MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
GOIANO - CAMPUS RIO VERDE

LUÍS GUILHERME CORDEIRO SANTOS SILVA

SEGURANÇA EM IOT, UTILIZANDO AMBIENTE RASPBERRY PI

RIO VERDE
2019

LUÍS GUILHERME CORDEIRO SANTOS SILVA

SEGURANÇA EM IOT, UTILIZANDO AMBIENTE RASPBERRY PI

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia Goiano - Campus Rio Verde ligado ao Ministério da Educação, como requisito parcial da disciplina Prática de Laboratório de Pesquisa (tcc - Parte II) para a obtenção do título de Bacharel em Ciências da Computação.

Orientador: Rafael Carvalho de Mendonça
Instituto Federal Goiano

Coorientador: Marcio Rubens Sousa Santos
Universidade de Rio Verde

RIO VERDE
2019

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

S586s

Silva, Luís Guilherme Cordeiro Santos
Segurança em IoT, Utilizando Ambiente Raspberry Pi / Luís Guilherme Cordeiro Santos Silva; orientador Rafael Carvalho Mendonça; co-orientador Marcio Rubens Sousa Santos. -- Rio Verde, 2019.
40 p.

Tese (Doutorado em Bacharelado em Ciências da Computação) -- Instituto Federal Goiano, Campus Rio Verde, 2019.

1. Segurança. 2. IoT. 3. Vulnerabilidades. I. Mendonça, Rafael Carvalho, orient. II. Santos, Marcio Rubens Sousa, co-orient. III. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

INSTITUTO FEDERAL
Goiano

Repositório Institucional do IF Goiano - RIIF Goiano
Sistema Integrado de Bibliotecas

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

Identificação da Produção Técnico-Científica

[ ] Tese	[ ] Artigo Científico
[ ] Dissertação	[ ] Capítulo de Livro
[ ] Monografia – Especialização	[ ] Livro
[X] TCC - Graduação	[ ] Trabalho Apresentado em Evento
[ ] Produto Técnico e Educacional - Tipo: _____	

Nome Completo do Autor: Luís Guilherme Cordeiro Santos Silva
Matrícula: 2016102192010102
Título do Trabalho: Segurança em IoT, Utilizando Ambiente Raspberry Pi

Restrições de Acesso ao Documento

Documento confidencial: [X] Não [ ] Sim, justifique: _____

_____

Informe a data que poderá ser disponibilizado no RIIF Goiano: 30/09/2020
O documento está sujeito a registro de patente? [ ] Sim [X] Não
O documento pode vir a ser publicado como livro? [ ] Sim [X] Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

1. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
2. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
3. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Rio Verde, 28/09/2020
Local Data

Luis Guilherme C. S. Silva
Assinatura do Autor e/ou Detentor dos Direitos Autorais

Ciente e de acordo:

Rafael Carvalho de Mendonça
Assinatura do(a) orientador(a)

INSTITUTO FEDERAL GOIANO – CÂMPUS RIO VERDE
DIRETORIA DE ENSINO
GERÊNCIA DE ENSINO DE GRADUAÇÃO

ATA DE DEFESA DO TRABALHO DE CURSO (TC)

ANO	SEMESTRE
2019	2º

No dia 16 do mês de dezembro de 2019, às 13 horas e 30 minutos, reuniu-se a banca examinadora composta pelos docentes Rafael Carvalho de Mendonça, Marlus Dias Silva e Lionel Diógenes Carvalhais Alvarenga, para examinar o Trabalho de Curso (TC) intitulado Segurança em IoT, Utilizando Ambiente Raspberry PI, do(a) acadêmico(a) Luis Guilherme Cordeiro Santos Silva, Matrícula nº 20161021920101O2 do curso de Ciência da Computação do IF Goiano – Câmpus Rio Verde. Após a apresentação oral do TC, houve arguição do candidato pelos membros da banca examinadora. Após tal etapa, a banca examinadora decidiu pela aprovação do(a) acadêmico(a). Ao final da sessão pública de defesa foi lavrada a presente ata, que segue datada e assinada pelos examinadores.

Rio Verde, 16 de dezembro de 2019.

Rafael Carvalho de Mendonça
Nome:
Orientador(a)

Lionel Diógenes Carvalhais Alvarenga
Nome:
Membro

Marlus Dias Silva
Nome:
Membro

Observação:
( ) O(a) acadêmico(a) não compareceu à defesa do TC.

RESUMO

SILVA, Luís Guilherme Cordeiro Santos. Segurança em IoT, utilizando ambiente Raspberry Pi. 2019. 29 f. Trabalho de Conclusão de Curso – Bacharelado em Ciências da Computação, Instituto Federal de Educação, Ciência e Tecnologia Goiano - Campus Rio Verde. Rio Verde, 2019.

Este trabalho trata de uma necessidade que tem sido notícia frequente nas mídias de tecnologia e de notícias em geral, refere-se às falhas de segurança causadas por produtos IoT (Internet of Things – Internet das Coisas). Estes produtos, cada vez mais, comuns nas residências e em ambientes corporativos, como dispositivos de automação que se conectam à Internet, eletrodomésticos que oferecem algum recurso oferecido por interfaces que se comunicam por rede cabeada ou sem fio e afins. Normalmente, são projetados para automatizar tarefas comuns com menor grau de complexidade em seu projeto, possibilitando sua inserção no mercado com preços competitivos. Este cenário possibilitou a utilização destes produtos como um meio de comunicação desprotegido para acessar redes internas de ambientes corporativos. Este estudo analisa um cenário IoT para identificar quais falhas de segurança pode haver, o que cada falha poderia causar em uma rede interna e o que pode ser feito para minimizar ou eliminar estas falhas.

Palavras-chave: Segurança. IoT. Vunerabilidades.

ABSTRACT

SILVA, Luís Guilherme Cordeiro Santos. Title in English. 2019. 29 f. Trabalho de Conclusão de Curso – Bacharelado em Ciências da Computação, Instituto Federal de Educação, Ciência e Tecnologia Goiano - Campus Rio Verde. Rio Verde, 2019.

This work addresses a need that has been frequent news in technology and news media in general, refers to the security flaws caused by IoT (Internet of Things) products. These products are increasingly common in homes and corporate environments, such as automation devices that connect to the Internet, appliances that offer some feature offered by interfaces that communicate over a wired or wireless network and the like. Typically, they are designed to automate common tasks with less complexity in their design, making it possible to enter the market with competitive prices. This scenario allowed the use of these products as an unprotected means of communication to access internal networks of corporate environments. This study examines three IoT environments to identify which security holes each can make possible, what each failure could cause on an internal network and what can be done to minimize or eliminate these faults.

Keywords: Security. IoT. Vulnerabilities.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

IoT	Internet of Things
RFID	Radio-Frequency IDentification
NASA	National Aeronautics and Space Administration
JPL	Jet Propulsion Laboratory
API	Application Programming Interface
TCP	Transmission Control Protocol
LLN	Low-Power and Lossy Networks
OWASP	Open Web Application Security Project
RPL	Routing Protocol for Low Power and Lossy Networks
DoS	Denial of Service
MQTT	Message Queuing Telemetry Transport
IDS	Intrusion Detection System
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
DDoS	Distributed Denial of Service
NFC	Near Field Communication
RPL	Routing Protocol for Low Power and Lossy Networks
SSH	Secure Shell
VNC	Virtual Network Computing

SUMÁRIO

1 INTRODUÇÃO

Em 1999, no Laboratório de Auto-ID do MIT, onde eram realizadas pesquisas no campo de identificação por radiofrequência em rede (RFID), Kevin Ashton propôs o termo "Internet das Coisas", durante uma apresentação sobre RFID e a cadeia de suprimentos de uma companhia. E, dez anos depois, publicou um artigo denominado "A Coisa da Internet das Coisas".

"A Internet das Coisas é uma inovação tecnológica, baseada em artefatos já consolidados como a Internet e objetos inteligentes" (GALEGALE et al., 2016).

Nesheim e Rosnes (2016) afirmam que as casas inteligentes já fazem parte de 0,77% das famílias do mundo todo e que se espera um crescimento de 2,79% até 2020.

Com todo este aumento, surge uma preocupação quanto à garantia de segurança e integridade desses dispositivos e dos dados que estes dispositivos armazenam. Esta preocupação se deve à existência de inúmeras vulnerabilidades nos dispositivos de IoT.

De acordo com (MUKHERJEE et al., 2018),

> Os sistemas de Internet das coisas (IoT) geralmente são compostos por uma rede de dispositivos conectados ou "coisas". O termo "coisa"aqui pode constituir qualquer dispositivo inteligente, desde dispositivos sensores automóveis, dispositivos bioquímicos sensores na segurança interna, para dispositivos de monitoramento do coração dentro de um corpo humano. Na verdade, qualquer objeto que tenha a capacidade de coletar e transferir dados pelo rede para "nó"ou core plataforma de computação em nuvem pode ser uma parte de um sistema IoT.

Um exemplo que demonstra a necessidade de que se estude a respeito de segurança e a segurança aplicada à Internet das Coisas, é devido a um ataque à NASA (National Aeronautics and Space Administration) em Abril de 2018. O ataque ocorreu, após um Raspberry Pi que não estava autorizado a ser vinculado à rede do JPL (Jet Propulsion Laboratory), foi alvo de hackers. Os invasores conseguiram roubar 500 megabytes de dados de um dos principais sistemas do laboratório. Além disso, eles usaram essa conexão para encontrar uma porta que lhes permitisse ir mais fundo na rede do JPL. Com isso, eles tiveram acesso a várias informações importantes, incluindo a Deep Space Network da NASA - uma rede de instalações de comunicação de espaçonaves. Como resultado, as equipes de segurança de alguns programas espaciais, como o Veículo de Tripulação Orion e a Estação Espacial Internacional, optaram por se desconectar da rede da agência.

Outro exemplo de ataque, que foi realizado por culpa de dispositivos inteligentes, aconteceu em Londres, no ano de 2018, onde um grupo de hackers conseguiu roubar informações de um cassino ao acessar a base de dados da empresa, através de uma vulnerabilidade em um termômetro de aquário localizado no lobby do edifício.

O presente trabalho busca apresentar a necessidade de se estudar mais a respeito de segurança da informação e a segurança a aplicada a IoT visto que está sendo amplamente

utilizada como foi dito acima, e visa identificar e documentar as falhas de segurança em simulações de ambientes IoT.

2 OBJETIVOS

2.1 Objetivo Geral

Esta pesquisa tem como enfoque geral demonstrar o quanto os produtos IoT podem gerar problemas no que se refere à segurança em redes internas de uma corporação, ou mesmo, em redes domésticas por acessos não autorizados, causados por códigos maliciosos ou pessoas mal intencionadas, além de identificar e documentar as falhas que forem encontradas através dos testes de invasão e vulnerabilidade.

2.2 Objetivos Específicos

A proposta do projeto possui o objetivo de documentar detalhadamente as vulnerabilidades de uma rede interna causadas por dispositivos e/ou produtos IoT e, também, tornar evidente os problemas que as mesmas podem acarretar em uma rede interna no que diz respeito à confidencialidade e integridade dos dados de uma empresa ou até mesmo em um ambiente doméstico. Para isso, foram levantados os seguintes objetivos específicos:

- Estudar como é o uso de dispositivos inteligentes em contextos diferentes, como, por exemplo, residencial e empresarial, e como eles influenciam no dia a dia do usuário.
- Estudar as principais falhas de seguranças de dispositivos inteligenstes que já foram detectadas e documentadas.
- Pesquisar casos em que as falhas de segurança foram exploradas por atacantes e que acarretou problemas maiores os seus usuários.
- Realizar testes de invasão e vulnerablidade nos ambientes propostos.
- Documentar todas as falhas de segurança que forem encontradas a partir do feitio dos testes.
- Propor soluções para as falhas de segurança que forem encontradas.
- Tornar evidente a necessidade de segurança para estes dispositivos.

3 JUSTIFICATIVA

Desde o surgimento dos primeiros eletrodomésticos nos Estados Unidos, os fabricantes já utilizavam o termo "Casa do Futuro", devido ao fato de que seus equipamentos tornariam as tarefas cotidianas mais simples e poupariam tempo, que foi impulsionado pela melhora da tecnologia da criação de motores da época (BOLZANI, 2007).

De acordo com IoT-Analytics, o mercado das casas inteligentes teve um crescimento de 95% entre o segundo semestre de 2016 e o segundo semestre de 2017, aproximadamente, um crescimento de 3.3 bilhões de dólares.

Como visto no Capítulo 1, deste trabalho e, no parágrafo acima, é vista a crescente utilização deste tipo de tecnologia, levando, assim, à necessidade de que se tenha uma preocupação maior quanto se trata a respeito da segurança da informação, a fim de beneficiar tanto o usuário final desta tecnologia quanto os responsáveis por tais avanços, resultando uma rede segura e mais próxima de atingir sua maturidade.

Com o aumento do uso de dispositivos inteligentes e a mobilidade de alguns destes dispositivos, a Internet das Coisas se torna exposta a várias vulnerabilidades.

De acordo com Atzori, Iera e Morabito (2010),

> A Internet das Coisas é extremamente vulnerável a ataques por uma série de razões. Primeiro, muitas vezes, seus componentes passam a maior parte do tempo desacompanhado; e assim, é fácil atacá-los fisicamente. Em segundo lugar, a maioria das comunicações são sem fio, o que torna a espionagem extremamente simples.

Segundo o que foi dito por Ribeiro (2018),

> Na IoT há uma interconexão de dispositivos, onde vários objetos se encontram conectados, caso um deles tiver sua segurança comprometida e conectado à internet irá afetar todo o conjunto de dispositivos conectados, assim prejudicando a segurança e a resiliência da internet.

Com base em um estudo feito por Miessler (2014), é possível afirmar que cerca de 70% dos dispositivos de Internet das Coisas é vulnerável a algum tipo de ataque. Câmeras de segurança, termostatos, alarmes, controladores de portas foram estudados e cada um desses tinha um serviço orientado para a nuvem e tinha um aplicativo de celular.

Além disto e pelo fato de tentar ser o mais genérico possível para que se aumente o número de usuários afetados, será utilizado o Raspberry Pi pois é uma das principais plataformas de aprendizagem para a Internet das coisas juntamente com o Arduino. O Raspberry Pi (RPi) é um microcomputador completo, com processador, memória RAM e ROM (basicamente um cartão de memória MicroSD), portas USB, HDMI e Ethernet. Esse computador tem aproximadamente o tamanho de um cartão de crédito, opera com apenas 5 volts e possui interfaces que podem ser conectadas a diversos dispositivos. Já o

Arduíno é uma plataforma de prototipagem composta de uma placa microcontroladora, uma IDE e uma linguagem de programação própria, baseada em C e C++. O hardware segue os princípios do "hardware open source", ou seja, tem uma especificação que pode ser fabricada por qualquer pessoa que estiver disposta a construir sua própria placa. O motivo de ter optado por utilizar o Raspberry e não o Arduino será apresentado no capítulo 6 deste trabalho.

A forma de maior sucesso para a detecção de vulnerabilidades é chamada de Teste de Invasão ou Pentest, sendo este uma exploração de vulnerabilidades presentes que ajuda a determinar quais vulnerabilidades são exploráveis e qual é o grau de exposição da informação. E devido a esse sucesso, será utilizado este tipo de teste a fim de explorar as falhas no ambiente para que, dessa forma, possa solucioná-las.

4 REVISÃO BIBLIOGRÁFICA

Existe uma escassez a respeito de trabalhos e estudos que tratam a segurança em dispositivos inteligentes em diferentes tipos de ambientes e, também, que propusesse soluções para as vulnerabilidades encontradas. Foram encontrados trabalhos que apenas analisaram as vulnerabilidades ou, então, que corrigiram um problema pontual do ambiente descoberto pela análise do mesmo.

Os pesquisadores vem propondo frameworks para análise de vulnerabilidades de dispositivos IoT), porém, esta abordagem não abrange muitos dos dispositivos ou tecnologias que andam sendo amplamente utilizadas. Um outro aspecto estudado é em relação à solução de determinados problemas, a partir de uma análise específica em um ambiente específico.

Ribeiro (2018), em seu trabalho, construiu um cenário de testes, utilizando o sistema operacional Contiki, trabalhando combinado ao simulador Cooja. Este estudo possui o objetivo de simular ataques em uma rede RPL a fim de mostrar o quanto uma rede IoT pode ser vulnerável a certos tipos de ataques, porém, esta pesquisa não apresenta nenhuma solução para as vulnerabilidades encontradas, apenas propõe isso como um trabalho futuro.

Já Martins e Zarpelão (2018), em seu estudo, propõem um framework que investiga vulnerabilidades em dispositivos IoT e cenários de rede LLN, utilizando metodologia OWASP. Neste estudo, foram realizados diferentes tipos de ataques ao protocolo RPL, como, por exemplo, Hello Flood (é causado por um nó que transmite um pacote Hello com um poder muito alto, de modo que um grande número de nós, mesmo longe na rede, o escolhe como o nó pai. Todas as mensagens agora precisam ser roteadas de multi-hop para esse pai, o que aumenta o atraso. As mensagens de saudação são transmitidas para um grande número de nós em uma grande área da rede), SinkHole (é um ataque interno que um intruso compromete um nó dentro da rede e em seguida, o nó comprometido tenta atrair todo o tráfego dos nós vizinhos com base na métrica de roteamento usada no protocolo de roteamento), Wormhole (um atacante recebe pacotes em um ponto da rede, "encapsulá-os" para outro ponto na rede e, em seguida, reproduzi-los na rede a partir desse ponto), BlackHole (é um tipo de ataque de negação de serviço em que um roteador que deve retransmitir pacotes, em vez disso, os descarta) e Selective Forwarding (nós maliciosos se comportam como um buraco negro e podem se recusar a encaminhar certas mensagens e simplesmente soltá-las, garantindo que elas não sejam propagadas), além disso, também, foram feitos testes de ataques DoS direcionados ao protocolo MQTT, entretanto, este estudo apenas dita uma possível solução, mas não a coloca em prática.

Foi realizado uma pesquisa que identificou e classificou os ataques que agem contra o protocolo RPL em três categorias principais. Dentre esses, estavam os ataques contra

recursos, ataques contra a topologia e, por último, ataques contra o tráfego de rede. Os ataques contra recursos reduzem a vida da Internet através da geração de controle de mensagens falsas ou construção de loops. Já os ataques contra a topologia fazem a Internet convergir para uma configuração não otimizada ou isolando nós. E nos ataques contra o trafego de rede deixam um nó malicioso capturar e analisar uma grande parte do tráfego. Baseado nisso, o autor comparou a propriedade de tais ataques e discutiu técnicas que fossem capazes de proteger as topologias RPL (KAMBLE; MALEMATH; PATIL, 2017).

Um outro estudo encontrado na literatura possui o objetivo de desenvolver uma ferramenta capaz de garantir segurança para dispositivos IoT, utilizando uma quantidade mínima de recursos possíveis. Em seu protótipo, o autor utilizou como dispositivo de teste um Raspberry Pi, que tem como objetivo testar o funcionamento do IDS desenvolvido. Foram realizados cinco tipos diferentes de ataques, dentre esses, estavam Syn Flood (é um ataque rede por saturação que explora o mecanismo de aperto de mão em três tempos (em inglês Three-ways handshake) do protocolo TCP), Land Attack (consiste em enviar um pacote que possui o mesmo endereço IP e o mesmo número de porta nos campos fonte e destino dos pacotes IP), ICMP Flood (este ataque ocorre como resultado de pacotes ICMP que transbordam os servidores e o pipe até o ponto de falha do sistema), Smurf Attack (é um ataque distribuído de negação de serviço (DDoS) distribuído pela rede) e UDP Flood (UDP flood é um tipo de ataque DoS no qual o atacante sobrecarrega portas aleatórias no host alvo com pacotes IP contendo datagramas UDP) e sendo estes realizados no ambiente que fora desenvolvido. Ao final do trabalho, foi possível identificar que durante tais ataques o IDS-IoT conseguiu-se detectar as informações que caracterizassem cada um dos ataques acima citados (SOUSA, 2016).

Foi encontrada, na literatura, uma pesquisa que apresentou estudos feitos desde 2010 até 2016, nos quais expôs os problemas relacionados à segurança, entre outros, e as soluções das quais esses trabalhos propuseram, dentre tais, estão Subashini e Kavitha (2011) que apresentaram alguns problemas como, por exemplo, o fato de que os clientes corporativos ainda estão relutantes em implantar IoT e a nuvem em seus negócios, e, também, que a segurança é um dos principais problemas que reduz o crescimento de computação em nuvem e complicações com privacidade e proteção de dados continuam a atormentar o mercado e sugeriu como solução um novo modelo que visasse melhorar as funcionalidades de um modelo já existente e que este não deve arriscar ou ameaçar outras características importantes o modelo atual.

Já Domingues (2012) desenvolveu um trabalho em que apresentou os motivos de fazer um teste de invasão, além de conceitos amplamente utilizados em áreas da segurança da informação. Neste estudo, contém um conjunto de ferramentas e técnicas para a obtenção de informações, varreduras, invasão, manutenção de acesso e para cobrir rastros, além disso, é apresentada uma simulação de uma invasão em um ambiente controlado por uma distribuição Windows XP, através de uma máquina, contendo a distribuição Backtrack 5,

sendo uma tentativa de simular um ambiente corporativo.

Outro estudo que trata a respeito de segurança da informação é o de Bertoglio e Zorzo (2015), em que conduziu um mapeamento sistemático do campo de testes de invasão, visando encontrar evidências que podem ser usadas para aperfeiçoar as pesquisas da área. Além disso, buscou identificar tendências de pesquisa, metodologias, cenários e ferramentas de uso.

Na pesquisa de Mirjalili, Nowroozi e Alidoosti (2014), é apresentado um survey voltado a teste de penetração web, discutindo metodologias e comparando ferramentas de escaneamento de vulnerabilidades, além do levantamento de trabalhos, contendo novas propostas de métodos ou ferramentas direcionados ao Pentest.

5 TIPOS DE ATAQUES

A definição dos tipos de ataques é necessária, pois pelo fato de que, a partir dela, é possível classificar cada um dos ataques que foi realizado contra o alvo e, para que assim seja possível definir, também, os pilares da segurança da informação que são afetados.

Após analisar os trabalhos citados no capítulo 4, deste estudo, e de acordo com o trabalho de Akram, Konstantas e Mahyoub (2018) é possível separar os ataques à Internet das Coisas em quatro tipos:

1. **Ataques Físicos:** são ataques que possuem como alvo o hardware, ou seja, componentes, como, por exemplo, tags RFID, microcontroladores, atuadores e sensores.
2. **Ataques a Protocolos:** esse tipo de ataque é voltado aos protocolos os quais a Internet das Coisas utiliza, sejam tais protocolos da camada de conectividade, rede, roteamento, aplicação e de transporte.
3. **Ataques aos Dados:** é um tipo de ataque que possui como foco apenas os dados localizados tanto no componente ou na nuvem.
4. **Ataques ao Software:** são voltados a aplicações localizadas em componentes de Internet das Coisas, firmware, sistemas operacionais, gateway da aplicação e serviços.

Após essa classificação é necessário definir agora quais são os pilares da segurança da informação os quais tais ataques podem acabar infringindo.

- **Confidencialidade:** O processo de comunicação segura existe para garantir que as mensagens sejam compreendidas somente pelo remetente e pelo destinatário (KUROSE, 2010).
- **Integridade** O processo que assegura que o conteúdo dos dados comunicados não tenha sido alterado durante a transmissão (KUROSE, 2010).
- **Não-repudiação** O processo no qual um sistema de Internet das Coisas pode validar o incidente ou não de um evento.
- **Disponibilidade** é a garantia de que os dados estejam disponíveis a qualquer tempo e garante a prestação contínua do serviço (TRIBUNAL DE CONTAS DA UNIãO, 2012).
- **Privacidade** O processo no qual um sistema de Internet das Coisas segue regras ou políticas de privacidade e permite que os usuários controlem seus dados sensíveis.
- **Auditabilidade** Garantir a capacidade de um sistema de Internet das Coisas de executar o monitoramento firme de suas ações.
- **Prestação de contas** O processo no qual um sistema de Internet das Coisas mantém os usuários encarregados de suas ações.
- **Confiabilidade** A garantia da capacidade de um sistema de Internet das Coisas de remover a identidade e confirmar a confiança em terceiros.

Coelho, Araújo e Bezerra (2014) afirmam que vulnerabilidade é como uma fala

que permite o surgimento de deficiências na segurança e, por isso, é necessário que sejam utilizados controles de segurança por meio de políticas, processos, procedimentos, estruturas de hardware e software, com constante monitoramento, auditorias e contínuo melhoramento.

Após isto, é possível classificar alguns ataques e definir quais pilares podem ser atingidos.

5.1 Ataques Físicos

Os ataques físicos são ataques que possuem como alvo o hardware, ou seja, componentes que estão presentes no ambiente. A lista a seguir apresenta os principais ataques deste tipo de ataque.

- **Ataques de replicação de objetos:** um adversário primeiro captura fisicamente apenas um ou poucos nós legítimos, depois clona ou replica os que fabricam essas réplicas com a mesma identidade (ID) com o nó capturado e, finalmente, implanta um número de clones crítico por toda a rede.(KHAN et al., 2013)
- **Trojan de Hardware:** uma alteração ou inclusão maliciosa em um circuito integrado (CI) que alterará sua função pretendida ou fará com que ela execute uma função maliciosa adicional (ROONEY; SEEAM; BELLEKENS, 2018) (CHAKRABORTY; NARASIMHAN; BHUNIA, 2009).
- **Object Jamming:** é definido como a interrupção das comunicações sem fio existentes, aumentando a razão sinal e/ou ruído no lado do receptor, através da transmissão de sinais sem fio interferentes (OSANAIYE; ALFA; HANCKE, 2018) (GROVER; LIM; YANG, 2014).
- **Engenharia Social:** é o ato de tirar proveito das vítimas para obter informações confidenciais, que podem ser usadas para fins específicos ou vendidas no mercado negro e dark web (SALAHDINE; KAABOUCH, 2019).

5.1.1 Classificação

Ataques	Pilares
Ataques de replicação de objetos	Todos
Trojan de Hardware	Todos
Object Jamming	Todos
Engenharia Social	Todos

Tabela 1 – Ataques Físicos e os pilares comprometidos

5.2 Ataques a Protocolos

Este tipo de ataque é voltado aos protocolos os quais a Internet das Coisas utiliza, sejam tais protocolos de camada de conectividade, rede, roteamento, aplicação e de transporte. Abaixo são apresentados os principais protocolos os quais a Internet das Coisas utiliza e a lista com os principais ataques a cada um destes protocolos.

5.2.1 RFID

A lista apresentada a seguir representa os principais ataques ao protocolo RFID.

- **Replay:** Um dispositivo contraditório é colocado clandestinamente entre uma etiqueta RFID legítima e o leitor. Este dispositivo é capaz para interceptar e modificar o sinal de rádio entre a etiqueta legítima e o leitor. Posteriormente, uma conexão efêmera é retransmitida do tag / leitor legítimo através do dispositivo secundário para o leitor / tag legítimo (MITROKOTSA; RIEBACK; TANENBAUM, 2010).
- **Spoofing:** Nesse tipo de ataque, um adversário representa uma etiqueta RFID válida para obter seus privilégios. Essa representação requer acesso total aos mesmos canais de comunicação que a tag original (MITROKOTSA; RIEBACK; TANENBAUM, 2010).
- **Man-in-the-Middle:** Um ataque MITM é um ângulo de ataque que aproveita a confiança mútua de terceiros ou a representação simultânea de ambos os lados de uma confiança bidirecional (RFID. . . , 2005).

5.2.2 NFC

A lista, abaixo, representa os principais ataques ao protocolo NFC.

- **Eavesdropping:** Utiliza métodos de autenticação dinâmica de senha e sistema de back-end. Ele pode efetivamente impedir as vulnerabilidades de segurança, como ataques de dicionário, ataques de repetição, interceptação de dados e falsificação de tags (IVAN; VUJIC; HUSNJAK, 2016).
- **Relay:** Para esse ataque, o adversário deve encaminhar a solicitação do leitor à vítima e retransmitir sua resposta ao leitor em tempo real, a fim de realizar uma tarefa que finge ser o proprietário do cartão inteligente da vítima (RIYAZUDDIN, 2011).
- **Man-in-the-Middle:** Um invasor pode interceptar os dados, modificando e retransmitindo-os para objetos maliciosos (ABDUL-GHANI; KONSTANTAS; MAHYOUB, 2018).

5.2.3 Bluetooth

Os itens, a seguir, representam os principais ataques ao protocolo Bluetooth.

- **Bluesnarfing:** O ataque envolve invadir um telefone celular e roubar qualquer dado armazenado no telefone, como contatos, entradas de calendário, imagens e etc

(MOSENIA; JHA, 2017). Durante o ataque, o atacante se conecta explorando o OBEX File Transfer Protocol, um programa de transferência de arquivos usado no Bluetooth (WACHSMANN; SADEGHI, 2014). Isso permite o invasor emparelhar com o dispositivo do usuário.

- **BlueBugging:** O ataque ocorre no protocolo RFCOMM (KHEDR, 2013). As conexões físicas são feitas via banda base L2CAP + e emula conexões RS-232 seriais (KHEDR, 2013). Durante o ataque, o atacante se conecta ao dispositivo de destino sem o conhecimento do proprietário.
- **Bluejacking:** permite que o adversário acesse arquivos no dispositivo de destino. Os dispositivos envolvidos no ataque e a fonte exata da mensagem recebida precisam estar dentro de um intervalo específico, 10m, para que o ataque seja bem-sucedido. Esse ataque é comumente usado em áreas lotadas.
- **Denial of Service:** o atacante tenta travar a rede ou reiniciar o sistema, enviando pacotes para o sistema de destino (LONZETTA et al., 2018).
- **Spoofing:** Uma ferramenta de detecção pode ser usada para capturar o UUID do farol por um invasor, imitar o farol e quebrar as regras estabelecidas pelos aplicativos para verificar a identidade, para que ele possa acessar os serviços (TAY; TAN; NARASIMHAN, 2016)

5.2.4 Wi-Fi

A lista, a seguir, apresenta representa os principais ataques ao protocolo Wi-Fi.

- **ChopChop:** O ataque Chopchop permite que um atacante criptografe as mensagens de troca sem conhecer a chave (CANEILL; GILIS, 2010).
- **Google Replay:** Ao definir o Google.com, como uma página inicial, um invasor pode simplesmente descobrir parte do fluxo principal do log do Google baixado toda vez que os usuários abrem o site (CANEILL; GILIS, 2010).
- **Dictionary Attack:** Um ataque de dicionário é uma técnica na qual um invasor pode violar um Wi-Fi protegido por senha, adivinhando sua senha, tentando milhões ou bilhões de possibilidades, como palavras em um dicionário (CANEILL; GILIS, 2010).

5.2.5 ZigBee

A lista, abaixo, representa os principais ataques ao protocolo ZigBee.

- **Sniffing:** Como a maioria das redes ZigBee não usa nenhuma técnica de criptografia, elas podem estar vulneráveis a ataques de sniffing. O invasor pode interceptar alguns pacotes para executar atividades maliciosas (FAN et al., 2017).
- **Replay:** O ataque de repetição depende muito da intercepção do tráfego de rede. Sendo capaz de interceptar os pacotes, o atacante poderia retransmitir os dados interceptados como se fossem enviados por um usuário legítimo (FAN et al., 2017).

5.2.6 RPL

Os itens, a seguir, representam os principais ataques ao protocolo RPL.

- **Sinkhole attack:** o objetivo do adversário é atrair quase todo o tráfego de uma área específica através de um nó comprometido. (JEBA; PARAMASIVAN, 2012)
- **Wormhole attack:** um invasor grava pacotes (órbitas) em um local na rede, encapsulá-os em outro local e os transmite novamente para o rede. (JEBA; PARAMASIVAN, 2012)
- **Sybil attack:** um único nó apresenta várias identidades para outros nós na rede. (JEBA; PARAMASIVAN, 2012)
- **Hello flooding attack:** um invasor envia ou substitui os pacotes HELLO de um protocolo de roteamento de um nó para outro com mais energia. (JEBA; PARAMASIVAN, 2012)

5.2.7 6loWPAN

A lista, abaixo, apresenta os principais ataques ao protocolo 6loWPAN.

- **Fragmentation Attack:** Tendo projetado com mecanismo de fragmentação, o 6loWPAN permite a transmissão de pacotes IPv6 pelo IEEE 802.15.4. Sendo projetado sem nenhum tipo de autenticação, um invasor pode inserir seu fragmento na cadeia de fragmentação (AHMED; KO, 2016).
- **Authentication Attack:** Devido à falta de autenticação no 6loWPAN, qualquer objeto pode ingressar na rede e obter acesso não autorizado (AHMED; KO, 2016).
- **Confidentiality Attack:** Devido à ausência de técnica de criptografia no 6loWPAN, muitos ataques podem ser iniciados como MITM, interceptação e falsificação (AHMED; KO, 2016).

5.2.8 TCP-UDP

A lista a seguir apresenta representa os principais ataques ao protocolo TCP-UDP.

- **UDP flood:** um invasor envia um grande número de pacotes UDP aleatoriamente para diferentes portais para forçar tantos objetos a enviar pacotes ICMP de volta, o que pode tornar alguns objetos inacessíveis (KUMARASAMY; GOWRISHANKAR, 2012).
- **TCP Hijacking:** um invasor seleciona e adivinha os números de sequência e as somas de verificação das entidades comunicadas. Em seguida, o invasor pode injetar um pacote TCP malicioso que contém os números de soma e de sequência esperados pelo destinatário, que não possui um mecanismo para validar a origem do pacote, considerando-o legítimo (ZHENG; POON; BEZNOSOV, 2009).
- **TCP SYN flooding:** Esse ataque consiste em um conjunto de pacotes TCP SYN espionados, direcionados à porta da vítima. Servidores da Web, como servidores

de correio e servidores FTP e os objetos conectados, são vulneráveis a esse ataque (KUMARASAMY; GOWRISHANKAR, 2012).

5.2.9 Classificação

Ataques	Pilares
RFID	
Man-in-the-Middle	Confidencialidade, Integridade, Privacidade, Não-repudiação
Replay	Confidencialidade, Integridade, Prestação de Contas, Não-repudiação, Privacidade
Spoofing	Todos
NFC	
Eavesdropping	Confiabilidade, Privacidade, Não-repudiação
Man-in-the-Middle	Confidencialidade, Integridade, Privacidade, Não-repudiação
Relay	Confiabilidade, Integridade, Prestação de Contas, Não-repudiação, Privacidade
Bluetooth	
Bluesnarfing	Todos
BlueBugging	Todos
Bluejacking	Não-repudiação, Auditabilidade, Confiabilidade
Denial of Service	Disponibilidade, Prestação de Contas, Auditabilidade, Não-repudiação, Privacidade
Spoofing	Privacidade, Integridade, Auditabilidade, Confiabilidade, Não-repudiação
Wi-Fi	
ChopChop	Privacidade, Integridade, Auditabilidade, Confiabilidade, Não-repudiação, Confidencialidade
Google Replay	Privacidade, Integridade, Auditabilidade, Confiabilidade, Não-repudiação, Confidencialidade
Dictionary Attack	Privacidade, Integridade, Auditabilidade, Confiabilidade, Não-repudiação, Confidencialidade
ZigBee	
Sniffing	Confidencialidade, Não-repudiação, Privacidade
Replay	Confidencialidade, Integridade, Prestação de Contas, Não-repudiação, Privacidade
RPL	
Sinkhole Attack	Disponibilidade, Confidencialidade, Integridade
Wormhole Attack	Confidencialidade, Integridade, Prestação de Contas, Não-repudiação, Privacidade
Sybil Attack	Confidencialidade, Integridade, Prestação de Contas, Não-repudiação, Privacidade
Hello Flooding Attack	Confidencialidade, Integridade, Prestação de Contas, Não-repudiação, Privacidade, Disponibilidade
6loWPAN	
Fragmentation Attack	Privacidade, Integridade, Auditabilidade, Confiabilidade, Não-repudiação
Authentication Attack	Confidencialidade, Integridade, Privacidade, Não-repudiação
Confidentiality Attack	Confidencialidade, Integridade, Privacidade, Não-repudiação
TCP-UDP	
UDP Flood	Disponibilidade, Auditabilidade, Não-repudiação, Privacidade
TCP Hijacking	Privacidade, Integridade, Auditabilidade, Confiabilidade, Não-repudiação, Confidencialidade
TCP SYN Flooding	Disponibilidade, Prestação de Contas, Auditabilidade, Não-repudiação, Privacidade

Tabela 2 – Ataques a Protocolos e os pilares comprometidos

5.3 Ataques aos Dados

Os ataques aos dados possuem como foco apenas os dados localizados tanto no componente ou na nuvem. A seguir é apresentada uma lista com os principais ataques a este tipo de ataque.

- **Account hijacking:** Senhas fracas e engenharia social podem ser usadas para executar o sequestro de uma conta. Um atacante pode comprometer, manipular e redirecionar os dados confidenciais (ALLIANCE, 2010b).
- **Vazamento de Dados:** A falta de métodos seguros de processamento, armazenamento e transmissão de dados são as principais consequência desse ataque, por exemplo, armazenar dados não criptografados na nuvem ou em objetos de IoT (GROBAUER; WALLOSCHEK; STOCKER, 2011).

- **Denial of Service:** Tornar os dados da IoT inacessíveis por usuários legítimos é o principal objetivo desse ataque. Os ataques exploram as vulnerabilidades dos programas de interface de aplicativos (API) (ALLIANCE, 2010a), (DAWOUD; TAKOUNA, 2010).
- **Brute-force attack:** Esse tipo de ataque depende de um método de tentativa e erro para obter informações como senhas de usuário ou número de identificação pessoal (PIN). O ataque de força bruta usa software automatizado para gerar um grande número de suposições sequenciais para descriptografar o texto cifrado (JACKSON, 2008).
- **Hash collision:** O principal objetivo do ataque de colisão é descobrir duas sequências de entrada de uma função de hash que fornece o mesmo valor de hash. Como as funções hash têm comprimentos de entrada variáveis e uma saída curta de comprimento fixo, existe a possibilidade de que duas entradas diferentes gerem a mesma saída e, neste caso, é conhecido como colisão (STEVENS; LENSTRA; WEGER, 2007).

5.3.1 Classificação

Ataques	**Pilares**
Account hijacking	Todos
Vazamento de Dados	Confidencialidade, Integridade
Denial of Service	Privacidade, Autenticidade
Brute-force attack	Confidencialidade, Integridade
Hash collision	Confidencialidade, Integridade

Tabela 3 – Ataques a Dados e os pilares comprometidos

5.4 Ataques ao Software

Os ataques ao software são voltados a aplicações localizadas em componentes de Internet das Coisas, firmware, sistemas operacionais, gateway da aplicação e serviços. A lista, a seguir, apresenta os principais ataques deste tipo de ataque.

- **Malicious code injection:** Nesse tipo de ataque, um invasor injeta um código maldoso em alguns pacotes para roubar ou modificar dados confidenciais (SWAMY; JADHAV; KULKARNI, 2017).
- **Reprogram attack:** A reprogramação remota dos objetos da IoT, como em alguns ambientes, pode ser alcançada, usando um sistema de programação de rede. Uma vez que o processo de programação não esteja protegido, o invasor poderá sequestrar esse procedimento para controlar uma grande parte da rede (SABEEL; MAQBOOL, 2013).
- **Malware:** O processo de infecção de aplicativos da Web com um programa malicioso é conhecido como malware.

- **Distributed Denial of Service:** Uma das principais técnicas que podem ser usadas para estabelecer um ataque DDOS é uma botnet. Um exemplo desse ataque é a prevenção de acesso a um recurso, inundando-o com tantas solicitações (MIRKOVIC; REIHER, 2004).
- **Reverse Engineering:** O principal objetivo desse ataque é analisar o firmware dos objetos para obter dados confidenciais, como credenciais (PAPP; MA; BUTTYAN, 2015).

5.4.1 Classificação

Ataques	Pilares
Malicious code injection	Todos
Reprogram attack	Todos
Malware	Todos
Distributed Denial of Service	Disponibilidade, Prestação de Contas, Auditabilidade, Não Repudiação, Privacidade
Reverse Engineering	Todos

Tabela 4 – Ataques a Software e os pilares comprometidos

Derivando desta classificação é possível ter como base algumas áreas as quais são possíveis de encontrar alguma falha de segurança, além de fornecer alguns tipos de ataques como exemplo para iniciar os testes de vulnerabilidade e, também, partindo desta premissa é possível classificar as falhas de segurança encontradas. Quando se consegue explorar uma falha de segurança é possível classificá-la dentre um dos quatro tipos de ataques e é possível classificar quais os pilares da segurança da informação que essa determinada falha está quebrando.

6 METODOLOGIA

Este trabalho explorou um cenário que será composto por um Raspberry Pi, poderia ser utilizado também Arduino, mas, devido ao fato de possuir baixa capacidade de processamento e pouca memória disponível, torna-se inviável para que este estudo fosse realizado, por isso e pelo fato de que utilizando o Raspberry Pi seria mais abrangente quando se trata a respeito de qual ambiente é mais "seguro" e menos sujeito a falhas. Os principais motivos de usar este dispositivo são:

- A possibilidade de apresentar falhas distintas;
- Para dar maior propriedade na análise das falhas e suas respectivas recomendações de implementação de segurança quanto a prevenção de acessos não autorizados;
- Da limitação de cada tecnologia em agregar recursos de segurança e, assim, das diferentes ações a serem realizada pelos sistemas gerenciadores da rede internet para lidar com tais vulnerabilidades.

Além disto, o Raspberry Pi foi escolhido pelo fato de ser uma placa pequena, fácil de se instalar em uma maquete, fácil de utilizar, baixo custo, com boa documentação e suporte da comunidade.

O Raspberry foi utilizado como servidor que recebeu as requisições feitas pelos clientes através de um smartphone.

Para a execução deste cenário foi implementada uma estrutura de cliente-servidor, pois esta facilitará a execução e implementação do mesmo, uma vez que, segundo Porto et al. (2014).

> O principal objetivo da [...] tecnologia cliente-servidor é proporcionar soluções que serão úteis em ambientes corporativos, acadêmicos e outros com a utilização da comunicação entre equipamentos, com aplicação distribuída que compartilha a carga de trabalho entre os fornecedores de um recuso ao serviço (servidor) e os requerentes (clientes).

Com o objetivo de estabelecer a comunicação entre o aplicativo e os dispositivos conectados ao microcontrolador, foi desenvolvida uma API na qual este aplicativo consumirá e podendo, assim, se comunicar.

Depois de terminado o ambiente, foram utilizadas ferramentas (sendo estas de código aberto) para que pudesse ser colhido os resultados dos testes de penetração (pentest) e de falhas de segurança e, após finalizado, foram levantadas as possíveis alterações que deverão ser feitas para que se corrijam as falhas encontradas.

6.1 Lista de Equipamentos

(a) Raspberry Pi 3[1]: Placa pequena e portátil que pode funcionar como um computador. Irá funcionar como um servidor neste trabalho.

6.2 Lista de Softwares

(a) Raspbian OS: É a imagem oficial para o Raspberry sendo uma distribuição Linux considerado o sistema operacional padrão do computador da Raspberry Foundation. Por este motivo, é visto que, pelo fato de ser amplamente utilizado, é interessante que ele também passe por tais testes de vulnerabilidades, para que, após documentadas, tais falhas possam ser resolvidas pela empresa responsável.

(b) ControLar: Este aplicativo foi desenvolvido em Dart por meio do framework Flutter que possibilita o desenvolvimento em multiplataforma por meio de um único código e este aplicativo será responsável por realizar a comunicação com a API, por meio do protocolo HTTP e faz com que seja permitido ao usuário o total controle de dispositivos eletrônicos inteligentes de uma residência ou empresa, através de um aplicativo mobile que será executado sobre o sistema operacional Android.

(c) API de Comunicação: API desenvolvida em Python, utilizando uma biblioteca chamada Flask que facilita o desenvolvimento, pois já fornece módulos prontos, como, por exemplo, requisições HTTP, ferramentas para Login, e etc. Esta API será utilizada para que o aplicativo consiga acessar às portas seriais e digitais do Arduíno e do Raspberry.

(d) Wireshark: É uma ferramenta pública de análise de protocolos para sistemas Unix e Windows. Permite a observação de dados capturados da rede em tempo real ou previamente capturados e guardados num ficheiro ou disco. Pode-se navegar interativamente nos dados capturados, observando resumos ou informação pormenorizada de cada datagrama. O Wireshark possui diversas facilidades poderosas nomeadamente, uma linguagem rica para filtragem dos dados apresentados e a possibilidade de observar o fluxo de dados de uma sessão TCP reconstruída.

(e) Netcat: Programa que irá ler e escrever dados de uma rede, usando os protocolos TCP e UDP. É uma ferramenta poderosa para analisar problemas ou explorar uma rede, uma vez que permite criar praticamente qualquer tipo de ligação que seja necessária e possui diversas capacidades intrínsecas interessantes.

(f) Nmap: é um software livre utilizado para avaliar a segurança dos computadores e para descobrir serviços ou servidores em uma rede de computadores e será utilizado, também, para realizar testes nas portas para detectar possíveis brechas no sistema operacional e na API.

[1]https://www.Raspberry Pi.org/products/raspberry-pi-3-model-b/

(g) Nessus: é um scanner de vulnerabilidades, conhecido há muito tempo, no mercado, conta com mais de 67.000 plugins divididos por categorias (família de plugins) que fazem a verificação de diversas informações pertinentes a um vulnerability assessment, como: enumeração de serviços, bruteforces, verificação de serviços vulneráveis e etc.

(h) Maltego: é uma ferramenta de análise e análise de links visuais, fornecendo uma biblioteca de plugins, que são usados para executar consultas em fontes abertas, a fim de reunir informações sobre um determinado destino e exibi-los em um gráfico.

Além dos equipamentos e ferramentas listadas acima, também foi utilizado o ExploitDB[2] como repositório de exploits para que, após tenha sido levantada a falha de segurança, fosse possível realizar a busca para ver se já existe algum exploit que pode ser utilizado para explorar aquela determinada falha. Foi usado, também, o CVE[3] como repositório de falhas de segurança que já foram documentadas.

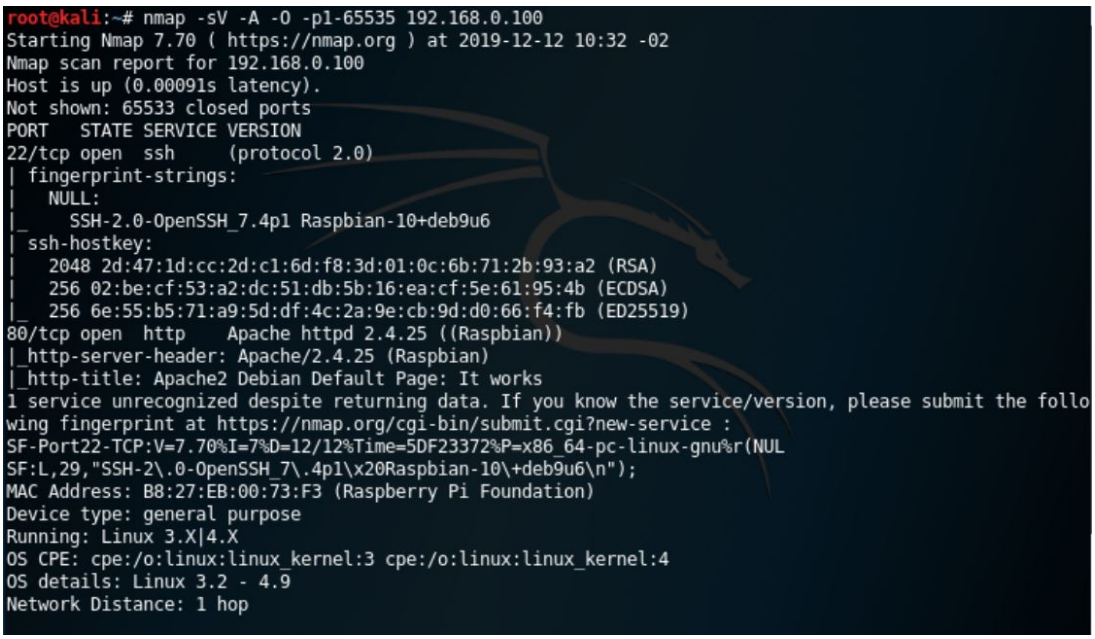
[2]https://www.exploit-db.com/
[3]https://cve.mitre.org/index.html

7 RESULTADOS E DISCUSSÃO

Antes de apresentar os resultados dos testes, é necessário definir primeiramente o que é um teste de penetração ou Pentest ou Penetration Test, é um método para testar e descobrir vulnerabilidades em uma rede ou sistemas. Esse teste utiliza métodos de avaliação de segurança, aplicando simulações de ataques para a verificação de falhas e, assim, realizar ajustes nos mecanismos e políticas de segurança (GIAVORATO e SANTOS, 2013).

Para que fosse possível saber por onde iniciar os testes de penetração foi utilizada a ferramenta nmap para realizar a análise de vulnerabilidades para se ter uma noção de quais portas e serviços estão sendo executados no alvo e assim fosse possível explorar as falhas em tais serviços e portas. A Figura 1 representa o resultado da análise de vulnerabilidades.

Figura 1 – Resultado da Análise de Vulnerabilidade



Fonte: O Autor

Com base na Figura 1, é possível perceber que os serviços de SSH e Apache estão rodando no alvo e sendo as portas desses serviços 22 e 80, respectivamente. A partir disso foi possível realizar testes de vulnerabilidade em cada um desses serviços.

Durante a realização do pentest foram encontradas algumas falhas de segurança que serão descritas abaixo, bem como o que pode conseguir explorando aquela determinada falha e quais os pilares da segurança da informação são quebrados. Além das ferramentas descritas no capítulo 5, deste trabalho, foram realizados testes com alguns exploits para que fosse visto se ainda estava suscetível à aquele ataque.

- **Linux.MulDrop.14**
- **Dirty Cow**

- **Shellshock**
- **Optionsbleed**

7.1 Linux.MulDrop.14

Segundo o Dr. Web, o fabricante de antivírus russo, o malware vem na forma de um script Bash que contém um programa de mineração compactado com gzip e criptografado com base64. Após o lançamento, o script encerra muitos processos e instala bibliotecas como Zmap e sshpass, necessárias para sua operação.

O malware tem como alvo dispositivos Raspberry Pi com portas SSH abertas para conexões externas. Ele obtém acesso ao dispositivo, usando o login padrão do Raspberry Pi ”pi”e a senha ”raspberry”.

O malware altera a senha do usuário e continua instalando os programas de mineração de criptomoedas. Depois, instala o Zmap, a ferramenta de varredura, para varrer a Internet, em busca de outros dispositivos Raspberry Pi vulneráveis com porta SSH aberta e credenciais de login padrão.

Basicamente, ele tem como alvo placas Raspberry Pi que usam login e senha padrão e têm porta SSH aberta. Considerando que o usuário padrão ainda tem acesso de administrador para instalar aplicativos, o malware pode usar esta vulnerabilidade para instalar qualquer tipo de programa.

Existem duas maneiras de proteger seu dispositivo contra esse malware:

- Atualize o sistema operacional. Ao fazer isso, o ID da porta SSH é desativado. O Raspbian desativou o servidor SSH por padrão em novembro de 2016 para forçar os usuários a alterar a senha padrão.
- Mude a senha padrão. A melhor maneira de interromper o ataque de malware é alterando sua senha e login padrão, pois eles são infectados usando o usuário e a senha padrão do Raspberry Pi. Isso protege um dispositivo que ainda não foi atacado pelo malware.

7.2 Dirty Cow

Dirty Cow é uma vulnerabilidade no kernel Linux que afeta todos os sistemas operacionais baseados nele, incluindo o Android. Trata-se de um bug para elevação de privilégios local que explora uma condição de corrida na implementação do mecanismo de copy-on-write. O bug está presente no kernel Linux desde a versão 2.6.22 lançada em setembro de 2007 e tem sido explorado desde outubro de 2016.

Embora seja um bug local de elevação de privilégios, invasores remotos podem usá-lo juntamente com outros exploits que permitem execução de código não privilegiado para conseguir acesso com privilégios de superusuário no computador. O ataque por si só não deixa rastros no log do sistema.

A falha do Kernel permite que qualquer programa ou aplicativo malicioso possa configurar uma condição de concorrência. A alteração permite mudar as permissões de executáveis que deveriam ser read-only. Um usuário comum poderia se utilizar dessa falha e escalar seu privilégio para o root do sistema.

Os motivos pelos quais essa falha pode ser considerada de alto risco são:

- Relativamente simples de desenvolver exploits para tal;
- Vulnerabilidade encontrada diretamente numa seção do Kernel do sistema, o que a torna presente em praticamente todas as distribuições do sistema operacional, como por exemplo, Debian, Ubuntu, Suse e RedHat;
- Possibilidade de estar presente, também, no Android, dado que ele utiliza o Kernel do Linux.

Esta falha é identificada pelo Common Vulnerabilities and Exposures como CVE-2016-5195[1]

Para corrigir a vulnerabilidade Dirty Cow, basta apenas atualizar o sistema com o gerenciador de pacotes padrão como apt, yum e outros. Já, em equipamentos embarcados e celulares, a solução depende de atualizações disponibilizadas pelo próprio fabricante, que nem sempre abrange todos os equipamentos. Modelos mais antigos podem continuar vulneráveis até o final de suas vidas úteis.

7.3 Shellshock

O Shellshock, conhecido como Bashdoor, é uma família de bugs de segurança no shell Unix Bash, o primeiro divulgado em 24 de setembro de 2014. O Shellshock pode permitir que um invasor faça com que o Bash execute comandos arbitrários e obtenha acesso não autorizado a muitos sites da Internet, como servidores da Web, que usam o Bash para processar solicitações.

Shellshock é uma vulnerabilidade de escalonamento de privilégios que oferece aos usuários de um sistema uma maneira de executar comandos que devem estar indisponíveis para eles. Isso acontece pelo recurso ”exportação de funções”do Bash, no qual os scripts de comando criados em uma instância em execução do Bash podem ser compartilhados com instâncias subordinadas. Esse recurso é implementado pela codificação dos scripts em uma tabela compartilhada entre as instâncias, conhecida como lista de variáveis de ambiente. Cada nova instância do Bash varre esta tabela em busca de scripts codificados, e monta um comando que define esse script na nova instância e o executa. A nova instância assume que os scripts encontrados na lista vêm de outra instância, mas não pode verificar isso, nem verificar se o comando que ele criou é uma definição de script, formado corretamente. Portanto, um invasor pode executar comandos arbitrários no sistema ou explorar outros erros que possam existir no interpretador de comandos do Bash, se o invasor puder

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195

manipular a lista de variáveis de ambiente e fazer com que o Bash seja executado.

Existem várias maneiras pelas quais um usuário ou uma organização pode proteger seus ambientes de computação do shellshock. Para corrigir uma máquina host vulnerável, uma atualização simples será necessária para a aquisição da versão mais recente do bash. Dependendo do gerenciador de pacotes, a emissão dos seguintes comandos o atualizará (DELAMORE; KO, 2015).

- apt update
- apt install –only-upgrade bash

7.4 Optionsbleed

A vulnerabilidade Optionsbleed existe quando um arquivo .htaccess configurado incorretamente faz com que a resposta OPTIONS contenha dados da memória. Se algum dos métodos HTTP configurados por um administrador não for aplicável, a vulnerabilidade Optionsbleed é acionada e os dados retornados vêm da memória do software do servidor Apache, isso pode incluir conteúdo de outros clientes ou do próprio servidor e possivelmente incluir informação sensível.

Um invasor remoto não autenticado pode acionar propositadamente a vulnerabilidade, enviando uma solicitação HTTP OPTIONS ao servidor, afetando os dois ambientes em que vários sites estão no mesmo servidor da web ou quando um único site está em um servidor da web.

Como forma do usuário se proteger desta falha, ele pode seguir as formas de resolver o problema:

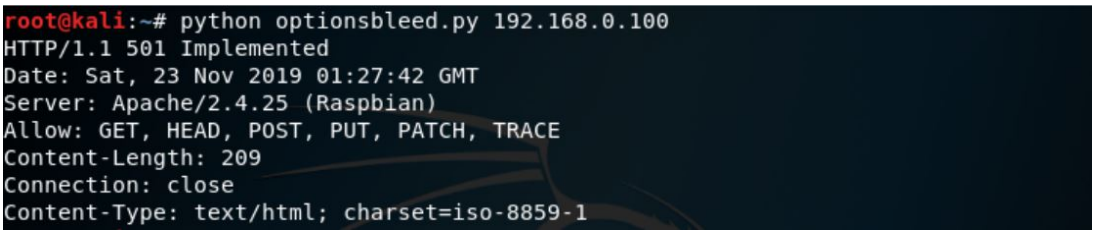
- Aplicar o patch disponível nos servidores de código-fonte Apache no link:
- Verificar se o seu provedor de hospedagem está executando uma versão não afetada do Apache Web Server.
- Para servidores Web Apache hospedados localmente, verificar a configuração do arquivo .htaccess.

Após o levantamento de tais falhas, utilizando as correções que foram propostas e o feitio novamente dos testes, foi possível confirmar que as correções propostas conseguem solucionar as falhas de segurança apresentadas no início deste capítulo. Como forma de comprovar que as falhas foram resolvidas, a Figura 2 e Figura 3 apresentam os resultados dos testes, comprovando a afirmação de que foram resolvidas.

A Figura 2 apresenta o resultado da análise de vulnerabilidade da falha "Optionsbleed"que foi apresentada anteriormente, mostrando assim que a solução proposta para esta falha cumpriu o seu objetivo.

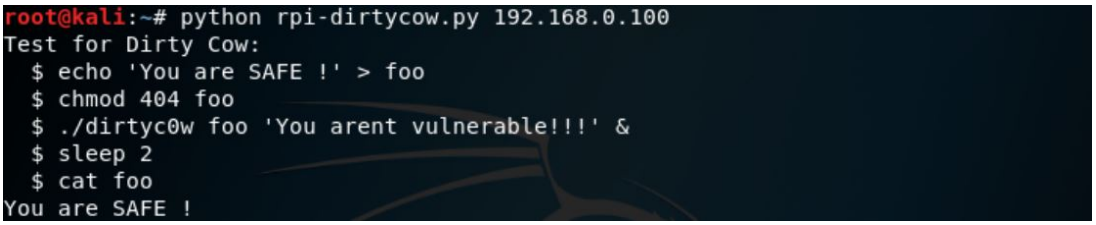
A Figura 3 apresenta o resultado da análise de vulnerabilidade da falha "Dirty Cow"que foi apresentada anteriormente, mostrando que a solução proposta para esta falha cumpriu o seu objetivo.

Figura 2 – Resultado da Análise de Vulnerabilidade do Dirty Cow



Fonte: O Autor

Figura 3 – Resultado da Análise de Vulnerabilidade do Optionsbleed



Fonte: O Autor

8 CONCLUSÃO

Os dispositivos inteligentes disponíveis para automação residencial possuem interfaces individuais de controle, muitas vezes, bem diferentes entre si, tornando o processo de controle de um ambiente multidispositivos mais difícil para o usuário, além disso torna o processo de manter a segurança da informação de todo o ambiente sob controle muito mais difícil.

Para que este estudo fosse realizado, foram definidos alguns objetivos necessários para que ele pudesse ser desenvolvido com sucesso e tais objetivos eram estudar como é o uso de dispositivos inteligentes em contextos diferentes, como, por exemplo, residencial e empresarial, e como eles influenciam no dia a dia do usuário, estudar as principais falhas de seguranças de dispositivos inteligentes, que já foram detectadas e documentadas, pesquisar casos em que as falhas de segurança foram exploradas por atacantes e acarretaram problemas maiores os seus usuários, realizar o teste de invasão e vulnerabilidade no ambiente proposto, documentar todas as falhas de segurança que foram encontradas, a partir do feitio dos testes, propor soluções para as falhas de segurança que foram encontradas e tornar evidente a necessidade de segurança para estes dispositivos.

O desenvolvimento do ambiente, utilizando o Raspberry se revelou desafiador devido à falta de trabalhos explorando este ambiente e exemplos de aplicações para automação desenvolvidas com essas tecnologias, até mesmo por serem relativamente recentes durante a realização deste trabalho. Porém, após finalizados os testes, é possível afirmar que todos os objetivos foram cumpridos com sucesso e tais tecnologias e ferramentas são suficientes para o desenvolvimento deste tipo de aplicação.

Após o desenvolvimento do ambiente, é possível afirmar que, a partir dos testes realizados e das falhas encontradas, é necessário que se continue pesquisando e realizando novos testes para que assim seja possível desenvolver um ambiente seguro para a Internet das Coisas, ou seja, confirma-se a justificativa deste estudo.

8.1 Trabalhos Futuros

Sugere-se para trabalhos futuros a ampliação da quantidade da diversidade dos cenários de testes, além de propor soluções para as falhas que forem encontradas, uma vez que o Raspberry não representa 100% dos ambientes de Internet das Coisas, podendo se utilizar de um Arduino e, também, de soluções de automação residencial e empresarial que já estão disponíveis no mercado, fazendo com que se tenha uma maior precisão e melhor representação das falhas de segurança, as quais a Internet das Coisas está sujeita.

Referências

ABDUL-GHANI, H. A.; KONSTANTAS, D.; MAHYOUB, M. A comprehensive iot attacks survey based on a building-blocked reference model. **International Journal of Advanced Computer Science and Applications**, v. 9, n. 3, 2018. Citado na página 11.

AHMED, F.; KO, Y.-B. A distributed and cooperative verification mechanism to defend against dodag version number attack in rpl. In: INSTICC. **Proceedings of the 6th International Joint Conference on Pervasive and Embedded Computing and Communication Systems - Volume 1: PEC, (PECCS 2016)**. [S.l.]: SciTePress, 2016. p. 55–62. ISBN 978-989-758-195-3. Citado na página 13.

AKRAM, H.; KONSTANTAS, D.; MAHYOUB, M. A comprehensive IoT attacks survey based on a building-blocked reference model. **International Journal of Advanced Computer Science and Applications**, The Science and Information Organization, v. 9, n. 3, 2018. Citado na página 9.

ALLIANCE, C. S. **Cloud Security Alliance**. 2010. Citado na página 15.

ALLIANCE, C. S. **Top Threats to Cloud Computing V1.0**. 2010. Citado na página 14.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. **Computer Networks**, Elsevier BV, v. 54, n. 15, p. 2787–2805, oct 2010. Tradução Nossa. Citado na página 4.

BERTOGLIO, D. D.; ZORZO, A. F. Um mapeamento sistemático sobre testes de penetração. **Porto Alegre: Faculdade de Informática PUC-RS**, 2015. Citado na página 8.

BOLZANI, C. A. M. Desmistificando a domótica. **Sinergia**, v. 8, n. 1, p. 17, jan. 2007. Citado na página 4.

CANEILL, M.; GILIS, J.-L. Attacks against the wifi protocols wep and wpa. **Journal, no. December**, 2010. Citado na página 12.

CHAKRABORTY, R. S.; NARASIMHAN, S.; BHUNIA, S. Hardware trojan: Threats and emerging solutions. In: **2009 IEEE International High Level Design Validation and Test Workshop**. [S.l.]: IEEE, 2009. Citado na página 10.

COELHO, F. E. S.; ARAúJO, L. G. S. de; BEZERRA, E. K. **Gestão da segurança da informação: NBR 27001 e NBR 27002**. 1. ed. [S.l.], 2014. Citado na página 9.

DAWOUD, W.; TAKOUNA, I. Infrastructure as a service security: Challenges and solutions. **IEEEE**, maio 2010. Citado na página 15.

DELAMORE, B.; KO, R. K. L. A global, empirical analysis of the shellshock vulnerability in web applications. In: **2015 IEEE Trustcom/BigDataSE/ISPA**. [S.l.]: IEEE, 2015. Citado na página 23.

DOMINGUES, D. E. R. Testes de invasão em ambiente corporativo. **Universidade Católica de Brasília**, 2012. Citado na página 7.

FAN, X. et al. **Security analysis of zigbee**. [S.l.]: MIT. edu, 2017. Citado na página 12.

GALEGALE, G. P. et al. Internet das coisas aplicada a negócios - um estudo bibliométrico. **Journal of Information Systems and Technology Management**, TECSI, v. 13, n. 3, dec 2016. Citado na página 1.

GROBAUER, B.; WALLOSCHEK, T.; STOCKER, E. Understanding cloud computing vulnerabilities. **IEEE Security & Privacy Magazine**, Institute of Electrical and Electronics Engineers (IEEE), v. 9, n. 2, p. 50–57, mar 2011. Citado na página 14.

GROVER, K.; LIM, A.; YANG, Q. Jamming and anti-jamming techniques in wireless networks: a survey. **International Journal of Ad Hoc and Ubiquitous Computing**, Inderscience Publishers, v. 17, n. 4, p. 197, 2014. Citado na página 10.

IVAN, C.; VUJIC, M.; HUSNJAK, S. Classification of security risks in the IoT environment. In: **DAAAM Proceedings**. [S.l.]: DAAAM International Vienna, 2016. p. 0731–0740. Citado na página 11.

JACKSON, K. **Hacker's Choice: Top Six Database Attacks.** 2008. Citado na página 15.

JEBA, S.; PARAMASIVAN, B. False data injection attack and its countermeasures in wireless sensor networks. **European Journal of Scientific Research**, v. 82, 07 2012. Citado na página 13.

KAMBLE, A.; MALEMATH, V. S.; PATIL, D. Security attacks and secure routing protocols in RPL-based internet of things: Survey. In: **2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)**. [S.l.]: IEEE, 2017. Citado na página 7.

KHAN, W. Z. et al. Detection and mitigation of node replication attacks in wireless sensor networks: A survey. **International Journal of Distributed Sensor Networks**, SAGE Publications, v. 9, n. 5, p. 149023, jan 2013. Citado na página 10.

KHEDR, W. I. SRFID: A hash-based security scheme for low cost RFID systems. **Egyptian Informatics Journal**, Elsevier BV, v. 14, n. 1, p. 89–98, mar 2013. Citado na página 12.

KUMARASAMY, S.; GOWRISHANKAR, A. An active defense mechanism for tcp syn flooding attacks. **arXiv preprint arXiv:1201.2103**, 2012. Citado 2 vezes nas páginas 13 e 14.

KUROSE, K. W. R. J. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 4. ed. [S.l.]: Pearson Universidades, 2010. ISBN 9788588639973. Citado na página 9.

LONZETTA, A. et al. Security vulnerabilities in bluetooth technology as used in IoT. **Journal of Sensor and Actuator Networks**, MDPI AG, v. 7, n. 3, p. 28, jul 2018. Citado na página 12.

MARTINS, R. A.; ZARPELãO, B. B. Desenvolvimento de um framework para investigação de vulnerabilidades em dispositivos de internet das coisas. **Universidade Estadual de Londrina**, 2018. Citado na página 6.

MIESSLER, D. Hp study reveals 70 percent of internet of things devices vulnerable to attack. **Retriev**, 2014. Citado na página 4.

MIRJALILI, M.; NOWROOZI, A.; ALIDOOSTI, M. A survey on web penetration test. **ACSIJ Advances in Computer Science: an International Journal**, v. 3, n. 12, p. 15, 11 2014. ISSN 2322-5157. Citado na página 8.

MIRKOVIC, J.; REIHER, P. A taxonomy of DDoS attack and DDoS defense mechanisms. **ACM SIGCOMM Computer Communication Review**, Association for Computing Machinery (ACM), v. 34, n. 2, p. 39, apr 2004. Citado na página 16.

MITROKOTSA, A.; RIEBACK, M. R.; TANENBAUM, A. S. Classification of rfid attacks. **Gen**, Citeseer, v. 15693, p. 14443, 2010. Citado na página 11.

MOSENIA, A.; JHA, N. K. A comprehensive study of security of internet-of-things. **IEEE Transactions on Emerging Topics in Computing**, Institute of Electrical and Electronics Engineers (IEEE), v. 5, n. 4, p. 586–602, oct 2017. Citado na página 12.

MUKHERJEE, B. et al. Flexible IoT security middleware for end-to-end cloud–fog communication. **Future Generation Computer Systems**, Elsevier BV, v. 87, p. 688–703, oct 2018. Citado na página 1.

NESHEIM, M. B.; ROSNES, K. S. **A smarter home, the smarter choice?** Dissertação (Mestrado) — Universitetet i Stavanger, 2016. Citado na página 1.

OSANAIYE, O.; ALFA, A.; HANCKE, G. A statistical approach to detect jamming attacks in wireless sensor networks. **Sensors**, MDPI AG, v. 18, n. 6, p. 1691, may 2018. Citado na página 10.

PAPP, D.; MA, Z.; BUTTYAN, L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In: **2015 13th Annual Conference on Privacy, Security and Trust (PST)**. [S.l.]: IEEE, 2015. Citado na página 16.

PORTO, R. S. M. et al. Aplicação baseada na tecnologia cliente e servidor utilizando invocação de método remoto. In: **COBENGE**. [S.l.: s.n.], 2014. Citado na página 17.

RFID Attacks. In: RFID Security. [S.l.]: Elsevier, 2005. p. 83–99. Citado na página 11.

RIBEIRO, R. M. O. Segurança em iot simulação de ataque em uma rede rpl utilizando contiki. **Universidade Federal de Uberlândia**, 2018. Citado 2 vezes nas páginas 4 e 6.

RIYAZUDDIN, M. Nfc: A review of the technology, applications and security. **ABI research**, 2011. Citado na página 11.

ROONEY, C.; SEEAM, A.; BELLEKENS, X. Creation and detection of hardware trojans using non-invasive off-the-shelf technologies. **Electronics**, MDPI AG, v. 7, n. 7, p. 124, jul 2018. Citado na página 10.

SABEEL, U.; MAQBOOL, S. Categorized security threats in the wireless sensor networks: Countermeasures and security management schemes. **International Journal of Computer Applications**, Foundation of Computer Science, v. 64, n. 16, p. 19–28, feb 2013. Citado na página 15.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. **Future Internet**, MDPI AG, v. 11, n. 4, p. 89, apr 2019. Citado na página 10.

SOUSA, B. F. L. M. **Um Sistema de Detecção de Intrusão para Detecção de Ataques de Negação de Serviço na Internet das Coisas**. Dissertação (Mestrado) — Universidade Federal do Maranhão, 2016. Citado na página 7.

STEVENS, M.; LENSTRA, A.; WEGER, B. de. Chosen-prefix collisions for MD5 and colliding x.509 certificates for different identities. In: **Advances in Cryptology - EUROCRYPT 2007**. [S.l.]: Springer Berlin Heidelberg, 2007. p. 1–22. Citado na página 15.

SUBASHINI, S.; KAVITHA, V. A survey on security issues in service delivery models of cloud computing. **Journal of Network and Computer Applications**, Elsevier BV, v. 34, n. 1, p. 1–11, jan 2011. Citado na página 7.

SWAMY, S. N.; JADHAV, D.; KULKARNI, N. Security threats in the application layer in IOT applications. In: **2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)**. [S.l.]: IEEE, 2017. Citado na página 15.

TAY, H. J.; TAN, J.; NARASIMHAN, P. A survey of security vulnerabilities in bluetooth low energy beacons. **Carnegie Mellon University Parallel Data Lab Technical Report CMU-PDL-16-109**, 2016. Citado na página 12.

TRIBUNAL DE CONTAS DA UNIãO. **Boas práticas em segurança da informação**. Brasília, 2012. Citado na página 9.

WACHSMANN, C.; SADEGHI, A.-R. Physically unclonable functions (PUFs): Applications, models, and future directions. **Synthesis Lectures on Information Security, Privacy, and Trust**, Morgan & Claypool Publishers LLC, v. 9, n. 1, p. 1–91, dec 2014. Citado na página 12.

ZHENG, O.; POON, J.; BEZNOSOV, K. Application-based TCP hijacking. In: **Proceedings of the Second European Workshop on System Security - EUROSEC**. [S.l.]: ACM Press, 2009. Citado na página 13.