FACULDADE DE TECNOLOGIA DE AMERICANA MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Priscila Stéfane Alves Martins Rodrigues
Rodrigo Oliveira Abreu

Ameaças e vulnerabilidades em dispositivos IoT

Americana,

SP

2021

FACULDADE DE TECNOLOGIA DE AMERICANA MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Priscila Stéfane Alves Martins Rodrigues
Rodrigo Oliveira Abreu

Ameaças e vulnerabilidades em dispositivos IoT

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Dra. Maria Cristina Aranda
Área de concentração: Segurança da Informação.

Americana,

SP

2021

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

R615a RODRIGUES, Priscila Stéfane Alves Martins
Ameaças e vulnerabilidades em dispositivos IoT. / Priscila Stéfane Alves Martins Rodrigues, Rodrigo Oliveira Abreu. – Americana, 2021.
66f.
Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza
Orientador: Profa. Dra. Maria Cristina Aranda
1 Segurança em sistemas de informação 2. Internet das coisas I. ABREU, Rodrigo Oliveira II. ARANDA, Maria Cristina III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Ameaças e vulnerabilidades em dispositivos IoT.

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 21 de junho de 2021.

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
Fatec Americana Ministro Ralph Biasi

Daniele Junqueira Frosoni
Especialista
Fatec Americana Ministro Ralph Biasi

Cleberson Eugenio Forte
Doutor
Fatec Americana Ministro Ralph Biasi

AGRADECIMENTOS

Em primeiro lugar queremos agradecer a Deus pela vida e pela saúde nesse momento tão difícil, e também agradecer à nossa orientadora Dra. Maria Cristina Aranda, por acreditar no nosso potencial e conhecimento, agradecer nossos familiarias que tiveram sempre nos apoiando ao longo de nossa formação.

DEDICATÓRIA

Dedicamos esse trabalho para os nossos pais que sempre nos apoiaram em todos os obstáculos ao longo desse curso e que sempre ajudaram em todos os momentos difíceis da vida, dedico também aos professores do curso de segurança da informação da Fatec Americana Ministro Ralph Biasi, pelo amplo conhecimento, paciência, apoio, dedicação e esforço que tiveram durante esses anos.

RESUMO

A IoT vem crescendo desde o início da Internet, visto que em 1999, foi apresentado pela primeira vez o conceito de IoT. Após vinte anos de implementações, inovações e atualizações desta tecnologia, existe vários relatos de invasão através de brechas e vulnerabilidades exploradas nesses dispositivos. A IoT está presente em quase todas as tarefas do dia a dia de uma sociedade moderna, e com essa mudança, pode tornar mais ágeis processos antes demorados, porém existe uma preocupação com esses dispositivos de certa forma, visto que os fabricantes ainda enfrentam uma dificuldade abrangente de implementar segurança nos dispositivos. A proteção e a privacidade dos dados é uma questão importante e que será um grande desafio para os fabricantes e usuários. Gerenciar os dados e tornar seguros em um ambiente confiável e íntegro será o papel da organização em conjunto com as demais partes relacionadas. Será apresentado algumas ferramentas utilizadas para a exploração de ameaças e vulnerabilidades em um dispositivo IoT, foi utilizado como estudo de caso a Lâmpada LED Intelbras modelo EWS 410, o objetivo é analisar todos os protocolos e serviços utilizado pelo dispositivo, afim de orientar usuários, organizações e os fabricantes sobre os problemas reportados.

Palavras Chave: IoT, Segurança da Informação, Privacidade de dados, Teste de penetração.

ABSTRACT

The IoT has been growing since the beginning of the Internet, as in 1999, the concept of IoT was first introduced. After twenty years of implementations, innovations and updates of this technology, there are several reports of breaches through exploits and vulnerabilities of devices. IoT is present in almost every day-to-day tasks of a modern society, and with this change, it can make processes that were previously time-consuming more agile, but there is a concern with these devices in a way, since manufacturers still face a difficulty includes implementing security on devices. Data protection and privacy is an important issue and will be a major challenge for manufacturers and users. Managing the data and securing it in a trustworthy and safe environment will be the organization's role in conjunction with other related parties. Some tools used for reviewing and exploiting vulnerabilities in an IoT device will be presented, it was used as a case study of an Intelbras LED lamp model EWS 410, the objective is to analyze all protocols and services used by the device, in order to guide users, associations and manufacturers on reported issues.

Keywords: *IoT, Information Security, Data Privacy, Penetration Testing.*

SUMÁRIO

1. INTRODUÇÃO.

A Internet facilita realizar muitos procedimentos, sejam eles dos mais simples, como enviar um *e-mail,* conversar com amigos e familiares, através das redes sociais. *whatsapp*, *twitter, facebook, instagram,* até os mais complexos como trabalho *home office*, aula remota, entrevistas de emprego através de videoconferência, compras, acesso a aplicativos de bancos, agendamento de consulta, visualizar resultados de exames, etc.

Em meio ao grande avanço tecnológico, viu-se a necessidade de conectar H2M *Human to Machine,* M2M *Machine to Machine,* e P2P *People to People* tornando tudo integrado e conectado e, a partir daí surgiu o conceito de IoT. Segundo a Cisco (2020) em até 2023, 66% da população mundial estará conectada à Internet. A pesquisa mostrou que 23% dessas conexões serão de dispositivos IoT. A IoT veio para inovar, tendo como foco facilitar processos que são repetitivos e desgastantes para um humano. Utilizando conceitos da indústria 4.0, realiza a integração de máquinas e ERP - Enterprise Resource Planning através da conexão com a Internet, aumentando a praticidade, agilidade, facilidade, economia, rapidez, precisão, automação a processos que antes eram manuais.

Hoje a IoT é utilizada em diversas áreas, as cinco mais utilizadas são: otimização da produção, gestão de cadeia de fornecimento, acompanhamento e gerenciamento de ativos, tomada de decisões e experiência ao cliente.

Além disso, a sociedade moderna é cercada de dispositivos interconectados em casa como: *smartTV*, assistente virtual, interruptores de luz, *home theater*, cafeteira, geladeira, ar-condicionado entre outros, levando assim ao conceito de *smarthome*. Também há outras tecnologias integradas à IoT como: API - Application Programming Interface, análise de dados, criptografia, computação em nuvem, *big data e* inteligência artificial. A necessidade de implementar e atualizar ferramentas de segurança nessas aplicações é grande e preocupante.

Os dispositivos podem transmitir milhões de dados por segundo através da rede de computadores, e muitos deles não possuem protocolos de segurança mais atualizados e criptografia com padrões mais seguros. Os grandes fabricantes ainda passam por dificuldades em realizar implementação de segurança, visto que a tecnologia existente e mais segura, de outras aplicações

como *smartphone* e computadores não são totalmente compatíveis em relação a *software*, *hardware* e *firmware* dos dispositivos IoT.

O objetivo desse trabalho é apresentar algumas ameaças e vulnerabilidades nos dispositivos, utilizando algumas ferramentas para análise de serviços que possua ameças e vulnerabilidades, afim de alertas os usuários, fabricantes e organizações que utilizam IoT. Esse tema se torna altamente comentado quando é possível pensar que automatizar coisas, se encontra cada vez mais presente no cotidiano atual, a fim de poder alertar uma preocupação com essa tecnologia, alertando o usuário final, a organização que a utiliza, ou fabricante sobre os problemas reportados nessas soluções.

2 INTERNET DAS COISAS

A Internet das coisas ou como é dito em inglês *Internet of Things* (IoT) é a tecnologia que conecta coisas à Internet. Conforme Magrani (2019, p.19).

> A Internet das Coisas é a expressão que busca designar todo o conjunto de novos serviços e dispositivos que reúnem ao menos três pontos elementares: conectividade, uso de sensores e capacidade computacional de processamento e de armazenamento.

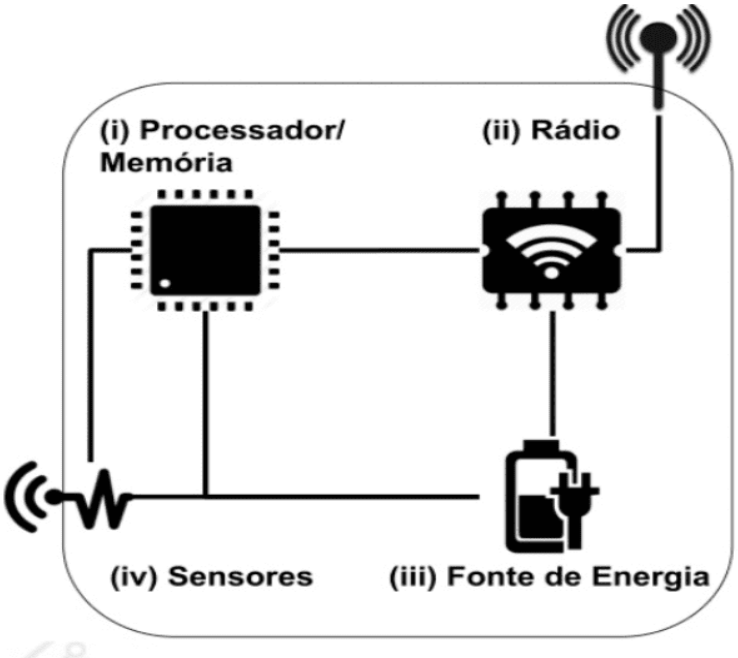
Esses dispositivos estão sendo utilizados a algum tempo, porém quase não se percebe a presença deles, a IoT é praticamente qualquer “coisa” que pode se conectar à Internet, enviar, receber e processar dados, tornando conectado muitas “coisas” que possui a mesma tecnologia empregada, formando assim uma rede, onde pode-se automatizar uma ou várias “coisas” ou conectar pessoas a “coisas”.

Um dispositivo inteligente é automaticamente relacionado com inovação e tecnologia, IoT se originou de uma tecnologia que já era existente, porém com uma outra ideia, conceito e aplicabilidade, a ideia de conectar “coisas”, processar e realizar tomadas de decisões com a evolução da tecnologia se tornou real.

A arquitetura de IoT e suas funcionalidades basicamentes são compostas por quatro unidades são eles:

- Processador/Mémoria são responsáveis por processar os dados e armanezar informação, um micro controlador e um conversor analógico- digital que recebe o sinal dos sensores.
- Rádio é um sensor que faz a conexão podendo ser ele bluetooth, LPWAN (Low Power Wide Area Network), 3g, 4g,5g e etc.
- Sensores tranforma o ambiente fisico em informação, os sensores capturam valores de grandezas física como umidade, pressão, temperatura e presença.
- Fonte de energia pode ser de uma energia fixa permanente ou a fonte de energia pode ser uma bateria recarregável, e um conversor AC-DC que tem a função de alimentar os componentes.

Figura 1: Arquitetura IoT



Fonte: Sousa, 2018

Na figura 1 pode-se ver um modelo de arquitetura IoT, com um *hardware* que possui sensores, fonte de energia, processador, memória e um transmissor de dados via RFID. Em IoT utilizam-se transdutores, que são sensores e atuadores, e a função de um transdutor é transformar a energia que ele recebe em informação para ser utilizada posteriormente.

Existem dois tipos de transdutores sendo eles, ativos e passivos. Os transdutores ativos não necessitam de um sinal externo para produzir um sinal elétrico como saída, já os transdutores passivos precisam de um sinal externo.

2.1 A história da tecnologia IoT.

No ano de 1990 o comércio varejista da época utilizava cartões de fidelidade, onde era utilizado conexão RFID - Radio Frequency Identification. Esses cartões tinham inclusos *chips* de rádio frequência para a transmissão de informações, que trafegam apenas por rádio frequência, não sendo utilizado cabos para a transmissão. Em 1991 Bill Joy, cofundador da Sun Microsystems, imaginou utilizar conexão TCP/IP Transmission Control Protocol e IP - Internet Protocol para conectar dois dispositivos D2D - Device to Device.

A tecnologia chegou às mãos de Kevin Auston, que teve a ideia de utilizar

a mesma tecnologia na cadeia de suprimentos de sua loja, ele vendia os produtos da *Procter & Gamble*. Em 1999, Kevin Auston refere-se a essa tecnologia denominando-a com o termo *Internet of Things*. Conforme Auston (2009).

> Não é apenas um código de barras com esteróides ou uma forma de acelerar estradas com pedágio, e nunca devemos permitir que nossa visão encolha a essa escala. A Internet das Coisas tem o potencial de mudar o mundo, assim como a Internet fez. Talvez ainda mais.

A IoT está em todas as áreas da sociedade atual, como: economia, agropecuária, indústria automobilística, tecnologia da informação, trânsito e transporte, ciência, biomedicina, biotecnologia, nanotecnologia, cidades inteligentes, telecomunicação, *marketing*, meio ambiente, logística entre outros.

2.1.2 A IoT na automação residencial.

Dispositivos IoT focado exclusivamente para automatização residencial, cresceu nos últimos anos, recentemente a Nest se integrou com a Google Home*,* que é um aplicativo para Android criado pela Google para gerenciar dispositivos inteligentes em uma casa, assim fornecendo uma experiência mais fácil, rápida e precisa para seus clientes.

Alguns dispositivos podem ser adquiridos diretamente na loja de aplicativos Play Store. Esses dispositivos são: assistente de voz, sistema de segurança, alarme, sensores de presença, câmera, iluminação, sensores de fumaça, termostatos, campainha e fechadura, todos possuem integração com aplicativos para *smartphone*.

É possível realizar monitoramento e controle em todas as áreas de uma residência que possua uma interconectividade através do *smartphone* conectado com a Internet, e caso não exista Internet esses dispositivos não funcionarão somente com a rede local.

2.1.3 Dispositivos IoT facilitam processos para a área da saúde.

A Internet das coisas a cada dia que passa, está favorecendo a área da saúde. Pode-se impulsionar tarefas que eram impossíveis de serem realizada

sem a tecnologia atualmente existente, em combate a pandemia do *Covid-19*, Computerworld (2020), informou a parceria entre o Incor Instituto do Coração do HCFMUSP Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo, o NETi Núcleo Especializado em Tecnologia da Informação, e a *healh tech carenet*, está trazendo inovações e ferramentas que podem ajudar no tratamento da doenças.

E já é possível realizar uma análise em tempo real de dados dos pacientes, como: monitorar respiração, batimento cardíaco e saturação de oxigênio, e esses dados ficam em relatório digitais onde é possível visualizar através de dispositivos móveis, um exemplo de uso na atual pandemia do *Covid-19* que é altamente contagiosa, é possível realizar todas essas atividades sem estar no mesmo local físico que o paciente, trazendo segurança e comodidade para as equipes que trabalham na linha de frente e não proporcionando aglomeração de pessoas em consultórios.

A Apple (2015) apresentou uma novidade em um novo dispositivo IoT chamado *Apple Watch*, o relógio inteligente conta com recursos inovadores que podem analisar os batimentos cardíacos de um humano, e nas versões mais recentes do dispositivo já é possível gerar um eletrocardiograma em apenas 30 segundos.

Vale destacar que o *Apple Watch* já salvou vidas, com uma função que quando o usuário sofre uma queda, os sensores conseguem perceber o impacto e em 3 segundos realiza uma ligação de emergência. A Apple (2020) introduziu novas funcionalidades ao relógio em função da pandemia do *Covid-19*, o oxímetro que tem a função de medir o nível de oxigênio no sangue, e também foi adicionado outra função que tem como objetivo alertar os usuários a realizar a higienização das mãos, de tempos em tempos essa notificação é mostrada como alerta.

2.1.4 A utilização do IoT em carros autônomos.

A Tesla Motors já está a alguns anos investindo em carros autônomos, os carros possuem sensores que podem enviar e receber dados através da Internet, além de compartilhar serviços de geolocalização e seus carros podem ser controlados através de computadores. A Tesla trouxe uma realidade antes não imaginada, e a empresa vem investido bastante em tecnologia para os

seus automóveis, Musk (2020), disse que em 2021 alguns modelos de carros autônomos estariam circulando pelas ruas, e já é possível encontrar esse tipo de veículo em alguns países.

As empresas automobilistas que apostarem nessa tecnologia deverão fazer atualizações constante de seus mapas, pois no mundo real o carro irá assumir responsabilidades de um ser humano, devendo manter os mapas de bordo atualizados é essencial para um bom funcionamento, rapidez, praticidade e segurança. Esses mapas deverão ser sincronizados em tempo real, e permitem precisão em manobras mais complexas, informações importantes de incidentes reportados, vias disponíveis para localizações, entre outros.

Para isso o carro necessariamente deverá estar conectado à Internet. A grande quantidade de dados gerados, faz a segurança da informação ser um destaque importante, o governo da China demonstrou estar preocupado com os carros autônomos para a utilização do USA - United States of America em espionagens, sabendo-se que possuem alta tecnologia e muitas câmeras podem ser acionadas remotamente.

2.1.5 Novas tecnologias para integração em IoT.

A Cisco (2020) trouxe uma tecnologia em suas aplicações em IoT trazendo um engajamento em muitas áreas, a empresa oferece um leque de oportunidades e de mudanças para a utilização dos seus dispositivos IioT - Industrial Internet of Things.

Alguns dos benefícios oferecidos pela empresa é a automatização industrial, nesse processo é visível a viabilidade de benefícios como redução de custo, redução de tempo de produção, processos com menos índices de erros, entre outros.

Com os interruptores industriais é possível o monitoramento das aplicações e gerenciamento remoto, através do *software* próprio do Cisco DNA Center e utilizando a solução SD-Access, pode ser oferecido automação desde a borda do dispositivo até a nuvem, o *software* utiliza a inteligência artificial e aprendizagem de máquina para aplicação em processos da empresa, realizando assim tomada de decisões.

Com seus equipamentos de rede, é possível operar em áreas muito

quentes, chegando a mais de 70º, e em áreas muito frias chegando a menos de 40º. A Cisco realizou uma parceria com a Microsoft integrando a aplicação *Azure IoT Hub Service* e *Azure IoT Hub Device Provisioning Service* com a plataforma *Edge Intelligente.*

Essa integração tem como objetivo gerenciar e processar dados com mais facilidade, os dados armazenados nos dispositivos serão enviados à nuvem do *Microsoft Azure*, segundo a Cisco essa integração facilitará para que o processo de transformação e inovação seja acelerado, permitindo futuramente a integração de novos clientes e parceiros de negócios.

2.2. Controle de tráfego com IoT.

Os dispositivos IoT já são utilizados no controle de tráfego para a utilização de coleta de dados das informações do trânsito, alertas, acidentes, radares, reconhecimento de placas de veículos. Com os novos modelos de carros que trazem a conexão com a Internet, uso de GPS *Global Positioning System*, e a integração com os *smartphones*, os aplicativos de mapas disponíveis conseguem trazer informações em tempo real do trânsito, como lugares com maior engarrafamento, lentidão, disponibilizando soluções para algumas situações, como rotas alternativas para a fluidez do trânsito.

Com a adoção da IoT é possível realizar análise de dados do trânsito, como por exemplo, as rotas mais frequentadas, e os horários com mais movimento, com esses dados o governo consegue investir em novos projetos, para que a população seja beneficiada.

Através desse tipo de análise de dados é possível conscientizar o cidadão, apresentando os dados analisados, para que ele tenha a possibilidade de usar o transporte coletivo ao invés de usar condução própria, sendo assim possibilitando melhor fluidez do trânsito, mais rapidez em lugares de difícil acesso, diminuição de poluição em função da menor circulação de automóveis nas ruas.

2.2.1 Viabilidade em tornar os dispositivos inteligentes.

A IoT facilita as atividades diárias de um cidadão e facilitará ainda mais com o passar dos anos. Não é possível saber até onde a indústria da Internet das coisas irá chegar, porém ao passar dos anos as empresas de tecnologia

tendem a induzir ao uso produtos que fazem com que o usuário tenha uma sensação de benefício e praticidade quando o adquire.

As indústrias de tecnologia lançam novos objetos IoT todos os dias, porém essa tecnologia é encontrada com um valor alto no mercado brasileiro mas com o passar dos anos isso tende-a mudar.

Atualmente não se sabe a dimensão de dados gerados em função desse crescimento de uso. E com a alta utilização dos dispositivos IoT, vê-se uma preocupação em fatores ambientais, segundo a IDC (2019) - International Data Corporation até 2025 estima-se que haverá aproximadamente 41,6 bilhões de dispositivos IoT conectados, gerando 79,4 *zettabytes* de dados.

2.2.3 Vulnerabilidades e ameaças em IoT.

A Internet das coisas com a nova geração de dispositivos e serviços, trouxe acesso rápido à informação e hoje a sociedade moderna vive em uma era de tecnologia, onde milhões de dados são trafegados por segundos em dispositivos. Um usuário que utiliza alguns dispositivos IoT em sua residência e que tem o controle total desses dispositivos e esse cenário pode mudar em poucos segundos, pois a vulnerabilidade de um dispositivo conectado a Internet é muito grande, ataques cibernéticos são cada vez mais reais, pode-se ver através de pesquisa e da midia que esse número cresceu.

Dados emitidos pela USP (2020) revelam que em meio à pandemia do Covid-19, em período de isolamento social, apenas no Brasil o aumento de ataques cibernéticos foi de 131% em relação a março de 2019. Ataques como *Ransomware, Malware, Botnets e DDoS Distributed Denial-of-service* foram os que mais cresceram nesse período.

A Amazon em 2020 foi acionada e comunicada porque um dos seus dispositivos IoT, a assistente virtual chamada Alexa, teve uma ameaça de segurança que permitia o atacante ter acesso a informação dos usuários da mesma e, de acordo com Checkpoint Research (2020), nesse tipo de ataque o *hacker* requer a criação de um *link* malicioso, onde o mesmo é enviado para um usuário desativado, que ao clicar nesse *link* teria uma lista de funções e ferramentas instaladas na Alexa. Através dessa vulnerabilidade o criminoso digital consegue mudar a habilidade da assistente, e instalar outro aplicativo

mal intencionado, e com o comando de voz solicitado pela próxima voz a assistente acessava o aplicativo que foi instalado e modificado pelo invasor.

Com base nessa vulnerabilidade era possível acessar o histórico de conversas dos usuários na aplicação, visualizar saldo em contas bancárias entre outras informações que poderiam ser exploradas. De acordo com dados da Ponemon Institute Study (2020), 80% das aplicações utizadas para controlar os dispositivos IoT não são testadas devidamente, sendo que 70% delas estão vulneráveis a ataques.

As organizações não estão preparadas para a próxima evolução da Internet das coisas, pois o atual cenário é muito preocupante, visto que *hardwares* como sensores e baterias são muito pequenos e não oferecem uma autonomia e melhor *performance* em relação a outros padrões. Em TI entende-se por vulnerabilidade tudo aquilo que é sensível a determinadas ameaças. São brechas que acabam permitindo um ataque ou que se associam a determinados riscos. Podendo dizer que a vulnerabilidade favorece a ameaça em si.

De acordo com a norma ISO/IEC 27000 (2018) uma vulnerabilidade é uma fraqueza de um ativo que poderia ser potencialmente explorada por uma ou mais ameaças. Ela também define uma ameaça como qualquer causa potencial de um incidente não desejado que possa resultar em dano ao sistema ou organização.

A OWASP (2018) - Open Web Application Security Project, divulgou algumas das principais vulnerabilidades, através de um infográfico, com alguns comentários:

- *Passwords* fracas, previsíveis ou codificadas, ou seja, o uso de credenciais fáceis, disponíveis ou imutáveis, que inclui *backdoors* em *firmware* ou *software* cliente que concede acesso não autorizado aos sistemas que são implantados.
- Serviços de redes inseguros, aqueles serviços desnecessários que são executados no próprio dispositivo e que são expostos à Internet, que comprometem a confidencialidade, integridade, autenticidade e/ou disponibilidade de informação, podem permitir o controle não autorizado.
- Interfaces inseguras - APIs inseguras, APIs de *back-end*, nuvem

ou *interfaces* móveis no ecossistema (fora do dispositivo) permitem o comprometimento do dispositivo ou de seus componentes relacionados a problemas comuns como falta de criptografia e falta da filtragem de entrada e saída.

- Falta de mecanismos e atualização, ou seja, falta de atualização do dispositivo de segurança o que inclui a validação de *firmware* no dispositivo, falta de não criptografia em trânsito, falta de mecanismos anti reversão e a falta de notificações de alterações de segurança devido às atualizações.(Um problema muito sério para os aplicativos IoT é que na maioria das vezes as empresas não se preocupam em pensar no futuro de seus dispositivos e implementações). Sendo este fato para a OWASP considerado nem sempre é um problema tecnológico, mas podem ser:

  1. O uso de componentes desatualizados e inseguros ou seja, uso de componentes obsoletos ou inseguros que podem comprometer o dispositivo ou ainda pode-se incluir neste contexto o uso de *software* ou componentes de *hardware* de terceiros já comprometidos.
  2. Proteção de privacidade insuficiente para informações pessoais de usuários armazenadas nos dispositivos que podem ser usadas de maneira imprópria ou sem permissões.
  3. Transferência de dados ou armazenamentos inseguros, falta de criptografia ou controle de acessos a dados confidenciais em qualquer parte do fluxo da informação ou processamento.
  4. Falta de gerenciamento de dispositivos ou seja, falta de suporte de segurança em dispositivos implantados na produção que inclui o gerenciamento de ativos, gerenciamento das atualizações, monitoramento do sistema ou recursos de respostas.
  5. Configurações padrão inseguras em dispositivos ou sistemas que não mantêm configurações padrão ou a falta de tornar o sistema seguro que restringem os operadores de modificar as suas configurações.

6. Falta de força fisica registro de monitoramentos insulficientes, que permite que atacantes obtenham informações confidenciais que podem ajudar em um futuro ataque remoto ou dar o total controle local do dispositivo.

Até a presente data a OWASP não fizeram novas atualizações que haviam sido prometidas para dali a 2 anos em relação a, mudanças no setor e expansão para outros aspectos da IoT, como segurança embarcada e Sistemas de Controle Industrial e Controle de Supervisão e Sistemas de Aquisição de Dados (ICS / SCADA).

Há planos também para outros projetos da OWASP, um deles como o ASVS - Application Security Verification Standard, sendo que esse projeto fornece uma base para testar controles técnicos de segurança de aplicativos *web* e que fornece aos desenvolvedores uma lista de requisitos para um desenvolvimento seguro. O principal objetivo desse projeto é normalizar o alcance da cobertura e do nível de rigor disponível quando se trata das verificações de segurança de aplicativos da *web*.

2.2.4 Vulnerabilidades de dispositivos inteligentes infantis.

Partindo do princípio de que os dispositivos infantis que utilizam tecnologias inteligentes deveriam ser os mais seguros, surpreendentemente isso não ocorre. Em fevereiro de 2019, um relógio inteligente para crianças fabricado na Alemanha foi encontrado com vulnerabilidades significativas.

O dispositivo poderia potencialmente ter sido comprometido para permitir que *hackers* rastreassem os movimentos da criança em tempo real, ou falsificassem os dados de localização do GPS para enganar os pais. Esse é apenas um exemplo do que pode acontecer, segundo uma pesquisa realizada pelo Avast (2018), onde indica-se que apenas 20% dos usuários têm compreensão confortável da tecnologia inteligente e mais de 50% não estão preocupados com a questão de privacidade. Pode-se dizer que qualquer objeto que possa ter um processador, ou que esteja conectado à Internet pode ser hackeado remotamente.

2.2.5 Ameaças de segurança para IoT nas organizações.

As empresas precisam estar cientes das diferentes ameaças de segurança de IoT e se protegerem, desenvolvendo estratégias de segurança cibernética para tal. A evolução da IoT em diversos setores tais como: agricultura, manufatura, serviços públicos e varejo, ajudaram a melhorar a eficiência e produtividade. Algumas das ameaças que podem ocorrer com a segurança da IoT instalados nesses setores são, por exemplo DDoS, *ransomware* e engenharia social, as quais podem ser utilizadas para roubar informações e dados de pessoas ou empresas. Esses tipos de ameaças são muito preocupantes, pois seus usuários frequentemente as, desconhecem, não tendo como diminuir esses riscos. Alguns tipos de ameaças, segundo Joshi (2019), podem incluir

1. *Botnets* é uma rede que combina vários sistemas que controlam remotamente o sistema da sua vítima e distribui malware. Os *botnets* podem ser controlados através de servidores *Command-and-Control* que roubam dados confidenciais e podem também adquirir dados bancários *on-line* e executar ataques cibernéticos como DDoS e *phishing*.
2. Um ataque DoS causa uma sobrecarga no sistema de destino, enviando várias solicitações. Ao contrário do ataque de *phishing* os invasores que utilizam ataques de negação de serviços não pretendem roubar dados críticos. No entanto, os DoS podem ser utilizados para desacelerar ou desabilitar um serviço para prejudicar a reputação da empresa.
3. O ataque utilizando o MiTM (Man in the-middle), onde o *hacker* rompe o canal de comunicação entre os dois sistemas individuais em uma tentativa de interceptar mensagens entre eles. Os atacantes ganham controle sobre a comunicação e enviam mensagens ilegítimas para os sistemas participantes. Podem ser utilizados para invadir dispositivos IoT, pois compartilham dados em tempo real.
4. Identidade e roubo de dados onde as informações pessoais, confidenciais e sensíveis, dados de cartão de crédito, endereços e e-mails, podem ser roubados. Os *hackers* podem também

atacar dispositivos IoT para obter dados adicionais sobre usuários e organização.

5. A engenharia social é a habilidade de conseguir acesso a informações confidenciais através de habilidades de persuasão, os cibercriminosos podem usar a engenharia social para acessar sistemas, para instalar *softwares* maliciosos secretamente. Geralmente esses ataques são executados usando *e-mails* de *phishing*, em que o invasor cria e envia um *e-mail* convincente para manipular as pessoas.
6. A Ameaça Persistente Avançada é um ataque cibernético direcionado, em que o intruso obtém acesso ilegal a uma rede e permanece nela por muito tempo sem ser descoberto, os atacantes visam monitorar a atividade da rede e roubar dados cruciais.
7. *Ransomware*, nesse ataque o *hacker* usa *malware* para criptografar dados que podem ser necessários para operações comerciais. O invasor irá descriptografar dados críticos somente depois de receber um resgate. O ransomware pode ser uma das mais sofisticadas ameaças à segurança IoT.
8. Gravação Remota o WikiLeaks em 2017 mostrou que as agências de inteligência sabem sobre a existência de explorações de dia zero. Essa exploração é um ataque que ocorre no mesmo dia em que um ponto fraco do *software* é descoberto ou seja ele é explorado antes que o fornecedor possa disponibilizar a sua correção,em dispositivos IoT, *smartphones* e *laptops*, e também podem ser usadas por criminosos ciberneticos para gravar conversas de usuários de IoT. Essa divulgação implicam que as agências de segurança estavam planejando gravar secretamente conversas públicas.

   As empresas devem implantar tecnologias modernas, como por exemplo *big data, blockchain* e inteligência artificial, para aprimorar seus esforços de segurança cibernética.

2.3 Protocolos de comunicação e segurança em IoT.

Os protocolos são responsáveis pelo transporte e pela segurança dos dados que trafegam na rede, desde a interface do dispositivo até a nuvem, eles são essenciais para proteger os dados de um ataque, principalmente quando integra-se dispositivos à nuvem, só os protocolos de segurança não são essenciais para tornar-se uma rede segura.

2.3.1 O protocolo MQTT.

Esse protocolo é utilizado para comunicar máquina a máquina, é um protocolo que possui uma boa transmissão de dados e é dinâmico a conexões de banda, e consegue desempenhar um bom trabalho em relação à escalabilidade e latência da rede em comparação a protocolos existentes, mesmo em dispositivos que possui uma limitação de hardware ele é capaz desempenhar um bom trabalho, além de possuir suporte a diversas linguagens de programação.

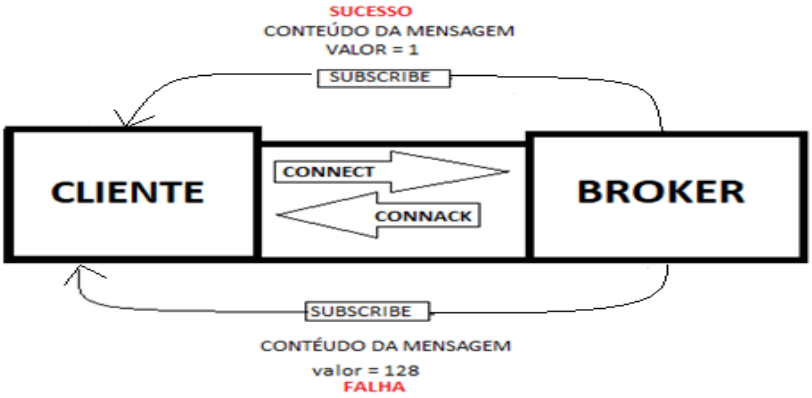
Esse protocolo foi criado pela *IBM* em 1990. O MQTT - Message Queue Telemetry Transport é um protocolo assíncrono, onde os dispositivos podem enviar requisições e a rede irá descobrir de que modo ela irá entregar a requisição. O MQTT pode ser usado com conexão TCP/IP utilizando-se criptografia TLS -Transport Layer Security ou SSL - Secure Sockets Layer.

O protocolo MQTT funciona com o modelo de publicação e assinatura. Nesse método o servidor é o *broker* demonstrado na Figura 2, ele recebe o "tópico" de mensagem das aplicações cliente, sejam elas sensores ou outros dispositivos interligados no nó da rede, e utilizando os métodos de sincronização o *broker* encaminha as mensagens recebidas a todos as aplicações que assinam o "tópico".

Um cliente pode assinar um ou mais tópicos. Ao utilizar o método de QoS - Quality of Service é possível definir a garantia da mensagem entrega ao tópico, essa classificação é definida como mostrará a seguir a figura 2 se o *broker* retorna com o conteúdo da mensagem sendo igual ao valor 0, significa que a conexão não é confiável, e que a mensagem será entregue no máximo uma única vez, caso o cliente esteja *offline*, a mensagem será perdida. Caso o

conteúdo da mensagem seja retornado como 1, significa que a mensagem será entregue pelo menos uma vez. Caso o conteúdo da mensagem seja 2, significa que a mensagem deve ser entregue exatamente uma vez. Caso o conteúdo da mensagem seja 128, significa que ocorreu uma falha.

Figura 2 Método de conexão.



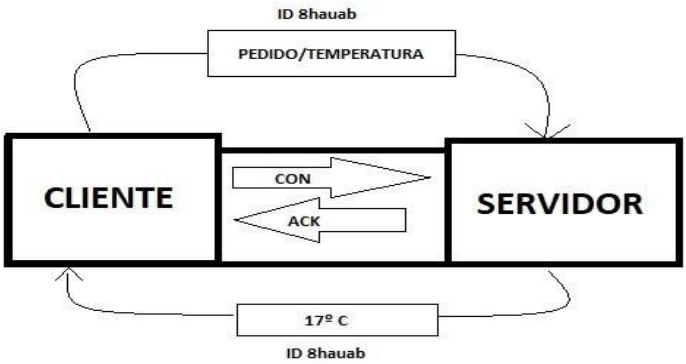
Fonte: Os autores

2.3.2 O protocolo CoAP.

Esse Protocolo foi projetado por IETF, para qual não é necessário muito recurso computacional e funciona em redes com alta latência, é um protocolo não confiável, e para tornar-se seguro deve-se utilizar o método de segurança DTLS - Datagram Transport Layer Security para criptografia com chaves de 128 *bits*, com conexões UDP. A troca de mensagens é feita de forma assíncrona, entre os nós.

O CoAP, é um protocolo de transferência *web* e foi desenvolvido para conectar sensores e atuadores que possua uma baixa limitação computacional, esse protocolo é utilizado nas conexões M2M, onde para cada mensagem enviada é utilizado um ID para identificação, sendo assim não acontecerá duplicidade de eventos, o ID é utilizado como confiabilidade dos dados. A figura a seguir figura 3 traz uma representação de uma conexão utilizando o protocolo CoAP.

Figura 3 Método de conexão CoAP.



Fonte: Os Autores.

Na figura 3 pode-se observar que a aplicação cliente realizou uma requisição com o servidor por meio de um comando chamado CON e o servidor recebe uma resposta com o comando ACK, obtendo assim sucesso, e o cliente solicita a informação Temperatura e o servidor responde com o valor atribuído 17ºC.

Caso o servidor não consiga responder imediatamente, ele retorna com uma mensagem vazia de confirmação, e dessa forma o cliente não irá mais realizar solicitação. O protocolo TCP/IP, surgiu em 1971 e foi formalizado em 1983, com o modelo OSI - Open Systems Interconnection, onde foi estabelecido 4 camadas para a arquitetura TCP/IP. As camadas são: 1. física enlace, 2. rede, 3.transporte e 4. aplicação.

A quarta camada de aplicação é responsável por enviar e receber os dados das outras aplicações e *softwares* que se comunicam como o DNS, que é um serviço de gestão de nomes, utilizado para atribuir um nome ao endereço de IP. O HTTP - Hypertext Transfer Protocol é utilizado em páginas da *web* como o HTML. O SMTP é utilizado como protocolo no envio de *e-mail*, TELNET.

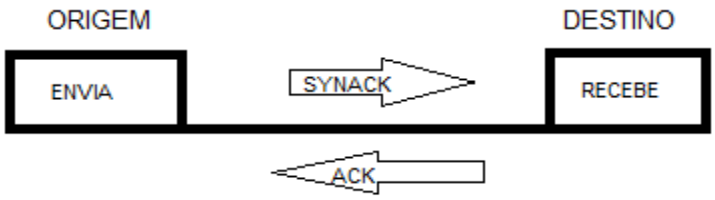
A terceira camada de transporte é responsável por receber os dados, e dividir em diversos pacotes de menor tamanho, utilizando o IP, nessa camada os pacotes são enviados sem uma sequência, e será organizado no seu destino.

Na segunda camada de rede, é adicionado um endereço de IP no

cabeçalho no pacote para o *host* de destino.

A primeira camada de enlace valida o tipo de rede física, *Ethernet, Wi-Fi, WAN* entre outros, responsável por direcionar o endereço de rede lógico para o endereço físico que todo dispositivo possui, o *Mac Adress, que é um* endereço de identificação único implantado pelas fabricantes.

Figura 4 Método de conexão TCP/IP.



Fonte: Os autores.

2.3.3 O protocolo LPWANS.

Utilizado em grandes campos de aplicação, os LPWANs - Low Power Wide Area Networks enviam pequenas quantidades de dados com uma baixa taxa de transmissão de dados, e pode ser operado com o uso de baterias, esse tipo de tecnologia é aplicável a áreas onde não necessariamente precise de dados em tempo real.

O dispositivo não precisa ficar conectado o todo tempo, podendo ter um grande gerenciamento energético. O LPWANS é muito utilizado em cidades inteligentes pois é mais barato para implementar do que a tecnologia *Wi-Fi* e através da utilização de um *gateway* é possível receber mensagens desses sensores que podem estar a uma distância de aproximadamente 45 Km/h. Através do acrônimo 6LowPAN é possível implementar *IPv6* nas redes.

2.3.4 O protocolo Hart.

O protocolo HART - Highway Addressable Remote Transducer é um dos protocolos mais utilizados em IIoT (Internet das coisas industriais), surgiu no ano de 1989, ele tem vantagens sobre outros protocolos, porque possui uma alta compatibilidade com sinal analógico, possui o padrão de sinal 4-20mA para automação industrial e atende o requisito para o gerenciamento de informações para plataformas digitais. A taxa de transmissão é de 250Kbps, caso não tenha comunicação, os dispositivos entram em modo de hibernação, podendo realizar um bom gerenciamento de energia.

2.3.5 O protocolo ZigBee.

É um protocolo que oferece um curto alcance de transmissão chegando a menos do que 100 metros, porém utiliza-se pouco consumo energético. Ele pode oferecer uma taxa de transmissão alta, é um protocolo que pode ser utilizado para automatização residencial por conta da sua alcançabilidade.

2.3.6 O protocolo SigFox.

É um protocolo de comunicação que utiliza a transferência de dados sem a necessidade de conexão de rede, a transmissão é feita por meio de RFID, os dispositivos IoT que utilizam esse tipo de comunicação não realizam o processamento de dados no próprio dispositivo, os dados são enviados para uma central via rádio frequência e lá os dados são processados. A taxa de transmissão é de 100 a 600 bit/s. Pode-se utilizar em lugares que abrangem um grande espaço, como em áreas agrícolas.

2.3.7 O protocolo XMPP.

Esse protocolo surgiu em 1999 pela comunidade de código aberto Jabber, ele é baseado no padrão XML. Por ser um protocolo de código aberto é possível implementar e desenvolver aplicações e incorporar serviços ao utilizá-lo.

2.3.8 O protocolo ARP.

ARP é um protocolo de camada-2, camada de datalink, usado para determinar o endereço de camada 2 do *host*, dado o endereço de camada de rede camada 3. O ARP foi criado para funcionar com qualquer formato de endereço de camada 2 e camada 3 e seu uso mais comum é mapear os endereços de IP para endereços de *hardware* Ethernet.

O ARP opera na rede local e não pode ser roteado. Mesmo que o protocolo ARP faça uso de endereços IP, ele não é um protocolo baseado em IP e a sua varredura de ARP pode ser usada em uma *interface* que não está configurada para IP. O ARP é usado somente pelos *hosts* IPv4.

2.3.9 O protocolo IRC.

Internet Relay Chat ou IRC como é mais conhecido, é um tipo de *chat* bem antigo e seu projeto foi lançado em 1988 por Jarrko Oikarinen em um sistema de chat mundial utilizado para teleconfêrencias em modo texto que requeria uma conexão à Internet e um cliente de IRC, enviando e recebendo mensagens através do servidor de IRC, o IRC usa TCP que é um protocolo aberto. O servidor de IRC transmite mensagens para todos os usuários conectados a um dos muitos canais de IRC e cada usuário deve possuir seu próprio ID.

O cliente é implementado em *sockets* e normalmente utiliza as portas 6666, 6667 ou 6668 para comunicar-se com o servidor. Esta comunicação ocorre sobre TCP/IP, utilizando o protocolo TCP na camada de rede. O protocolo IRC é baseado em troca de mensagens constituídas de até 512 octetos. Para mensagens que são assíncronas não existe uma garantia de resposta.

O protocolo entre servidores é o mesmo entre clientes e servidores, porém existem restrições para o segundo tipo de conexão onde algumas mensagens de clientes não são aceitas. As mensagens utilizadas pelo IRC são constituídas de três partes prefixo que é utilizada em algumas situações para indicar o servidor ou cliente de origem.

Comando é uma string ou conjuntos de números que indica uma resposta númerica,parâmetros de comando até 15 argumentos que podem ser enviados através de mensagens.

2.3.10 O protocolo UDP.

UDP - User Datragam Protocol Protocolo de camada 4 de transporte cujo objetico é permitir comunicação entre aplicações e suas características não são confiáveis: o datagrama UDP é enviado ao destinatário, porém não existe garantia, nem confirmação de entrega.

Não é orientado a conexão: não é necessário o estabelecimento de conexão antes de enviar um datagrama UDP. Esse processo fica associado a uma porta UDP de forma indireta para identificação do processo associado ao serviço. Por se tratar de um protocolo simples se for comparado ao TCP, somente alguns protocolos utilizam-se dele para transportes de dados sendo eles: o TFTP, SNMP, DHCP, DNS.

Algumas vulnerabilidades do protocolo UDP funcionam como as vulnerabilidades do TCP que utiliza portas para a comunicação. Um dos primeiros passos que um *hacker* pode explorar é fazer a verificação das portas que estão abertas para comunicação. Caso o administrador da rede queira impedir a invasão no sistema ele poderá fechar as portas, mas isso significa ficar sem comunicação, então esta não é a melhor solução.

2.4 A rede rede 3G conectando a IoT.

Criada em 1995 pela Qualcomm, sendo uma das primeiras redes móveis a ser utilizada popularmente em *smartphones*, a terceira geração de redes móveis ainda é utilizada, a taxa de transmissão é de aproximadamente de 10Mbps. Como sua latência é alta, em aplicações IoT o tempo de envio e resposta é considerado um pouco mais demorado, as conexões 3G para IoT servem para campos e setores onde a rapidez de envio e resposta dos dados não é uma prioridade.

2.4.1 A rede 4G conectando a IoT.

A *Orthogonal Frequency Division Multiplexing*, que é o tipo de frequeência utilizada na quarta geração de redes móveis, foi desenvolvida por R.W. Chang do Bell Labs em 1966, porém o 3GPP implementou a sua versão em 2009, sendo a versão 8, e com o passar dos anos foi sendo atualizada. A taxa de

transmissão da rede 4G é de aproximadamente 100 Mbps.

2.4.2 A rede 5G conectando a IoT.

Através da quinta geração de redes móveis já é possível conectar mais dispositivos simultaneamente, essa rede possibilita até 100 conexões, e também é compatível com outros tipos de conexões. Com a rede 5G os dispositivos IoT terão longevidade nas conexões, além de possuir um gerenciamento energético de bom desempenho. Estudos apontam que com espectros eletromagnéticos espalhados, a rede 5G pode alcançar uma taxa de transmissão de até 20Gbps.

2.4.3 A tecnologia RFID.

A tecnologia de rádio frequência - RFID, utiliza duas antenas, uma antena realiza a transmissão de informações, e as outra antena recebe as informações enviadas por meio da radiação.

As antenas receptoras possuem uma bateria empregada, e uma memória para que seja possível gravar informações. A tecnologia RFID é muito usada em etiquetas eletrônicas. Existem baterias de vários tipos de duração, etiquetas eletrônicas são automatizáveis sem a necessidade de trabalho manual e com uma alta praticidade.

2.4.4 A tecnologia NFC.

A tecnologia empregado no NFC - Near Field Communication, diferente da tecnologia RFID, é utilizada para transmissão de dados mais próximos, podendo ter um alcance de até 10 cm de distância, essa tecnologia é utilizada muito em *tags* e cartões de crédito ou débito, as *tags* são etiquetas ou objetos que possuem a tecnlogia NFC.

Elas podem se conectar em *smartphones*, podendo ser programadas para executar alguma função no caso das *tags*, ou enviar informações no caso dos cartões de crédito e débito ao ser aproximado de sensores que possuem a mesma tecnologia.

2.4.5 A tecnologia Bluetooth Low Energy.

Essa é uma tecnologia já conhecida, porém em uma nova versão, o Bluetooth Smart ou Bluetooth 4.0. Essa nova versão permite que sensores utilizem a tecnologia com pouco consumo de energia. A tecnologia Bluetooth Low Energy é utilizado em HUBs onde é possível realizar o envio de dados para as nuvens.

2.4.6 A tecnologia Infravermelho.

É um tipo de comunicação muito utilizado em controles de televisores, portões, entre outros, ela possui uma taxa de transmissão de até 4 mbps, podendo atingir até 30 metros de distância. Existem dois tipos de comunicação através da luz infravermelho, sendo comunicação ponto a ponto e comunicação difusa.

A comunicação ponto a ponto permite que o dispositivo envie dados na mesma linha de visão e torna o dispositivo mais seguro, utilizando pouco consumo de energia. Na comunicação difusa os dispositivos receptores precisam estar próximos, mas não necessariamente na mesma linha de visão.

2.5 Pentest

O pentest conforme Softwall (2021) serve para visibilidade, exploração e correção, realizando documentações de erros e falhas que foram encontradas em um ambiente que está exposto a internet, ele é importante para definir o nível de maturidade de uma organização em relação a segurança, através de seus métodos utilizados para impedir ataques e roubo de informações.

2.5.1 Planejamento e Pré-acordo

Essa etapa consiste em realizar um acordo tanto a empresa quanto ao cliente do que será testado, como será testado, e o cliente precisa definir quais são os seus objetivos e espectativas que deverão de ser obtidos em relação ao teste.

2.5.2 Reconhecimento e Assessment

Esse método consiste em realizar a recolha de informações sobre o dispositivo a ser analisado. É possível realizar buscas através de ferramentas que utilizam técnicas de OSINT Open Source Intelligence, algumas ferramentas são SHODAN, Metagoofil, GHBD, Cyberstalking.
Conforme (Hackersec), os processos de OSINT são:

- Reconhecimento,
- Fontes de informação,
- Coleta de dados,
- Processamento de dados,
- Análise de dados
- Inteligência.

A recolha de informações em fontes gratuitas, sites, blog, canais de comunicação, fóruns.

O github é um repositório de fontes Opensource, e lá são disponibilizado alguns projetos de aplicações. [1]

API, conforme techtudo (2020), API Application Programming Interface, que significa em português interface de programação de aplicação, é um conjunto de normas com uma série de padrões e protocolos, que possibilita os desenvolvedores a realizar a comunicação entre aplicações.

O APKmirror [2]é uma loja de aplicativos alternativa a Playstore no Android e é possível realizar a busca de versões antigas de aplicativos, e também obter versões de aplicativos com antecipação de atualizações disponíveis, antes mesmo do que na Playstore essa é uma das lojas que são alternativas a Playstore e é considerada segura.

[1] disponível em https://github.com/ Acesso em 20 maio 2021.
[2] disponível em https://www.apkmirror.com/ Acesso em 20 maio 2021.

2.5.3 Testes de Intrusão.

Depois da etapa 2 definida é possível realizar a exploração de brechas e ameaças de forma mais acertiva ao alvo, também é possível realizar uma análise em item por item que foi classificado na etapa 2, podendo garantir acertividade e sucesso nos testes a serem realizados.

2.5.4 Análise de código de aplicação.

Nessa etaque é realizado uma análise do código fonte da aplicação, buscando encontrar vulnerabilidade ou brechas que possa tornar a aplicação ou dispositivo vulneravél a ataques cibernéticos.

2.5.5 Documentação

A etapa de documentação visa listar as brechas encontradas, possibilitando criar métodos que deverão ser aplicados para mitigar a organização de roubo de informações ou ataques cibernéticos.

3 Projeto prático

O Projeto prático realizado, possibilita a identificação de ameaças e vulnerabilidades, que podem ser encontradas em um dispositivo IoT. Existe aplicações *opensource*, o mesmo termo em português que significa código aberto que possíbilita profissionais de TI a realizar *pentest* penetration test, através do teste de penetração o profissional é capaz de realizar uma análise profunda, podendo definir as fraquezas e ameças existente nas aplicações, assim é possível realizar métodos de mitigar ataques cibernéticos e roubo de informações.

É possível também realizar uma análise nos componentes interno do dispositivo, podendo-se obter mais informações técnicas como número de série, versões de firmware entre outros.

Algumas ferramentas que foram utilizadas para a análise:

3.1 Ferramenta aircrack-ng/airodump.

É um conjunto de ferramentas completo para avaliar a segurança da rede sem fio, e filtrar as informações dos dispositivos da rede em que está sendo analisada, conforme aircrack-ng[3]. Análises serão realizadas sobre essa ferramenta no ambiente prático disponibilizado no capítulo 3.

3.1.2 Ferramenta Nmap.

É um *software opensource* de Port Scanning que utiliza pacotes IP para identificar todos os aparelhos conectados a uma rede conforme gitbook[4]. Sendo possível coletar informações sobre os serviços e os sistemas operacionais que estejam rodando.

Algumas informações que a ferramenta pode explorar são:

- Encontrar endereço os IPs dos dispositivos conectados.
- Escaneamento de portas abertas.
- Identificação de qual programa que está sendo executado, e em qual porta e versão que estão.

Manual da ferramenta está diponível no site.[5]

3.1.3 Ferramenta Arp-scan.

Arp-scan é uma ferramenta de linha de comando para a descoberta do sistema e impressões digitais. É enviado requisições ARP para os endereços IP especificos e ele exibe as respostas que são recebidas, conforme wordpress[6]

A varredura arp- permite:

---

[3] disponível em http://aircrack-ng.org/ Acesso em 20 maio de 2021.

[4] disponivel em: https://gitbook.ganeshicmc.com/redes/ferramentas/nmap. Acesso em 20 maio de 2021.

[5] disponível em: https://nmap.org/download.html Acesso em 20 maio 2021.

[6] disponível em: https://mxdebug.wordpress.com/2016/08/20/arp-scan/. Acesso em 20 maio de 2021.

- Enviar pacotes ARP para qualquer número de *hosts* de destino, utilizando uma taxa de largura de banda de saída ou pacote configurável.
- Isso é útil para a descoberta do sistema, e pode ser usada para fazer a varredura em espaços de endereços de grandes dimensões.
- Construir o pacote ARP de saída de forma flexível, Arp scan dá o controle de todos os campos do pacote ARP e os campos no cabeçalho do quadro Ethernet.
- Arp scan irá decodificar e exibir qualquer pacote que recebeu ARP e procurará o fornecedor usando o endereço MAC.

3.1.4 Ferramenta Netdiscover.

Netdiscover é uma ferramenta de varredura de rede para que possa relacionar todos os *hosts* que estão ativos, e através do *help* pode-se encontrar diversas opções que trazem resultados personalizados. Pode ser usado tanto no modo ativo quanto no passivo, conforme debian.org[7]. Já no modo inativo envia-se solicitações aos *hosts* para obter informações, mas de outra forma está funcionando no modo silencioso chamado modo passivo ou modo de escuta. O nediscover funciona apenas na rede interna, então é necesário saber qual a endereço *gateway* da rede.

3.1.5 Ferramenta Wireshark.

É um *software opensource* de análise de pacotes, a sua utilidade consiste em captar o tráfego de dados numa rede local, capturando pacotes de dados para serem analizados, conforme documentação do wireshark[8]. Seu manual está disponível no site da empresa[9].

Neste trabalho foi utilizado a Lâmpada LED Intelbras modelo EWS 410 conforme mostra na figura 5, que conta com integração em redes Wi-Fi de padrão IEE 802.11 b/g/n, tensão de entrada 110/220 Vac / 50-60 Hz.

---

[7] disponível em: https://manpages.debian.org/unstable/netdiscover/netdiscover.8.en.html. Acesso em 10 maio de 2021.

[8] disponível em : https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs. Acesso em 10 maio de 2021.

[9] disponível em : https://www.wireshark.org/download.html. Acesso em: 10 maio 2021.

No site do fabricante foi encontrado o manual do usuário – EWS 410, Manual do usuário IzySmart e a filha técnica – EWS410. [10]

Figura 5: Lâmpada Wi-Fi Intelbras.

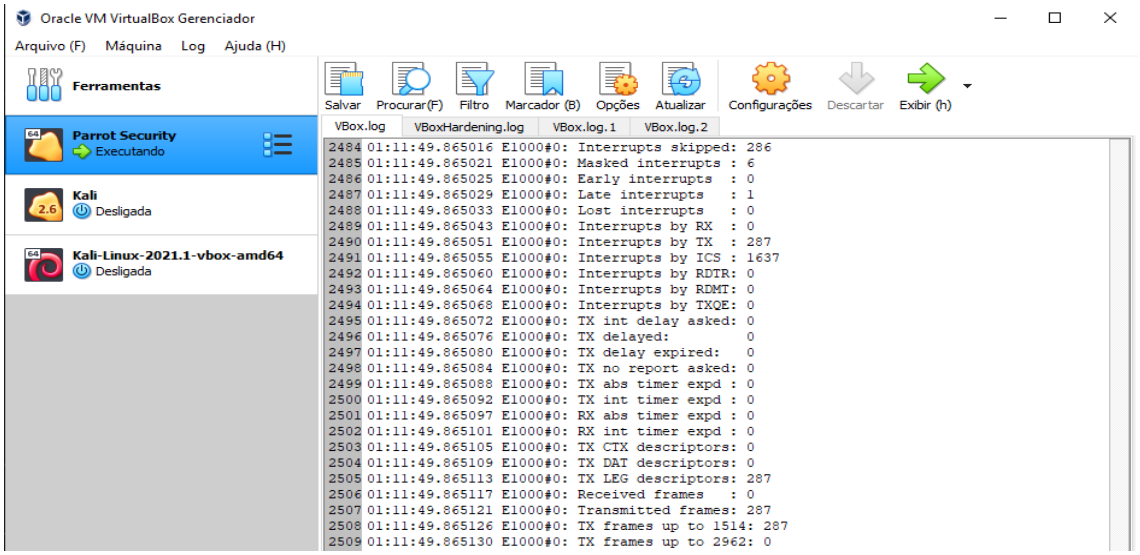
Fonte: Intelbras

Esse dispositivo IoT possuí integração com o aplicativo para smartphone Izysmart e compatível com Android e iOS (Apple), conforme mostra a figura 5.

[10] disponível em https://loja.intelbras.com.br/izy. Acesso em 29 abril 2021.

Foi importado a máquina virtual que está disponível para o ambiente do virtualbox no site da organização ParrotOS.[11], conforme mostra a figura 6.

Figura 6. Virtual Box executando Parrot OS.



Fonte: Os autores.

Foi conectado à Lâmpada LED Intelbras modelo EWS 410 no aplicativo Izysmart,conforme a figura7 , utilizando a plataforma IOS14.4.2.

[11] disponível em https://www.parrotsec.org/security-edition. Acesso em 20 maio 2021.

Figura 7. Aplicativo Izysmart.

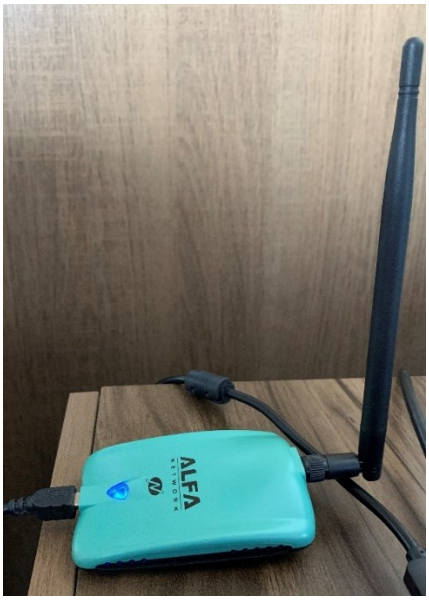
Fonte: Informações do dispositivo no aplicativo izysmart.

Na figura 7, é possível identificar o IP externo do dispositivo, *o mac address,* a região e o sinal.

3.2 Análise com o airodump.

Para ter uma análise melhor do tráfego da rede e analisar todas as redes que se encontradas foi utilizado com uma ferramenta para de teste de penetração um adaptador USB da marca Alfa modelo AWUS036NH padrão IEE 802.11 b/g/n, esse adaptador é bastante utilizado para realizar análises em rede e testes de penetração.

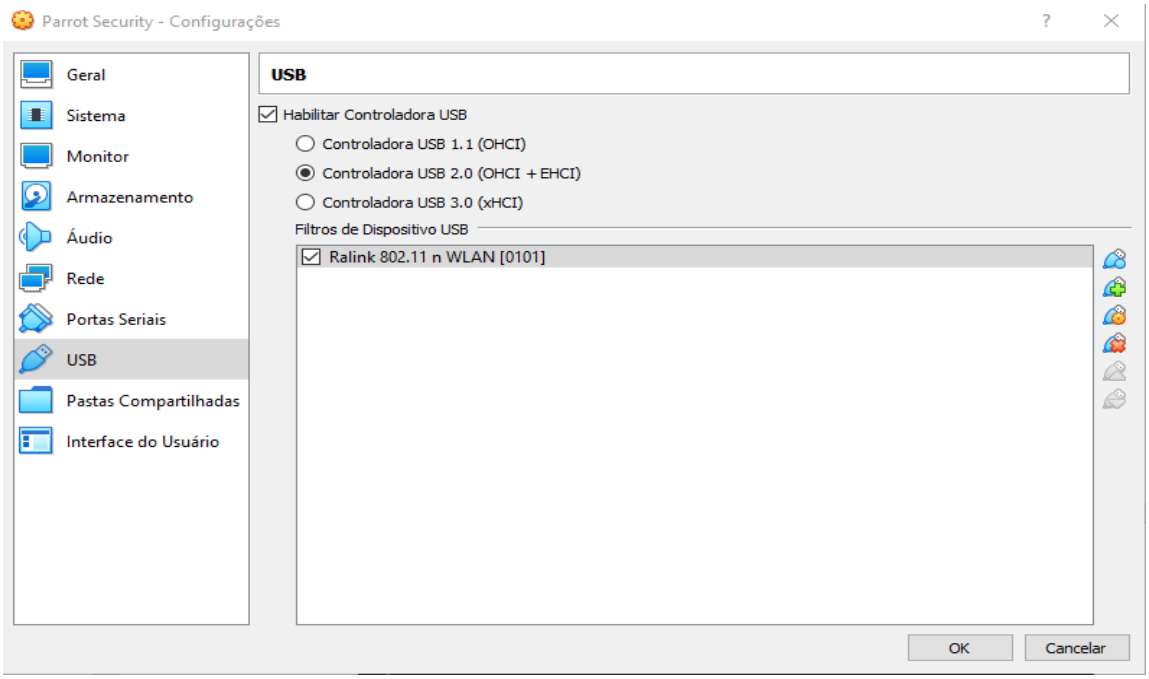
Figura 8. Adaptador USB alfa



Fonte: Os autores.

A seguir na figura 9 estão as configurações da máquina virtual, e foi adicionado o dispositivo utilizando a controladora USB 2.0.

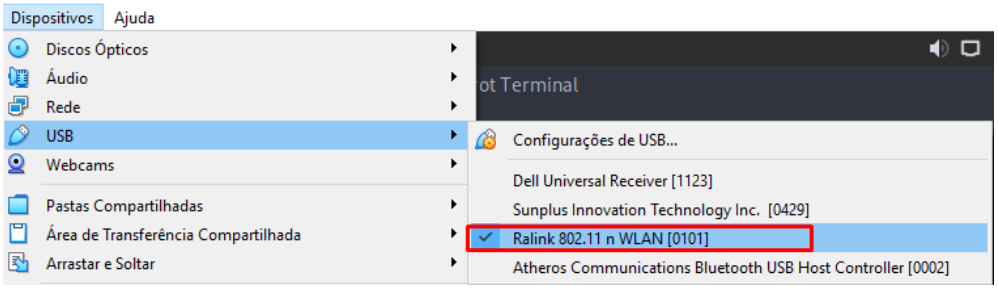
Figura 9. Habilitando controladora USB.



Fonte: Os autores.

Logo após iniciar a máquina, é necessário conferir se o adaptador foi conectado corretamente, e se o dispositivo está sendo reconhecido na máquina virtual, conforme a Figura 9.

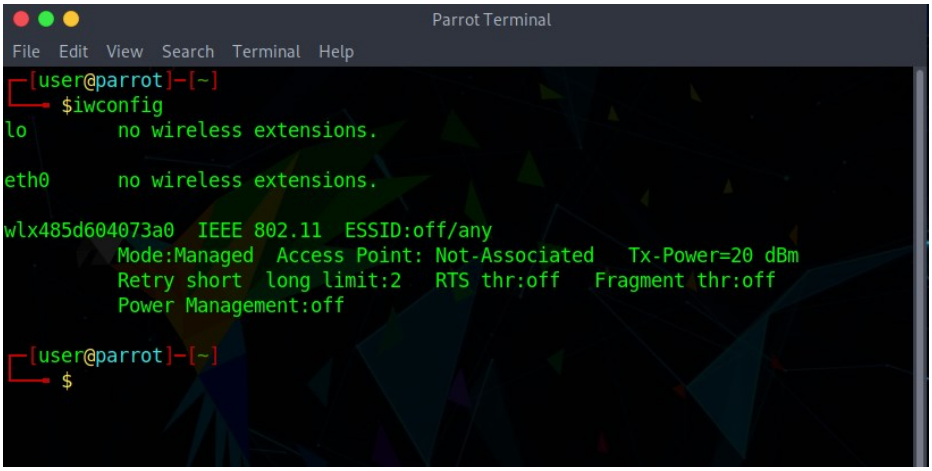
Figura 10. Dispositivo USB Ralink 802.11 n conectado.



Fonte: Os autores.

Depois de conectar o adaptador de rede, foi utilizado o comando: **iwconfig** para verificar se o adaptador foi reconhecido pelo sistema operacional, conforme mostra a figura 11.

Figura 11. resultado do comando iwconfig.



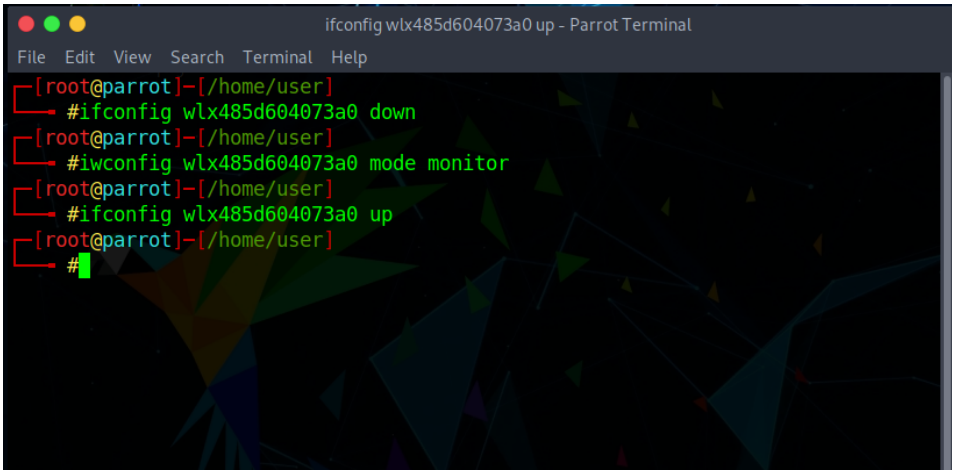
Fonte: Os autores.

Nota-se na figura 11, que o adaptador de rede foi identificado, porém ele está habilitado no modo managed, e é preciso habilitar o modo monitor.

- Primeiramente é necessário derrubar a *interface* de rede **wlx485d604073a0**.
- Com o comando: **ifconfig wlx485d604073a0 down**, pois por padrão o dispositivo fica conectado ao modo gerenciamento e o modo monitor não vem ativado automáticamente.
- Para habilitar o modo monitor utiliza o comando: **iwconfig wlx485d604073a0** mode monitor.

- Habilitar a interface de rede novamente utilizando o comando: **ifconfig wlx485d604073a0 up,** conforme observamos na figura 12.

Figura 12. Habilitando modo monitor.

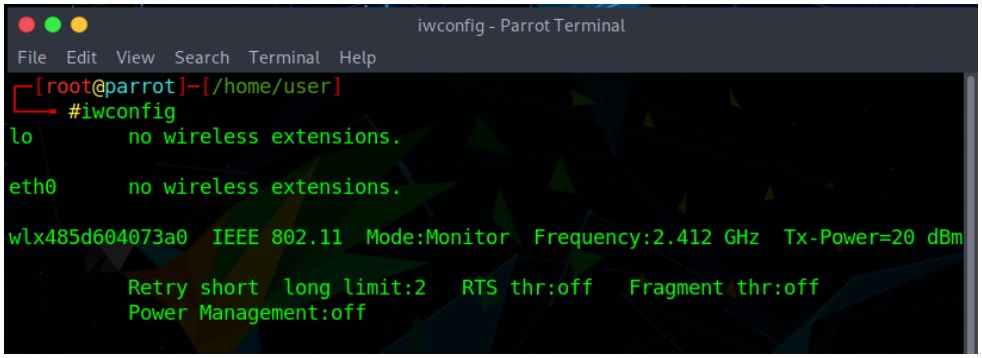


Fonte: Os autores

Na figura 12 mostra o resultado de todos os comandos realizados na etapa anterior.

Utilizando o comando **iwconfig** conforme mostrado na figura 13 é possível visualizar as interfaces de rede.

Figura 13. Modo monitor habilitado.

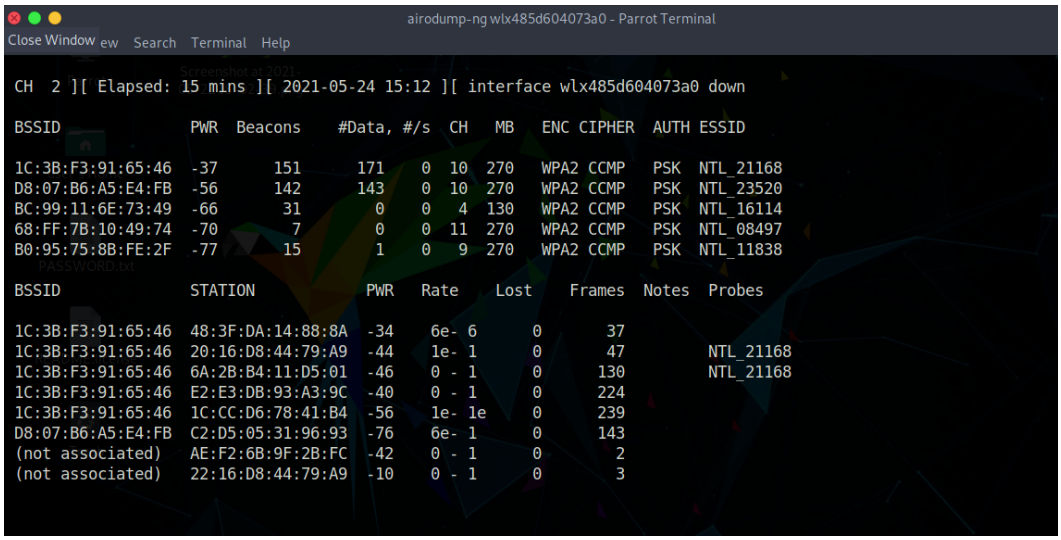


Fonte: Os autores.

É possível observar que o modo monitor já está habilitado conforme mostra a figura 13.

Na figura 14 é apresentado o resultado do comando: **airodump-ng wlx485d604073a0**. Esse comando é utilizado para filtrar todas as redes que estão ao alcance do adaptador Wi-Fi.

Figura 14. Resultado do comando airodump-ng wlx485d604073a0.



Fonte: Os autores.

Através do breve menu que é encontrado no site[12].da ferramenta. É possível verificar algumas opções que facilitam a identificação das informações.

- BSSID é o endereço MAC do AP (Access Point).
- PWR é a força do sinal. Alguns drivers não informam.
- Beacons é o número de beacon frames recebidos. Se você não tem a força do sinal, você pode estimar usando o número de beacons: quanto mais beacons, melhor a qualidade do sinal.
- Data é o número de frames de dados recebidos.
- CH é o canal no qual o AP está operando.
- MB é a Velocidade ou Modo do AP. 11 significa 802.11b e 54 significa 802.11g. Valores entre 11 e 54 são uma mistura.
- ENC é a Encriptação:
- OPN: sem criptografia
- WEP: criptografia WEP
- WPA: criptografia
- WPA ou WPA2
- WEP? WEP ou WPA a criptografia ainda não foi identicada.
- ESSID é o nome da rede, pode aparecer como não acossiado.

[12] disponível em https://www.aircrack-ng.org/doku.php?id=pt-br:airodump-ng.

Na parte inferior conforme mostra a figura 14 são os clientes encontrados:

- BSSID O endereço MAC do AP no qual esse cliente está associado.
- STATION O endereço MAC do cliente.
- PWR Força do sinal. Alguns *drivers* não informam.
- Probes Nomes das redes (ESSIDs) que este cliente sondou.

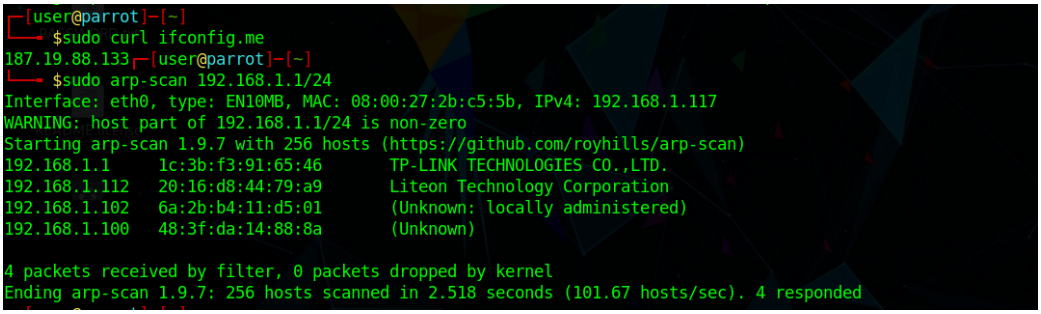
Observando o resultado da figura 14 é possível visualizar que:

- O *macaddress* 48:3F:DA:14:88:8A da lâmpada está associado ao O *macaddress* do roteador 1C:3B:F3:91:65:46.
- O tipo de criptografia utilizado na rede é WPA2 utilizando o método de autenticação PSK através de uma chave pré compartilhada.
- A rede que está acossiada ao *macaddress* 1C:3B:F3:91:65:46 utiliza o canal 10.

3.2.1 Análise com arp-scan

Com a ferramenta arp-scan citada anteriormente, utilizando o comando **arp-scan 192.168.1.1/24**, é possível verificar os dispositivos conectados na rede. Na figura 15 é apresentado o resultado do comando:

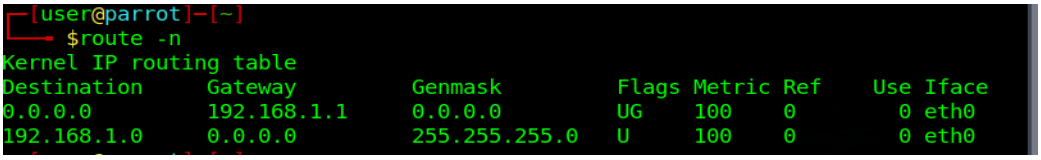
Figura 15. Resultado do comando arp-scan 192.168.1.1/24.



Fonte: Os autores.

Foi identificado 4 hosts na rede, TP-LINK Technology CO.,LTD, é o roteador com o endereço associado é 192.168.1.1.

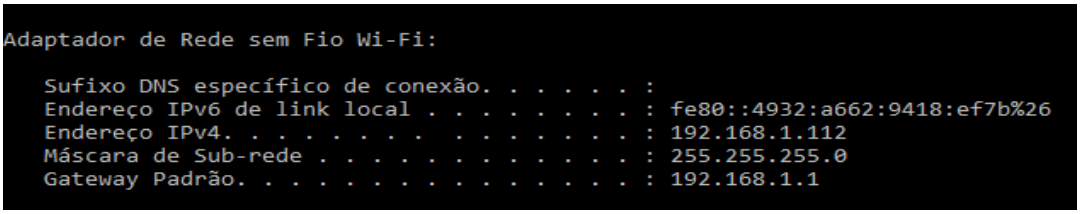
Figura 16. Resultado do comando route-n.



Fonte: Os autores.

O segundo endereço da rede é o da máquina hospedeira, que utiliza o Windows 10 como sistema operacional, conforme a figura 17.

Figura 17. Resultado do comando utilizado ipconfig no cmd da máquina hospedeira.



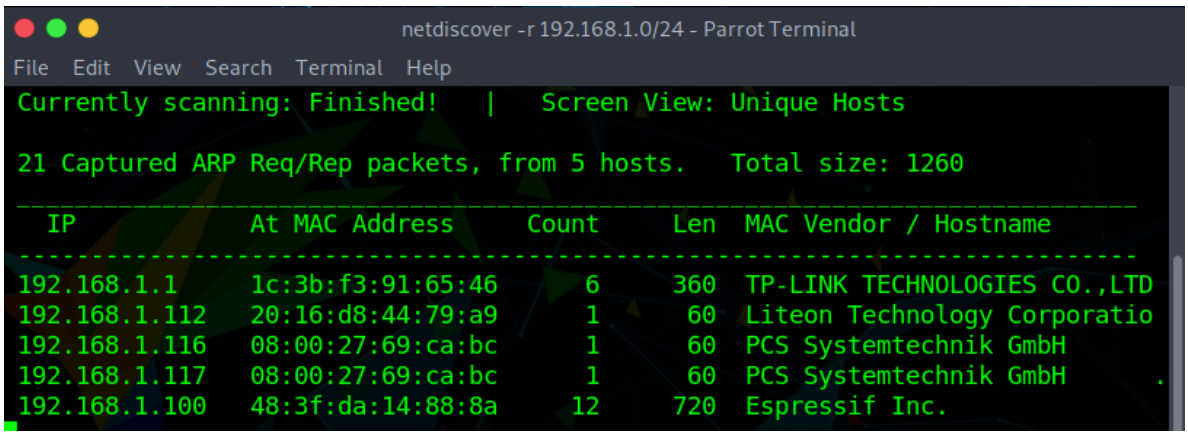
Fonte: Os autores.

O endereço 192.168.1.100 motrado na fugura 17 é o endereço da lâmpada LED Wi-Fi EW 410, que também aparece como desconhecido.

3.2.2 Análise com o netdiscover.

Utilizando a ferramenta netdiscover, é possível explorar mais informações, exibindo o resultado do comando: **netdiscover -r 192.168.1.0/24**, conforme mostrado na figura 18.

Figura 18. Resultado do comando netdiscover -r 192.168.1.0/24.



Fonte: Os autores.

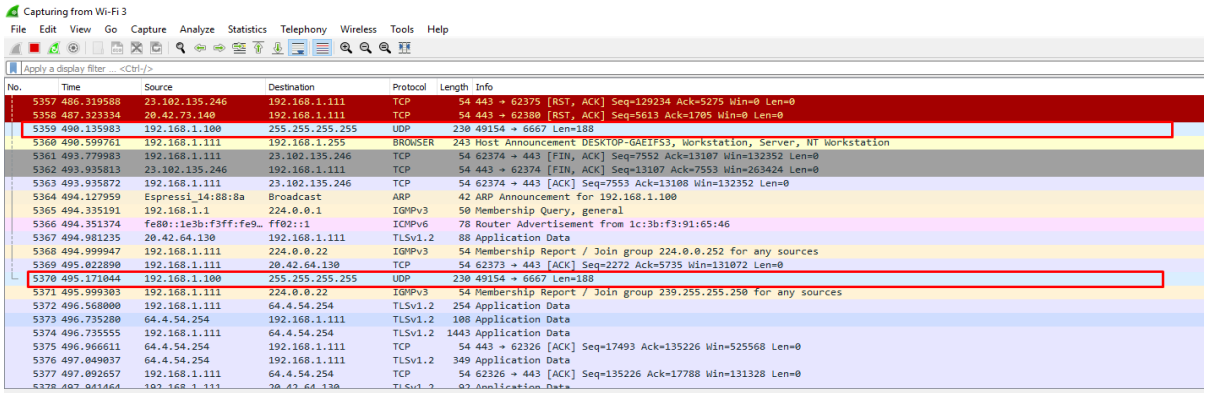
Na figura 18 é possível notar que o endereço 192.168.1.100 associado à

lâmpada LED Wi-Fi EW 410, aparece um nome definido como Espressif Inc.

3.2.3 Análise com o *wireshark.*

Com o wireshark foi selecionado a interface de rede Wi-Fi, essa ferramenta foi utilizada no sistema operacional windows 10.

Figura 19. Captura do protocolo UDP.



Os autores.

A seguir mostra o manual da ferramenta que está está disponível no site[13].

- No é o número da ordem que o pacote foi capturado. Nesse caso, a linha significa que tal pacote faz parte de uma conversa.
- Time é o tempo que o pacote foi capturado após você começar a capturar pacotes.
- Source é o enredeço que enviou o pacote.
- Destination é o IP de destino do pacote.
- Protocol é o tipo de pacote trafegando na rede, por exemplo, TCP, DNS, DHCPv6, or ARP.
- Length é o tamanho do pacote em bytes.
- Info é uma coluna que mostra informações adicionais sobre o conteúdo do pacote, o qual varia dependendo do tipo de pacote.

A figura 19 mostra que o dispositivo utiliza:

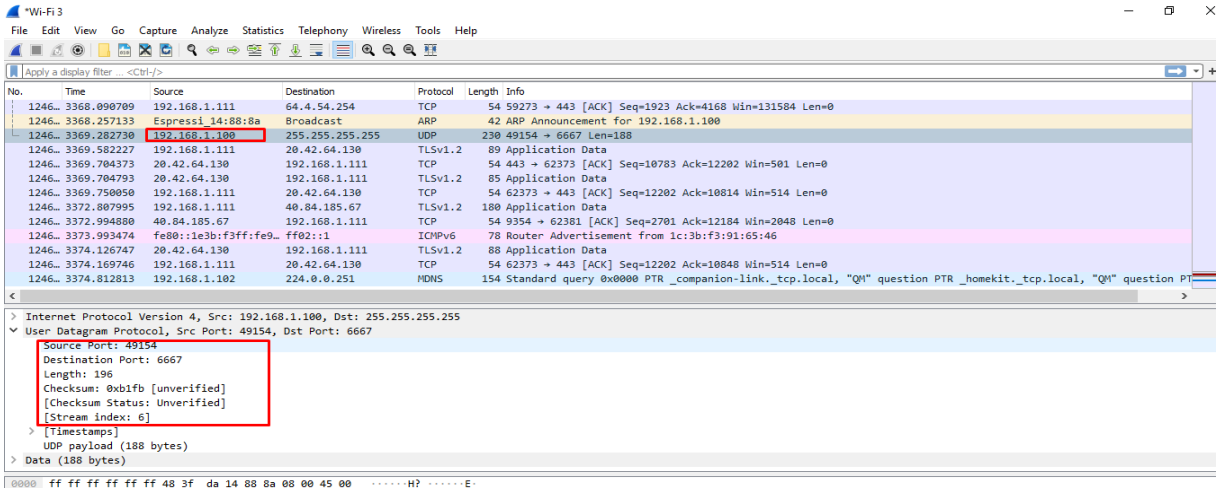
[13] disponível em : https://www.wireshark.org/download.html. Acesso em: 10 maio 2021.

- Camada de rede o protocolo ARP, propagando *broadcast* na rede, mesmo não estando em operação com o aplicativo *izysmart*.

- Camada de transporte utilizou o protocolo UDP, utilizar protocolo UDP é um problema, pois ele não apresenta nenhum dos pilares da segurança da informação que é a confiabilidade, integridade e disponibilidade da informação.

Na figura 20 é apresentado a captura de um pacote transmitido na rede pelo dispositivo.

Figura 20. Análise pacote UDP capturado.



Os Autores.

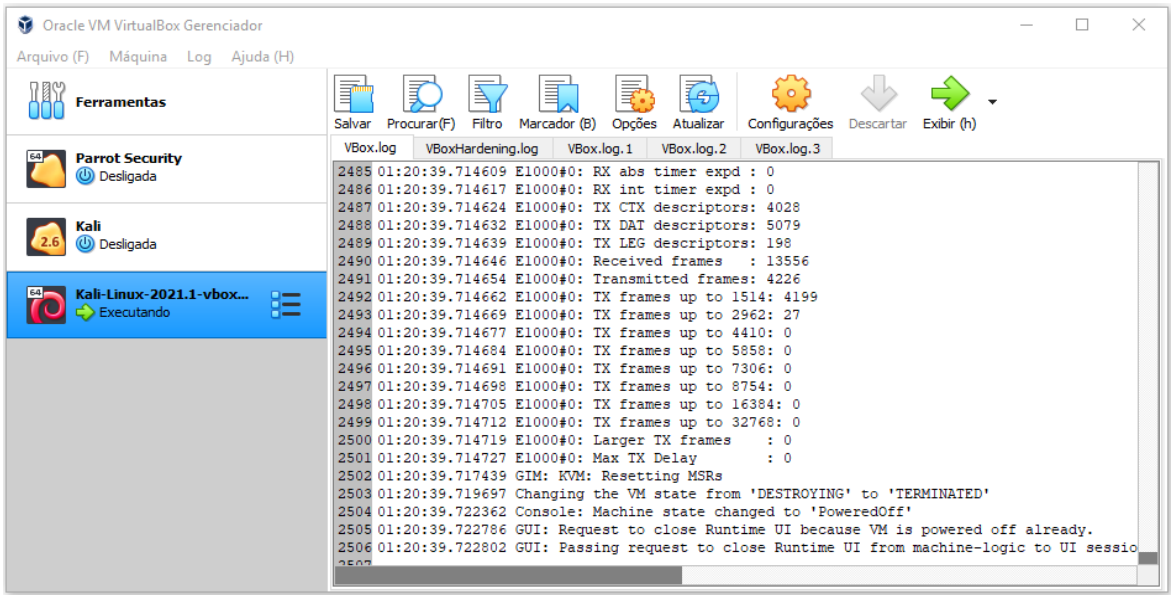
Na figura 20, é possível verificar a porta de origem e destino em que foi trafegado o pacote trafegou.

- Porta de origem 49154.
- Porta de destino 6667.

3.2.4 Análise da ferramenta nmap

Para a ferramenta nmap, foi utilizado utilizado uma máquina virtual com o sistema operacional Kali Linux, conforme a figura 21.

Figura 21. Máquina virtual Kali Linux.



Os Autores.

Foi iniciado a máquina virtual com o sistema operacional Kalilinux, conforme figura 21.

O nmap é uma ferramenta que por padrão já vem no sistema operacional mas caso não se encontre disponível é possível instalar utilizando o comando: **sudo apt install nmap**.

Figura 22. Instalação do Nmap.

Os autores.

Na figura 22 é possível verificar que a ferramenta nmap já estava instalada e os pacotes já estava atualizados.

Figura 23. Resultado do comando nmap -sT 192.168.1.0/24.

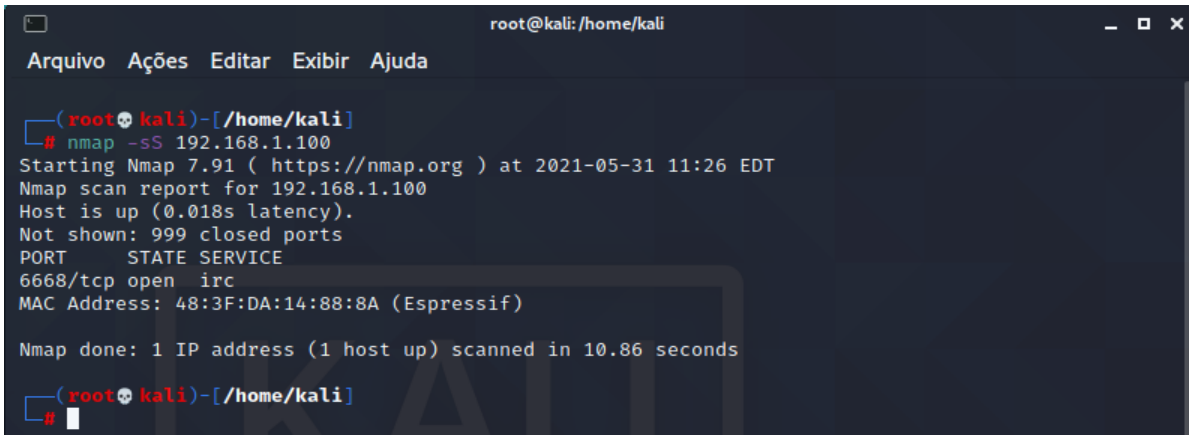
Os autores.

Utilizando o comando nmap -sT 192.168.1.0/24 a ferramenta descobriu portas abertas em dois equipamentos, mas a lâmpada não foi reconhecida nessa primeira análise, conforme a figura 23.

- **-sT TCP connect scan**

É uma técnica de TCP scanning, ele envia um sinal para todas as portas.

Figura 24. Resultado do comando nmap -sS 192.168.1.100.



Os autores.

- **-sS TCP SYN scan**

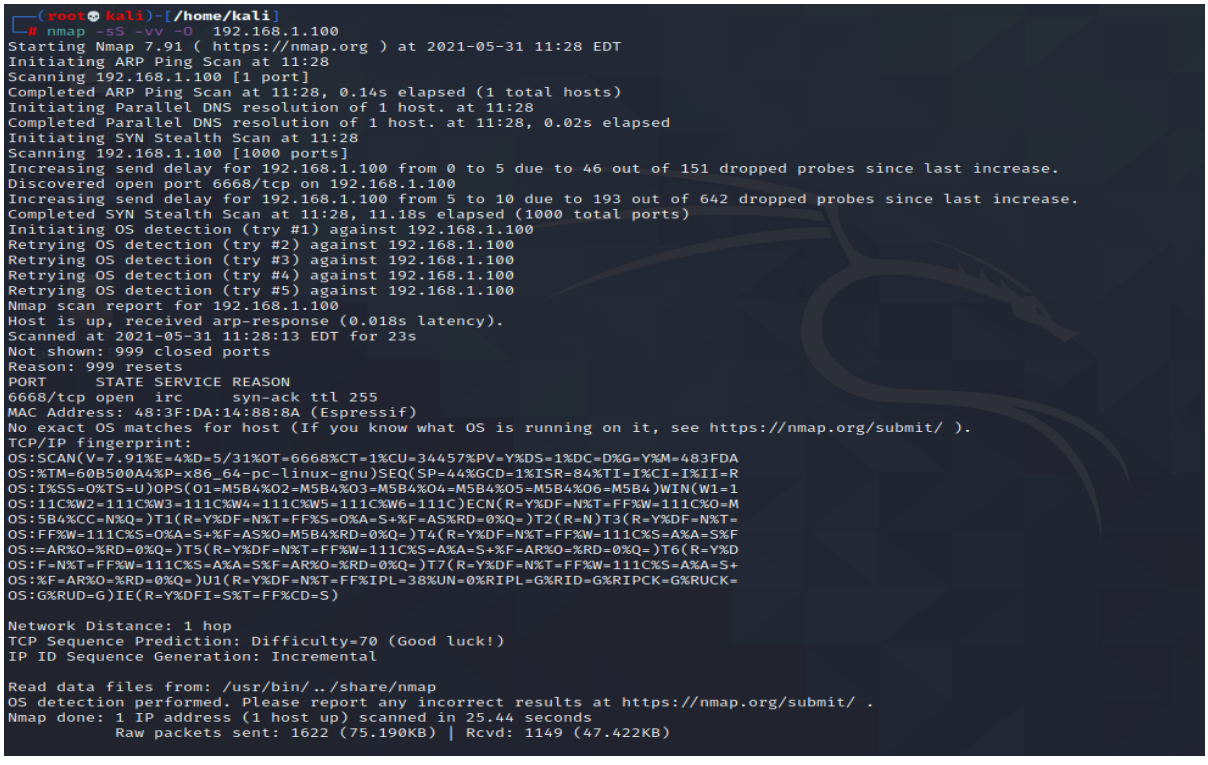
  É uma técnica é envia pacotes SYN em uma conexão TCP, caso o pacote SYN-ACK seja recebido porta está aberta.

Em outras análises descobrimos o endereço IPv4 da lâmpada, foi realizado uma análise diretamente no endereço do dispositivo, o resultado foi conforme a figura 24.

A porta 6668 TCP/IP está aberta, e o serviço mostrado para essa porta é o protocolo IRC. Conforme o a documentação disponível no site[14]

A figura 25 apresenta o resultado do comando **nmap -sS -vv -O 192.168.1.100**

Figura 25. resultado do comando nmap -sS -vv -O 192.168.1.100.



Os autores.

- -vV mostra o modo verbose durante a análise, motrando o nível de

[14] disponível em https://datatracker.ietf.org/doc/html/rfc1459. Acesso em 29 maio de 2021.

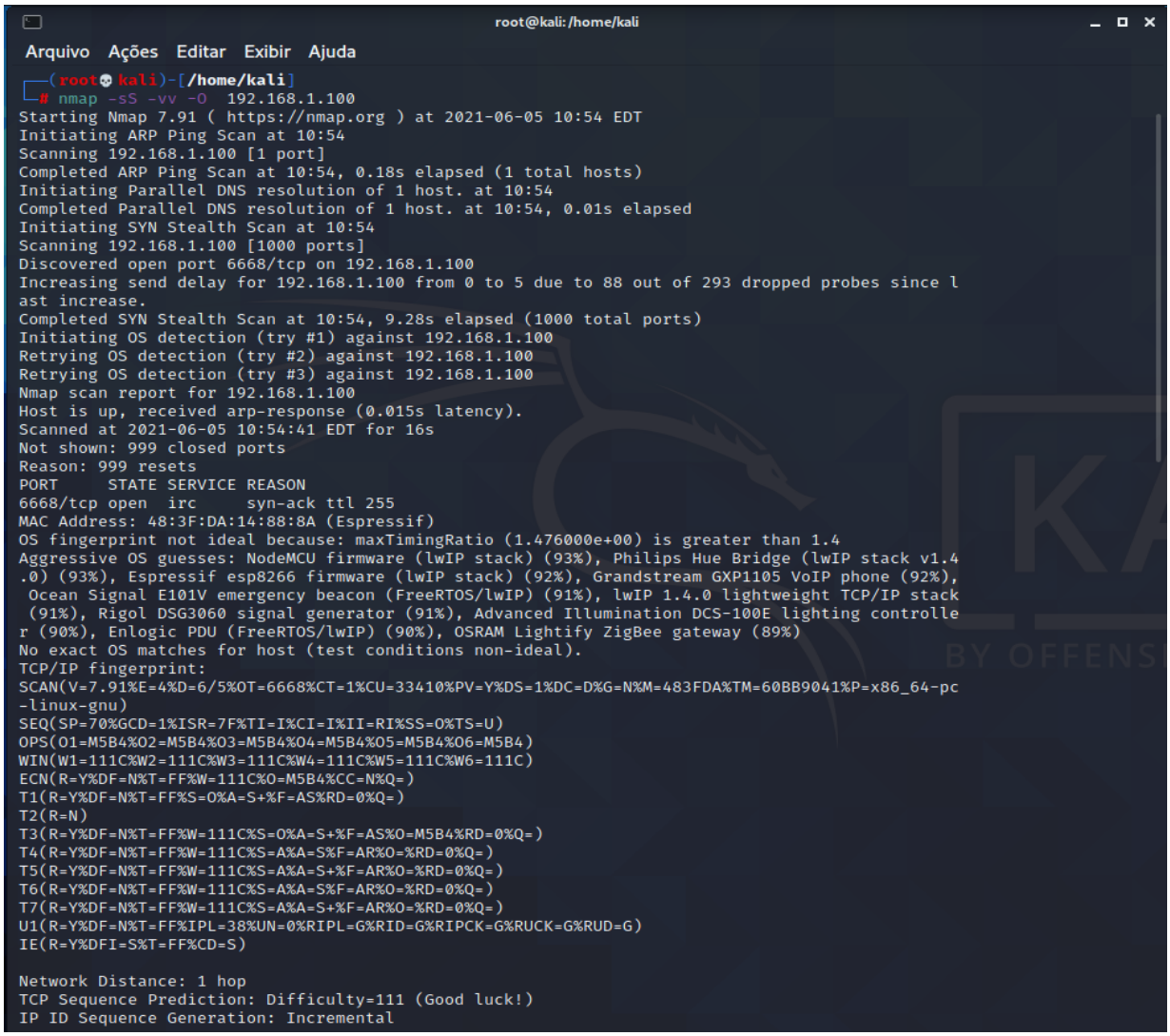
detalhamento maior.

- -O utilizado para que a ferramenta tente filtrar o sistema operacional.
- -sS É uma técnica é envia pacotes SYN em uma conexão TCP.

O resultado do comando nmap -sS -vv -O 192.168.1.100, mostrado na figura 25, a ferramenta nmap tentando identificar o sistema operacional cinco vezes, e depois de não conseguir apresentou TCP/IP fingerprint.

O figerprint é mostrado, quando não é possível detectar o sistema operacional do dispositivo, conforme apresentado na figura 26, O nmap faz a comparação do TCP/IP fingerprint do dispositivo escaneado com mais de 1500 sistemas operacionais conhecidos, e se tiver alguma correspondência é mostrado o fabricante, sistema operacional, versão, e tipo de dispositivo.

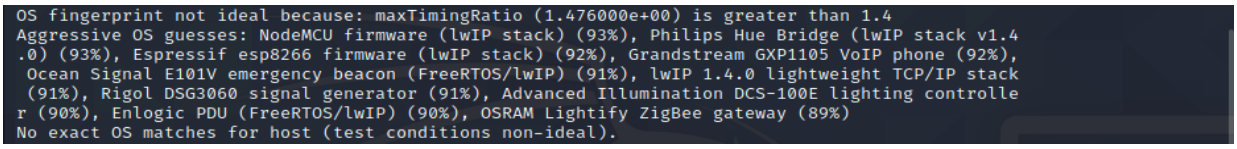
Figura 26. Resultado do comando nmap -sS -vv -o 192.168.1.100.



Os autores.

Nessa segunda análise o TCP/IP fingerprint se apresenta de uma forma mais organizado, e apresenta algumas informações do dispositivo que não foram apresentadas anteriormente. A ferramenta nmap mostra que não teve uma compatibilidade de correspondência exata e apresenta alguns dispositivos que pode ser o endereço IPv4 192.168.1.100 escaneado.

Figura 27. FingerPrint do sistema operacional.



Os autores.

O lwIP stack, apresentado na frente de cada dispositivo, conforme (Nongnu) é uma implementação independente TCP/IP, utilizado para reduzir o uso de RAM, apresentado no site.[15]

Uma das correspondências encontradas conforme a figura 27 pode ser o Nodem firmware (lwIP stack) com 93% de possibilidades. O firmware se encontra disponível no github[16]

O dispositivo possuí uma placa NodeMCU que é uma placa SoC (System on a chip), é integrada a pilha TCP/IP que permite integração com a rede Wi-Fi e foi criada pela Espressinf Systemms em 2008.

Outra informação apresentado é Espressif esp8266 firmware, que idica que 92% de possibilidade de ser esse sistema operacional.

Conforme huinfinito (2019), informações disponíveis no site [17] o dispositivo possui:

- Firmware esp8266 integrado com a placa NodeMCU
- Único processador com 32 *bits* a 80MHz.

Dos dispositivos citados pela ferramenta nmap o NodeMCU firmware e Espressif esp8266 firmware, tem mais porcentagem em semelhança com a

[15] disponível em https://www.nongnu.org/lwip/2_1_x/index.html. Acesso em 30 de maio 2021.

[16] disponível em https://github.com/nodemcu/nodemcu-firmware. Acesso em 30 de maio 2021.

[17] disponível em https://www.huinfinito.com.br/blog/artigos/o-que-e-nodemcu. Acesso em 30 de maio 2021.

Lâmpada LED Intelbras modelo EWS 410.

3.5 Analise no código fonte do firmware do dispositivo.

A análise do código fonte apresentado no firmware esp8266 disponível no site do fabricante.[18]

Figura 28. Cliente solicitando método de encriptação

Firmware da aplicação ESP8266&ESP8285_Adaptivity&Blocking_V210_26M_20200714.

Pode-se ver o cliente solicitando a conexão utilizando o protocolo de autenticação PEAP-MSCHAPv2, conforme o destaque em azul na figura 28, operando sobre o canal encriptado TLS que é fornecido pelo PEAP, nota-se que a primeira tentativa de autenticação falhou, retornando sem identificação de chave.

Então a segunda tentativa obteve sucesso, o protocolo utiliza o método de geração de chaves de criptografia secreta compartilhada, utilizando o método de desafio MMPE, conforme mostrado na figura 29, o EAP conforme (UFRJ) é um protocolo que foi projetado para funcionar PPP Protocolo Ponto a ponto, e ele possui algumas mensagens básicas de conexão como Requisição,

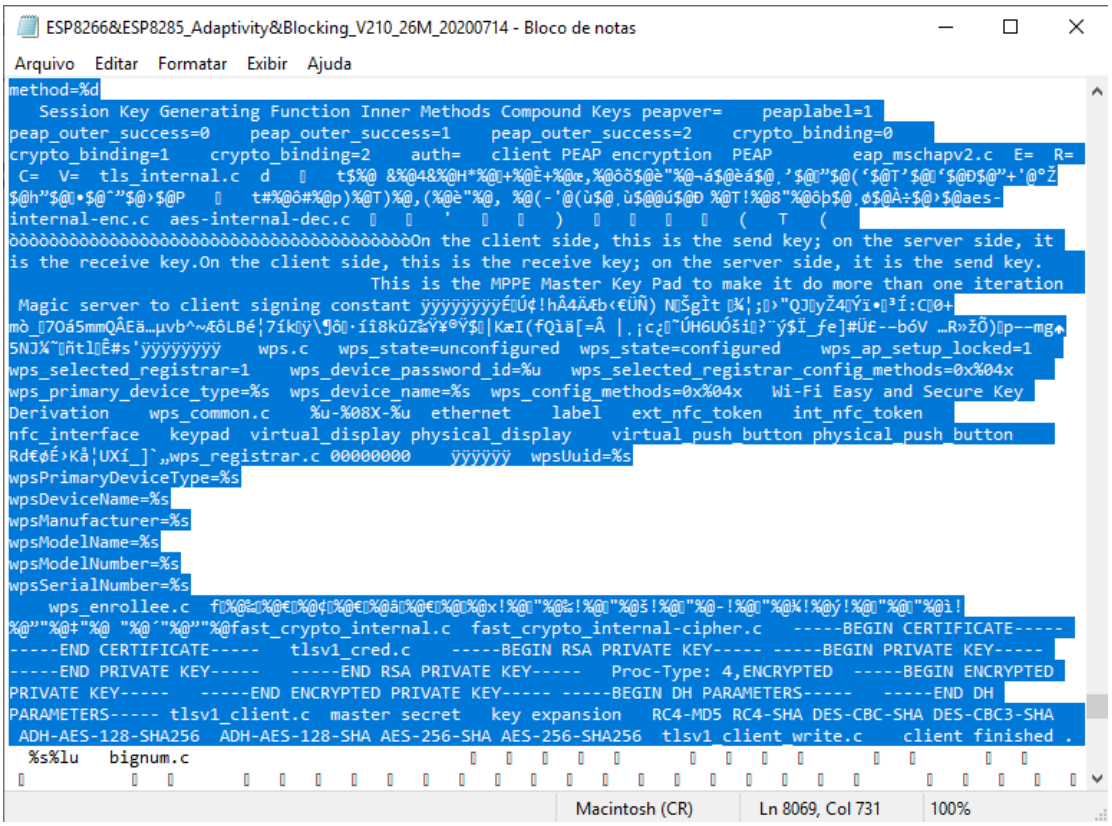
[18] Disponível em https://www.espressif.com/en/support/download/other-tools?keys=&field_type_tid%5B%5D=14. Acesso em 1 jun de 2021.

Resposta, Sucesso e Falha.

- Protocolo de autenticação de handshake de desafio da Microsoft versão 2 (MS - CHAP v2).

Conforme microsoft (2012) esse método de autenticação é falho e apresenta problemas de segurança.

Figura 29. Cliente encriptado.



Firmware da aplicação ESP8266&ESP8285_Adaptivity&Blocking_V210_26M_20200714.

EAP-MD5 CHAP, é utiliza o método de autenticação cliente e servidor, o cliente solicita a conexão ao servidor, o mesmo solicita a identificação com a chaves, enquanto o cliente também solicita a autenticação ao servidor, caso a as duas solicitações tiverem sucesso, é iniciada a sessão criptografada. É possível observar que o método de criptografia utiliza cifras ADH-AES-128-SHA256 TLS versão 1.2 e ADH-AES256-SHA256 TLS versão 1.2.

Figura 29. Falha de segurança WPA2.

Firmware da aplicação ESP8266&ESP8285_Adaptivity&Blocking_V210_26M_20200714.

Na figura 29. Pode- se ver uma faha ao tentar solicitar a conexão utilizando a criptografia WPA2. Também é possível observar que o endereço Peer Ponto a ponto, não suporta a criptografia para o serviço de multicast que o dipositivo utiliza.

3.6 Documentação.

Nessa etapa será listado os serviços utilizados pela dispositivo e as informações obtidas durante toda a análise realizada anteriormente.

- Lâmpada LED Intel Intelbras modelo EWS 410.
- Endereço TCP/Ipv4 192.168.1.100.
- MacAdress 48:3F:DA:14:88:8A.
- Fabricante Espressif Inc.
- Portas abertas 6668.
- Protocolo UDP utilizado na camada de transporte TCP/IP .
- Protocolo ARP utilizado na camada de rede TCP/IP
- Protocolo IRC utilizado na camada de aplicação TCP/IP
- Protocolo DHCP utilizado na camada de aplicação TCP/IP.
- Porta de comunicação origem 49154, e destino 6667.
- Placa NodeMCU SoC (System on a chip), processador com 32 bits e 80Mhz.
- Firmware esp8266.
- Método de criptografia EAP-MD5 CHAP, utilizando chaves compartilhadas.

4 CONSIDERAÇÕES FINAIS

A segurança da informação está presente em diversos aspectos, seja em aspectos práticos até os mais técnicos e complexos, é visível que as tecnologias existente nos dispositivos IoT, para que torne um dispositivo operacional e seguro exige a integração com diversas outras tecnologias já existentes, e assim é possível usufruir as vantagens e benefícios que a tecnologia pode oferecer.

Em certas situações, implementar funções digitais e automatizáveis em objetos que já oferecem uma praticidade na sua função analógica, pode não se tornar viável, com isso o objeto pode acabar prejudicado a sua usabilidade.

As vulnerabilidades empregadas nos dispositivos IoT, faz com que essa tecnologia não esteja preparada para a integração com diversas áreas da sociedade. Integrar tecnologia à sociedade não é fácil e os fabricantes de dispositivos IoT precisam se preparar quanto a procedimentos de segurança, além de conformidade e *compliance* com a leis de proteção e privacidade dados.

Como os dispositivos IoT utilizados em indústrias são *gateways* IoT torna o processo mais seguro, visto que os dados são transmitidos para o *gateway*, esse ambiente oferece grande vantagem em relação a ferramentas de segurança para as aplicações.

Os dados são processados e analisados e assim apenas os dados consideráveis são enviados para a nuvem. Os dispositivos IoT precisam ter grande proteção de dados durante a transmissão para o ambiente em nuvem, no processamento e também no armazenamento.Com a análise de ameaças e vulnerabilidades realizada com o teste de penetração e enumeração de serviços, pode-se ver que a lâmpada Wi-Fi LED Intelbras modelo EWS 410, possui a porta 6668 aberta, observou-se que o dispositivo utiliza o protocolo UDP na camada de transporte TCP/IP, e que a comunicação não é direta ao usuário conectado à aplicação izysmart. Através da análise realizada, observou-se que o firmware Espressif esp8266, utiliza método de autenticação não seguro. O dispositivo propaga *broadcast* através do protocolo ARP utilizado na camada de rede TCP/IP assim enviando pacote de dados para todos os usuários conectados.

O protocolo UDP não atende os pilares da segurança da informação confiabilidade, integridade e disponibilidade, os pacotes enviados não tem garantia de entrega, notou-se que com a utilização do aplicativo *Izysmart*

algumas funções demoram para ser responsivas nas solicitações feitas na aplicação. Como a lâmpada utiliza o protocolo UDP é possível realizar a injeção de pacotes no dispositivo, ou interferir no tráfego de pacotes na rede em que está conectado, um crimonoso digital, pode invadir o dispositivo em uma rede que não possua uma segurança em suas credenciais de acesso, utilizando o adaptador USB da marca Alfa modelo AWUS036NH é possível realizar um ataque de dicionário, ou força bruta através do protocolo de segurança WPA e WPA2, tendo acesso a rede local em que o dispositivo esteja conectado a segunda etapa será invadir o dispositivo que não possui os métodos de segurança mais eficazes.

O dispositivo em modo *standyby* pode-se observar pacotes trafegados na rede a todo momento. A automação residencial, ainda é um grande problema, os fabricantes devem lançar pacotes de atualizações de segurança para esses dispositivos, os *firmwares* precisam estar sempre atualizados, também deve-se certificar se os dispositivos possui um selo de autenticação e segurança, e alertar o usuário sobre o tipo de ambiente adaptável que poderá tornar os dispositivos mais seguros, o que o usuário deve fazer para mitigar um ataque caso o mesmo seja detectável. Tendo em vista que os ataques a esses dispositivos estão cada vez mais presentes - porém, vale lembrar que implementar dispositivos IoT em uma rede que não possuem políticas de segurança, utilização de aplicações para monitoramento de tráfego de dados, protocolos que possuem uma criptografia com alta segurança, utilização de *proxy* e outras ferramentas que filtre os dados não tornará o ambiente seguro.

REFERÊNCIAS

ALECRIM Emerson. **o que é internet das coisas (iot)?.** 19 abr 2020. Disponível em: https://www.infowester.com/Iot.php. Acesso em 10 nov. 2020.

AMÂNCIO Anderson. **Narrowband – internet das coisas (NB-IoT)** 13 ago 2018. Disponível em: http://wireengenharia.com.br/br/tag/IoT/. Acesso em 25 mar 2021.

APPLE. **Apple watch series 6** 2020 Disponível em: https://www.apple.com/br/apple-watch-series-6/ Acesso em 10 nov. 2020.

BOECKL Kaitlin; FAGAN Michael; FISHER William; LEFKOVITZ Naomi; MEGAS Katerina; NADEAU Ellen ,PICCARRETA Ben; O'ROURKE Gabel Danna ; SCARFONE Karen. **Considerações para gerenciar riscos de privacidade e segurança cibernética na Internet das coisas (IoT).** jun 2019. Disponível em: https://csrc.nist.gov/publications/detail/nistir/8228/final. Acesso em 10 ou 2020.

Blogspot **Exploit0x00 2018 disponível em:** https://0x7331.blo gspot.com/2018/06/realizando-varredura-na-rede-com.html. Acesso em 20 abr. 2021.

ČERMÁK Miloš. **Pesquisadores descobrem que amazon echo e kindle são vulneráveis a ataques krack** 21 out. 2019. Disponível em: https://www.welivesecurity.com/br/2019/10/21/pesquisadores-descobrem-que-amazon-echo-e-kindle-sao-vulneraveis-a-ataques-krack/. Acesso em 01 nov. 2020.

CHECK POINT SOFTWARE TECHNOLOGIES. **Keeping your gate locked on your iot devices: vulnerabilities found on amazon alexa** 13 ago. 2021. Disponível em: https://www.youtube.com/watch?v=xfqGYic4hj8. Acesso em 01 nov. 2020.

CyberPratibha. **Netdiscover – Network scanning tool in kali linux tutorial for beginners**. disponível em https://www.cyberpratibha.com/blog/netdiscover/. Acesso em 15 maio 2020

CIO. **5 áreas mais impactadas pela Internet das coisas.** 13 fev 2019. Disponível em: https://cio.com.br/tendencias/5-areas-mais-impactadas-pela-internet-das-coisas/ Acesso em 02 nov. 2020.

Cisco community. **Peer Address.** disponível em https://community.cisco.com/t5/vpn/peer-address/td-p/1697880. Acesso em 20 abril 2021.

CISCO. **Rede baseada em intenções e ampliação do white paper da empresa.** 10 jun. 2019. Disponível em: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-intent-based-networking-aag-cte-en.html?oid=aagen016865. Acesso em 27 abr. 2021.

COZER Carolina. **Como a privacidade do usuário pode ser garantida nos dispositivos IoT? voz.** 13 jun 2020. Disponível em: https://www.whow.com.br/novas-tecnologias/privacidade-usuario-dispositivos-IoT/. Acesso em 25 mar 2021.

COSTA Cristiano André. Internet relay chat. disponível em: http://penta2.ufrgs.br/rc952/trab1/irc.html. Acesso em 3 maio 2021.

DIGIX. **Smart cities o que são e quais os benefícios para a gestão pública.** 3 out. 2018. Disponível em: https://www.digix.com.br/smart-cities-o-que-sao-e-quais-os-beneficios- para-a-gestao-publica/. Acesso em 12 nov. 2020.

ESTADÃO. **Primeiro projeto de carro autônomo data de 1920** 13 mar. 2020. Disponível em: https://summitmobilidade.estadao.com.br/carros-autonomos/primeiro-projeto-de-carro-autonomo-data-de-1920/#:~:text=O%20primeiro%20modelo%20realmente%20aut%C3%B4nomo, NavLab%201%2C%20lan%C3%A7ado%20em%201986. Acesso em 11 nov. 2020.

Grupo de Teleinformática e Automação. **Segurança na internet protocolo ssl/tls** disponível em https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/bernardo/tls.html. Acesso em 20 abr de 2021.

HBM. **Transdutores**: o sistema nervoso da IIoT. Disponível em: https://www.hbm.com/pt/7501/transdutores-e-a-internet-das-coisas/. Acesso em 01 nov. 2020.

Introdução à segurança digital. **Resumo das ferramentas.** Disponivel em https://gitbook.ganeshicmc.com/redes/ferramentas/ferramentas_resumos. Acesso em 20 abr. 2021.

IGNACIO Bruno. **Um bug de segurança na alexa da amazon permitiu acesso ao histórico de voz** 14 ago 2020. Disponível em: https://www.oficinadanet.com.br/seguranca/32367-um-bug-de-seguranca-na-alexa-da-amazon-permitiu-acesso-ao-historico-de-voz. Acesso em 01 nov. 2020.

JUSBRASIL CANAL CIÊNCIAS CRIMINAIS**. Papel do direito na sociedade em rede**: Internet das coisas (IoT) 2018. Disponível em : https://canalcienciascriminais.jusbrasil.com.br/artigos/573706676/o-papel-do-direito-na-sociedade-em-rede-internet-das-coisas-IoT. Acesso em 29 out. 2020.

KEVIN Auston. **that 'internet of things' thing.** 22 jun 2009 https://www.rfidjournal.com/that-internet-of-things-thing. Acesso em 27 abr. 2021.

LEMOS Simone. **Ataques cibernéticos crescem muito durante quarentena.** Disponível em: https://jornal.usp.br/atualidades/ataques-ciberneticos-crescem-muito-durante-quarentena/. Acesso em 12 nov. 2020.

LOUREIRO Rodrigo. **Musk espera que carros totalmente autônomos estejam nas ruas já em 2021.** 03 dez. 2020. Disponível em: https://exame.com/inovacao/musk-espera-que-carros-totalmente-autonomos-estejam-nas-ruas-ja-em-2021/. Acesso em 20 abr. 2021.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018. 192 p. Disponível em: https://bibIIoTecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas. pdf. Acesso em 29 out. 2020.

MAGRANI, Eduardo. **Entre dados e robô**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial Ltda, 2019. 304 p. Disponível em: http://eduardomagrani.com/wp-content/uploads/2019/07/Entre-dados-e-robo%CC%82s-Pallotti-13062019.pdf. Acesso em 16 mar. 2021.

MAGRANI, Eduardo. **Sinal vermelho para o 'lixo da Internet das coisas'** 04 maio. 2017**.** Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&UserActiveTemplate=mobile&infoid=45086&sid=17#.YIF-fuhRUk. Acesso em 11 nov. 2020.

MATSU Carla. **Internet das coisas na medicina já atua no combate à covid-19 no Brasil** 27 jun 2020. Disponível em: https://computerworld.com.br/inovacao/internet-das-coisas-na-medicina-ja-atua-nocombate-a-covid-19-no-brasil/. Acesso em 22 mar 2020.

Microsoft. **EAP (protocolo de autenticação extensível) para acesso à rede.** Disponível em: https://docs.microsoft.com/pt-br/windows-server/networking/technologies/extensible-authentication-protocol/network-access. Acesso em 20 abr. 2021.

MDN Web docs. **IRC.** disponível em https://developer.mozilla.org/pt-BR/docs/Glossary/IRC**. Acesso em 20 abr. 2021.**

MTB digital bussiness assurace. **OSINT, esse grande desconhecido.** disponível em https://mtp.com.br/osint-esse-grande-desconhecido. Acesso em 23 maio 2021.

NAVEEN Joshi. **8 Types of security threats to iot.** 19 de ago 2019. Disponível em: https://www.bbntimes.com/en/technology/8-types-of-security-threats-to-iot. Acesso em 15 de abril de 2021.

New security world. **Aircrack-ng Pacote de Ferramentas para Monitorizar e Analisar Redes sem Fio. Disponível em** https://nsworld.com.br/aircrack-ng-pacote-de-ferramentas-para-monitorizar-e-analisar-redes-sem-fio/. Acesso em 21 abr. 2021.

NETWORKWORLD**. Internet das coisas em 2020**: mais vital do que nunca 13 maio 2020. Disponível em: https://cio.com.br/tendencias/internet-das-coisas-em-2020-mais-vital-do-que-nunca. Acesso em 01 nov. 2020.

Open access peer-reviewed chapter. **Fingerprint recognition.** https://www.intechopen.com/books/advanced-biometric-technologies/fingerprint-recognition. Acesso em 20 abr. 2021.

PASTORINO Cecília. **Análise de dispositivos IoT**: vulnerabilidades mais comuns e formas de encontrá-las. 11 jun 2019. Disponível em: https://www.welivesecurity.com/br/2019/06/11/analise-de-dispositivos-iot-vulnerabilidades-mais-comuns-e-formas-de-encontra-las/. Acesso em 15 de abril de 2021.

Paim Rodrigo R.**. WEP, WPA e EAP.** disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/eap.html. Acesso em 20 abr. 2021.

PAUL Fredric. **10 principais vulnerabilidades da Internet das coisas** 18 jan 2019. https://cio.com.br/gestao/10-principais-vulnerabilidades-da-internet-das-coisas/. Acesso em 15 abr. 2021.

REDEMAT **"Estudo comparativo do comportamento de aços (trilhos) premium na tenacidade à fratura e na propagação de trinca por fadiga, de aplicação ferroviária" disponível em** https://www.repositorio.ufop.br/bitstream/123456789/5699/6/DISSERTA%C3%87%C3%83O_EstudoComparativoComportamento.pdf. Acesso em 20 abril 2021.

ROSCOE Beatriz. **Apple destaca funções voltadas para a saúde em novos lançamentos** 15 set 2020 Disponível em: https://www.poder360.com.br/tecnologia/apple-destaca-funcoes-voltadas-para-a-saude-em-novos-lancamentos/. Acesso em 10 nov. 2020.

SANTOS Raphael . **O que é tcp/ip? aprenda de uma vez por todas como funciona!** 4 nov 2019. Disponível em: https://blog.hosts.green/tcp-ip/. Acesso em 25 mar 2021.

SCOLA Alvaro**. Botnet mirai está de volta e ameaça a internet** 20 mar 2019. Disponível em : https://olhardigital.com.br/dicas_e_tutoriais/noticia/a-botnet-mirai-esta-de-volta-e-ameaca-a-internet-saiba-como-se-proteger/83890. Acesso em 29 out. 2020.

Secure W2. **PEAP-MSCHAPv2 Vulnerability Allows For Credential Theft** https://www.securew2.com/blog/peap-mschapv2-vulnerability. Acesso disponível em 20 abr 2021.

SECURITY REPORT. **As vulnerabilidades e necessidades de segurança em IoT** 29 set 2016. Disponível em: https://www.securityreport.com.br/overview/mercado/vulnerabilidades-necessidades-seguranca-IoT/#.X58rMYhKjIV. Acesso em 01 nov. 2020.

Segurança **Detecção de sistema operacional remotamente via o fingerprinting da pilha tcp/ip. Disponível em** https://nmap.org/nmap-fingerprinting-article-pt.html. Acesso em 21 abr. 2021.

SEG INFO. **41,6 bilhões de dispositivos de IoT gerarão 79,4 zettabytes de dados em 2025.** 26 jun. 2019. Disponível em: https://seginfo.com.br/2019/06/26/416-bilhoes-de-dispositivos-de-iot-gerarao-794-zettabytes-de-dados-em-2025/ Acesso em 12 nov. 2020.

SIN Secretaria geral de informática **Esta página contém informações sobre o bloqueio de portas com vulnerabilidades pelo Firewall da Universidade Federal de São Carlos** – disponível em https://www.sin.ufscar.br/servicos/conectividade/redes-firewall-bloqueio-de-portas-com-vulnerabilidades-conhecidas. Acesso em 17 maio 2021.

SHAKIB Tony. **Azure iot apresenta integração perfeita com cisco iot** 03 mar. 2020. Disponível em: https://azure.microsoft.com/en-us/blog/azure-Iot-introduces-seamless-integration-with-cisco-Iot/ Acesso em 11 nov. 2020.

Sobre linux **Windows Wi-Fi com 802.1X + EAP-TTLS + EAP-MSCHAPv2 e certificados de cliente** disponível em https://sobrelinux.info/questions/493228/windows-wi-fi-with-802-1x-eap-ttls-eap-mschapv2-and-client-certificates. Acesso em 21 mai0 2021.

Softwall. **Pentest ou Testes de Invasão: O que é e quais são as etapas?**. disponível em https://www.softwall.com.br/blog/pentest-testes-de-invasao-o-que-e-quais-etapas/. Acesso em 23 maio 2021.

SUNTECH DO BRASIL. **IoT no trânsito.** Disponível em: https://www.stdobrasil.com.br/site/novo/Iot-no-transito/ Acesso em 11 nov. 2020.

TEIXEIRA, Mariane Mendes. **Transdutor.** Brasil Escola**.** Disponível em: https://brasilescola.uol.com.br/fisica/transdutor.htm. Acesso em 22 de abr. 2021.

THE WESTERN PA HEALTHCARE NEWS TEAM. **5 examples of IoT in healthcare**. Nov 2017. Disponível em:https://www.wphealthcarenews.com/5-examples-IoT-healthcare/. Acesso em: 22 mar. 2021.

Tudo celular. **Alternativas seguras: conheça outras lojas de apps para fugir da Google Play.** disponível em https://www.tudocelular.com/android/noticias/n81555/melhores-lojas-alternativas-para-Android. Acesso em 23 maio de 2021.

TOWNSEND Kevin. **The state of things in the internet of things** 30 Abr 2019**.** https://blog.avast.com/how-vulnerable-is-the-internet-of things?_ga=2.18360251.342034119.1618479480-660476230.1615906016. Acesso em 15 abr. 2021.

UDP **Aspectos de segurança.** disponível em http://www.cbpf.br/~sun/pdf/udp.pdf. Acesso em 1 jun 2021.

VEJA TECNOLOGIA. **Elon Musk diz que sua fábrica de carros elétricos jamais faria espionagem.** 20 mar 2021. Disponível em: https://veja.abril.com.br/tecnologia/elon-musk-diz-que-sua-fabrica-de-carros-eletricos-jamais-faria-espionagem/. Acesso em 20 abr. 2021.

VILLARINO Julia. **Internet das coisas:** um desenho do futuro 16 nov. 2016. Disponível em:https://www.proof.com.br/blog/internet-das-coisas/. Acesso em 04 nov. 2020.

WHITE PAPER. **Cisco annual internet report.** 9 Mar 2020. Disponível em: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Acesso 03 nov. 2020.

YUAN Michael. **Conhecendo o MQTT.** 04 out 2017. disponível em: https://developer.ibm.com/br/technologies/IoT/articles/IoT-mqtt-why-good-for-IoT/. Acesso em 23 mar. 2020.