                             [Hardware cache event]
L1-icache-prefetches                              [Hardware cache event]
L1-icache-prefetch-misses                         [Hardware cache event]
LLC-loads                                         [Hardware cache event]
LLC-load-misses                                   [Hardware cache event]
LLC-stores                                        [Hardware cache event]
LLC-store-misses                                  [Hardware cache event]
```

```
$ perf stat

         Performance counter stats for 'make':

      83723.452481      task-clock:u (msec)       #    1.004 CPUs
      utilized
                 0      context-switches:u        #    0.000 K/sec
                 0      cpu-migrations:u          #    0.000 K/sec
         3,228,188      page-faults:u             #    0.039 M/sec
   229,570,665,834      cycles:u                  #    2.742 GHz
   313,163,853,778      instructions:u            #    1.36  insn per
   cycle
    69,704,684,856      branches:u                #  832.559 M/sec
     2,078,861,393      branch-misses:u           #    2.98% of all
     branches

        83.409183620 seconds time elapsed

        74.684747000 seconds user
         8.739217000 seconds sys
```

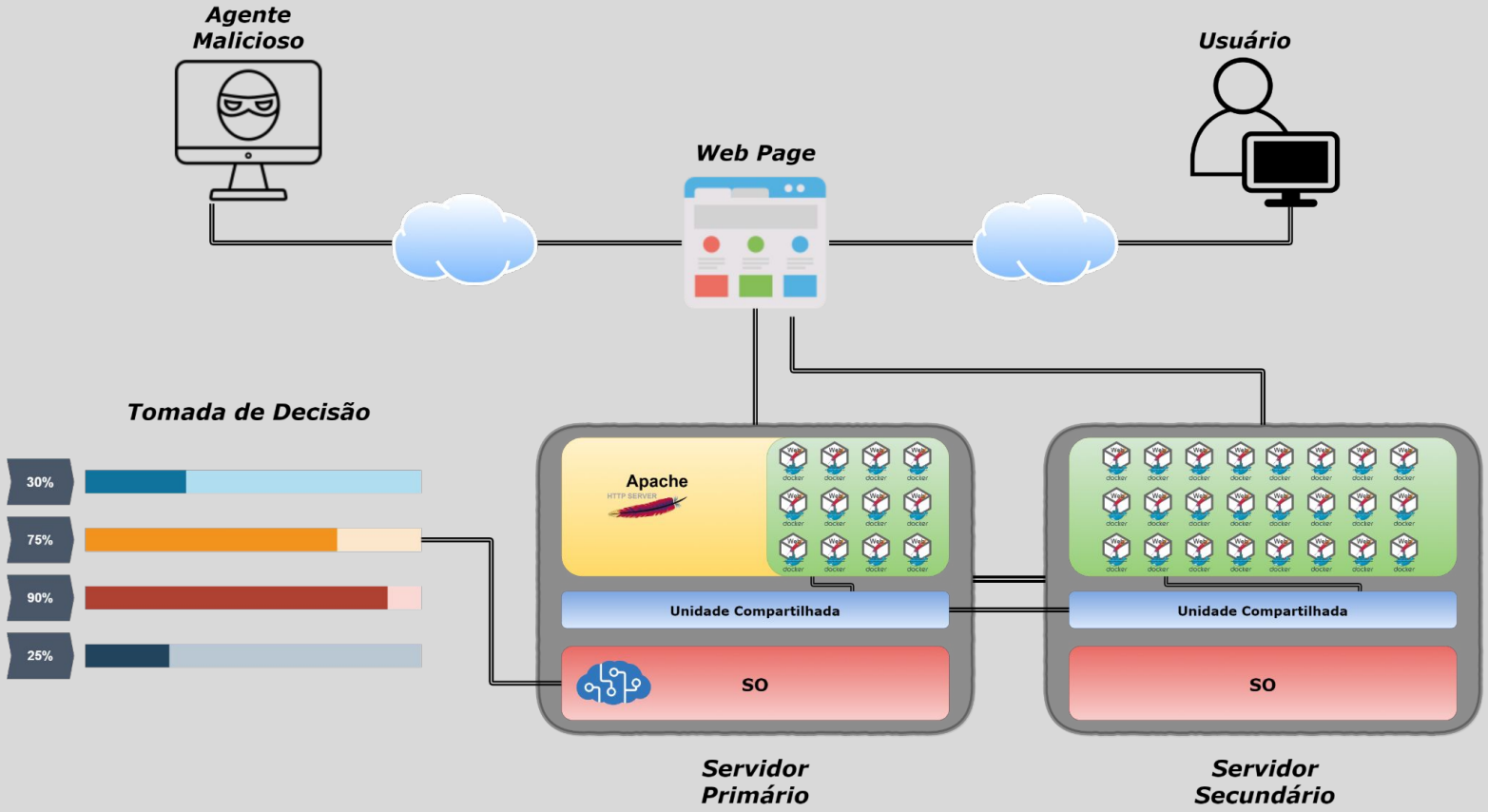
Justificativa

- ➔ Tendência de ataques crescente
- ➔ Proteção tradicional insuficiente
- ➔ Conjunto de dados incompatíveis
- ➔ Hardware não escalonável

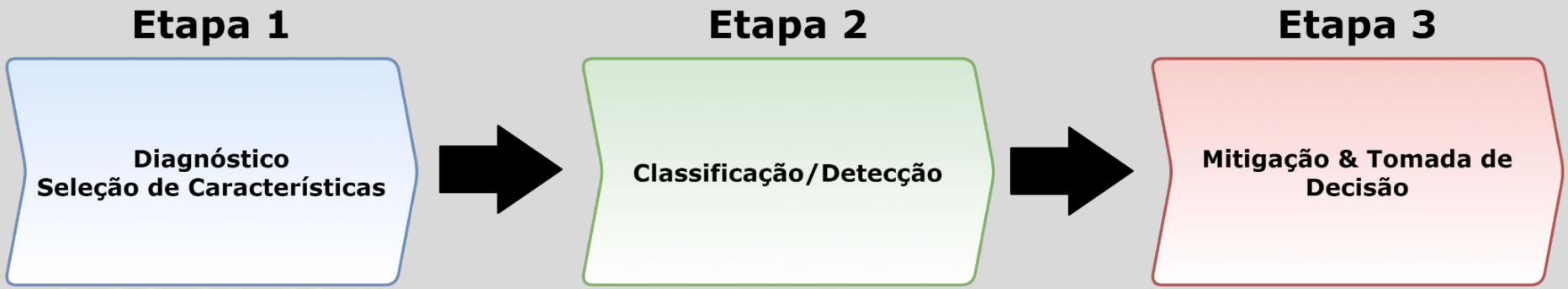
Objetivos

- Desenvolver um mecanismo de **detecção não intrusiva** para **classificação** de situações de ataques de **DDoS** em servidores de **segmento corporativo.**
- O **mecanismo** também possibilitará a classificação de **perfis** comportamentais através da seleção das **características** e dos **HPCs** mais **influentes**.
- Criar um mecanismo de **contramedida** e **tomada de decisão** para **mitigar** ataques **DDoS** e **situações adversas** no sistema.

Solução Proposta

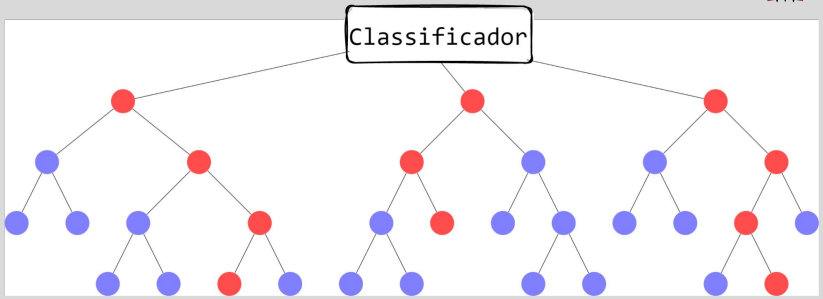


Solução Proposta



Solução Proposta

Random Forest(RF)/ Floresta Aleatória



- A execução não acontece com base em **todas** as **variáveis disponíveis**.
- O algoritmo irá escolher de maneira **aleatória** algumas **variáveis**, e então realizar os **cálculos** com base nas **amostras** selecionadas, para definir qual dessas variáveis será utilizada no nó **raiz**.
- No próximo **nó**, novamente serão escolhidas duas (ou mais) **variáveis**, e o processo de escolha se **repetirá**. Desta forma a árvore será **construída** até o último **nó**.
- Depois que o **modelo** é gerado, as **previsões** são feitas a partir de **votações**. Cada **árvore** toma uma **decisão** a partir dos dados apresentados. A decisão mais **votada** é a **resposta** do algoritmo.

Estudo de caso

Ferramental

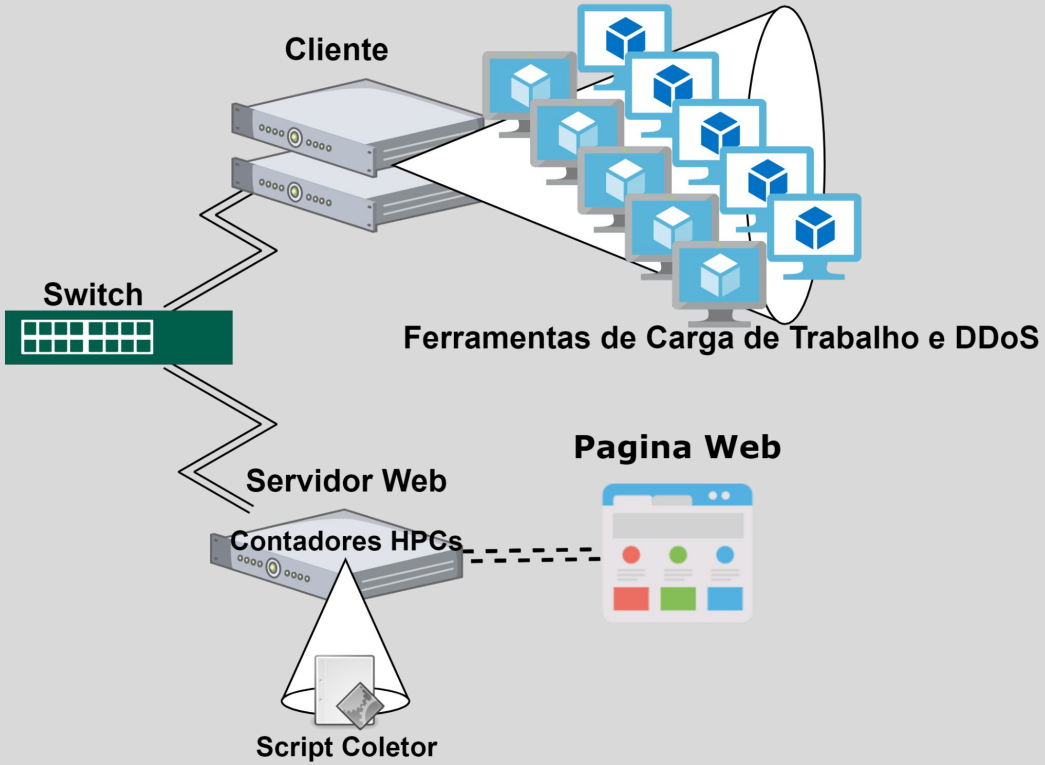
Carga de trabalho

Ataque Dos/DDoS

- **H.O.I.C** (High Orbit ION Cannon)
- **H.U.L.K.** (HTTP Unbearable Load King)
- **L.O.I.C.** (Low Orbit Ion Cannon)
- SwitchBlade
- Tor's Hammer

Estudo de caso

Ambiente



Contribuições

Publicações

COMPUTERS & SECURITY 110 (2021) 102434

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A methodology for selecting hardware performance counters for supporting non-intrusive diagnostic of flood DDoS attacks on web servers

Pablo Pessoa do Nascimento, Paulo Pereira, Jr Marco Mialaret, Isac Ferreira, Paulo Maciel*

Centro de Informática – Universidade Federal de Pernambuco (UFPE) Av. Prof. Moraes Rego, 1235 - Cidade Universitária, Recife - PE, 50670-901, Brazil

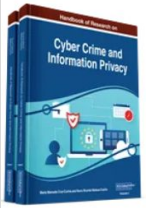
ARTICLE INFO

Article history:
Received 8 February 2021
Revised 12 June 2021
Accepted 2 August 2021
Available online 8 August 2021

Keywords:
Methodology
Diagnosis
Distributed Denial of Service
Hardware Performance Counters
Infrastructure
Web Server

ABSTRACT

Web server outages caused by a Distributed Denial of Service (DDoS) attacks have increased considerably over the years. Intrusion Detection Systems (IDS) are not sufficient to detect threats in the system, even when used in conjunction with Intrusion Prevention Systems (IPS) and even considering the use of data sets containing information about typical situations and attacks on the system's service. Performing analyzes with a very dense amount of observed variables can cost a significant amount of host resources. Furthermore, these data sets are at risk of not representing the system's behavior properly, and they cannot always be shared as they may contain confidential information in the diagnostic data. This paper presents a non-intrusive diagnostic methodology to select hardware performance counters in HTTP flood DDoS attacks on enterprise-level web servers, combining methods and techniques from different segments. The proposed approach uses low-level resource appliances such as Hardware Performance Counters (HPCs) for diagnosis, creating behavioral profiles in the face of attacks and usual service usage. The proposed strategy supports delivering reliable diagnoses with accurate characterization without third-party data sets. With the proposed methodology, we were able to reduce HPCs by 26%, compared to the initial group.



Handbook of Research on Cyber Crime and Information Privacy (2 Volumes)

Maria Manuela Cruz-Cunha (Polytechnic Institute of Cávado and Ave, Portugal) and Nuno Ricardo Mateus-Coelho (Polytechnic Institute of Management and Technology, Portugal)

Release Date: August, 2020 | Copyright: © 2021 | Pages: 753
DOI: 10.4018/978-1-7998-5728-0
ISBN13: 9781799857280 | ISBN10: 179985728X | EISBN13: 9781799857297

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

Chapter 25

Prediction, Detection, and Mitigation of DDoS Attacks Using HPCs: Design for a Safer Adaptive Infrastructure

Pablo Pessoa Do Nascimento
Universidade Federal de Pernambuco, Brazil

Isac F. A. F. Colares
Universidade Federal de Pernambuco, Brazil

Ronierison Maciel
Universidade Federal de Pernambuco, Brazil

Humberto Caetano Da Silva
Universidade Federal de Pernambuco, Brazil

Paulo Maciel
Universidade Federal de Pernambuco, Brazil

ABSTRACT

Web service interruptions caused by DDoS (distributed denial of service) attacks have increased considerably over the years, and intrusion detection systems (IDS) are not enough to detect threats on the network, even when used together with intrusion prevention systems (IPS), taking into account the increase of assets in the traffic path, where it creates unique points of failure in the system, and also taking into account the use of data that contains information about normal traffic situations and attacks, where this comparison and analysis can cost a significant amount of host resources, to try to guarantee the prediction, detection, and mitigation of attacks in real-time or in time between detection and mitigation, being crucial in harm reduction. This chapter presents an adaptive architecture that combines techniques, methods, and tools from different segments to improve detection accuracy as well as the prediction and mitigation of these threats and to show that it is capable of implementing a powerful architecture against this type of threat, DDoS attacks.

DOI: 10.4018/978-1-7998-5728-0.ch025

Conclusões

Resultados obtidos

- Desenvolvimento de uma **metodologia não intrusiva** para **diagnóstico** de situações de ataques de **DDoS** em **servidores de segmento corporativo.**
- Geração de **perfis comportamentais** de ataques de **DDoS**, através das **características** do sistema e da seleção dos **HPCs** mais **influentes**.
- Utilização de várias técnicas **estatísticas** e de **IA** para análises de dados do **diagnóstico**.

Trabalhos Futuros

- Implementar os dados em um **detector/classificador**;
- Implementar **mecanismos** de **mitigação**;
- Estender os **tipos** de ataques;
- Estender os **HPCs** utilizados;
- Investigar a utilização dos **HPCs** em outros **ambientes**;
- Análises **adicionais** nas **variáveis**;
- **Integrar** com outras **ferramentas** de administração de rede;
- Realizar análises de **Disponibilidade** e **Confiabilidade**

OBRIGADO!

THANK YOU!

ARIGATŌ!

Classificação e Mitigação de Ataques DDoS de Inundação em Servidores Web utilizando Contadores de Desempenho de Hardware.

Aluno: Pablo Philipe Pessoa (ppp2@cin.ufpe.br)
Orientador: Prof. Dr. Paulo Maciel

Centro de Informática UFPE

Universidade Federal de Pernambuco

MoDCS Research Group