XXI Escola Regional de Redes de Computadores / VIII Workshop de Segurança (ERRC/WRSeg). DOI: 10.5753/errc.2024.4683

Artigo Curto/Short Paper

Avaliação e comparação de honeypots: auxiliando administradores de rede na escolha e adoção

Honeypots evaluation and comparison: helping network administrators in the selection and adoption process

Pamela Moura Gonçalves • 2022005992@aluno.restinga.ifrs.edu.br
Instituto Federal do Rio Grande do Sul (IFRS)
Fabiano da Silva Santos • 2022005820@aluno.restinga.ifrs.edu.br
Instituto Federal do Rio Grande do Sul (IFRS)
Fernando Guerreiro Chemello • 2023009628@aluno.restinga.ifrs.edu.br
Instituto Federal do Rio Grande do Sul (IFRS)
Roben Castagna Lunardi • roben.lunardi@restinga.ifrs.edu.br
Instituto Federal do Rio Grande do Sul (IFRS)

resumo. Honeypots podem simular vulnerabilidades em hosts para atrair e detectar possíveis atacantes, possibilitando a análise e estudo de comportamentos maliciosos. Este trabalho tem como objetivo apresentar um trabalho em andamento onde avaliamos diferentes honeypots. Neste trabalho, consideramos diversos aspectos dos honeypots, desde seu funcionamento até sua adequação para uso. Para isso, utilizaremos uma honeynet chamada T-pot para facilitar o uso e comparação destes honeypots. Desta forma, demonstraremos alguns de pontos fortes e fracos dos honeypots e o quanto eles podem ser eficientes para supervisionar serviços e hosts na rede. Por fim, apresentamos os passos necessários para a continuação do trabalho.

abstract. Honeypots can simulate vulnerabilities in hosts to attract and detect potential attackers, allowing the analysis and study of malicious behaviour. This paper aims to present an ongoing work where we evaluate different honeypots. This work considers several aspects of honeypots, from their operation to their suitability for adoption. Therefore, we will use a honeynet called T-pot to facilitate using and comparing these honeypots. Additionally, we will demonstrate some of the strengths and weaknesses of honeypots and how efficient they can be in monitoring services and hosts in the network. Finally, we present relevant steps for the future work.

palavras-chave: Cibersegurança • Honeypot • Honeynet
keywords: Cibersecurity • Honeypot • Honeynet

1 Introdução

Não é novidade que as invasões às redes de computadores representam um problema grave e crescente para organizações e indivíduos em todo o mundo. Nesse cenário, os honeypots surgem como uma estratégia para detectar ameaças, atuando como iscas para atrair atividades maliciosas[1]. Honeypots permitem estudar o comportamentos dos atacantes em um ambiente controlado, proporcionando informações valiosas para a segurança. Ainda, os honeypots são estruturados conforme os objetivos planejados por cada projeto, podendo existir algum mecanismo de ação/resposta ao invasor durante a coleta dos dados[2]. Portanto, é possível diferenciar os honeypots pelo seu nível de interação com o atacante. Uma significativa vantagem dos honeypots é a capacidade de poder projetá-los para operar em conjunto em uma rede, o que acaba formando assim, uma honeynet. Essa abordagem não apenas amplia o leque de funcionalidades e serviços disponíveis, mas também gera uma semelhança mais próxima com um sistema real.

Embora os honeypots se revelem eficazes na detecção de invasões, diversos desafios emergem em sua implementação e manutenção. Alguns problemas comuns são: a dificuldade em distinguir entre tráfego legítimo e malicioso quando possui um volume de dados grande; a possibilidade de um atacante detectar o honeypot e utilizá-lo como ponto de partida para explorar a rede; os custos associados à manutenção contínua dos sistemas para não representar um risco alto; a complexidade da análise e correlação dos logs gerados que demandam tempo; a documentação do próprio sistema dos honeypots não atualizadas[3] [4]. Além disso, a evolução constante das técnicas de ataque mediante avanço da tecnologia exige atualizações contínuas e a adaptação das estratégias de honeypots.

O principal objetivo deste trabalho é avaliar diferentes honeypots, utilizando o projeto de uma plataforma chamada T-pot, que além de possuir diversos honeypots, também contém ferramentas disponíveis que facilitam o monitoramento. Por fim, discutiremos trabalhos futuros, com foco na adoção de Inteligência Artificial (IA) para melhoria dos resultados de coleta e mecanismos de defesa.

2 Evolução de Honeypots

O surgimento de honeypots se destaca no final dos anos 1980, Clifford Stoll [5] [6] para monitoramento de comportamento de ataques. Com o passar do tempo, honeypots evoluíram. Por exemplo, quando um honeypot conseguiu identificar um *exploit* inédito associado a um serviço em sistemas Solaris, ressaltando a capacidade deles de detectar novas vulnerabilidades [7].

Desde então, tem-se criado diversos honeypots e com diferentes objetivos, evoluindo junto com os sistemas, serviços e ferramentas disponíveis. Por exemplo, com a evolução do conceito de Internet das Coisas, novos desafios tem sido encontrados devido ao volume de dados produzidos e riscos que os dispositivos apresentam [8]. Ainda, honeypots são fundamentais na indústria, particularmente pelo alto nível de automação e integração com sistemas em rede [9, 10].

Atualmente, um dos principais focos de estudos está relacionado com a utilização com inteligência artificial (IA) para analisar os dados gerados, podendo oferecer análises sobre as ações e comportamentos dos atacantes, entre outras vantagens [11]. No entanto, a implementação de honeypots que são baseados em IA enfrenta alguns desafios, como a necessidade de equilibrar de forma cuidadosamente a segurança e a atividade das iscas [12]. Essa evolução nas tecnologias de honeypots traz implicações significativas para a segurança de redes e sistemas críticos, especialmente em um cenário onde as ameaças cibernéticas estão em constante mudança e evolução [13].

3 Avaliação

Como mencionado anteriormente, os honeypots apresentam desafios significativos em termos de manutenção, e a documentação é um elemento necessário para realizá-la de forma eficiente. Por isso, é importante garantir atualizações constantes, com mais detalhes possível para ter uma compreensão coerente do que é necessário para seu funcionamento. Evitando representar diversos riscos para a integridade dos dados de uma organização, e sem comprometer suas ferramentas.

O projeto T-Pot [14] facilita consideravelmente essa tarefa, sendo projetado para ter baixa manutenção por ser baseado a partir de imagens docker e com atualização frequente delas. Para gerenciar melhor todos os containers com os honeypots e executá-los de forma simplificada, é utilizado o Docker compose. permitindo criar uma honeynet eficiente, com monitoramento integrado em um único ambiente. Desta forma, é preciso somente uma instalação, o restante são configurações específicas que são bem explicadas na documentação. Oferecendo vinte e quatro (24) imagens com honeypots de diferentes serviços e diversas ferramentas auxiliares, como o Kibana, que é demonstrado na figura 1 a visualização de *dashboards* para análise facilitada dos *logs*. Além de sua boa documentação, contendo detalhes técnicos importantes para entender sua arquitetura, partições para planejamento, certificados e entre outras configurações importantes em geral, como personalizar os serviços e honeypots. É importante destacar que existe uma configuração padrão nele, ao qual os dados são enviados e coletados para a comunidade aprimorar coletivamente a segurança, alimentando o Sicherheitstacho [15], onde possui alertas dos países de origem do atacante e do alvo, além da categoria de qual seria o honeypot.

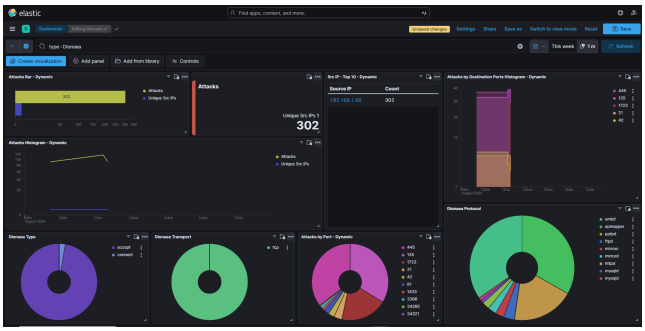

Figura 1. Dashboards do Dionaea no Kibana.

Assim como os outros honeypots quando implementados, é necessário ter um planejamento e definir quais serão utilizados e onde seriam configurados, para não serem facilmente descobertos por atacantes e isolá-los em uma área onde não tenha dados sensíveis. A avaliação do projeto foi realizada usando Máquinas Virtuais com o monitor VirtualBox, para simular ataques nos honeypots antes da implantação em redes reais. Para poder realizar uma comparação entre os honeypots, o t-pot foi instalado em duas VMs com configurações diferentes e rodar honeypots distintos. Após alguns testes com ferramentas de PENTEST, determinamos que escolheríamos aqueles que oferecessem diferentes serviços. Além de ficar mais parecido com um sistema, eles acabaram não demonstrando diferenças significativas, mesmo quando comparados entre serviços iguais. Ao final, foram selecionados seis honeypots diferentes, conforme apresentado na tabela 1 onde são apresentados quais seriam os escolhidos e seus detalhes mais essenciais, como: qual seria seu **tipo**, **interação** e **serviços**.

A primeira classificação apresentada na tabela 1 é referente ao **tipo** (passivo ou ativo). Essa classificação está relacionada à identificação de possuir ou não uma ação ao entrar em contato com alguma atividade considerada maliciosa. A sua **interação**, se refere ao quanto o atacante teria contato, interferindo diretamente na quantidade de dados que vai ser gerado e ao risco que pode apresentar. Possuindo três níveis de interatividade: alta, média e baixa. Aqueles que são de alta, fornecem um ambiente mais realista, com diversos

Honeypot	Tipo	Interação	Serviços
Cowrie	Passivo	Média	SSH e Telnet
Hellpot	Ativo	Média	HTTP
Heralding	Passivo	Baixa	Diversos
Dionaea	Passivo	Baixa	Diversos
Ddospot	Passivo	Baixa	Baseados em UDP
Mailoney	Passivo	Baixa	SMTP

Tabela 1. Comparação dos honeypots testados.

serviços, aplicações e sistema operacional real. O que gera mais dados, mas também, pode acabar deixando a desejar em sua vulnerabilidade pela sua complexidade. Os de baixa interatividade são mais simples e menos informativos, mesmo que perceba do que se trata, não tem acesso a um sistema real. Já aqueles que são de média interação, acabam ficando entre os dois tipos, contendo o necessário, mas sem conter a complexidade dos de alta. Os **serviços** é um critério bem importante, pois a partir dele é onde vamos saber o que vai ser simulado, conseguindo tomar cuidado no planejamento e evitar que fique visualmente perceptível.

Por ser do tipo ativo e fazer uma ação, o Hellpot contém diferença significativa entre os demais. Ele foi projetado para enganar bots maliciosos, mandando um fluxo infinito de dados, o que acaba causando uma sobrecarga no sistema do atacante e o deixando instantaneamente incapacitado. Os Honeypots Cowrie, Mailoney, Ddospot e Heralding não apresentaram problemas técnicos aparentes com os testes estabelecidos. Todavia, o Mailoney não apresenta muitos detalhes em questão da documentação, critério importante mencionado anteriormente.

Durante um dos testes realizados para fazer varreduras e identificação, utilizou-se as ferramentas Metasploit em conjunto com o Nmap para conseguir guardar as informações no banco de dados do Kali. Com o objetivo de descobrir assim, quais eram as versões dos sistemas em execução nas portas de todos os honeypot. Após a execução deste processo, acabou sendo identificado um problema com o Dionaea. Onde deveria dizer qual era o serviço rodando naquela porta, estava indicando seu nome, como mostrado na Figura 2. Com este teste foi possível perceber que o metasploit pode reconhecer um honeypot, mesmo que seja um pequeno erro, acaba dando ao atacante de antemão do que se trata, perdendo assim a sua eficácia. Apesar de em [16] propor que o Dionaea é recomendado por ser estável por longo período, como também executar de forma consistente, outros critérios são importantes à serem considerados. Por exemplo, o honeypot foi detectado no teste realizado, perdendo a sua eficácia.

Figura 2. Captura de uma falha no Dionaea.

4 Conclusões & Trabalhos Futuros

Embora durante o trabalho tenha sido mostrado um problema específico relacionado ao Dionaea, os honeypots em geral ainda demonstram ser uma ferramenta poderosa e estratégica no combate a ameaças cibernéticas. Todos os testes realizados com diferentes honeypots no T-Pot, considerando as variações em suas configurações e na quantidade de dados coletados, ambos forneceram uma apresentação com uma base sólida para a sua análise de intrusões. O T-pot se destacou positivamente, como uma implementação de honeynet facilitada pelo Docker compose, o que auxilia significativamente no gerenciamento. O que possibilita a utilização em conjunto em apenas um arquivo, otimizando a coleta de dados e a análise dos dados com praticidade, com a utilização do kibana e seus *dashboards*. Mesmo com a facilidade de instalação do T-pot e o seu gerenciamento, não quer dizer que é isenta de desafios, tudo depende de como vai ser projetado sua implementação e seus objetivos.

A falta de atualização nas documentações e a manutenção inadequada dos honeypots podem torná-los obsoletos e suscetíveis a falhas inesperadas, como no caso do Dionaea. Uma documentação bem elaborada também é essencial para compreender a estrutura do sistema em questão. Mesmo na ausência de falhas visíveis, a falta de clareza pode levar a configurações incorretas ou incompletas pela incompreensão sobre o funcionamento do sistema. Assim como, a evolução da Inteligência Artificial aplicada aos honeypots pode apresentar avanços significativos para determinar uma otimização de tempo, proporcionando maior automação e *insights* aprofundados sobre o comportamento dos invasores, já que são muitos dados gerados.

Desta forma, como trabalhos futuros pretende-se explorar a utilização de Inteligência Artificial para classificar e prever atividades suspeitas, permitindo uma análise preditiva e, consequentemente, uma resposta mais rápida a possíveis ataques. Além disso, a IA pode ajudar na automação do processo de coleta de dados e na geração de relatórios, reduzindo a carga de trabalho dos administradores de segurança e aumentando a precisão das análises.

Declarações complementares

Financiamento

Este trabalho teve financiamento do IFRS e da FAPERGS. Além disso, teve bolsas de Iniciação Científica financiadas pela FAPERGS e CNPq.

Referências

1 Javadpour, A. *et al.* A comprehensive survey on cyber deception techniques to improve honeypot performance. *Computers & Security*, v. 140, p. 103792, 2024. ISSN 0167-4048.

2 Zhang, F. *et al.* Honeypot: a supplemented active defense system for network security. *In*: PROCEEDINGS of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies. 2003. P. 231–235.

3 Qassrawi, M. T.; Zhang, H. Client honeypots: Approaches and challenges. *In*: 4TH International Conference on New Trends in Information Science and Service Science. 2010. P. 19–25.

4 Razali, M. F. *et al.* IoT Honeypot: A Review from Researcher's Perspective. *In*: 2018 IEEE Conference on Application, Information and Network Security (AINS). 2018. P. 93–98.

5 Stoll, C. *Stalking the Wily Hacker. Communications of the ACM.* Association for Computing Machinery, 1988.

6 Stoll, C. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Doubleday, 1989.

7 Spitzner, L. *Honeypots: Tracking Hackers.* Addison-Wesley, 2002.

8 Franco, J. *et al.* A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems. *IEEE Communications Surveys & Tutorials*, v. 23, n. 4, p. 2351–2383, 2021.

9 Wei, X.; Yang, D. Study on Active Defense of Honeypot-Based Industrial Control Network. *In*: 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). 2021. P. 2019–2022.

10 Sun, Y. *et al.* Honeypot Identification in Softwarized Industrial Cyber–Physical Systems. *IEEE Transactions on Industrial Informatics*, v. 17, n. 8, p. 5542–5551, 2021.

11 Paul, S. *et al.* Exploring the Impact of AI-based Honeypots on Network Security. *Educational Administration: Theory and Practice*, Educational Administration: Theory e Practice, p. 251–258, jun. 2024.

12 Matin, I. M. M.; Rahardjo, B. The Use of Honeypot in Machine Learning Based on Malware Detection: A Review. *In*: 2020 8th International Conference on Cyber and IT Service Management (CITSM). 2020. P. 1–6.

13 HONEYPOT and cyber deception as a tool for detecting cyber attacks on critical infrastructure. 2023. Disponível em: https://ceur-ws.org/Vol-3374/paper06.pdf.

14 T-POT - The All In One Multi Honeypot Platform. Nov. 2024. Disponível em: https://github.com/telekom-security/tpotce.

15 SICHERHEITSTACHO. Nov. 2024. Disponível em: https://www.sicherheitstacho.eu/#/en/about.

16 Moric, Z. *et al.* Honeypots in Cybersecurity: Their Analysis, Evaluation and Importance. *Preprints*, Preprints, ago. 2024. Disponível em: https://doi.org/10.20944/preprints202408.0946.v1.