Um honeypot-cluster baseado em SDN e Raspberry Pis contra ameaças de segurança

Aluno: Davi de Menezes Pereira
Supervisor: Daniel Macêdo Batista

26 de Abril 2022

1 Introdução

A quantidade cada vez maior de aplicações web com diversos elementos interligados, como aquelas em cidades inteligentes e em internet da coisas (IoT), levam a um interesse cada vez maior na melhoria de sistemas, observado pelo crescente investimento em dispositivos globalmente conectados e em pesquisa na área de IoT, por exemplo. Porém, fatos recentes têm demonstrado que esses sistemas e dispositivos não têm recebido a devida atenção quando o assunto é segurança da informação. Apesar de já existirem serviços e propostas com a intenção de atuar nesse problema, eles podem ser muito caros. Com isso, surge a necessidade da criação de métodos e dispositivos que sejam mais baratos no monitoramento e estudo de ameaças a esses sistemas.

Com essa demanda, é possível notar esforços, tanto na academia quanto na indústria, na busca por soluções para o problema. Dentre eles, é possível citar o GT-BIS [1][2], que teve por objetivo o desenvolvimento de um sistema para análise de quantidades massivas de dados heterogêneos capturados em redes de computadores a fim de detectar incidentes de segurança, além de trabalhos que utilizaram clusters de Raspberry Pi no monitoramento de ataques [3] [4] [5]. No contexto desses projetos, os estudos sugerem que o uso de plataformas de computação de baixo custo, em especial SBC (*single board computers*), como o Raspberry Pi, em sistemas de monitoramento de ameaças seria uma boa alternativa.

Com base nessa informações, este projeto visa desenvolver um honeypot a partir de um cluster composto por Raspberry Pis com o objetivo de monitorar e estudar acessos suspeitos em um servidor, tomando como base sistemas existentes de detecção de ameaças. Os tipos de ataques abordados serão de negação de serviço e de *SQL injection*, e cada um desses ataques terá uma configuração diferente a ser executada pelo sistema. Por exemplo, para ataques de negação de serviço, podem ser necessários 5 computadores, enquanto para o outro tipo de ataque pode ser necessário somente um. Pensando nesta situação, surge a necessidade da utilização de um balanceamento de carga para dar vazão ao ataque sem o atacante perceber. Um destaque desta proposta é o fato de que ela

será desenvolvida num ambiente de rede definida por software (SDN), o que exigirá diversas tomadas de decisão em torno da implementação de um controlador para a rede.

De forma geral, o trabalho explorará principalmente conceitos aprendidos nas matérias Redes de Computadores e Sistemas Distribuídos (MAC0352) e Programação Concorrente e Paralela (MAC0219). Além disso, em relação a outros trabalhos que estão servindo como base, o diferencial do projeto está em criar um sistema de segurança que consegue lidar com mais de um tipo de ataque, e uma contribuição relevante será a implementação do controlador SDN que permitirá a migração do tráfego sem alertar o atacante de que ele está sendo monitorado.

2 Conceitos Básicos

2.1 Ataques contra aplicações Web

Os tipos de ameaça de segurança que estamos levando em consideração neste trabalho são os ataques de negação de serviço (DoS) e ataques de *SQL injection*.

Os do primeiro tipo são aqueles que causam uma grande quantidade de entradas nos *logs* do servidor. Dentre essas ameaças específicas, as mais comuns são as do tipo DoS (*Denial of Service*), que visam atacar um serviço com uma grande quantidade de acessos simultâneos, por vezes efetuados por diversos agentes diferentes.

Os do segundo tipo aproveitam falhas em sistemas que interagem com bancos de dados SQL em que o atacante consegue inserir uma instrução SQL personalizada numa consulta na entrada da aplicação.

2.2 Computadores de placa única (SBC)

Computadores de placa única, ou SBCs (*single board computers*), são computadores completos montados em apenas uma placa, ou seja, possuem processador, memória e entrada e saída de dados [6]. São vantajosos porque não têm um custo muito elevado, consomem pouca energia e, apesar de não serem tão potentes como computadores mais caros, podem ser utilizados como nó de processamento em sistemas horizontalmente escaláveis, como em clusters. Neste trabalho, o SBC escolhido foi o Raspberry Pi 3 model B+ [7].

2.3 Cluster

Um cluster consiste em computadores conectados que trabalham em conjunto, de modo que podem ser considerados como um único sistema, pois cada computador executa a mesma tarefa. Tudo isso controlado por software [8].

2.4 Honeypot

Honeypot é um mecanismo de segurança em que o computador é configurado para detectar, desviar ou neutralizar tentativas de uso não autorizado de sistemas. Geralmente, um Honeypot consiste de um servidor que parece ser uma parte legítma do sistema, que contém informações atrativas para o atacante, e é configurado de forma a apresentar, propositalmente, falhas de segurança, mas que, na verdade, está isolado e controlado. Com isso, é possível monitorar e bloquear ou analisar invasores [9].

2.5 Rede definida por software (SDN)

Rede definida por software (SDN) é uma abordagem de infraestrutura que abstrai os recursos de rede para um sistema virtualizado (citar). Ela separa as funções de encaminhamento e de controle de rede para criar uma rede que possa ser gerenciada e programada de maneira central. Com a SDN, as equipes de operações de TI controlam o tráfego de rede em topologias complexas por meio de um painel centralizado. Assim, elas não precisam gerenciar cada dispositivo de rede manualmente [10].

3 Cronograma e principais atividades

- Fevereiro - Março
  Leitura de tópicos e trabalhos relacionados.
- Março- Maio
  Planejamento e análise do ambiente experimental (essencialmente ambiente emulado controlado via SDN com OpenFlow).
- Maio
  Configuração do ambiente experimental do ponto de vista de balanceamento de carga.
- Junho
  Configuração do ambiente experimental do ponto de vista de classificação de tráfego
  Projeto dos algoritmos e implementação no ambiente baseado em Raspberry Pis para instanciação automática do honeypot no caso de *SQL injection*.
- Julho
  Projeto dos algoritmos e implementação no ambiente baseado em Raspberry Pis para instanciação automática do honeypot no caso de DoS.
- Agosto - Setembro
  Realização dos experimentos e análise dos resultados
- Setembro - Outubro
  Escrita e revisão da monografia.

Referências

[1] CAMPIOLO, R. et al. Uma Arquitetura para Detecção de Ameaças Cibernéticas Baseada na Análise de Grandes Volumes de Dados. In: *Workshops do SBRC – WSCDC*. [S.l.: s.n.], 2018.

[2] GT-BIS. *GT-BIS – Mecanismos para Análise de Big Data em Segurança da Informação*. 2018. `http://gtbis.ime.usp.br/`. Último acesso em 23/07/2021.

[3] DJANALI, S. et al. Sql injection detection and prevention system with raspberry pi honeypot cluster for trapping attacker. In: *2014 International Symposium on Technology Management and Emerging Technologies*. [S.l.: s.n.], 2014. p. 163–166.

[4] JEREMIAH, J. Intrusion detection system to enhance network security using raspberry pi honeypot in kali linux. In: *2019 International Conference on Cybersecurity (ICoCSec)*. [S.l.: s.n.], 2019. p. 91–95.

[5] TRIPATHI, S.; KUMAR, R. Raspberry pi as an intrusion detection system, a honeypot and a packet analyzer. In: *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*. [S.l.: s.n.], 2018. p. 80–85.

[6] ORTMEYER, C. Then and Now: A Brief History of Single Board Computers. In: *Electronic Design Uncovered, issue 06*. [S.l.: s.n.], 2014. p. 1–4.

[7] Raspberry Pi Foundation. *Raspberry Pi 3 Model B+*. 2021. `https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/`. Último acesso em 23/07/2021.

[8] Wikipedia. *Cluster (computing)*. 2022. `https://simple.wikipedia.org/wiki/Cluster_(computing)`.

[9] Wikipedia. *Honeypot (computing)*. 2022. `https://en.wikipedia.org/wiki/Honeypot_(computing)`.

[10] RedHat. *O que é rede definida por software?* 2022. `https://www.redhat.com/pt-br/topics/hyperconverged-infrastructure/what-is-software-defined-networking`.