Mitigação de Riscos para Internet das Coisas com uso de *Honeypot* de Baixa Interatividade

Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie (UPM) – São Paulo – SP – Brasil

eduardoccg2106@gmail.com, rodrigoc.silva@mackenzie.br

Orientador: Dr. Rodrigo Cardoso Silva

Resumo. *O objetivo da pesquisa é simular um honeypot de baixa interatividade na rede Internet das Coisas ou Internet of Things (IoT) e enteder na prática todo o processo de interação com os agentes maliciosos, desde o primeiro contato com o invasor até a saída dos dados capturados pelo nosso honeypot.*

Palavras-chaves: *Honeypot*, *IoT*, Segurança

Abstract. *The objective of the research is to simulate a low interactivity honeypot in the Internet of Things (IoT) network and understand in practice the entire process of interaction with malicious agents, from the first contact with the attacker to the output of captured data by our honeypot.*

Keywords: *Honeypot*, *IoT*, *Security*

1. Introdução

Por meio da Internet das Coisas ou *Internet of Things* (*IoT*), conseguimos unir o mundo real com o mundo digital. Um dispositivo *IoT* nada mais é que um eletrônico que consegue se comunicar com outros sistemas, em outras palavras, é um dispositivo capaz de armazenar, coletar e trasmitir dados com outros aparelhos conectados a *internet*. Eles nos possibilitam cumprirmos diversas tarefas sem sair do lugar, conecta pessoas, máquinas e equipamentos. Torna a vida mais dinâmica. A *ORACLE,* por exemplo utilizam sensores em suas aplicações SaaS responsáveis por coletar dados do ambiente ou dispositivo em que estão aplicados e depois transformar essas informações em dados úteis para obter inidicadores de desempenho, estatística do tempo médio entre falhas e outras informações.

O número de dispositivos que se encaixam nessa categoria é gigantesco e embora a diversidade de dispositivos nos permita conectar quase qualquer coisa, carrega junto

muitas preocupações de segurança, por conta de sua heterogeneidade. Esse é um dos, senão o principal problema que nos deparamos quando pensamos em *IoT*, porque cada tipo de dispositivo tem diferentes tamanhos, processamentos, locação, além do orçamento limitado para desenvolver e testar *firmware* seguro, que é influenciado pelos preços dos dispositivos e seu ciclo de desenvolvimento curto. A própria IBM aponta que criar um dispositivo confiável e com recursos limitados que possa se conectar a uma rede sem fio, use pouco energia e ainda seja barato, é extremamente difícil.

De acordo com os dados coletados pelo *NSFOCUS Security Labs*, os laboratórios focados na descoberta e análise de ameaças, detectaram no Brasil em média 1236 ataques por empresa em 2021. O número representa alta de 57% em relação a 2020. O principal ataque ocorre por meio de *malwares* específicos para dispositivos *IoT* que são alvos fáceis em decorrência dos problemas de vulnerabilidade que essa tecnologia apresenta.

Porém como podemos garantir a segurança e confidencialidade desses dispositivos sem exigir muitos recursos do aparelho? E se esses serviços estão sempre conectados à *internet,* o que garante que outras pessoas não consigam acessá-las? Como uma resposta para essas perguntas propomos o uso de um *honeypot* de baixa interatividade como uma solução de garantir maior segurança a rede *IoT*. Um *honeypot* é basicamente um sistema criado para ser vulneravel e atrair a atenção de invasores. Como o *honeypot* é um ambiente totalmente monitorado e controlado, todas as interações realizadas com ele são capturadas, ou seja, teremos todas as ações realizadas pelo agente malicioso durante o ataque. Outro caracteristica importante é que não consomem muitos recursos de *hardware* e *software*, sendo assim não exigem muito da infraestrutura da empresa. Quando implantados na rede de *IoT*, funcionarão igual a outro dispositivo e servirá como atrativo para invasores, que estarão dentro de uma armadilha pensando estar dentro do sistema real. Dessa forma, conseguimos identificar, estudar e neutralizar ataques sem que eles atinjam aplicações reais e sem consumir nenhum recurso dos dispositivos *IoT* que são muito limitados.

O objetivo dessa pesquisa é simular um o *honeypot* de baixa interatividade e entender na prática todo o processo de interação com os agentes maliciosos, desde o primeiro contato com o invasor até a saída dos dados capturados pelo nosso *honeypot*. É importante dizer que a pesquisa aborda um ambiente controlado sem exposição de dados e informações de uma rede particular.

2. Metodologia de pesquisa

Este estudo baseou-se em uma estratégia inicial qualitativa e mais adiante uma estratégia quantitativa de estudo, de caráter descritiva por meio de pesquisas e análises. Neste capítulo tem foco em demostrar os procedimentos de pesquisas utilizados.

O método descritivo foi utilizado com finalidade de analisar a *cyber* segurança em dispositivos *IoT*, mais especificamente a utilização de um*honeypot* de baixa interatividade na rede para melhorar a segurança.

Para isso a pesquisa será baseada em estudos de autores como, por exemplo, Marie O'Niell, Joshi R. C. entre outros e centros de pesquisa dedicados a estudo e analise de incidentes de segurança como o CERT.br.

Partindo disso, em um primeiro momento será analisado de modo geralo que é e como funciona um *honeypot*, baseado nos conceitos apresentados pelos autores da área. Em um segundo momento o foco é compreender as ameaças que a *Internet of Things(IoT)* possuem, levando em base centros de pesquisa sobre respostas a incidentes de segurança como o CERT.br e o *NSFOCUS Security Labs*, que hoje são fontes atualizadas e pertinentes sobresegurança em um ambiente *IoT*. Quando os conceitos acima estiverem claros,o objetivo é elaborar o ambiente para realizar a simulação do *honeypot* de baixa interatividade para entender na prática o processo de interação de agentes maliciosos em dispositivos *IoT*.

As simulações foram realizadas através do *VirtualBox* no Windows 10 em uma máquina i3-4170 CPU @ 3.70Hz com 8GB de memória. Para facilitar o processo de criação e configuração das máquinas virtuais optamos pelo uso do Vagrant, utilizamos o Ubuntu *Trusty64* como SO em ambas as máquinas e disponibilizamos 4GB de memória para nosso agente malicioso e 2GB para nosso *Honeypot*.

Os *softwares* utilizados foram o *PentBox*, que é *open source* e nos permite emular um *honeypot* de baixa interatividade leve, simples e eficiente e o Protocolo *Telnet*, que é o principal alvo explorado por invasores em dispositivos *IoT*.

O estudo terá essencialmente um caráter qualitativo, com foco em referenciais teóricos e bibliográficos, ganhando mais para frente um caráter quantitativo nas aplicações práticas do estudo.

3. Referencial teórico

O referencial teórico dessa pesquisa foi dividida em dois tópicos: O que é um *Honeypot*; e *Honeypot* e segurança de dispositivos *IoT*.

3.1 O que é *Honeypot?*

Honeypot é um sistema conectado à rede e configurado como chamariz para atrair os ataques cibernéticos, em outras palavras, um ambiente controlado e monitorado que tem a função de ser um alvo em potencial para *hackers*.

De acordo com Michele Adams em sua pesquisa, "*Honeypots: Concepts, Approaches and Challenges*", um honeypot pode ter funções diversas dentro de uma rede como apenas distrair os invasores, fornecer aviso prévio de novo ataques e como ambiente de estudo aprofundado sobre invasores e suas técnicas. Segundo ela, uma das suas maiores vatangens é sua taxa nula de falsos-positivos, isso porque como não deveria existir nenhuma interação com o *honeypot*, todo tráfego destinado a ele é por definição malicioso.

Para entendermos melhor o papel de um *honeypot*, vamos pensar em um ataque *zero-day*, de acordo com o *Kaspersky* (umas das referencias globais no mercado de cibersegurança) é um termo amplo que descreve as vulnerabilidades de segurança desconhecidas ou recentemente descobertas que os *hackers* podem usar para atacar sistemas. É extremamente difícil de se tratar uma ameaça quando sabe-se pouco ou nada sobre como e o que foi explorado, com certeza os ataques *zero-day* são uma das grandes ameaças hoje quando falamos sobre segurança. Porém se essa nova técnica de invasão for executada em um *honeypot,* teremos todos as ações realizadas pelo invasor, tornando mais fácil a mitigação desses ataques antes desconhecidos.

O CERT.br, Centro de estudos, resposta e tratamentos de incidentes de Segurança no Brasil, divide os *honeypots* em dois tipos. O primeiro é o de baixa interatividade, que são simples e apenas emulam sistemas onde o invasor irá agir, sem conexão direta com sistemas finais da empresa. Um grande exemplo de *honeypot* de baixa interatividade é o projeto *SpamPot*, coordenado pelo CERT.br, que nada mais é que vários *honeypots* de baixa interação emulando servidores de *proxy* aberto que coletam dados relacionados ao abuso de *spammers*, onde possível identificar *phising*, *malwares* e *botnets*. A figura 1 abaixo descreve a arquitetura do projeto *SpamBot*:

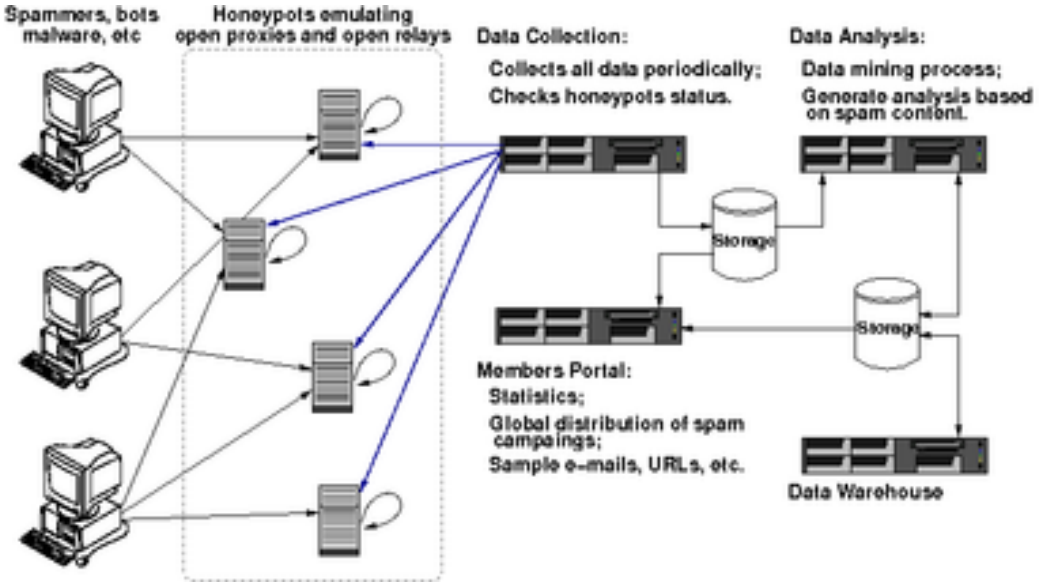

Figura 1. Arquitetura do projeto SpamBot coordenada pelo CERT.br

Fonte: CERT.br; https://honeytarg.cert.br/spampots/

O segundo é o de alta interatividade, onde os invasores interagem com sistemas que se comunicam com fluxo de informação, aplicações e serviços reais e vão além de apenas emular um sistema, consistem em uma rede projetada para ser comprometida. O *honeypot* de alta interatividade é mais complexo e trás maior risco a intituição, porém obtemos um estudo muito mais aprofundado sobre o agente malicioso e suas técnicas. Nessa pesquisa optamos em trabalhar com honeypots de baixa interatividade, exatamente porque eles são leves em termos de recursos e não exigem muito do hardware, o que é perfeito já que nosso objetivo é proteger dispositivos e redes com capacidades e processamentos limitados.

3.2 *Honeypots* e segurança de dispositivos *IoT*

Com o passar do tempo hackers desenvolveram novas técnicas a partir de vulnerabilidades para roubar dados ou afetar negativamente um dispositivo, aplicação ou servidor. De acordo com os laboratórios focados na descoberta e análise de ameaças, *NSFOCUS Security Labs*, só no Brasil em 2021, houve um aumento de 57% de ataques direcionados a empresas através dos dispositivos *IoT* comparado ao ano anterior. E esse número é um espelho das vulnerablidades que essa tecnologia apresenta, fica muito claro que a limitação que esses dispositivos possuem tazem muito risco as empresas e que a evolução da segurança deles não está acompanhando o desenvolvimentos das técnicas utilizadas por agente maliciosos. Tendo isso em mente temos que partir para uma solução indireta, ou seja, garantir maior segurança desviando o foco de invasores dos dispositivos

reais e mantendo maior integridade a nossa rede.

É aqui que entra o papel do *honeypot* de baixa interatividade, podemos emular esses dispositivos conectados a rede para direcionar a atenção de *hackers* para esse ambiente controlado. E a partir daí conseguimos identificar vulneralibidades no *firmware* e corrigi-las através de atualizações, ou podemos utilizar os dados coletados sobre o invasor para bloquea-lo de nossa rede. Outra opção é emular aplicações de segurança de nossa rede, como por exemplo o *firewall* que é a primeira barreira que o invasor se deparar ao tentar ingressar de forma indevida a rede, e da mesma maneira através do *honeypot* conseguiremos identificar falhas e vulnerabilidades que ao serem corrigidas garantirão maior integridade e segurança a toda infraestrutura.

Na figura 2 abaixo R. C. Joshi, em seu livro *Honeypots A new Paradigm to information Secvurity,* exemplifica tudo isso com uma arquitetura onde colocamos o *honeypot* em diversas camadas da rede e se passando por outros sistemas e aplicações com o intuito de encontrar falhas e brechas a serem corrigidas.

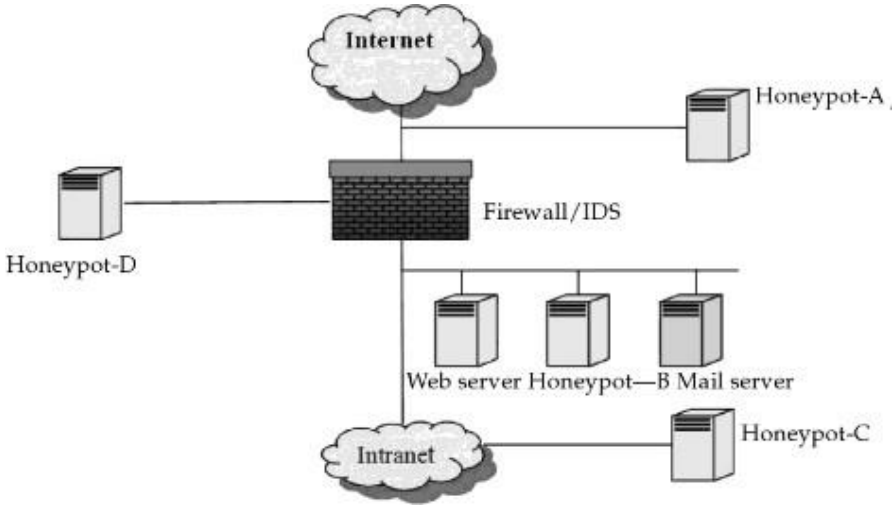

Figura 2. Exemplo de arquitetura de uma rede com honeypots.
Fonte: Joshi, R. C.; Honeypots A new Paradigm to Information Security

4. Ambiente de Simulação Controlado

A segunda etapa dessa pesquisa se caracterizará pela elaboração de um ambiente prático e controlado, onde simulamos um *honeypot* de baixa interatividade para saber como ele responde e captura informações quando são realizadas qualquer tipo de troca de informações ou ações maliciosas. Para isto, foi escolhido o *software PentBox* para ser simulado nesta pesquisa. Ele é um *software open source* que nos possibilita emular serviços utilizados em dispositivos de *Internet of Things* (*IoT*).

Nosso ambiente é composto por duas máquinas conectadas na mesma rede, a primeira é a *honeypot* que fará o papel do dispositivo *IoT*, e a segunda agirá como agente malicioso.

Ambas as máquinas são *Ubuntu*, foram emuladas através do *VirtualBox* e o software utilizado para simular o *honeypot* pode ser encontrado através do *GitHub* (*https://github.com/technicaldada/pentbox*). Para facilitar a simulação utilizamos o *Vagrant* para realizar a criação e configuração das máquinas, através dele conseguimos destruir e recriar as máquinas de forma muita prática e rápida.

Atribuímos ao *Honeypot* o IP 192.168.10.99 e ao agente malicioso o IP 192.168.10.105, como pode ser visto na figura 3 abaixo:

```
Vagrant.configure("2") do |config|
        config.vm.box = "ubuntu/trusty64"

        config.vm.define "honeypot" do |hp|
                hp.vm.network "private_network", ip: "192.168.10.99"
        end

        config.vm.define "agente_malicioso" do |am|
                am.vm.network "private_network", ip: "192.168.10.105"
        end

end
```

Figura 3. Configuração do *Vagrantfile* para criamos as máquinas virtuais com seus respectivos endereços IP.

Fonte: Elaborado pelo autor

Agora que já fizemos as configurações de nossas máquinas, vamos cria-las através do comando *"vagrant up"* e após o termino acessa-las utilizando o protocolo SSH, como é mostrado nas figuras 4 e 5, respectivamente:

```
  config.vm.synced_folder '/host/path', '/guest/path', SharedFoldersEnableSymlinksCreate: false
==> default: Clearing any previously set network interfaces...
==> default: Preparing network interfaces based on configuration...
    default: Adapter 1: nat
==> default: Forwarding ports...
    default: 22 (guest) => 2222 (host) (adapter 1)
==> default: Booting VM...
==> default: Waiting for machine to boot. This may take a few minutes...
    default: SSH address: 127.0.0.1:2222
    default: SSH username: vagrant
    default: SSH auth method: private key
    default: Warning: Connection aborted. Retrying...
    default: Warning: Connection reset. Retrying...
    default:
    default: Vagrant insecure key detected. Vagrant will automatically replace
    default: this with a newly generated keypair for better security
```

Figura 4. Iniciando a criação das máquinas.

Fonte: Elaborado pelo autor

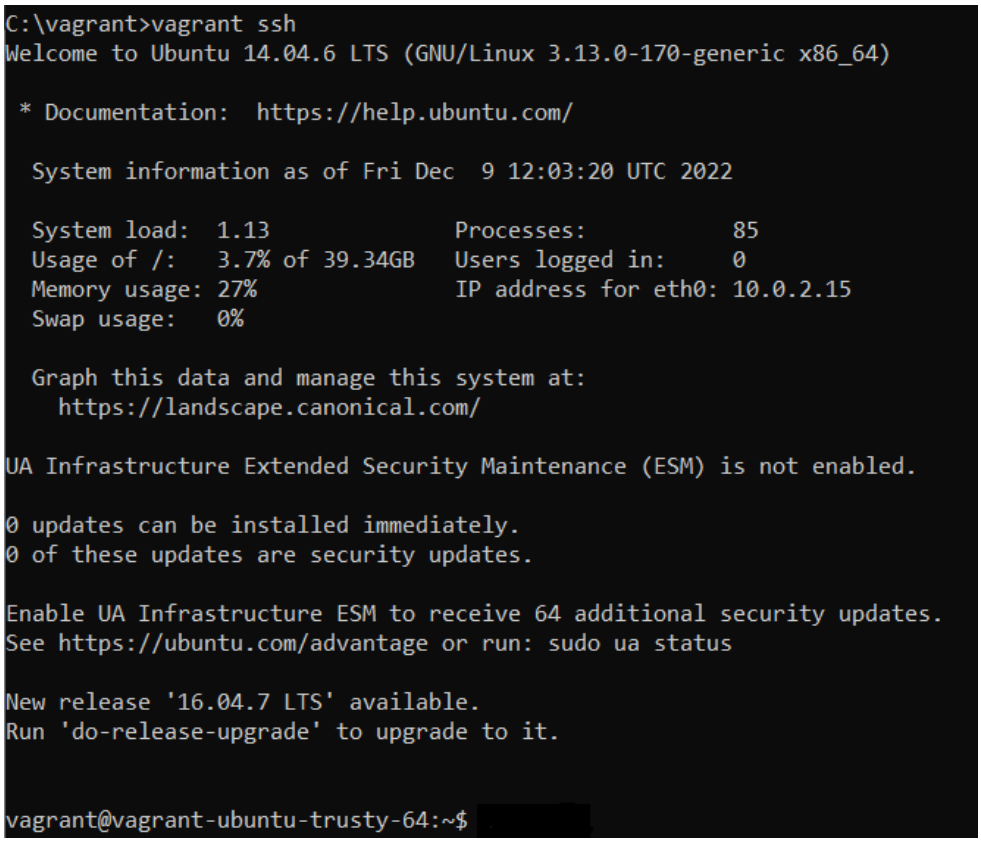

Figura 5. Acessando nosso *honeypot* através do protocolo SSH.

Fonte: Elaborado pelo autor

Pronto, estamos dentro de nossas máquinas configuradas e prontas para iniciarmos a simulação, na figura 6 e 7 a seguir podemos ver as configurações de rede que atribuimos a elas em nosso *Vagrantfile*:

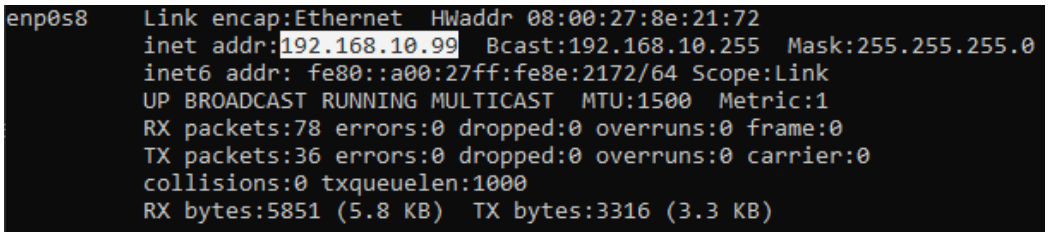

Figura 6. Configuração de rede do nosso *Honeypot*.

Fonte: Elaborado pelo autor

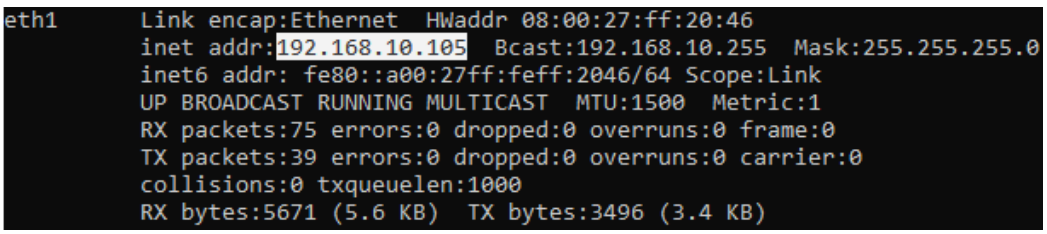

Figura 7. Configuração de rede de nosso agente malicioso.

Fonte: Elaborado pelo autor

Vamos começar configurando nosso honeypot. O *PentBox* nos oferece um *honeypot* de baixa interatividade, onde informamos qual porta ele deverá monitorar e qualquer interação detectada é capturada. De acordo com o CERT.br, a porta que foi o maior alvo de varreduras, em dispositivos *IoT* durante 2020, foi a 23 que é atribuída ao protocolo *Telnet*. Esse protocolo possibilita uma conexão remota entre duas máquinas, permitindo a execução de comandos escritos a partir de um computador em outro. Ou seja, um agente malicioso, uma vez conectado, poderia executar qualquer comando na máquina alvo.

Por conta disso iremos simular a conexão da nossa máquina maliciosa com o *honeypot* através desse protocolo. Começamos executando o *PentBox* e definindo que a porta 23 deve ser monitorada. Feito isso, nosso *Honeypot* irá escutar a porta 23 e qualquer interação com ela irá ser capturada e salva em um *log*. A figura 8 abaixo mostra a configuração realizada para o *honeypot* monitorar a porta 23:

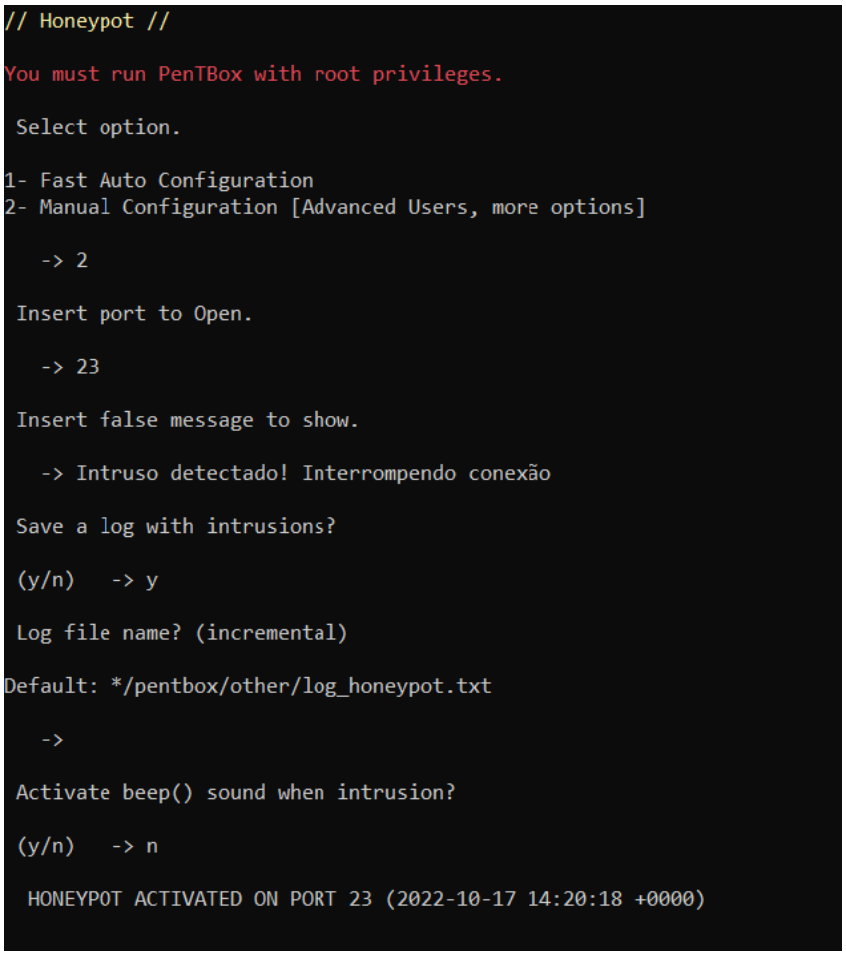

Figura 8. Configurando o *honeypot* para monitorar a porta 23.

Fonte: Elaborado pelo autor

Agora que nosso *honeypot* está pronto, vamos tentar realizar uma conexão a partir de nossa máquina maliciosa através do protocolo *Telnet*. Como podemos ver na figura 9, conseguimos nos conectar utilizando o comando *"telnet 192.168.10.99 23"* (informamos o protocolo, endereço de IP da máquina que desejamos nos conectar e a porta por qual irá ser feita a conexão):

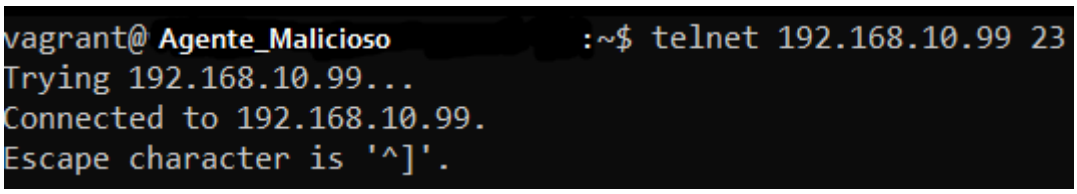

Figura 9: Realizada a conexão com o *honeypot* a partir da máquina intrusa, via *Telnet*.

Fonte: Elaborado pelo autor

Do outro lado podemos ver que o *honeypot* imediatamente já registrou que foi detectado um intruso e é bom notar que logo de cara já temos uma informação importante sobre nosso invasor, o endereço IP da máquina maliciosa como ilustrado na figura 10:

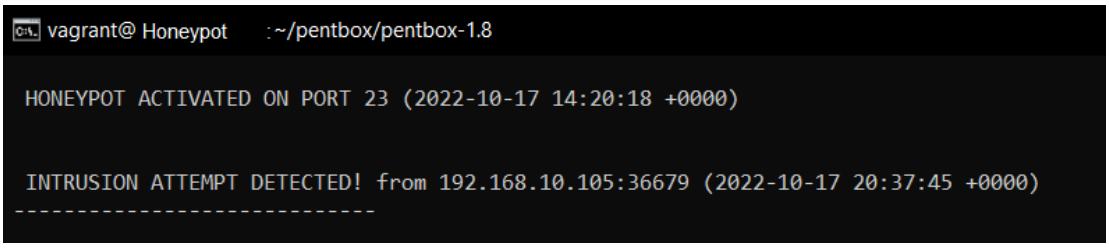

Figura 10. Captura da conexão realizada da máquina intrusa com o Honeypot.

Fonte: Elaborado pelo autor

A partir desse momento, nosso agente malicioso tem total liberdade dentro da máquina alvo, no caso o *honeypot*. O *PentBox*, por padrão, ao ser realizado a primeira execução de algum comando por parte do intruso, além de não ser executado, a conexão entre as duas máquinas é interrompida imediatamente, mas ainda sim conseguimos capturar esse comando utilizado pelo invasor. A figura 11 mostra a conexão do agente malicioso com nosso *honeypot* e a tentativa de execução do comando "*pwd"*, que deveria nos retornar o diretório atual que estamos e logo em seguida já é interrompida essa conexão pelo nosso *honeypot*. A figura 12 mostra a captura do comando utilizado pelo agente malicioso durante a tentativa de intrusão.

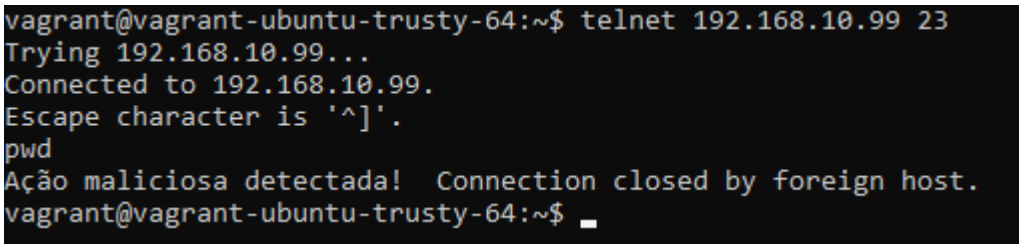

Figura 11. Conexão e tentativa de execução do comando "pwd" em nosso honeypot a partir do agente malicioso.

Fonte: Elaborado pelo autor

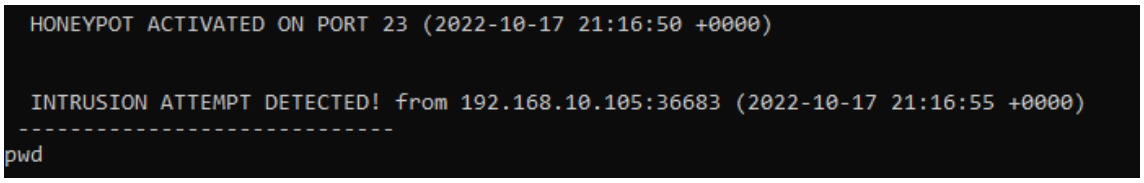

Figura 12. Captura pelo *honeypot* do comando utilizado pelo agente malicioso.

Fonte: Elaborado pelo autor

Dessa forma através do uso de um *honeypot* de baixa interatividade, foi possível identificar e mitigar umas das vulneralibidades mais exploradas em dispositivos *IoT*, de acordo com o CERT.br, o protocolo *Telnet*. Foi registrado todos os passos realizados pelo agente malicioso, desde o momento da conexão da máquina hostil até a interrupção dessa conexão por parte do *honeypot* como medida de segurança.

Durante todo esse processo as informações sobre o invasor e suas ações dentro da máquina alvo foram salvas dentro de um *log*, que é um expressão utilizada para descrever o processo de registro de eventos, ou seja, os dados coletados pelo *honeypot* foram salvos em um arquivo, como mostrado na figura 13 a seguir:

Figura 13. Log de ações realizadas durante a intrusão, capturado pelo honeypot e salvo em txt.

Fonte: Elaborado pelo autor

A figura 14 abaixo mostra conteúdo do arquivo "*log_honeypot.txt*", onde conseguimos enxergar todos os passos realizados pelo agente malicioso demonstrado em nossa simulação, desde a conexão até a tentativa de execução de um comando:

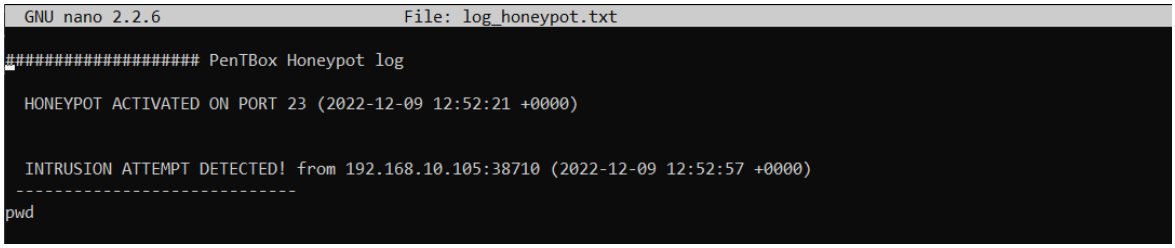

Figura 14. Conteúdo do arquivo "*log_honeypot.txt*".

Fonte: Elaborado pelo autor

5. Conclusão

Por meio da Internet das Coisas ou *Internet of Things* (*IoT*), conseguimos mesclar o mundo real e o mundo digital. Ela possibilita cumprimos diversas tarefas sem sair de onde estamos, conecta pessoas, máquinas e equipamentos, favorecendo a interação e tornando a vida muito mais dinâmica. Embora seja muito benéfica, a *IoT* apresenta vários problemas relacionados a segurança, entre eles vulnerabilidades de rede, *softwares* e *firmwares* desatualizadas, processamentos e capacidades limitadas entre outros. Tendo isso em mente precisamos procurar uma solução que não consuma do aparelho, então aqui entra o papel do *honeypot*. Mais especificamente um *honeypot* de baixa interatividade, que não faz grande exigências de hardware ou recursos e lidam bem com tráfego limitado. Com ele conseguiremos redirecionar a atenção de agentes maliciosos para longe dos sistemas reais para um controlado e monitorado. Onde poderemos analisar, entender e mitigar novas técnicas de intrusão, negações de serviços e roubos de informações. Além disso conseguimos manter a integridade de toda nossa rede, uma vez que implantar-mos o *honeypot* em diferentes camadas dela e houver uma interação com um agente malicioso, saberemos até onde ela foi comprimetida. Garantir maior segurança a rede significa garantir maior proteção a todos os dispositivos conectados a ela.

Como demonstrado capítulo 3, através da simulação fomos capazes de identificar a interação entre a máquina invasora e o *honeypot*, coletando informações como endereço IP dessa máquina, data e hora que foi realizada essa interação, além da captura do comando utilizado pelo agente malicioso e em seguida a interrupção da conexão entre as duas máquinas. Ou seja, com o uso do *honeypot* de baixa interatividade conseguimos acompanhar todos o passos do invasor e ainda mitigar a tentativa de ataque á nossa máquina, além de obtermos um arquivo com o *log* completo de todos esses eventos.

Então é possível garantir maior segurança, mesmo que indiretamente, com o uso

de *honeypots* de baixa interatividade aos dispositivos *IoT*. Descobrindo vulnerabilidades nesses aparelhos ou em outras ferramentas de segurança dentro da rede, assim como novas técnicas e softwares de invasão utilizada por agentes maliciosos.

6. Trabalhos futuros

É interessante também, para pesquisas futuras, abordar mais profundamente a mitigação de tentativas de ataques combinando o *honeypot* com um IDS e *machine learning*. É possível desenvolver uma ferramenta para mitigação de ataques que, sozinha e em tempo real, acompanha o agente malicioso, analisa e identifica as técnicas sendo utilzadas e age da forma mais eficaz possível a todas ela.

1. Referências

O'Niell, Marie (2016) "*Insecurity by Design: Today's IoT Device Security Problem"*

CERT.BR (2007) "Honeypots e Honeynets: Definições e Aplicações"

Joshi, R. C. *(*2011*) "Honeypots A new Paradigm to Information Security"*

Faiz Razali, Mohamad (2018) *"IoT Honeypot A Review from Research's Perspective"*

NSFOCUS Security Lab (2019) "2019 *Annual IoT Security Report"*

Kumar (2019) "*HIoTPOT: surveillance on IoT devices Against recent threats"*

Wang, CW (2019) "*IoT Security: ongoing challenges and research opportunities"*

Chamola, Vinay (2019) "*A survey on IoT security: application areas, security threats, andsolution architectures"*

Di Pietro, Roberto and V. Mancini, Luigi (2008) "*Intrusion Detection Systems*"

Wagh, Sharmila Kishor (2013) "*Survey on Intrusion Detection Systema using Machine Learning Techniques*"

Provos, Niels and Holtz, Thorsten (2007) "*Virtual Honeypots"*

Diebold, Patrick and Hess, Andreas (2005) "*A honeypot Architecture for Detecting and AnalyzingUnknown Networks Attacks*"

Verma, Kanchan and Debasish, Jena (2011) “*Honeypot in network security: a survey”*

Kaspersky Lab (2022) *“https://www.kaspersky.com.br”*

Oracle (2022) “*https://www.oracle.com/br/internet-of-things/what-is-iot/”*

IBM *(2022) “https://developer.ibm.com/articles/iot-anatomy-iot-malware-attack/”*