MAC0499 - Trabalho de Formatura Supervisionado

Análise de Desempenho de Computadores de Baixo Custo em um Sistema de Detecção de Intrusão

Lucas Seiki Oshiro
Supervisor: Daniel Macêdo Batista

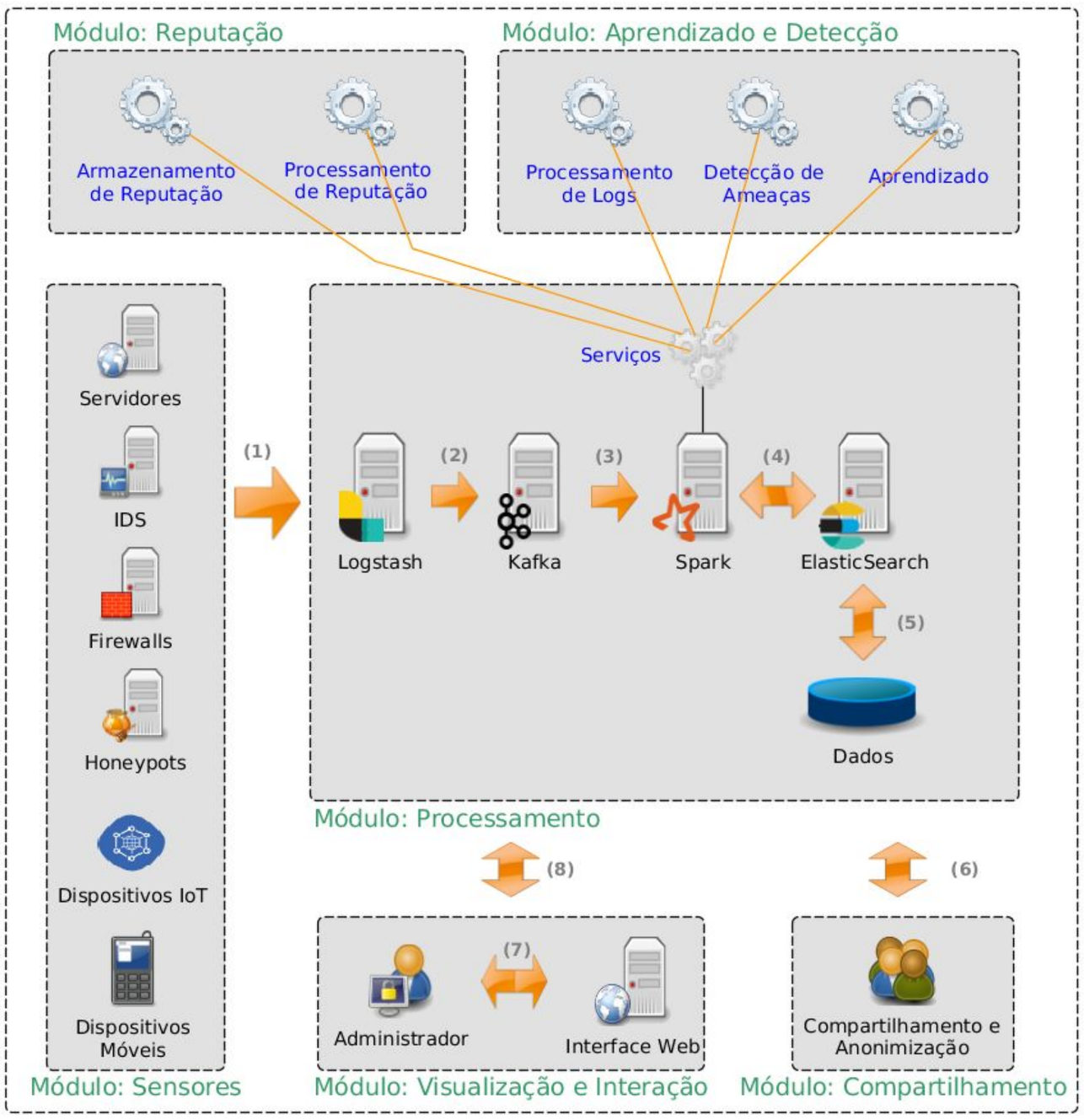
Durante o ano de 2017, durante o projeto **GT-BIS** da **RNP**, foi construído um sistema para detecção de ameaças em sistemas web.

Esse sistema consistia no uso de ferramentas de processamento de fluxo de dados para a análise dos logs vindos de servidores web. Cada ferramenta funcionava em uma máquina máquina virtual.

Através desses logs, o sistema era capaz de observar três tipos de ataques:

- **Injeção de SQL:** inserção de dados que, se não tratados, realizam ações indevidas no banco de dados;
- **XSS refletido:** Inserção de código HTML e JavaScript malicioso na URL, que é executado quando o site é aberto;
- **XSS persistido:** Envio de código HTML e JavaScript malicioso, que fica armazenado e é executado no navegador de todos que entram no site.

A arquitetura do sistema está descrita na imagem a seguir:



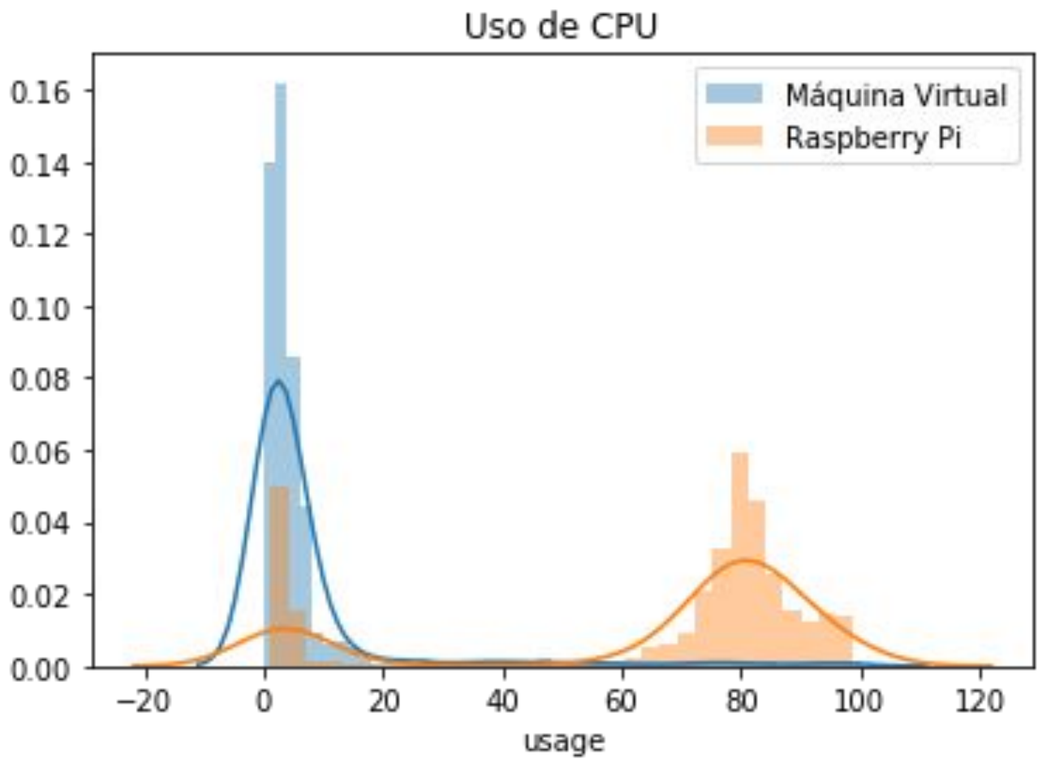
Arquitetura do sistema GT-BIS. Créditos: GT-BIS

Computadores de placa única, também conhecidos pelo acrônimo SBC, são placas de circuito impresso com processador, memória, e entrada e saída de dados. Em outras palavras, são computadores completos montados em apenas uma placa. O mais famoso deles é a Raspberry Pi.

O grande sucesso desse tipo de computador, junto ao baixo preço e baixo consumo de energia, levou-o a ser usado para a construção de clusters. Este trabalho analisa seu desempenho, e avalia a viabilidade do uso de SBCs no sistema mencionado anteriormente.

Para essa análise, foi feito um script para a leitura do uso de CPU, do uso de RAM, dos acessos ao disco e do uso de rede das máquinas, tanto físicas quanto virtuais. No caso da Raspberry Pi, também foi medida a temperatura do processador e o consumo de energia elétrica.

Um exemplo é mostrado no histograma a seguir, comparando o uso de CPU na máquina virtual e na Raspberry Pi, para a mesma aplicação (Logstash).



Uso de CPU da execução do Logstash na VM e na Raspberry Pi

Como é possível notar, o uso de CPU pela Raspberry Pi foi maior que na VM, porém, inferior a 100%, mostrando que ela é viável para a execução do Logstash no sistema.

Referências

- Página pessoal (acessado em 29/11/2019) https://linux.ime.usp.br/~lucasoshiro/mac0499/
- GT-BIS – Mecanismos para Análise de Big Data em Segurança da Informação (acessado em 22/03/2019) http://gtbis.ime.usp.br/
- Pahl, C., Helmer, S., Miori, L., Sanin, J., and Lee, B.(2016). A Container-Based Edge Cloud PaaS Architecture Based on Raspberry Pi Clusters.