Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Departamento de Computação e Sistemas

Estudo de técnicas de ataque e defesa em equipamentos da Indústria 4.0

Flávia Helena da Silva

TRABALHO DE CONCLUSÃO DE CURSO

ORIENTAÇÃO:
Dr. Theo Silva Lins

Janeiro, 2022
João Monlevade–MG

Flávia Helena da Silva

Estudo de técnicas de ataque e defesa em equipamentos da Indústria 4.0

Orientador: Dr. Theo Silva Lins

Monografia apresentada ao curso de Engenharia da Computação do Instituto de Ciências Exatas e Aplicadas, da Universidade Federal de Ouro Preto, como requisito parcial para aprovação na Disciplina "Trabalho de Conclusão de Curso II".

Universidade Federal de Ouro Preto

João Monlevade

Janeiro de 2022

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E APLICADAS
DEPARTAMENTO DE COMPUTACAO E SISTEMAS

FOLHA DE APROVAÇÃO

Flávia Helena da Silva

Estudo de técnicas de ataque e defesa em equipamentos da Indústria 4.0

Monografia apresentada ao Curso de Engenharia da Computação da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Engenharia da Computação

Aprovada em 13 de Janeiro de 2022

Membros da banca

Doutor Theo Silva Lins - Orientador(a) - Universidade Federal de Ouro Preto - DECSI
Doutor Marlon Paolo Lima - Universidade Federal de Ouro Preto - DECSI
Doutor Samuel Souza Brito - Universidade Federal de Ouro Preto - DECSI

Theo Silva Lins, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 25/01/2022

Documento assinado eletronicamente por **Theo Silva Lins**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 25/01/2022, às 22:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0272008** e o código CRC **0E8B1891**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: - www.ufop.br

Este trabalho é dedicado a toda minha família, que sempre esteve presente e me apoiando nos momentos difíceis e me fizeram ser a pessoa que sou hoje. Aos meus amigos, que se fizeram família durante toda essa jornada.

Agradecimentos

Agradeço primeiramente a mim, por nunca ter desistido de acreditar que seria capaz de vencer essa etapa e encerrar esse ciclo. Agradeço à Deus, por sempre iluminar meu caminho, me guiando para as melhores escolhas e por nunca me abandonar nos momentos difíceis. Ao meu pai, Francisco, e à minha mãe Lúcia. À minha irmã, Fernanda. Agradeço aos familiares e amigos. Aos professores, pelo conhecimento cedido.

"Science is more than a body of knowledge; it is a way of thinking."

— Carl Sagan (1934 – 1996),
in: The Demon-Haunted World: Science as a Candle in the Dark.

Resumo

Este trabalho analisa técnicas de exploração de falhas de segurança em um ambiente simulando uma Indústria 4.0 e como é possível defender de ataques de cibercriminosos. Assim, este estudo abrange diferentes técnicas utilizadas tanto por especialistas em segurança quanto por pessoas que tem o intuito de prover ataques à máquinas de manufaturas e mudar o comportamento das mesmas, podendo assim modificar uma linha de produção. A abordagem utilizada foi através de testes com ferramentas que exploram a vulnerabilidade da rede e ataques comumente utilizados por cibercriminosos. Com a execução dos testes foi possível inferir que segurança das redes ainda continua sendo uma barreira para que manufaturas adotem essa prática da interconectividade dos equipamentos uma vez que, isso possa vir a gerar prejuízos financeiros.

Palavras-chaves: Indústria 4.0. Segurança. Cibercriminosos.

Abstract

This work analyzes techniques for exploiting security flaws in an environment simulating an Industry 4.0 and how it is possible to defend against cybercriminal attacks. Thus, this study covers different techniques used both by security experts and people who aim to provide attacks on manufacturing machines and change their behavior, thus being able to modify a production line. The approach used was through tests with tools that explore the vulnerability of the network and attacks commonly used by cybercriminals. With the execution of the tests, it was possible to infer that network security still remains a barrier for manufacturers to adopt this practice of equipment interconnectivity, since this can generate financial losses.

Key-words: Industry 4.0. Security. Cybercriminals.

Lista de ilustrações

Sumário

1 Introdução

Ao longo do tempo é perceptível o quanto a tecnologia está ainda mais presente na vida de todos e como ela está evoluindo em diversas vertentes. As primeiras revoluções industriais foram o começo de toda essa transformação e são elas que ainda permitem com que nosso meio esteja em constante mudança.

Com todos esses anos de transformações e revoluções tecnológicas é chegado na era da Indústria 4.0 (SANTOS; ALBERTO; LIMA; CHARRUA, 2018), ou como alguns dizem, a quarta revolução industrial, que se resume ao lema de manufaturas inteligentes produzindo cada vez mais, melhor e de maneira mais inteligente. As indústrias de hoje, ainda que herdaram aspectos de todas as revoluções, começam a dar um passo importante para ficarem cada vez mais engenhosas.

A quarta revolução industrial está transformando a próxima geração de sistemas de manufatura, tornando-os mais inteligentes, bem conectados, auto-organizados, descentralizados e flexíveis. Isto é possível pela incorporação do *Cyber Physical Systems* (CPS) para monitorar e controlar as máquinas, e o uso da *Internet of Things* (IoT) (SANTOS; ALBERTO; LIMA; CHARRUA, 2018) para conectar vários componentes da planta de manufatura para a Internet, que são duas das principais tecnologias facilitadoras.

Mas sempre que há uma mudança generalizada, surgem novos desafios inerentes, especialmente no que diz respeito a questões de segurança da informação e das comunicações. A integração de novos sistemas e seu aumento hipotético e o acesso potencial de terceiros significa que toda uma nova gama de problemas de segurança surge neste contexto. A segurança é crítica para o sucesso de sistemas de manufatura inteligentes. É importante garantir a proteção das infraestruturas empresariais bem como os dados e informações contidas em seus sistemas contra uso indevido e acesso não autorizado (SANTOS; ALBERTO; LIMA; CHARRUA, 2018).

1.1 O problema de pesquisa

Esse processo de segurança das manufaturas inteligentes, e até mesmo das tecnologias em dispositivos a mão de pessoas, vem exigindo uma busca massante por soluções.

A troca de dados vem ficando ainda mais transparente, o acesso vem sendo popularizado, o avanço diário do desenvolvimento de aplicações que fazem surgir outras novas aplicações ainda mais avançadas e poderosas e dentre diversos outros fatores que culminam na aparição de diversas aberturas para por em risco a segurança. Sendo assim, ainda é necessário políticas além das existentes para medidas serem tomadas.

1.2 Objetivos

O objetivo do projeto é apresentar formas de elevar a segurança em redes de manufaturas inteligentes, através da execução de ataques que serão feitos a uma placa embarcada conectada em um braço robótico funcionando com uma Indústria 4.0.

1.2.1 Objetivos Específicos

Além do objetivo principal tem-se os seguintes objetivos específicos:

- Analisar e testar ferramentas mais conhecidas e utilizadas para estudos acadêmicos e por algumas organizações.
- Identificar os ataques mais utilizados por cibercriminosos nesse ambiente.
- Testar localmente e remotamente via rede cabeada (ethernet) e via rede WiFi.
- Levantar informações acerca da segurança cibernética em empresas, ferramentas que são utilizadas por hackers com a finalidade de prover ataques maliciosos.
- Reunir informações relevantes das ferramentas que são utilizadas para que se possa evitar esses ataques.
- Analisar como é o comportamento de diferentes tipos de acessos à sistemas e como é possível ter sistemas ainda mais seguros.

1.3 Metodologia

Para o desenvolvimento deste estudo, foi escolhido problemas de segurança que vêm sendo discutidos atualmente e por se tratar de uma revolução que está ocorrendo, além de que já há rumores de uma possível Indústria 5.0 (DEMIRA; DÖVENA; SEZENB, 2019) a caminho, onde robôs e humanos irão trabalhar juntos sempre que possível, o chamado coworking humano-robô (DEMIRA; DÖVENA; SEZENB, 2019). Visto que o cenário atual ainda detém de diversos gargalos na segurança das manufaturas e sabendo que um futuro ainda mais tecnológico está cada vez mais próximo de acontecer, a pesquisa foca em técnicas de segurança para se prover uma rede mais protegida à vulnerabilidades e assim, evitar que o processo de fabricação industrial passe por interferência de criminosos cibernéticos.

Para o presente estudo, serão realizados testes de segurança na placa embarcada BeagleBone Blue (BEAGLEBONE, 2018), que está conectada a um braço robótico ED-7220. Será utilizado o sistema Linux para manusear as ferramentas necessárias e providenciar os

ataques ao à placa embarcada. O computador utilizado possui 8GB RAM, Placa de vídeo AMD Radeon 535 2GB e processador Intel®Core™i7-8550U.

Diante da vasta quantidade de ferramentas que há para estudos de cibersegurança, as escolhidas foram com base no aspecto de variedade de funções que cada uma pode exercer. Além disso, os tipos de ataques a serem feitos à placa embarcada foram enunciados pensando na popularidade destes no meio da manufatura, ou seja, são ataques mais frequentes nas indústrias ou pelo menos são os que vem sendo tema de diversos outros estudos acerca da segurança cibernética.

Para que se possa ser feito todo o experimento, através do terminal do Linux, o braço robótico será acessado para que sejam feitos os testes. Ao acessar a placa embarcada via rede, será aplicado alguns ataques e utilizada algumas das ferramentas que serão detalhadas na Seção 2, para que se possa analisar o comportamento do braço robótico e da rede nesse período de teste.

Pensando no cenário em que existe um braço robótico conectado à uma placa embarcada, uma forma de ataque utilizada será o *Port Scanning Attack*. Através dele será testado qual porta da placa embarcada estará disponível para que se possa detectar vulnerabilidades, uma vez que essa placa embarcada também funciona como um computador. Ao achar uma porta disponível, o próximo passo será explorar as inseguranças presentes nela e analisar todo o comportamento do braço robótico, se ele irá responder à esta ação, se ele irá realizar movimentos fora do padrão, se para esse tipo de ataque não afeta em nada a sua produtividade, se demora mais o tempo de resposta a esta invasão, etc. Ainda realizando alguns ataques, também será utilizado o Ataque de Força Bruta para que se possa tentar hackear algum login e senha da placa embarcada e ver o quanto isso reflete no desempenho do braço robótico.

Tendo em vista que os ataques serão feitos via rede, a influência destes na rede demandará muito sobre o comportamento do braço robótico. Para que se possa ser feita essa análise das mudanças na rede, análise em determinadas portas, e todas as outras aplicações que necessitam ser escaneadas, será utilizado ferramentas como TCPdump para verificação dos pacotes de rede que estão chegando no braço robótico. Além disso, será também usado o recurso do SSH, que permitirá o acesso à placa embarcada permitindo ou não que haja alguma mudança considerável de alguma aplicação que está tentando manusear o braço robótico. Será utilizado o Nmap para análise de *port scanning* e de segurança de rede da placa embarcada. Por último, outra ferramenta utilizada será o T50, que possui a capacidade de enviar um número altíssimo de requisições de pacotes dos protocolos ICMP, IGMP, TCP e UDP sequencialmente com diferença de microssegundos, que são os ataques DDoS.

No trabalho em questão não foi considerado ataques exclusivos a rede Wifi, como por exemplo um ataque especial à criptografia TKIP (*Temporal Key Integrity Protocol*)

(HENRIQUES, 2020) que é uma criptografia exclusiva do Wifi, uma vez que apesar de estar presente na Indústria 4.0 a tecnologia IoT, grande parte dos equipamentos industriais como os braços robóticos ainda utilizam comunicação cabeada em detrimento da interferência (ruído) (VARGHESE; TANDUR, 2014). A Indústria 4.0 requer muitas vertentes para que se consiga garantir a confiabilidade da rede, como por exemplo, uma taxa de dados elevada caso todas as suas operações sejam mantidas e controladas por um meio virtual, o que implica na necessidade de uma rede que suporte essa transferência de dados. Sendo assim, teria de ser analisado muitos motivos de Wifi para que seja possível chegar a alguma conclusão que caracteriza problemas do Wifi em si, e a pesquisa evidencia problemas de segurança em equipamentos da indústria e não da rede.

Levando em conta tudo o que foi considerado para o desenvolvimento do trabalho, algumas limitações foram encontradas como possível bloqueio de firewall que poderia encontrar uma atividade suspeita no tráfego de pacotes. Além disso, os ataques foram feitos de apenas um notebook, podendo assim reduzir o volume de resultados consistentes.

As ferramentas/experimentos realizados neste trabalho são feitos com rede cabeada e rede sem fio com a mesma abordagem. Feito toda essa análise dos resultados e experimentos, será sugerido as melhores formas de se proteger desses tipos de ataques em um ambiente industrial.

1.4 Elaboração do projeto

O projeto que está sendo desenvolvido é uma iniciativa para abordagem do conceito de segurança cibernética, um dos maiores gargalos da indústria 4.0. Através das atividades propostas no projeto será realizado ataques a uma placa embarcada conectada a braço robótico que simula uma Indústria 4.0.

Alguns dos ataques que serão feitos são roubo de pacotes, Backtracking e DDos. Estes são alguns dos que, hoje em dia, ocorrem em redes distribuídas por exemplo e geram um enorme problema na aplicação. Será manuseada algumas aplicações de rede como TCPdump, Nmap, T50, etc. Todo o desempenho será avaliado pela latência, através do comando ping. Os experimentos serão feitos localmente e remotamente, via rede cabeada (ethernet) e via rede WiFi. Feito esses ataques, o próximo passo é observar o comportamento do braço robótico a eles, enunciando as principais características observadas em cada um.

1.5 Organização do trabalho

A divisão do trabalho se dá como segue: no Capítulo 2 encontra-se uma revisão bibliográfica que conta com descrições a respeito da Indústria 4.0, placas embarcadas, braços robóticos, problemas de segurança, as ferramentas utilizadas e os tipos de ataques

utilizados. No Capítulo 3, expõe-se alguns trabalhos relacionados que, inclusive, foram utilizados como base para realização deste e tratam de temas semelhantes ao abordado neste trabalho. A revisão conta com uma coleção de diversas referências para explorar o tema de segurança na Indústria 4.0, descrevendo suas diversas definições, formas de implementação e configuração e desafios encontrados nesse ambiente. No Capítulo 4, é apresentado a configuração do ambiente de trabalho e testes realizados com algumas ferramentas. Capítulo 5 contém a etapa de exploração de vulnerabilidades utilizando como base análise de ataques externos e simulações. O Capítulo 6 contém algumas possíveis soluções para melhoria de segurança. Por fim, uma dissertação que expõe as conclusões acerca do trabalho.

2 Revisão bibliográfica

Neste capítulo o objetivo é mostrar todos os conceitos que foram usados como base para a pesquisa. Para isso, a revisão bibliográfica foi planejada dividindo para cada subseção conceitos sobre temáticas relevantes. Desta forma abrange tópicos sobre Indústria 4.0, placas embarcadas, braços robóticos, problemas de segurança, ferramentas utilizadas e os tipos de ataques utilizados.

2.1 Indústria 4.0

O Conceito de Revoluções Industriais começa no final do séc XVIII, quando a primeira revolução marcou o mundo com a mudança de métodos de produção artesanais para processos de produção mecanizados. Após esse marco, e abordando os dias atuais, foram desenvolvidas diferentes tecnologias de informação (TI) e o resultado desse desenvolvimento foi inserido em processos de produção e foi capaz de trazer benefícios ao nível de toda cadeia de valor.

A partir de tantas transformações e de um cenário em que cada vez mais há a procura por produtos únicos, de maior complexidade, qualidade e custos reduzidos, o novo modelo de indústria que surge disso é a chamada Indústria 4.0 ou, para alguns, quarta revolução industrial (BITKOM et al., 2016).

A Indústria 4.0, procura abranger um conjunto de tecnologias de ponta ligadas à Internet com o intuito de fazer com que os sistemas de produção fiquem, cada vez mais, flexíveis e colaborativos. Nesse contexto, tem-se que as máquinas agora utilizam de diferentes tecnologias, como por exemplo a inteligência artificial, para realizar tarefas complexas, proporcionando eficiência de custo superior e bens de serviço de melhor qualidade. Com a implementação de diversos sensores no universo da indústria, os mundos físico e virtual se unem em apenas um, originando os CPS. Os CPS, são conectados através de IoT e, com isso, conseguem interagir entre si com o uso de protocolos padrão baseados na internet, e assim, analisam dados com o objetivo de prever falhas e adaptar-se às novas mudanças.

2.2 Placas Embarcadas

Ainda nesse cenário da quarta revolução industrial, onde diversas novas tecnologias surgem, cresce em larga escala o desenvolvimento de placas embarcadas, um dos pontos chaves desse projeto. Placas embarcadas vem ganhando mais espaço no nosso dia a dia,

mas já existem desde os anos 60, sendo que as principais mudanças durante esse tempo consistem na sua diminuição de valor e no aumento da capacidade computacional. Sistemas embarcados não seguem uma mesma vertente em todas as suas aplicações, podendo estar presentes na locomoção de um brinquedo ou em um sensor que regula temperatura de uma sala com diversos servidores. A principal diferença em si está no hardware usado e quais os componentes estão ligados nesse sistema.

Quando diz-se que um sistema é embarcado significa que este é dedicado a uma tarefa única além de interagir com o meio através de sensores e atuadores. Esse tipo de aplicação são projetadas para serem independentes de uma fonte fixa de energia, como por exemplo uma tomada. Nessas placas embarcadas, é possível observar uma certa capacidade computacional e independência de operação. Na Figura 1 e na Figura 2, há um exemplo de uma placa embarcada BeagleBone Blue, que foi utilizada no decorrer do projeto e também uma lógica de um sistema embarcado, respectivamente.

Figura 1 – Configuração de uma placa embarcada BeagleBone Blue.

Figura 2 – Exemplo de Sistema Embarcado.

2.3 Braços Robóticos

Ao longo dos anos houve diversas revoluções industriais que marcaram a história e determinaram os rumos para a economia e política além de impulsionarem o surgimento de inovações tecnológicas no mercado. Nos dias atuais, existe a quarta revolução industrial. Nesse novo contexto tem-se o surgimento de novos dispositivos de automatização nos processos de fabricação nas indústrias de diferentes ramos e portes no mercado, processo esse que necessita de equipamentos como braços robóticos industriais.

Esses braços robóticos fazem parte do conjunto de robôs industriais mais utilizados atualmente. Essas inovações tecnológicas são robustas, resistentes e estáveis, produzidas através de materiais resistentes que fazem parte da composição de suas estruturas e são programados diante de softwares de tecnologia avançada, fazendo uma aliança entre resistência e inteligência artificial.

Com toda essa inovação, torna-se possível garantir a execução de processos de forma ágil, segura, precisa e competente a quem faz a aquisição de braços robóticos em suas indústrias. Além disso, aumenta-se a produtividade dos empreendimentos que adquirem essa tecnologia e também os ganhos com a automatização dos processos. A Figura 3 traz tipos de braços robóticos industriais.

Figura 3 – Exemplo de Braços Robóticos Industriais.

Além dos processos industriais, essa tecnologia dos braços robóticos vem ajudando a traçar mudanças perceptíveis na vida de algumas pessoas. Existem vários estudos estudos de protótipos que originam exoesqueletos, que serão capazes de proporcionar a quem usa a reaquisição de movimentos que estariam comprometidos usando transmissores e tecnologias que decodificam impulsos nervosos (PEOPLE TECH AND ENGLISH, 2019). Com o mundo em constante avanço, muitos braços robóticos estão sendo desenvolvidos e ficando cada vez mais inteligentes para a rotina de trabalho pesado. Projetos de otimização estão sendo desenvolvidos para que o operador tenha maior facilidade em mover grandes

estruturas e possuírem maior precisão para realocá-las.

2.4 Braço Robótico ED - 7220

Para o desenvolvimento da pesquisa foi utilizado um braço robótico ED-7220 que é baseado em um sistema de cinco articulações, sistema essa que é bastante popular na indústria (ALMEIDA, 2015). Dessa forma, a experiência ao aplicar os testes, pode refletir nas necessidades reais de uma indústria. Os movimentos das articulações presentes no robô é possível de se detectar através de uma observação visual, o que facilita a análise do comportamento do mesmo aos ataques.

O braço robótico foi desenvolvido com finalidade acadêmica. Basicamente ele é constituído por um controlador monitorado via computador, uma ferramenta terminal e um *teach pendant*. Mesmo sendo de caráter acadêmico, com ele é possível simular exatamente como seria seu funcionamento em plantas industriais. Além disso, por ser um braço robótico modernizado, é possível realizar movimentos no espaço, o que fica ainda mais próximo do cenário ideal de uma indústria, ele é dito como robô autônomo.

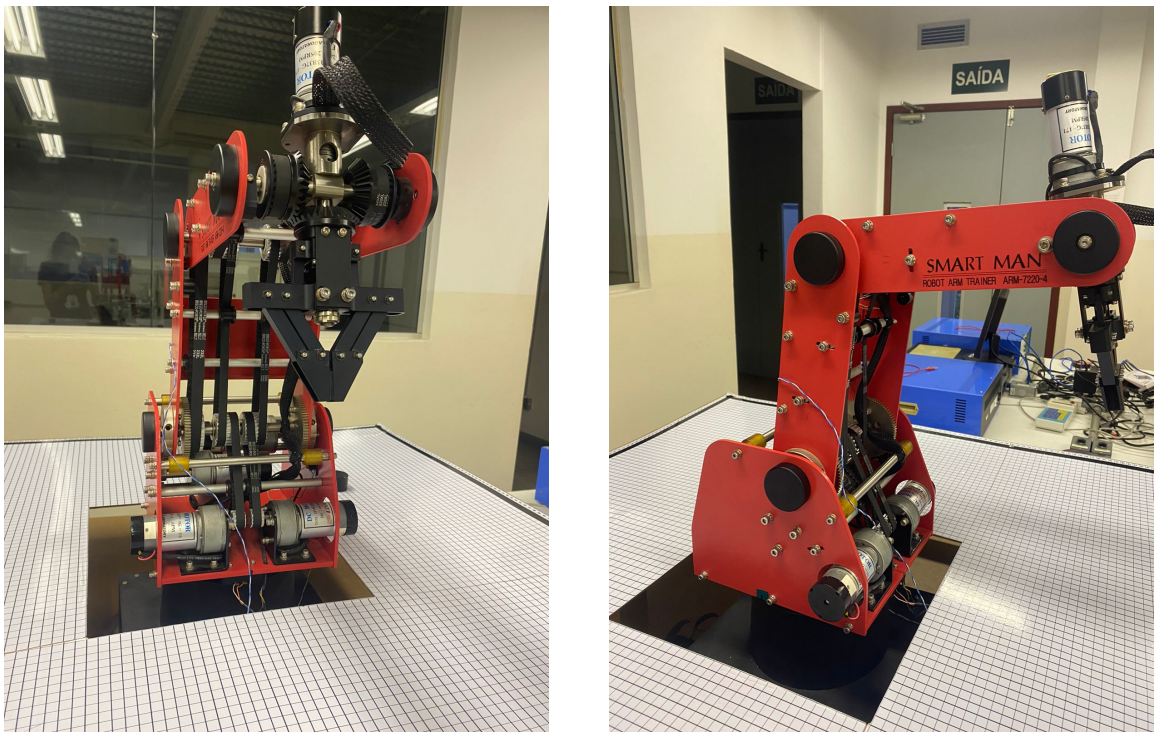

Figura 4 – Braço robótico simulando a Indústria 4.0

2.5 Problemas de Segurança

A evolução tecnológica trouxe mudanças significativas para dentro das organizações industriais. O crescente uso de novas tecnologias trouxeram diversos benefícios de

desempenho, custo, produtividade, dentre outros, mas também trouxe maiores riscos de segurança. Se a evolução continuar tão agressivamente a tendência é que tudo ao nosso redor venha a se tornar inteligente e é aí que deve-se ter em mente as implicações de segurança.

Os novos sistemas que vem surgindo tem por característica serem interconectados, o que tende a aumentar de forma significativa a exposição a muitos riscos de segurança, podendo ter impactos críticos e financeiros. Quem realiza esses ataques tem a intenção de explorar a vulnerabilidade da rede ou do software nos componentes do sistema, fazendo com que se interrompa toda a cadeia de produção por um longo período de tempo, ocasionando até mesmo defeitos fisicamente destrutivos. A Figura 5 ilustra um exemplo de alguns riscos de segurança em um processo de compra online.

Figura 5 – Riscos de segurança em um processo de negócios.

Além desse exemplo, é possível citar também a situação em que um cavalo de tróia é introduzido no painel de um carro, podendo roubar informações pessoais de seus motoristas. Os ataques físicos e ciberataques vem evoluindo com frequência e se tornando ainda mais sofisticados, podendo comprometer alvos críticos e causar problemas graves e globais. As ameaças à segurança enfrentadas pela Indústria 4.0 podem ser exemplificadas em um processo de espionagem cibernética corporativa, uma vez que, em detrimento dos processos de negócios inteligentes e conectados, ela fica mais vulnerável a isso. Existem

grupos organizados de cibercriminosos que tem como alvo hackear indústrias a fim de obter informações sensíveis e de propriedade intelectual. Outro tipo de ataque conhecido como *Distributed Denial of Service* (DDoS) (PEREIRA et. al, 2017) , que consiste em tornar um sistema ou aplicativo indisponível bombardeando o servidor com várias requisições a ponto de consumir todos os recursos do sistema.

Órgãos governamentais em todo o mundo vêm debatendo e defendendo as questões através da cibersegurança, além de desenvolver esforços e recursos significativos para fortalecer essa postura de ciberdefesa (PEREIRA et. al, 2017). Entretanto, encontra-se muita dificuldade para se ter soluções mais concretas e seguras para a proteção dos sistemas.

2.6 Ferramentas Utilizadas

Diante da exposição das empresas a problemas de segurança, os malwares tiveram ainda mais facilidade para explorar essas vulnerabilidades e controlar o acesso a recursos. Sabendo o quão isso pode ser prejudicial para o processo na empresa, iniciou-se um movimento de maior investimento em ferramentas que possam fazer com que esse cenário fique mais seguro. Também foram criadas novas políticas de segurança digital, a fim de que empresas não sofram prejuízos financeiros e judiciais quando seus sistemas são lesados. Com investimentos nessas ferramentas de segurança, uma empresa pode fazer com que sua infraestrutura digital seja mais confiável.

2.6.1 Wireshark

A ferramenta Wireshark (BRITO, 2012) foi um projeto iniciado em 1998 por Gerald Combs e seu desenvolvimento continua até hoje graças às contribuições voluntárias de especialistas por todo o mundo. Com essa ferramenta, é possível analisar protocolos de rede em tempo de execução usando a própria interface de rede do computador. Esse software, além de analisar protocolos, é também utilizado por administradores de rede a fim de detectar problemas e conexões suspeitas, testar se senhas que são usadas na rede estão de fato sendo criptografadas, além de realizar diversas outras atividades referente à segurança.

2.6.2 TCPdump

Assim como também é chamado o tipo do software Wireshark, o TCPdump, conhecido como um *Sniffer* de rede (LARA, 2013), é muito comum em sistemas Unix. Este tem por função capturar pacotes de rede que chegam e saem de alguma interface com o intuito de prover alguma análise. Através dele, é possível a inserção de diversos filtros para captura, podendo ou não usar resolução de nomes/ip, limitar o tamanho da captura e até mesmo exportar para um determinado arquivo essa captura. Tendo esse arquivo em

mãos, tem-se a possibilidade de uma melhor análise através de algum aplicativo gráfico, como por exemplo o Wireshark citado acima, ou algum outro de preferência do usuário.

2.6.3 Nmap

Nmap (NMAP, 2020) é um software livre bem conhecido por realizar a função de *port scanning* (NMAP, 2020). Através dele é possível analisar a segurança dos computadores e também descobrir serviços ou servidores em uma rede de computadores. Além disso, é muito conhecido pela sua rapidez e pela infinidade de opções dispostas. Alguns recursos incluídos no Nmap são: descoberta de hosts, scanner de portas, detecção de versão, detecção do sistema operacional. É também amplamente utilizado para descobrir serviços em sistemas conectados à Internet. Pode também ser usado por administradores de sistema para procurar falhas de segurança.

2.6.4 SSH

O protocolo SSH (*Secure Shell*) (FERREIRA, 2019) é um dos parâmetros de trabalho que garantem que as informações estarão devidamente protegidas. A principal função deste protocolo é permitir tanto aos usuários quanto aos desenvolvedores realizarem quaisquer mudanças em sites e servidores através de uma simples conexão, garantindo que não ocorra nenhuma invasão de arquivos e códigos, por exemplo. Desta forma, usa-se a criptografia para que possa garantir que somente dois pontos acessem determinada informação, que são o servidor e o computador que enviou os dados para tal local remoto. O SSH basicamente fornece um mecanismo de autenticação do usuário remoto, o que garante que esse usuário tenha permissão para se comunicar com o servidor. Dessa forma, é criada uma conexão por meio do protocolo e as informações são transportadas nesse modelo conhecido como secure shell, juntamente com a criptografia que protege os dados.

2.6.5 T50

Criada pelo brasileiro Nelson Brito (TACIO, 2011), cujo nome completo é T50 Sukhoi PAK FA Mixed Packet Injector, essa é mais uma ferramenta hacker que vem sendo manuseada para testes de invasão e estabilidade de uma rede ou sistema e até mesmo com o intuito de derrubar computadores comuns e servidores através de ataques DoS ou DDos, usando o conceito de *stress testing*. Através dessa ferramenta, é possível enviar um alto número de requisições de pacotes, de forma que o foco desse ataque não consiga atender a todas as requisições ou, caso consiga, atende de uma forma bem mais lenta que o normal, fazendo com que esse alvo possa vir a cair ou ficar lento. Com essa ferramenta também se tem a possibilidade de envio de requisições de pacotes de protocolos ICMP, IGMP, TCP e UDP sequencialmente com uma diferença de apenas microssegundos. Outro tipo de emissão de requisições do T50 é, por exemplo, o pacote SYN Flood, onde ele consegue

enviar mais de 1.000.000 de pacotes por segundo em uma rede 1000BASE-T (Gigabit Ethernet) (TACIO, 2011).

2.7 Tipos de Ataques Utilizados

Ataques à segurança da informação, que se tornaram comuns atualmente, são problemas de extrema gravidade para as empresas, uma vez que nessa situação a proteção de todos os dados da empresa se encontram em risco. Para ter um bom desempenho, a segurança da informação precisa se basear em quatro pilares: disponibilidade, integridade, autenticidade e confidencialidade (STEFANINI, 2019).

De maneira geral, o ataque passa por quatro processos: reconhecimento, análise, adaptação e execução (STEFANINI, 2019). A primeira é quando o criminoso vai em busca de alguma brecha no sistema. Após isso, é feito uma análise para que se possa elaborar a melhor forma de ataque. No processo de adaptação, o dispositivo já encontra-se em risco e, por fim, é realmente feito o ataque às informações contidas no sistema da empresa ou até mesmo para influenciar em um processo de manufatura.

2.7.1 Port Scanning Attack

Para que seja possível entender o *Port Scanning Attack* (BACKUP GARANTIDO, 2020), primeiro deve-se enunciar o que é *Port Scan*. De forma simples, *Port Scan* ou *Port Scanning* se dá por um processo que visa achar "portas abertas" em computadores, sendo que essas "portas" são os pontos de acesso ao qual a informação transita no dispositivo. Em um exemplo simples, é como testar a maçaneta de diversos carros para saber qual está trancado e qual está aberto.

No ataque às portas, esse método é utilizado para que seja possível achar pontos fracos e algumas brechas nas quais é possível entrar nos computadores das vítimas. Deste modo, se torna uma prática popular para descobrir serviços que podem ser explorados com o intuito de forçar a entrada em sistemas computacionais. Nesse cenário, dados que são extraídos via *port scanning* são usados para identificar sistemas potencialmente vulneráveis e ganhar acesso às redes desejadas, podendo também ser visado o roubo de dados.

Basicamente, o processo para identificar a vulnerabilidade é através do envio de uma certa mensagem para as portas de acesso, que irão emitir também uma resposta. Através dessa resposta, é possível identificar se a porta está ou não sendo utilizada, além de alguns possíveis pontos de insegurança que podem ser explorados.

Para que se possa proteger dessas ameaças de uma forma eficaz, deve-se investir em um Sistema de Prevenção de Intrusão (IPS) (BACKUP GARANTIDO, 2020) e também em um *firewall*. Essas duas formas são combinadas para se obter uma maior segurança. O

IPS detecta as possíveis *port scans* que estão operando e o *firewall* controla quais podem estar vulneráveis e para quais usuários elas não estarão visíveis.

2.7.2 Ransomware

Este é um tipo de malware que funciona sequestrando o computador de um usuário e fazendo-o de vítima. Através dele, é possível codificar dados do sistema operacional da vítima em segundo plano, sem que ninguém perceba, de forma que o usuário não consiga mais ter acesso. Feito isso, é emitido um pop-up para o usuário exigindo que este pague um determinado valor para obter a chave que permitirá o acesso novamente aos seus dados. Geralmente, esse valor sempre é cobrado usando a moeda virtual bitcoin (CARDOSO, 2017), pois através dela a tarefa de rastrear o criminoso se torna praticamente impossível. São várias as formas como o ransomware pode infectar um computador, como por exemplo, através de sites maliciosos, links suspeitos por e-mail ou através da instalação de aplicativos vulneráveis. Nos dias atuais, a forma mais utilizada para a disseminação desse vírus é através de links enviados por redes sociais.

No Brasil, em 2016 foi descoberto um ransomware pela Kaspersky Lab. Ele basicamente funcionava através da emissão de uma janela que imitava um pedido de atualização do Adobe Flash Player. Ao clicar nessa janela para "atualizar", rapidamente o malware infectava o computador e roubava os dados da vítima. Além disso, foi também descoberto que o valor ao qual os criminosos pediam às vítimas girava em torno de R$2 mil em bitcoin. Naquela época, levando em conta a cotação do bitcoin, 1 bitcoin equivalia a R$1800,00. Em agosto de 2021, 1 bitcoin corresponde a R$252.647,41 (CARDOSO, 2017).

Prevenir desses ataques se tornou um cansativo processo, pois sempre há o surgimento de novos malwares, e, quanto mais se é utilizado redes, mais vulnerável fica o usuário. Algumas empresas de TI procuram soluções específicas para esse tipo de ataque, que é o caso do Bitdefender Anti-Ransomware que foi produzido para permanecer ativo em segundo plano, sendo possível monitorar o sistema operacional de uma máquina, informando ao usuário sobre alguma tentativa de invasão. Muito semelhante a este software há o famoso Malwarebytes Anti-Ransomware.

Eliminar o ransomware é uma tarefa muito difícil, por isso recomenda-se sempre manter o antivírus atualizado e programá-lo para realizar buscas regulares no sistema para encontrar esse tipo de vírus, pois isso torna-se uma medida preventiva. Além disso, as dicas para todos os vírus são sempre válidas, como, não clicar em links de SPAM do e-mail, tomar cuidado com links vindo de redes sociais, atenção ao baixar e instalar programas, cuidado ao entrar em sites maliciosos, etc.

2.7.3 Zero-day

Quando falado em vulnerabilidade em software e sistemas operacionais, uma expressão bastante conhecida é o Zero-day ou 0day. Esse termo geralmente é utilizado quando encontra-se brechas graves de segurança e também quando é identificado hackers explorando essas brechas. Ao ocorrerem falhas do tipo zero-day, trata-se de uma vulnerabilidade de segurança ainda desconhecida do público e dos desenvolvedores do software. Significa dizer que, ao ser encontrada essa falha, o fabricante possui exatamente "zero dias"para desenvolver uma atualização e disponibilizá-la para o público antes que algum hacker tente explorar essa brecha.

De acordo com a forma como as brechas são reconhecidas, é através dela que os hackers exploram a vulnerabilidade. Se essa falha for descoberta por um cibercriminoso, por exemplo, este pode espalhar um vírus durante um tempo indeterminado até ser descoberto. Um outro cenário é quando ao ser descoberta a falha, tanto por usuários quanto por especialistas de segurança, estes avisam os desenvolvedores a respeito do problema que logo já se mobilizam para corrigir essa vulnerabilidade e após isso divulgar ao público. Entretanto, não é possível garantir que todos os usuários daquele software sempre o mantenha atualizado, dando a oportunidade para criminosos tirarem proveito.

Para este tipo de falha não se tem um resposta precisa de como se proteger a ela, pois é uma falha desconhecida. Entretanto, com o antivírus ativo, pode ser possível identificar possíveis malwares nessas brechas e assim reconhecer que existe tal falha.

2.7.4 Ataque de Força Bruta

Dentre os diversos incidentes de segurança realizados no âmbito da Internet, os ataques de força bruta, em que o atacante objetiva adivinhar, por tentativa e erro, logins e senhas de acesso de usuários legítimos de um determinado sistema e/ou serviço de rede, por exemplo, são tidos como uma das principais e mais populares ameaças da atualidade.

Esse cenário de tentativa e erro pode levar muito tempo até que um hacker consiga efetivamente captar logins e senhas, entretanto, para facilitar esse processo, são desenvolvidas ferramentas auxiliares. O ataque mais básico relacionado à força bruta é chamado de ataque de dicionário, é quando um hacker percorre dicionários normais ou especiais e agregam às palavras caracteres especiais e numerais a fim de obter sucesso, entretanto esse tipo de ataque sequencial se torna um pouco complicado, podendo durar até anos. Quando feito através de ferramentas, como Brutus, Medusa, THC Hydra, Aircrack-ng (KASPERSKY, 2021), John the Ripper (PROFISSIONAIS TI, 2020), dentre outros, essas funcionam como protocolos de um computador e assim permitem que hackers acessem modems sem fio, achem senhas fracas, descriptografem essas senhas e as convertam em *leetspeak* - por exemplo, “don’thackme” torna-se “d0n7H4cKm3” - e executem todas

as combinações possíveis de caractere e usem os ataques de dicionário, uma vez que em segundos apareceram as combinações no dicionário. Associações entre CPU e GPU aceleram drasticamente o poder de computação para o descobrimento de senhas. A adição da GPU à CPU pode fazer um computador testar 7.100 senhas por segundo e advinhar a senha em 3,5 dias.

Para que esse tipo de ataque não ocorra, administradores de sistemas devem ao máximo garantir que as senhas dos sistemas desenvolvidos por eles sejam criptografados com altas taxas de criptografia, como por exemplo a de 256 bits. Quando maior a quantidade de bits incorporados na criptografia, maior a segurança da senha e assim, mais difícil de adivinhá-la.

2.7.5 DDoS

Também conhecido como negação distribuída de serviço, este ataque sobrecarrega o alvo com tráfego de Internet indesejado, fazendo com que, o tráfego normal não possa atingir o destino pretendido. Os ataques DDoS exploram redes que possuem dispositivos conectados à internet para fazer com que os usuários sejam cortados do servidor ou do recurso de rede utilizado.

Geralmente, os provedores de ataques DDoS utilizam malwares ou aproveitam a falha de segurança para que consigam infectar e controlar de forma mal-intencionada, máquinas e dispositivos (AKAMAI, 2021). Com o dispositivo infectado, chamado de “bot”, o malware utilizado para infectá-lo consegue se espalhar ainda mais e assim ir infectando um número maior de dispositivos, ampliando o tamanho do ataque.

Quanto mais dispositivos infectados, maior esse exército e maior os ataques. Esse exército é conhecido como “botnets” (AKAMAI, 2021) e faz com que o invasor consiga enviar instruções remotas a cada bot, direcionando o ataque DDoS ao sistema alvo, sendo assim, a organização que foi vítima do ataque continua com inúmeras dificuldades em identificar os invasores.

Quando um botnet ataca uma rede ou um servidor, o invasor instrui os bots individuais a enviar solicitações ao endereço IP da vítima.O resultado desse tráfego esmagador cria uma negação de serviço, impedindo que o tráfego normal acesse o website, a aplicação da Web, a API ou a rede (AKAMAI, 2021).

2.7.6 Cavalo de Troia

Famoso por ser um dos primeiros malwares existentes, desde 1974 nos EUA, o Cavalo de Troia é um programa malicioso que se passa por inofensivo para que consiga fazer com que as pessoas o baixem. Através desse software, criminosos virtuais e hackers tentam obter acesso aos sistemas dos usuários permitindo que eles espionem o usuário, roubem

os dados confidenciais e obtenham acesso ao sistema pela porta de fundo. Diferentes de vírus mais comuns como worms, estes não tem a propriedade de se auto replicar e são classificados de diferentes formas de acordo com sua ação principal.

Além de notebooks e computadores, o cavalo de troia podem também infectar dispositivos móveis. Na sua forma mais geral, ele vem anexado a um programa que aparentemente causa a impressão de legítimo, entretanto é uma versão falsa, carregada com malware e a partir daí ele irá desempenhar uma certa função na máquina. Esse malware pode servir como um espião, que fica aguardando até que o usuário acesse alguma conta online ou insira dados de cartão de crédito para capturar os dados, podem também transformar os computadores em um zumbi fazendo seu computador um escravo dele em uma determinada rede ao qual o criminoso controla, pode ocultar determinados objetos ou atividades do sistema para que ele não seja reconhecido e possa continuar infectando a máquina, dentre outros.

Assim como outros vírus mais comuns, a técnica para evitar este tipo de situação mais eficaz é a instalação de um software antimalware eficiente que detecta e evita estes e outros tipos de ataques.

3 Trabalhos Relacionados

Neste capítulo serão apresentados alguns trabalhos que utilizaram como base a segurança da Indústria 4.0, experimentos de ataques e defesa, e diversas abordagens que convergem ao assunto abordado neste trabalho. É possível observar que o fato de que o mundo está cada vez mais convergindo ao uso ainda maior de equipamentos IoT. Por exemplo, estamos caminhando a evoluções que tendem a levar a indústria a uma maior interconectividade. Sendo assim começamos a ficar vulneráveis e é necessário mecanismos para tentar aumentar a confiabilidade da rede.

Um grupo de pesquisadores de sistemas de manufaturas na era da Indústria 4.0 (CHHETRI et al., 2017) traz uma abordagem a respeito dos problemas de segurança que essas novas tecnologias, quando integradas no ciclo de vida do produto desse tipo de sistema. Essa interconexão pode representar vários desafios para manter os requisitos de segurança, como por exemplo confiabilidade, integridade, e disponibilidade. Essa nova revolução industrial trará diversas mudanças nos sistemas já existentes de manufatura, mudanças essas que são muito positivas. Entretanto, as pesquisas e estudos realizados até hoje para se manter a segurança desse novo ecossistema ainda não são suficientes para que os sistemas não fiquem em vulnerabilidade.

Outra pesquisa, dessa vez com uma aplicação e avaliação de controles de segurança cibernética para sistemas de manufatura digital direta (DDM) (GLAVACH et al., 2017), traz para nós uma temática bem interessante sobre a discussão da segurança aplicado a um experimento. Os sistemas conhecidos como DDM, vem sendo uma tecnologia muito inovadora e que representa avanços tecnológicos de grande importância para a cadeia de suprimentos, bens de consumo e crescimento econômico. No entanto, essa inovação e criação que os sistemas DDM fornecem pode ser fundamental por criar vetores de ataques cibernéticos e assim impulsionar cenários em que se tem impactos negativos potenciais às cadeias de suprimentos. Por ser um sistema muito complexo, com vários sistemas operacionais interconectados, exige uma calibração consistente da rede operante, o que abre brechas para possíveis ataques cibernéticos.

Ismaill Ilhan e Mehmet Karaköse (ILHAN; KARAKÖSE, 2019) fizeram um estudo acerca da estrutura de segurança cibernética para requisitos de reparo, atualização e renovação na indústria 4.0. Eles trazem uma abordagem direta para os sistemas mecânicos que estão presentes nas manufaturas, sistemas esses que com a Indústria 4.0 passam a ser tecnológicos e inteligentes, criando assim uma arquitetura heterogênea. Essa estrutura formada se torna difícil de operar e gerenciar em conjunto, fazendo com que a tarefa de garantir os requisitos mínimos de segurança e conformidade nesses novos sistemas

cibernéticos se torne bem difícil.

Ademais, temos um estudo feito por (MERGENDAHL et al., 2017), traz uma abordagem a respeito da defesa a ataques DDoS em ambientes IoT. Esse tipo de ataque está cada vez mais corriqueiro em equipamentos IoT em grande escala. Sendo assim, o grupo de pesquisadores se reuniu para propor uma solução eficaz para essa situação já que as soluções existentes dificilmente são adequadas em ambientes IoT, uma vez que raramente consideram as restrições de recursos destes dispositivos (MERGENDAHL et al., 2017). Desta forma, o grupo apresenta a solução FR-WARD, essa solução utiliza o mecanismo de retransmissão rápida no controle de congestionamento do TCP para minimizar as penalidades de recursos em dispositivos IoT benignos (MERGENDAHL et al., 2017). Em suas duas funções principais o FR-WARD controla o tráfego DDoS que sai da rede ao qual ele está monitorando e, ao mesmo tempo, deve evitar penalidades no tráfego benigno. Com essa proposta de solução foi possível, através do mecanismo de retransmissão rápida do TCP, garantir que o fluxo de inundação DDoS da rede analisada não ultrapasse um período de tempo desprezível. Além disso, foi possível afirmar também que FR-WARD faz a minimização de penalidades de recursos em dispositivos IoT benignos, uma vez que estes enviam o tráfego a uma taxa mais alta.

Em um trabalho realizado por um grupo de pesquisadores (AZZEDIN et al., 2017), eles exploram o ataque Zero-Day e propõem um novo protótipo para detectar esses tipos de ataques, com base em ativos. A solução é composta de quatro fases, sendo elas a de coleta de informações, monitoramento, decisão e feedback. Na fase de coleta de informações, são identificados ativos críticos e assim é feita a construção de um gráfico de acessibilidade. A fase de monitoramento tem como objetivo garantir que os requisitos de segurança dos ativos críticos não sejam violados. Caso haja tentativa de violação, é necessária uma decisão para lidar com essa tentativa e um feedback é enviado para a camada de segurança. Com esse conceito e realizando testes em um ativo, o grupo pode concluir que, para o ambiente em questão, a proposta seria criar um novo ciclo de vida da segurança, onde o ponto chave é fazer com que os defensores conduzam o jogo da segurança e não os atacantes. Os resultados foram promissores, entretanto, ainda há muito a se discutir sobre se ainda serão feitas mais outros experimentos que darão continuidade ao trabalho.

Tendo em vista os trabalhos relacionados apontados e o trabalho realizado em questão, é possível inferir que, com a evolução constante das tecnologias em manufaturas e a necessidade das indústrias em acompanhar essa revolução, juntamente do desafio das vulnerabilidades na rede internet, a pesquisa se torna importante pela necessidade incessante de uma busca à uma solução realmente eficaz e segura para que a interconexão de equipamentos possa ser feita de forma resoluta. Além disso, os trabalhos apresentados utilizam de muitas ferramentas e ataques robustos, diferente do que foi abordado durante os testes neste projeto, onde o foco foi utilizar de ferramentas simples, acessíveis e não

tão robusta para explorarmos de forma fácil as vulnerabilidades da rede, e assim expor as fragilidades da segurança cibernética.

4 Desenvolvimento

Neste capítulo o intuito é apresentar as questões de segurança abordadas durante o trabalho. Para isso, o desenvolvimento foi estruturado dividindo para cada subseção, o experimento feito com uma ferramenta. Dessa forma é tratado, os experimentos com o Nmap e o T50 em dois cenários diferentes. Em sequência é abordado tudo o que foi utilizado no TCPdump e, por fim, os testes feitos utilizando o SSH.

4.1 Experimentos com o Nmap

Os testes abaixo foram focados em dois cenários, um remoto em redes diferentes usando a internet para comunicação e outro local, conectado na mesma rede. Em cada um destes cenários no braço robótico foram utilizados duas conexões de rede, via rede Wifi e via rede cabeada, enquanto que o computador, utilizando as ferramentas, ficou conectado na rede Wifi.

Para que fosse possível através do computador acessar a placa embarcada pela rede nos dois cenários, foi necessário descobrir o endereço do *Internet Protocol* (IP) (KASPERSKY, 2017) atribuído à ela em ambos os cenários de acordo com o tipo de conexão que estava atribuída a ela no momento.

O endereço IP é um identificador que permite o envio de informações entre dispositivos na rede: ele contém informações de localização e permite que os dispositivos se comuniquem. A Internet precisa de uma maneira de distinguir diferentes computadores, roteadores e sites. Os endereços IP fornecem isso e são uma parte importante do funcionamento da Internet (KASPERSKY, 2017). Sendo assim, é através do endereço que conseguimos testar as ferramentas na placa embarcada.

4.1.1 Cenário 1 - Acesso local

No primeiro cenário de testes, a placa embarcada e o computador estavam na mesma rede na UFOP (Universidade Federal de Ouro Preto). Para realizar os testes, em um primeiro momento a placa embarcada foi cabeada e em um segundo momento a conexão foi via Wifi. Já o computador, sempre se manteve conectado via Wifi. Após isso, foi descoberto o endereço IP para os dois experimentos, sendo eles 200.239.154.172 quando a placa embarcada se encontrava cabeada e 200.239.152.67 quando ela se encontrava conectada via Wifi.

A Figura 6 traz um organograma que simplifica esse primeiro cenário de testes para entendimento.

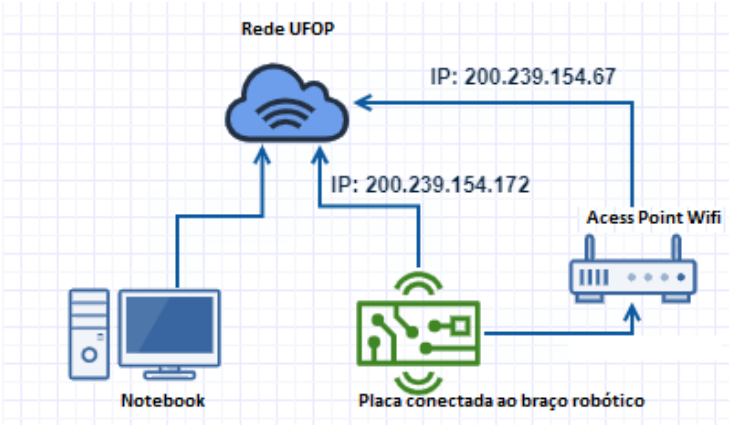

Figura 6 – Cenário 1.

4.1.1.1 Experimentos na rede cabeada

Foi iniciado os testes conectando a placa embarcada BeagleBone Blue na rede cabeada da UFOP para, assim, ser aplicado os comandos das ferramentas utilizadas.

A primeira ferramenta testada foi o Nmap, onde é possível realizar escaneamento de portas e detectar portas vulneráveis para aplicar ataques à aquela rede, impactando assim na Indústria 4.0. Sendo assim, com a busca de portas no IP da placa embarcada, o resultado mostrado na Figura 7.

```
^Croot@flavia:/home/flavia# nmap 200.239.154.172
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 15:23 -03
Nmap scan report for 200.239.154.172
Host is up (0.0045s latency).
Not shown: 978 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  closed pop3
143/tcp  closed imap
161/tcp  closed snmp
389/tcp  closed ldap
443/tcp  closed https
465/tcp  closed smtps
587/tcp  closed submission
636/tcp  closed ldapssl
990/tcp  closed ftps
993/tcp  closed imaps
995/tcp  closed pop3s
3389/tcp closed ms-wbt-server
5000/tcp closed upnp
5222/tcp closed xmpp-client
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.67 seconds
```

Figura 7 – Escaneamento de portas através do Nmap.

Além do escaneamento de portas em si, o Nmap permite fazer a exploração de rede, varredura de segurança e auditoria em um host e/ou rede, para que seja possível descobrir possíveis pontos de vulnerabilidades. Abaixo, uma sequência de comandos feitos através do Nmap, que auxiliam na cibercriminosos a infiltrar em alguma rede e prover um

ataque. Após fazer o escaneamento de portas abertas, mostrado na Figura 7, é possível observar uma infinidade de instruções que podem ser feitas nessas portas. Na figura 8, há a execução de um comando que permite analisar se o alvo escolhido é ou não protegido por um firewall. Nas informações contidas ao executar essa instrução, não há nenhuma restrição quanto ao alvo e que ele possui portas que não estão filtradas, ou seja, a porta está acessível.

```
root@flavia:/home/flavia# nmap -sA 200.239.154.172
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 15:24 -03
Nmap scan report for 200.239.154.172
Host is up (0.0065s latency).
Not shown: 999 filtered ports
PORT   STATE      SERVICE
80/tcp unfiltered http

Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
```

Figura 8 – Comando nmap -sA.

O estado de algumas portas é visto como não filtrado. Além disso, é possível ver a razão ao qual a porta se encontra naquele determinado estado, como mostrado na Figura 9.

```
root@flavia:/home/flavia# nmap --reason 200.239.154.172
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 15:25 -03
Nmap scan report for 200.239.154.172
Host is up, received reset ttl 64 (0.0045s latency).
Not shown: 978 filtered ports
Reason: 978 no-responses
PORT     STATE  SERVICE       REASON
20/tcp   closed ftp-data      reset ttl 63
21/tcp   closed ftp           reset ttl 63
22/tcp   open   ssh           syn-ack ttl 63
23/tcp   closed telnet        reset ttl 63
25/tcp   closed smtp          reset ttl 63
53/tcp   open   domain        syn-ack ttl 63
80/tcp   open   http          syn-ack ttl 64
110/tcp  closed pop3          reset ttl 63
143/tcp  closed imap          reset ttl 63
161/tcp  closed snmp          reset ttl 63
389/tcp  closed ldap          reset ttl 63
443/tcp  closed https         reset ttl 63
465/tcp  closed smtps         reset ttl 63
587/tcp  closed submission    reset ttl 63
636/tcp  closed ldapssl       reset ttl 63
990/tcp  closed ftps          reset ttl 63
993/tcp  closed imaps         reset ttl 63
995/tcp  closed pop3s         reset ttl 63
3389/tcp closed ms-wbt-server reset ttl 63
5000/tcp closed upnp          reset ttl 63
5222/tcp closed xmpp-client   reset ttl 63
8080/tcp open   http-proxy    syn-ack ttl 63

Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

Figura 9 – Comando nmap –reason.

Um outro comando que pode ser utilizado para explorar a segurança de uma porta é o “nmap -sN”. Ele é bem sútil e engana o firewall que possa estar presente na porta para obter uma resposta que possa ser satisfatória a algum ataque. Na figura 10, o estado das portas é visto como *open|filtered*, que é o verdadeiro estado da porta.

```
root@flavia:/home/flavia# nmap -sN 200.239.154.172
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 15:26 -03
Nmap scan report for 200.239.154.172
Host is up (0.0034s latency).
All 1000 scanned ports on 200.239.154.172 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 4.26 seconds
```

Figura 10 – Comando nmap -sN.

Através da ferramenta do Nmap também é possível mostrar pacotes enviados e recebidos por aquele host, semelhante ao que o Wireshark faz. Com essa informação de pacotes, você pode analisar o tráfego dos mesmos, saber se as senhas de determinada aplicação são realmente fortes, conseguir analisar uma possível criptografia.

```
root@flavia:/home/flavia# nmap ---packet-trace 200.239.154.172
nmap: unrecognized option '---packet-trace'
See the output of nmap -h for a summary of options.
root@flavia:/home/flavia# nmap --packet-trace 200.239.154.172
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 15:29 -03
SENT (0.0759s) ICMP [192.168.0.72 > 200.239.154.172 Echo request (type=8/code=0) id=29245 seq=0] IP [ttl=37 id=49079 iplen=28 ]
SENT (0.0760s) TCP 192.168.0.72:39060 > 200.239.154.172:443 S ttl=43 id=28660 iplen=44  seq=3180379387 win=1024 <mss 1460>
SENT (0.0760s) TCP 192.168.0.72:39060 > 200.239.154.172:80 A ttl=49 id=4634 iplen=40  seq=0 win=1024
SENT (0.0760s) ICMP [192.168.0.72 > 200.239.154.172 Timestamp request (type=13/code=0) id=4095 seq=0 orig=0 recv=0 trans=0] IP [ttl=44 id=3753
1 iplen=40 ]
RCVD (0.0799s) TCP 200.239.154.172:80 > 192.168.0.72:39060 R ttl=64 id=0 iplen=40  seq=3180379387 win=0
NSOCK INFO [0.1430s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1430s] nsock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.1430s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
NSOCK INFO [0.1430s] nsock_write(): Write request for 46 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.1430s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.1430s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [0.1790s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [127.0.0.53:53] (46 bytes): .$...........172.154.239.20
0.in-addr.arpa.....
NSOCK INFO [0.1790s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 34
NSOCK INFO [0.1790s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1790s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.2322s) TCP 192.168.0.72:39316 > 200.239.154.172:1720 S ttl=44 id=63948 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2323s) TCP 192.168.0.72:39316 > 200.239.154.172:554 S ttl=43 id=39577 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2323s) TCP 192.168.0.72:39316 > 200.239.154.172:1025 S ttl=42 id=60455 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2323s) TCP 192.168.0.72:39316 > 200.239.154.172:22 S ttl=42 id=23737 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2324s) TCP 192.168.0.72:39316 > 200.239.154.172:1723 S ttl=38 id=14818 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2324s) TCP 192.168.0.72:39316 > 200.239.154.172:80 S ttl=59 id=24740 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2324s) TCP 192.168.0.72:39316 > 200.239.154.172:110 S ttl=37 id=26343 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2324s) TCP 192.168.0.72:39316 > 200.239.154.172:8080 S ttl=58 id=44605 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2325s) TCP 192.168.0.72:39316 > 200.239.154.172:5900 S ttl=55 id=62911 iplen=44  seq=2284145962 win=1024 <mss 1460>
SENT (0.2325s) TCP 192.168.0.72:39316 > 200.239.154.172:199 S ttl=48 id=5461 iplen=44  seq=2284145962 win=1024 <mss 1460>
RCVD (0.2362s) TCP 200.239.154.172:80 > 192.168.0.72:39316 SA ttl=64 id=0 iplen=44  seq=2283642217 win=65228 <mss 1460>
RCVD (0.2362s) TCP 200.239.154.172:22 > 192.168.0.72:39316 SA ttl=63 id=0 iplen=44  seq=2773500641 win=29200 <mss 1460>
RCVD (0.2382s) TCP 200.239.154.172:110 > 192.168.0.72:39316 RA ttl=63 id=0 iplen=40  seq=0 win=0
RCVD (0.2383s) TCP 200.239.154.172:8080 > 192.168.0.72:39316 SA ttl=63 id=0 iplen=44  seq=2530679120 win=29200 <mss 1460>
```

Figura 11 – Comando nmap –packet-trace.

Esses são comandos usados de forma mais geral em um determinado host. Existe a possibilidade de previamente escolher uma porta e realizar instruções sobre ela. Abaixo, na Figura 12, é feito o *scan* nas portas 22 e 53, que são umas das portas em estado aberto, como mostrado na Figura 9.

```
root@flavia:/home/flavia# nmap -p 53 200.239.154.172
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 15:32 -03
Nmap scan report for 200.239.154.172
Host is up (0.0034s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@flavia:/home/flavia# nmap -p 22 200.239.154.172
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 15:32 -03
Nmap scan report for 200.239.154.172
Host is up (0.0038s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Figura 12 – Comando nmap -p.

Todos esses testes estão sendo feitos sob uma placa embarcada BeagleBone Blue, e é comum que essas placas venham com sistemas operacionais integrados. Na Figura 13, é realizado a execução de uma instrução que retorna uma resposta se há ou não um sistema operacional remoto.

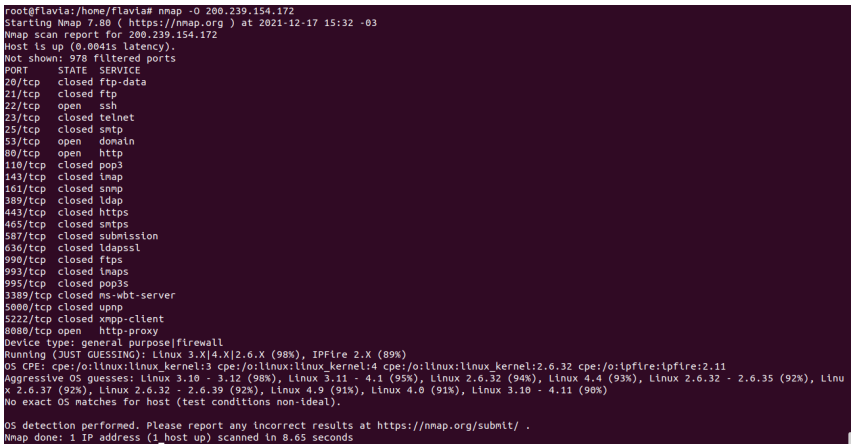

Figura 13 – Comando nmap -O.

Esse comando encontra um SO remoto e ainda fornece algumas informações sobre o SO que está inserido no host. Além disso, é possível detectar também alguns outros serviços remotos integrados à aquele host, mostrado na Figura 14.

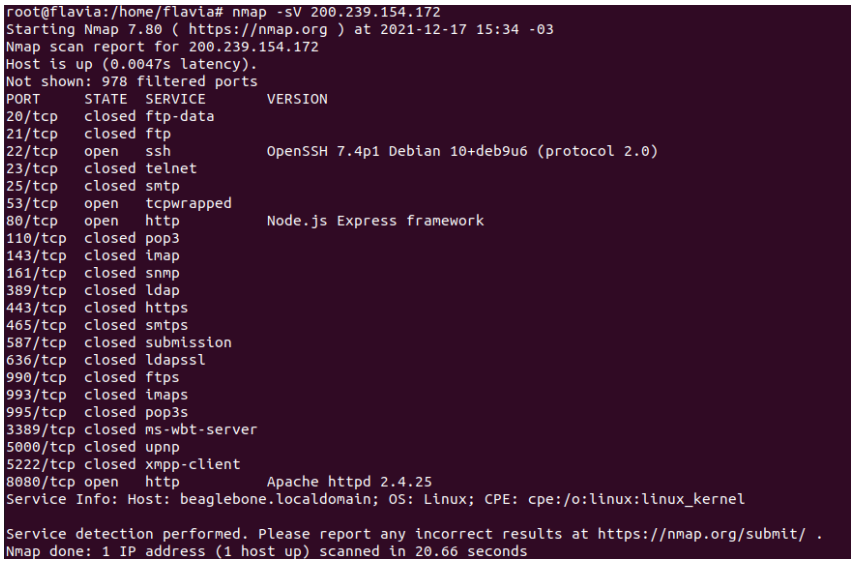

Figura 14 – Comando nmap -sV.

4.1.1.2 Experimentos na rede Wifi

Após realizado os testes com a placa embarcada conectada via rede cabeada, foi iniciado os testes onde conectou-se a placa embarcada a rede Wifi, para testar as vulnerabilidades através da rede. Foi realizado os mesmos teste feitos com a placa embarcada conectada via rede cabeada.

Na Figura 15, com o uso do comando nmap assim como na placa embarcada conectada via rede cabeada, foi mostrado as portas e seus respectivos estados. É possível observar uma diminuição do número de portas escaneadas e o surgimento de uma porta em estado aberto diferente de antes, que é a porta 3000.

```
root@flavia:/home/flavia# nmap 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:45 -03
Nmap scan report for 200.239.152.67
Host is up (0.056s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
3000/tcp open  ppp
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.05 seconds
```

Figura 15 – Comando nmap.

Com o comando do nmap -sA, demonstrado na Figura 16, existe um número bem maior de portas *unfiltered* do que antes.

```
root@flavia:/home/flavia# nmap -sA 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:46 -03
Nmap scan report for 200.239.152.67
Host is up (0.14s latency).
All 1000 scanned ports on 200.239.152.67 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
```

Figura 16 – Comando nmap -sA.

Na Figura 17, a única diferença para quando os testes estavam sendo feitos via rede cabeada é a quantidade de portas que o comando nmap –reason retorna.

```
root@flavia:/home/flavia# nmap --reason 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:46 -03
Nmap scan report for 200.239.152.67
Host is up, received echo-reply ttl 64 (0.025s latency).
Not shown: 995 closed ports
Reason: 995 resets
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 64
53/tcp   open  domain     syn-ack ttl 64
80/tcp   open  http       syn-ack ttl 64
3000/tcp open  ppp        syn-ack ttl 64
8080/tcp open  http-proxy syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 3.46 seconds
```

Figura 17 – Comando nmap –reason.

Na Figura 18, diferente de quando a placa embarcada estava via rede cabeada, apenas 4 portas foram classificadas como open|filtered. Antes o número de portas nesse estado foi de 1000.

```
root@flavia:/home/flavia# nmap -sN 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:47 -03
Nmap scan report for 200.239.152.67
Host is up (0.017s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
80/tcp   open|filtered http
3000/tcp open|filtered ppp
8080/tcp open|filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.75 seconds
```

Figura 18 – Comando nmap -sN.

Para o comando nmap –packet-trace, na Figura 19, apesar da placa embarcada estar em um ambiente de conexão diferente, os resultados não foram alterados.

```
root@flavia:/home/flavia# nmap --packet-trace 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:47 -03
SENT (0.0847s) ICMP [192.168.8.83 > 200.239.152.67 Echo request (type=8/code=0) id=1576 seq=0] IP [ttl=42 id=43613 iplen=28 ]
SENT (0.0848s) TCP 192.168.8.83:36753 > 200.239.152.67:443 S ttl=47 id=41607 iplen=44  seq=2399328120 win=1024 <mss 1460>
SENT (0.0848s) TCP 192.168.8.83:36753 > 200.239.152.67:80 A ttl=45 id=43806 iplen=40  seq=0 win=1024
SENT (0.0848s) ICMP [192.168.8.83 > 200.239.152.67 Timestamp request (type=13/code=0) id=46729 seq=0 orig=0 recv=0 trans=0] IP [ttl=51 id=2015
 iplen=40 ]
RCVD (0.1028s) ICMP [200.239.152.67 > 192.168.8.83 Echo reply (type=0/code=0) id=1576 seq=0] IP [ttl=64 id=34317 iplen=28 ]
NSOCK INFO [0.1600s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1600s] nsock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.1600s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
NSOCK INFO [0.1600s] nsock_write(): Write request for 45 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.1600s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.1600s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [0.1640s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [127.0.0.53:53] (45 bytes): .............67.152.239.200
.in-addr.arpa.....
NSOCK INFO [0.1640s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 34
NSOCK INFO [0.1640s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1640s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.2330s) TCP 192.168.8.83:37009 > 200.239.152.67:995 S ttl=58 id=13960 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2331s) TCP 192.168.8.83:37009 > 200.239.152.67:3389 S ttl=56 id=34125 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2331s) TCP 192.168.8.83:37009 > 200.239.152.67:111 S ttl=52 id=54442 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2331s) TCP 192.168.8.83:37009 > 200.239.152.67:993 S ttl=56 id=23485 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2332s) TCP 192.168.8.83:37009 > 200.239.152.67:445 S ttl=51 id=39109 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2332s) TCP 192.168.8.83:37009 > 200.239.152.67:22 S ttl=43 id=21456 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2332s) TCP 192.168.8.83:37009 > 200.239.152.67:113 S ttl=41 id=49191 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2333s) TCP 192.168.8.83:37009 > 200.239.152.67:139 S ttl=37 id=21928 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2333s) TCP 192.168.8.83:37009 > 200.239.152.67:8888 S ttl=54 id=8540 iplen=44  seq=1403823117 win=1024 <mss 1460>
SENT (0.2333s) TCP 192.168.8.83:37009 > 200.239.152.67:199 S ttl=43 id=40142 iplen=44  seq=1403823117 win=1024 <mss 1460>
RCVD (0.2438s) TCP 200.239.152.67:995 > 192.168.8.83:37009 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2454s) TCP 200.239.152.67:3389 > 192.168.8.83:37009 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2455s) TCP 200.239.152.67:111 > 192.168.8.83:37009 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2457s) TCP 200.239.152.67:993 > 192.168.8.83:37009 RA ttl=64 id=0 iplen=40  seq=0 win=0
```

Figura 19 – Comando nmap –packet-trace.

Quando feito o comando nmap -p, na Figura 20, o resultado apenas diferenciou no número da porta ao qual o comando estava sendo utilizado, não tendo influência nos resultados.

```
root@flavia:/home/flavia# nmap -p 22 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:48 -03
Nmap scan report for 200.239.152.67
Host is up (0.0067s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@flavia:/home/flavia# nmap -p 53 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:48 -03
Nmap scan report for 200.239.152.67
Host is up (0.19s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

Figura 20 – Comando nmap -p.

Por fim, para o comando nmap -O, a diferença demonstrada na Figura 21, é um número de portas menor do que o mostrado quando a placa embarcada estava conectada via rede cabeada.

```
root@flavia:/home/flavia# nmap -O 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-17 17:49 -03
Nmap scan report for 200.239.152.67
Host is up (0.014s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
3000/tcp open  ppp
8080/tcp open  http-proxy
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds
```

Figura 21 – Comando nmap -O.

4.1.2 Cenário 2 - Acesso Remoto

Nesse segundo cenário abordado, assim como no cenário 1, a placa embarcada ficou conectada via cabo em um primeiro momento, em seguida via Wifi, sempre na rede da UFOP. Enquanto o computador com as ferramentas estava conectado em outra rede Wifi, em uma cidade diferente.

Quando a rede estava conectada via cabo, descobrimos que o IP atrelado a ela foi o de 200.239.152.66 e 200.239.152.67 quando conectada via Wifi. Com essa informação, foi possível realizar os mesmos testes de segurança anteriormente feitos e analisar as vulnerabilidades. Na Figura 22, esse cenário é simplificado através de um organograma para entendimento.

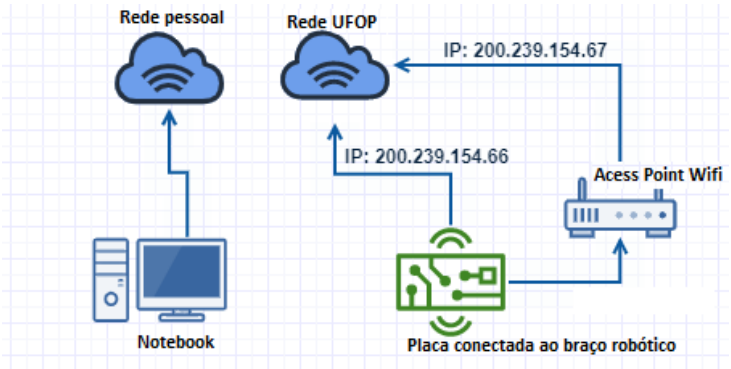

Figura 22 – Cenário 2.

4.1.2.1 Experimentos na rede cabeada

Ao realizar todos os testes com a placa embarcada conectada via rede cabeada, em uma rede diferente da que a do notebook que possui as ferramentas utilizadas, foi possível inferir que o comportamento dos comandos aplicados ao novo endereço IP nos retornaram os mesmos resultados de quando a placa embarcada foi conectada via Wifi utilizando a mesma rede, ou seja, apesar da mudança de ambiente, o comportamento dos resultados não modificaram. Isso pode ser concluído analisando as Figuras 23 a 29, onde é possível observar as mesmas saídas dos comandos aplicados.

```
root@flavia:/home/flavia# nmap 200.239.152.66
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 09:32 -03
Nmap scan report for 200.239.152.66
Host is up (0.021s latency).
Not shown: 929 filtered ports, 67 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.07 seconds
```

Figura 23 – Comando nmap.

```
root@flavia:/home/flavia# nmap -sA 200.239.152.66
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 09:33 -03
Nmap scan report for 200.239.152.66
Host is up (0.029s latency).
All 1000 scanned ports on 200.239.152.66 are filtered

Nmap done: 1 IP address (1 host up) scanned in 30.64 seconds
```

Figura 24 – Comando nmap -sA.

```
root@flavia:/home/flavia# nmap --reason 200.239.152.66
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 09:34 -03
Nmap scan report for 200.239.152.66
Host is up, received echo-reply ttl 50 (0.024s latency).
Not shown: 929 filtered ports, 67 closed ports
Reason: 929 no-responses and 67 resets
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 50
80/tcp   open  http       syn-ack ttl 50
3000/tcp open  ppp        syn-ack ttl 50
8080/tcp open  http-proxy syn-ack ttl 50

Nmap done: 1 IP address (1 host up) scanned in 4.00 seconds
```

Figura 25 – Comando nmap –reason.

```
root@flavia:/home/flavia# nmap -sN 200.239.152.66
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 09:35 -03
Nmap scan report for 200.239.152.66
Host is up (0.022s latency).
All 1000 scanned ports on 200.239.152.66 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 23.59 seconds
```

Figura 26 – Comando nmap -sN.

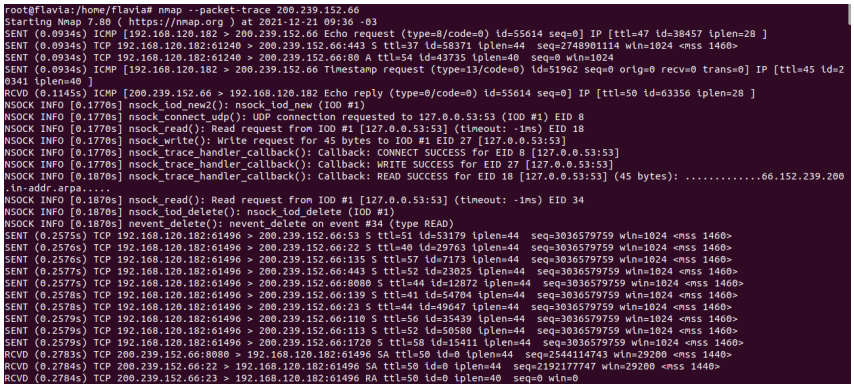

Figura 27 – Comando nmap -packet-trace.

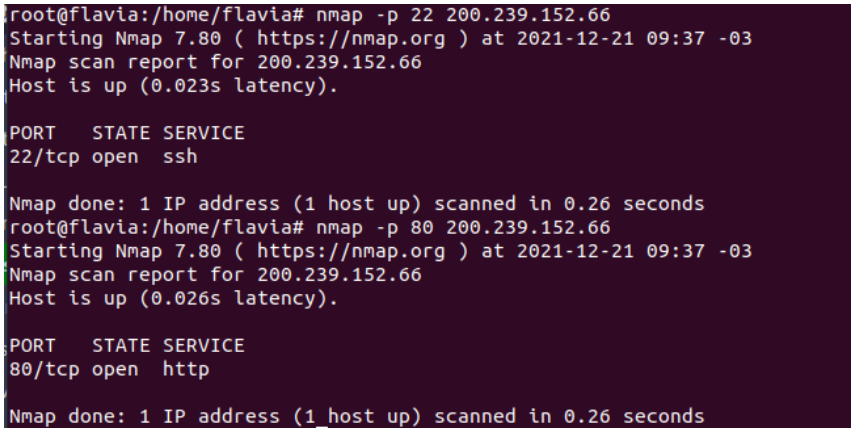

Figura 28 – Comando nmap -p.

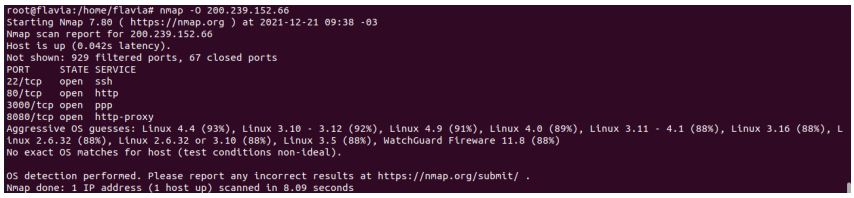

Figura 29 – Comando nmap -O.

4.1.2.2 Experimentos na rede Wifi

Ao término da utilização da ferramenta Nmap, com a placa embarcada conectada via Wifi em uma rede diferente da que o notebook estava conectado também foi analisado o mesmo comportamento de quando a placa embarcada estava em redes diferentes conectada via rede cabeada. Para concluir isso, as Figuras 30 a 36 retratam os resultados dos comandos aplicados.

```
root@flavia:/home/flavia# nmap 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 09:57 -03
Nmap scan report for 200.239.152.67
Host is up (0.12s latency).
Not shown: 929 filtered ports, 67 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 22.71 seconds
```

Figura 30 – Comando nmap.

```
root@flavia:/home/flavia# nmap -sA 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 09:58 -03
Nmap scan report for 200.239.152.67
Host is up (0.022s latency).
All 1000 scanned ports on 200.239.152.67 are filtered

Nmap done: 1 IP address (1 host up) scanned in 23.84 seconds
```

Figura 31 – Comando nmap -sA.

```
root@flavia:/home/flavia# nmap --reason 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 09:59 -03
Nmap scan report for 200.239.152.67
Host is up, received echo-reply ttl 50 (0.081s latency).
Not shown: 929 filtered ports, 67 closed ports
Reason: 929 no-responses and 67 resets
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 50
80/tcp   open  http       syn-ack ttl 50
3000/tcp open  ppp        syn-ack ttl 50
8080/tcp open  http-proxy syn-ack ttl 50

Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
```

Figura 32 – Comando nmap –reason.

```
root@flavia:/home/flavia# nmap -sN 200.239.152.67
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 10:00 -03
Nmap scan report for 200.239.152.67
Host is up (0.17s latency).
All 1000 scanned ports on 200.239.152.67 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 174.46 seconds
```

Figura 33 – Comando nmap -sN.

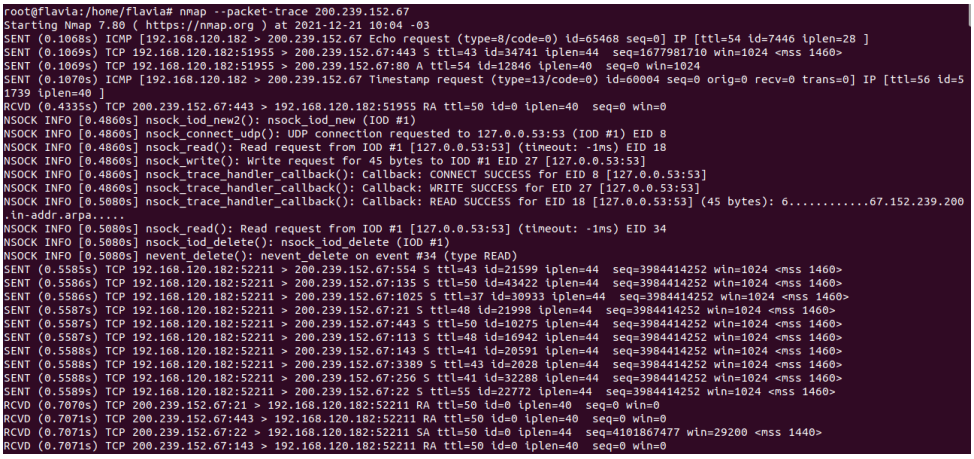

Figura 34 – Comando nmap –packet-trace.

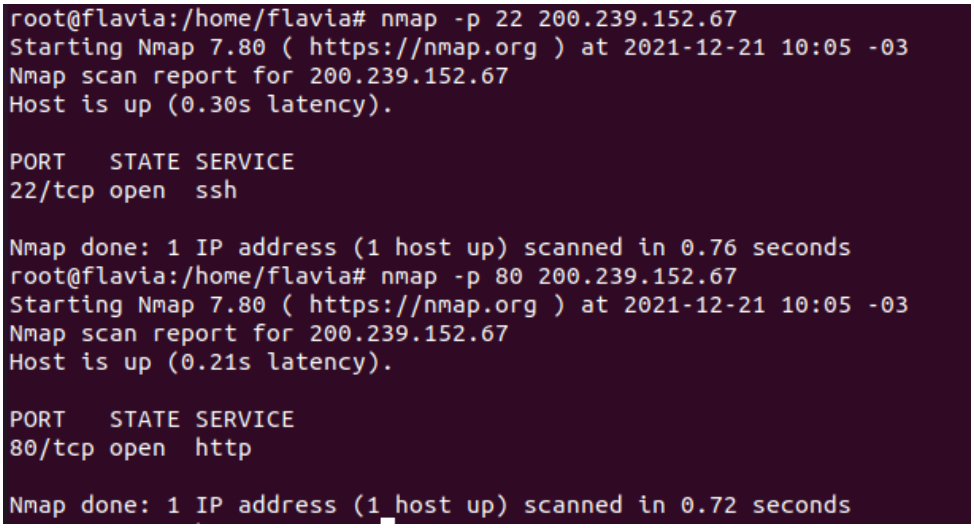

Figura 35 – Comando nmap -p.

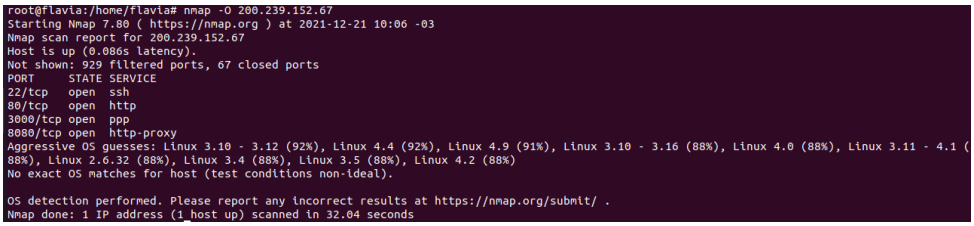

Figura 36 – Comando nmap -O.

4.2 Experimentos com o T50

Além do Nmap, também foi analisado a latência do tráfego de pacotes antes e durante comandos T50 que representam ataques DDoS, onde cibercriminosos tentam inundar a rede com diversas requisições e assim fazer com que o sistema fique sobrecarregado.

A análise de latência foi feita com o comando PING durante 1 minuto sem o comando T50. Posteriormente, foi realizado novamente o comando PING durante 1 minuto, porém no segundo 15 foi aplicado o comando T50 que funciona como um ataque DDoS.

4.2.1 Cenário 1 - Acesso local

O cenário utilizado para realizar os testes com a ferramenta T50 é o mesmo exemplificado na Figura 6.

A Tabela 1 traz os valores obtidos durante o experimento. Com a placa embarcada conectada via rede cabeada a latência média foi de 6,8 ms. Após isso aplicando o comando T50 o valor de 34,34 ms, o que representa um aumento de 27,54 ms em relação a latência sem o comando T50. Com a placa embarcada conectada via rede Wifi, tem-se uma latência de 21,58 ms, o que nos dá uma diferença de 14,78 ms em relação a latência obtida na placa embarcada via rede cabeada. Após isso, aplicando o comando T50, a latência passou a ser de 743,24 ms, uma diferença de 708,9 ms em relação a latência obtida com o comando T50 na placa embarcada conectada via rede cabeada e de 721,66 ms em relação a placa embarcada conectada via Wifi sem o comando T50.

	Experimento rede cabeada	**Experimento rede Wifi**
Ping	6,8 ms	21,58 ms
Ping com comando T50	34,34 ms	743,24 ms

Tabela 1 – Latência dos experimentos do cenário 1

4.2.2 Cenário 2 - Acesso Remoto

O cenário utilizado para realizar os testes com a ferramenta T50 é o mesmo exemplificado na Figura 22.

Na análise da latência no cenário 2, a Tabela 2 traz os resultados dos valores obtidos. Uma latência média de 24,23 ms com a placa embarcada cabeada. E um valor de 47,28 ms com o comando T50. O que nos dá uma diferença de 23,05 ms em relação a média anterior. No experimento via Wifi, primeiro foi obtido uma latência média no valor de 146,53 ms, o que representa 122,30 ms em relação a latência na placa embarcada conectada via cabo sem o comando T50, e de 99,25 ms em relação a rede Wifi local. Aplicando o comando T50, a latência média obtida foi de 202,81 ms, uma diferença de 155,23 ms relação à latência média obtida com o comando T50 com a placa embarcada conectada via rede cabeada e de 56,28 ms em relação ao obtido sem o comando T50.

	Experimento rede cabeada	**Experimento rede Wifi**
Ping	24,23 ms	146,53 ms
Ping com comando T50	47,28 ms	202,81 ms

Tabela 2 – Latência dos experimentos do cenário 2

Para sumarizar as médias obtidas durante os testes de latências segue a Tabela 9 abaixo:

	S/ T50	**C/T50**
Cenário 1	28,38 ms	777,58 ms
Cenário 2	170,76 ms	250,09 ms
Latência média	99,57 ms	513,83 ms

Tabela 3 – Média das latências obtidas.

4.3 Experimento com o TCPdump

Após realizar os testes que dependem dos cenários apresentados anteriormente, foi a vez de utilizar a ferramenta do TCPdump para realizar as análises de tráfego de pacotes que entram e saem da placa embarcada. Para isso, foi capturado os logs da utilização da ferramenta.

Na Figura 41, é possível observar uma amostra da saída do log obtido:

```
00:29:27.003970 IP (tos 0x10, ttl 64, id 15138, offset 0, flags [DF], proto TCP (6), length 96)
    200.239.152.66.ssh > 200-71-65-17.internetsuper.com.br.50898: Flags [P.], cksum 0x6add
00:29:27.004794 IP (tos 0x10, ttl 64, id 15139, offset 0, flags [DF], proto TCP (6), length 160)
    200.239.152.66.ssh > 200-71-65-17.internetsuper.com.br.50898: Flags [P.], cksum 0x6b1d
00:29:27.005182 IP (tos 0x10, ttl 64, id 15140, offset 0, flags [DF], proto TCP (6), length 88)
    200.239.152.66.ssh > 200-71-65-17.internetsuper.com.br.50898: Flags [P.], cksum 0x6ad5
00:29:27.033154 IP (tos 0x0, ttl 51, id 62782, offset 0, flags [DF], proto TCP (6), length 52)
    200-71-65-17.internetsuper.com.br.50898 > 200.239.152.66.ssh: Flags [.], cksum 0xcc1b
00:29:27.033322 IP (tos 0x0, ttl 51, id 62783, offset 0, flags [DF], proto TCP (6), length 52)
    200-71-65-17.internetsuper.com.br.50898 > 200.239.152.66.ssh: Flags [.], cksum 0xcbad
00:29:27.033353 IP (tos 0x0, ttl 51, id 62784, offset 0, flags [DF], proto TCP (6), length 52)
    200-71-65-17.internetsuper.com.br.50898 > 200.239.152.66.ssh: Flags [.], cksum 0xcb89
00:29:27.037377 IP (tos 0x0, ttl 64, id 58479, offset 0, flags [DF], proto UDP (17), length 74)
    200.239.152.66.57890 > 200.239.152.120.domain: [bad udp cksum 0xc2e1 -> 0xee69!] 32067+
00:29:27.065878 IP (tos 0x0, ttl 64, id 28126, offset 0, flags [DF], proto UDP (17), length 74)
    200.239.152.120.domain > 200.239.152.66.57890: [udp sum ok] 32067 NXDomain$ q: PTR?
00:29:27.067029 IP (tos 0x0, ttl 64, id 58484, offset 0, flags [DF], proto UDP (17), length 73)
    200.239.152.66.40461 > 200.239.152.120.domain: [bad udp cksum 0xc2e0 -> 0xaa70!] 16711+
00:29:27.068506 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 44)
    200.239.152.67.ssh > host-5-58-49-173.bitternet.ua.44712: Flags [S.], cksum 0x9838 (incorrect ->
00:29:27.094010 IP (tos 0x0, ttl 239, id 54321, offset 0, flags [none], proto TCP (6), length 40)
    zg-1117b-196.stretchoid.com.59271 > 200.239.153.82.45000: Flags [S], cksum 0x4d57 (correct),
```

Figura 37 – Log da ferramenta TCPdump.

Com as informações contidas a respeito de cada pacote, fica fácil para que um cibercriminoso consiga explorar alguma vulnerabilidade para assim infiltrar no dispositivo que será atacado.

É possível analisar a presença de dois protocolos diferentes, o TCP e o UDP. Já que o atacante terá conhecimento de que o host destino está recebendo pacotes do protocolo TCP, por exemplo, ele pode realizar um ataque de *SYN Flood* (Inundação SYN) (AMIM SAB; FERREIRA; ROZENDO, 2019). Nesse tipo de ataque, o invasor inunda a rede com pacotes TCP SYN, geralmente com um endereço IP de origem oculto. Cada um desses pacotes representa uma intenção de conexão, o que faz com que o servidor de destino aloque uma certa quantidade de memória para cada um deles para criar uma nova conexão e enviar de volta um pacote TCP SYN-ACK, que aguarda uma nova resposta (TCP ACK) , ele permitirá efetivamente que uma nova conexão seja estabelecida. Como o originador nunca enviará o pacote ACK esperado, quando a memória do servidor estiver totalmente alocada, as solicitações de conexão legítimas serão impedidas de serem atendidas até que o ataque termine. Além disso, algumas das conexões resultantes permitem que invasores acessem arquivos do servidor.

Assim como o TCP, o UDP também pode servir como uma porta para cibercriminosos realizarem ataques. Esse protocolo, da mesma forma que o TCP, utiliza portas para a comunicação. Sendo assim, um hacker pode, primeiramente, fazer uma verificação de portas que podem vir a estar abertas e assim aptas para receber comunicação. Após isso, sabendo que um host destino aceita protocolos UDP, uma vulnerabilidade pode ser explorada com o ataque *IP Spoofing* (CBPF, 2021), que envolve a alteração do IP do host de origem para outro. Isso geralmente é usado para proteger a identidade de hackers. Portanto, uma máquina espera dados de uma certa máquina, mas na verdade está recebendo dados de outra.

4.4 Experimento com o SSH

Para o experimento com o SSH, assim como no TCPdump, foram obtidos os logs com as tentativas de acesso SSH do ataque backtracking. Nesse estudo, o ataque backtracking ou ataque de força bruta, foi feito através da tentativa de descobrir senhas de usuários do sistema, ou seja, sempre que algum usuário tentava acessar a placa embarcada eram disparados comandos de força bruta para encontrar a senha do mesmo.

Sendo assim, de acordo com o log obtido no período de 17/12/2021 a 23/12/2021, totalizando 7 dias e um total de 6577 tentativas de localizar as senhas desses usuários. Na Figura 42, há um exemplo das saídas do log.

```
Dec 17 00:38:23 beaglebone sshd[1152]: Failed password for root from 192.168.8.125 port 56294 ssh2
Dec 17 00:38:34 beaglebone sshd[1152]: Failed password for root from 192.168.8.125 port 56294 ssh2
Dec 17 00:38:49 beaglebone sshd[1152]: Failed password for root from 192.168.8.125 port 56294 ssh2
Dec 17 00:38:59 beaglebone sshd[1154]: Failed password for root from 192.168.8.125 port 56296 ssh2
Dec 17 00:39:09 beaglebone sshd[1156]: Failed password for debian from 192.168.8.125 port 56298 ssh2
Dec 17 00:39:16 beaglebone sshd[1156]: Failed password for debian from 192.168.8.125 port 56298 ssh2
Dec 17 00:39:20 beaglebone sshd[1156]: Failed password for debian from 192.168.8.125 port 56298 ssh2
Dec 17 00:39:28 beaglebone sshd[1158]: Failed password for root from 192.168.8.125 port 56300 ssh2
Dec 17 00:39:47 beaglebone sshd[1158]: Failed password for root from 192.168.8.125 port 56300 ssh2
Dec 17 00:39:50 beaglebone sshd[1158]: Failed password for root from 192.168.8.125 port 56300 ssh2
Dec 17 00:39:57 beaglebone sshd[1160]: Failed password for root from 192.168.8.125 port 56302 ssh2
Dec 17 00:40:10 beaglebone sshd[1160]: Failed password for root from 192.168.8.125 port 56302 ssh2
Dec 17 00:40:15 beaglebone sshd[1162]: Failed password for root from 192.168.8.125 port 56304 ssh2
Dec 17 00:40:35 beaglebone sshd[1164]: Failed password for root from 192.168.8.125 port 56310 ssh2
Dec 17 00:40:44 beaglebone sshd[1164]: Failed password for root from 192.168.8.125 port 56310 ssh2
Dec 17 00:40:55 beaglebone sshd[1164]: Failed password for root from 192.168.8.125 port 56310 ssh2
Dec 17 00:47:41 beaglebone sshd[1182]: Failed password for root from 192.168.8.125 port 56468 ssh2
Dec 17 00:47:55 beaglebone sshd[1182]: Failed password for root from 192.168.8.125 port 56468 ssh2
Dec 17 00:48:07 beaglebone sshd[1184]: Failed password for debian from 192.168.8.125 port 56470 ssh2
Dec 17 00:48:56 beaglebone sshd[1184]: Failed password for debian from 192.168.8.125 port 56470 ssh2
Dec 17 00:49:04 beaglebone sshd[1184]: Failed password for debian from 192.168.8.125 port 56470 ssh2
Dec 17 00:49:19 beaglebone sshd[1187]: Failed password for root from 192.168.8.125 port 56538 ssh2
```

Figura 38 – Log de acesso do SSH.

Com os logs de tentativas em mãos, foi possível obter os usuários que mais tentaram acessar a placa embarcada. Foi um total de 465 usuários diferentes. Para um melhor direcionamento, foi elaborado um gráfico com os 10 usuários mais utilizados. O gráfico é mostrado na Figura 43.

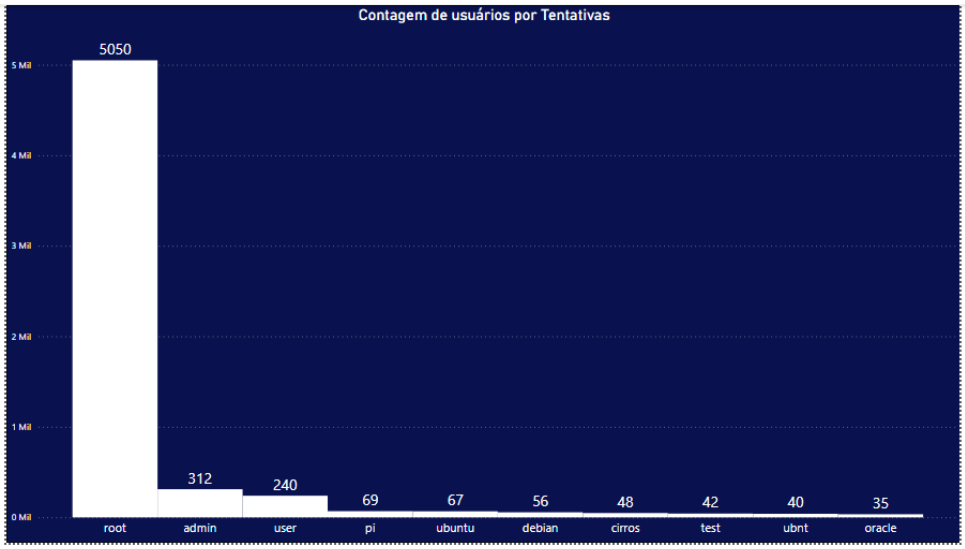

Figura 39 – 10 usuários mais utilizados.

Com os logs de captura de tentativas, foi acessado o arquivo shadow que contém as informações das senhas criptografadas dos usuários daquele sistema. A Figura 44, traz as características dos usuários contidos na placa embarcada.

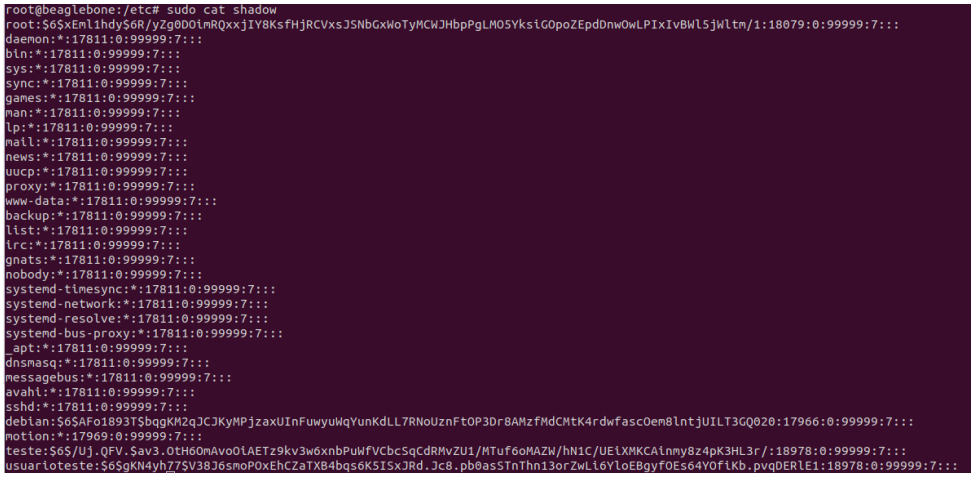

Figura 40 – Características dos usuários.

Feito isso, as informações presentes na Figura 44 foram copiadas e coladas em um arquivo de texto na máquina que contém as ferramentas utilizadas e, com a ferramenta do John The Ripper foi feita a quebra das senhas dos usuários.

Essa ferramenta funciona de forma semelhante às ferramentas utilizadas no log de tentativas de acesso, uma vez que, elas fazem uso do ataque de força bruta para determinado fim. Sendo assim, foi repetido todo o passo a passo desse ataque para descoberta de senhas.

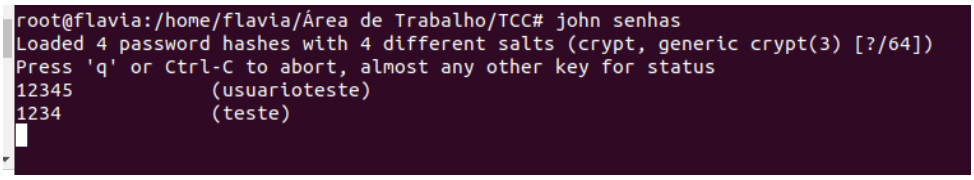

Figura 41 – Comando john para quebrar senhas.

Na Figura 45 ele consegue identificar 4 senhas para quebrar. O usuário teste e o o usuarioteste foram criados com senhas fáceis para que fosse possível mostrar como a ferramenta se comporta tendo sucesso. Sendo assim, rapidamente ele já faz a quebra de senhas mais fáceis.

Para confirmar que o John The Ripper conseguiu quebrar as senhas corretamente, com o comando john –show ele irá mostrar a senha utilizada para tal usuário nos primeiros números que aparecem logo após o nome do usuário. A Figura 46, traz o resultado.

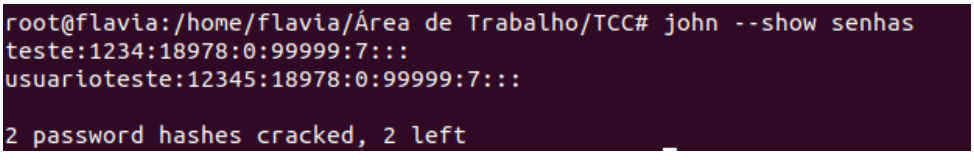

Figura 42 – Senhas dos usuários.

Como visto na Figura 43, o usuário mais utilizado foi o usuário root, sendo assim foi utilizado um ataque exclusivo a ele para que seja possível descobrir a senha, mostrado na Figura 47.

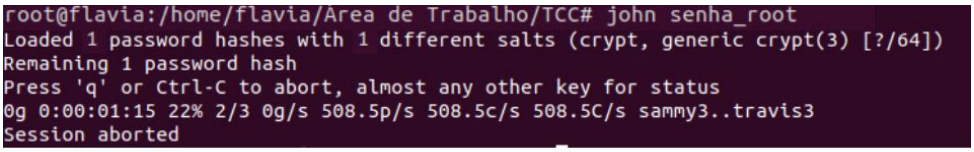

Figura 43 – Comando john para o usuário root

Dessa vez o John The Ripper não obteve sucesso ao tentar quebrar a senha do usuário root, uma vez que, para testes de força bruta, essa ferramenta utiliza usuários e senhas padrões para tentar decifrar, o que não se aplica a esse cenário.

Uma outra forma de se tentar decifrar as senhas são através de wordlist personalizada (os testes anteriores também utilizaram wordlists, mas as padrões da ferramenta), que podem ser encontradas na internet ou até mesmo feita manualmente. Essa técnica é utilizada quando se conhece mais a fundo o alvo e assim você dá a ferramenta uma noção de possíveis senhas que possam ser daquele usuário para que assim ele consiga quebrá-la.

5 Resultados

De acordo com os experimentos realizados, foi possível inferir alguns pontos principais nos resultados obtidos.

5.1 Uso do Nmap

Quando foi utilizado o Nmap, os testes foram centrados em explorar a rede e escanear as portas que mais tendem a ser vulneráveis. De acordo com os comandos aplicados via terminal, foi possível, inicialmente, fazer a análise se o alvo escolhido é ou não protegido por um firewall, de forma a fazer com que a escolha da porta seja mais assertiva do que uma possível escolha aleatória. Quando executada essa verificação, conseguimos observar se há ou não alguma restrição quanto ao alvo e se ele possui ou não portas que não estão filtradas, ou seja, portas acessíveis. Sendo assim, um atacante consegue ver o estado da porta e, a partir deste ponto, explorá-la, podendo aplicar, por exemplo, um ataque DDoS àquela porta e impedir o funcionamento da mesma.

É possível também, descobrir a razão pela qual aquela porta se encontra em determinado estado. Esta é uma outra oportunidade que um cibercriminoso tem de investigar, pois se ele encontra apenas portas fechadas e sabe o motivo delas estarem fechadas, ele consegue elaborar uma estratégia para abrí-la. Ainda através do Nmap, também é possível mostrar pacotes enviados e recebidos por aquele host, semelhante ao que o Wireshark faz. Com essa informação de pacotes, você pode analisar o tráfego dos mesmos, saber se as senhas de determinada aplicação são realmente fortes e conseguir analisar uma possível criptografia, fatores esses que auxiliam na escolha de um ataque.

No experimento em questão, sabemos que a placa embarcada BeagleBone Blue possui um sistema operacional integrado, o que também é possível visualizar através da manipulação no Nmap. Ao sabermos se um host possui ou não um SO, isso abre uma gama de possibilidades de ataques. Pois com um sistema operacional ativo na placa embarcada, pode-se, por exemplo, enviar um ransomware para o SO, um malware, um vírus, para que você obtenha controle do dispositivo. Podemos observar que é possível encontrar um SO remoto e ainda fornecer algumas informações sobre o SO que está inserido no host. Além disso, é possível detectar também alguns outros serviços remotos integrados à aquele host. Um framework, por exemplo, seria facilmente detectado.

Se pensarmos nessa situação, em um ambiente de manufaturas, é possível observar que o atacante irá possuir muitas informações valiosas a respeito dos equipamentos que funcionam naquela indústria e, com essas informações, realizar ataques mais incisivos que

possam vir a gerar um prejuízo de funcionamento de equipamentos, levando assim a uma perda de produção que pode gerar milhões de reais de prejuízo para a empresa.

5.2 Uso do SSH

Além do comando Nmap, um outra ferramenta interessante que pode auxiliar muito na tentativa de infiltrar em uma máquina e realizar ataques de diferentes formas é o SSH. Com o SSH, podemos encontrar mais uma gama de maneiras de distribuir algum tipo de ataque. Podemos dizer que com essa ferramenta é possível acessar a placa embarcada e, com qualquer comando que for realizado a partir de agora, terá reflexo por exemplo, nos diretórios e arquivos. Em um ambiente real, com o endereço IP de uma pessoa, um cibercriminoso pode sutilmente corromper arquivos e levar um vírus até ela. Trazendo para o cenário de estudo do braço robótico, é um dos comandos que nos possibilita um controle praticamente que total do braço, podendo fazer com que ele funcione de acordo com a preferência do atacante, o que, em uma linha de produção, poderia causar um dano gigante à manufatura. Através dessa manipulação com o SSH, é possível a criação de diretórios, arquivos, instalação de programas potencialmente perigosos e mais uma infinidade de coisas benéficas ao atacante.

Um exemplo de uma outra ferramenta poderosa para testes de segurança, é o John The Ripper, que funciona como um verificador de senha para que seja possível descobrir senhas de diretórios, usuários, programas, dentre outros. Desta forma, quando estamos utilizando o SSH para determinado fim e encontramos alguma barreira de senha, esse pode ser um excelente aliado dos atacantes.

5.3 Uso do TCPdump

Outra ferramenta poderosa é o TCPdump que é bem semelhante ao Wireshark. Através dela é possível fazer a captura de pacotes de rede e, com isso, obter informações preciosas para hackers que desejam prover algum ataque à rede. Pode-se fazer a captura de pacotes na interface escolhida. Sendo assim, é possível analisar todos os pacotes que estão passando por essa interface, e, a partir do momento que você consegue acessar esse tráfego, é possível obter informações importantes para prover um ataque. Quando analisamos o tráfego de protocolos na rede, podemos, por exemplo, visualizar a presença de protocolos TCP. Sendo assim, toda a informação da vítima passa pelo computador do criminoso, onde o mesmo é capaz de ler e modificar em tempo real absolutamente todos os pacotes. Desta forma, com a identificação de um protocolo TCP no tráfego, os criminosos podem empregar uma técnica chamada SYN Flood, que tem o propósito de realizar ataques de inundação ou explorar alguma falha com o propósito de ter acesso ao computador da vítima (AMIM et al., 2019).

Outra forma de fazer o scanner da rede e obter informações a respeito dos pacotes é fazendo a captura em uma porta específica. Esse comando, pode ser usado em conjunto com comandos de verificação de portas do Nmap, pois ao saber porta potencialmente boa para um ataque, você consegue fazer o scanner de tudo que passa nela, desta forma, consegue fazer com que um ataque IP Spoofing, por exemplo, seja mais incisivo, do que fazer de uma forma geral. Esse ataque é feito onde o invasor se passa por um host de origem que envia pacotes para um host destino e enviar dados potencialmente indesejados que podem acarretar em todo um mal funcionamento de uma linha de produção de uma Indústria 4.0.

5.4 Uso do T50

Ao utilizarmos o T50, o intuito foi simular quando a rede começa a sofrer ataques DDoS, ou seja, quando o tráfego de requisições é feito de forma indefinida até que inunde a rede e o sistema caia. Para analisarmos os efeitos desse comando, utilizamos a média da latência do envio de pacotes através do comando ping, pois é ela que reflete a lentidão do sistema.

Ao aplicar o comando T50 e analisar a latência, foi possível concluir que ela sempre aumenta ao começar a receber várias requisições, o que reflete algum tipo de ataque. Se pensarmos em um ambiente industrial, esse aumento de latência vai ficando cada vez maior, até que chega um momento em que o sistema entra em colapso e cai, o que pode acarretar no desligamento de máquinas além do mau funcionamento das mesmas ou, até mesmo, o funcionamento incorreto. Se estamos no meio de um processo de produção, isso pode vir a causar acidentes e a necessidade de interromper aquela cadeia produtiva, o que pode levar a indústria a um enorme impacto financeiro, pois quanto mais tempo ela ficar parada, mais dinheiro ela perde, podendo trazer diversos efeitos colaterais ao explorar uma vulnerabilidade de segurança da indústria. O T50 pode se comportar como uma ferramenta amiga de cibercriminosos.

6 Recomendações de Segurança

Tendo em vista os resultados obtidos após o desenvolvimento dos testes, algumas recomendações de segurança podem ser sugeridas para elevar a segurança da rede em manufaturas.

Uma medida que pode ser adotada é sempre manter senhas fortes nos usuários que acessam aquela rede. Como foi mostrado no teste de quebra de senhas com a ferramenta John The Ripper, em usuários onde a senha são muito simples a ferramenta obteve sucesso na descoberta da mesma, uma vez que essa ferramenta já utiliza um dicionário de senhas padrão e faz as tentativas. Sendo assim, o uso de senhas fortes faz com que ferramentas desse tipo não consigam fazer a quebra uma vez que a combinação de caracteres da senha provavelmente não estará nessa dicionário utilizado, o que dificulta o sucesso dessa descoberta.

Além disso, uma outra forma de proteção é manter um firewall para que este fique bloqueando as tentativas de cibercriminosos explorarem vulnerabilidades da rede. Ele será responsável por impedir que atacantes tentem infiltrar por alguma porta aberta e assim realizar algum ataque. Além disso, ele também irá monitorar o tráfego de pacotes que entra e saem da rede e decide se irá permitir ou bloquear alguns tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Ademais, uma recomendação de segurança também é reduzir a área da superfície do ataque, ou seja, minimizar a área da superfície que pode ser atacada pois assim é possível limitar as opções que os atacantes têm e assim permitir a criação de proteções em apenas um lugar. Uma forma de diminuir essa superfície é colocando os recursos de computação atrás de Redes de distribuição de conteúdo (CDNs) (AWS, 2020) e assim restringindo o tráfego direto da Internet a determinadas partes da infraestrutura da rede.

7 Conclusão

Feito todos os testes e realizando uma análise acerca dos resultados obtidos pode-se concluir primeiramente que os objetivos enunciados foram alcançados e que ainda que exista profissionais que se dediquem exclusivamente em garantir a segurança de manufaturas, softwares, dados, dentre outros, a segurança ainda se caracteriza como um gargalo profundo dos avanços tecnológicos. Ainda que se tenha diversas ferramentas que trabalham em prol de soluções para evitar situações indesejadas relacionadas à segurança, essas ferramentas também são utilizadas por cibercriminosos para modificar o comportamento de uma máquina, aplicar golpes, roubar dados, etc.

Outro fator que implica nesse estudo é o fato de que algumas falhas, por mais que sejam corrigidas por desenvolvedores, há uma dependência de que o usuário de determinado software mantenha sempre aquele programa atualizado. Além disso, não é possível controlar de forma sucinta tudo o que um usuário acessa em seu computador, e, na maioria das vezes, muitas pessoas não reconhecem um intruso em sua máquina por diversos fatores como simplesmente não manter um antivírus ativado e com isso esses alvos se tornam uma excelente porta de entrada para quem irá prover um ataque à segurança.

Esses ataques podem ser feitos de forma minuciosa, principalmente através da rede de internet, onde o tráfego de pacotes é imenso e as possibilidades de ataques nesses pacotes crescem em larga escala podendo fazer com que em uma simples aplicação do dia a dia que demandará o uso de um protocolo, esse protocolo pode sofrer uma alteração imperceptível pelo caminho e essa aplicação se to maliciosa. Além disso, pela rotina acelerada de grande parte das pessoas, tornou-se comum utilizar rede de estabelecimentos, que são redes não seguras. Essa situação se torna um alvo excelente para cibercriminosos.

Sendo assim, vemos que ainda é necessário sempre continuar realizando estudos sobre falhas de segurança, pois o avanço tecnológico irá continuar demandando atualizações e uma preocupação quase que em tempo real acerca das falhas de novas aplicações e assim continuar combatendo ataques.

Ademais, com os resultados obtidos e de acordo com a forma que foi conduzida a pesquisa, trabalhos futuros podem ser enunciados a partir deste projeto. Para um próximo desenvolvimento, é válida a utilização de mais notebooks realizando ataques DDoS simultâneos na rede para ser possível analisar de forma mais incisiva o comportamento da mesma à inundação de solicitações. Outro ponto é abranger ataques exclusivos à rede Wifi uma vez que a tendência das manufaturas é ficar conectada via rede Wifi. Além disso, outro ponto de melhoria se dá no uso do notebook conectado via rede cabeada nos experimentos do Nmap. Por fim, uso de diferentes redes de locais públicos para que se

possa analisar a mudança de comportamento dos resultados em um número maior de redes diferentes.

Referências

SANTOS, B. P.; ALBERTO, A.; LIMA, T. D. F. M.; CHARRUA-SANTOS, F. M. B. INDÚSTRIA 4.0: DESAFIOS E OPORTUNIDADES. **Revista Produção e Desenvolvimento**, v. 4, n. 1, p. 111-124, 31 mar. 2018.

DEMIRA, Kadir Alpaslan; DÖVENA, Gözde; SEZENB, Bülent. Industry 5.0 and Human-Robot Co-working. **Industry 5.0**, Turquia, p. 688-695, 2019. Disponível em: https://www.sciencedirect.com/. Acesso em: 6 maio 2021.

BEAGLEBOARD. BeagleBone Blue. In: **BeagleBone Blue.** [S. l.], 2019. Disponível em: https://beagleboard.org/black. Acesso em: 1 abr. 2021.

HENRIQUES, Pedro. **Saiba tudo sobre segurança wifi e proteja sua rede.** [S. l.], 16 jun. 2020. Disponível em: https://indicca.com.br/seguranca-wifi/: :text=Existem%20dois%20tipos%20de%criptografia,protocolo%20de%20seguran%C3%A7a%20wifi%20WPA. Acesso em: 21 jan. 2022.

VARGHESE, Anitha; TANDUR, Deepaknath. **Wireless requirements and challenges in Industry 4.0**. Industry 4.0, [s. l.], p. 634-638, 2014. Disponível em: https://ieeexplore-ieee-org.ez28.periodicos.capes.gov.br/stamp/stamp.jsp?tp=arnumber=7019732. Acesso em: 13 nov. 2021.

CHASE, Otavio. Sistemas Embarcados. **Embarcados**, [s. l.], ano 2007, 12 2007. Disponível em: www.sbajovem.org. Acesso em: 1 abr. 2021.

TAVARES, Henrique Leal. PLACAS EMBARCADAS E INTERNET DAS COISAS. **Embarcados**, São José dos Campos, 2017. Disponível em: https://fatecgarca.edu.br/ojs/index.php/efatec/article/view/33/145. Acesso em: 1 abr. 2021.

PEOPLE TECH AND ENGLISH. **Como braços robóticos funcionam?.** [S. l.], 21 fev. 2019. Disponível em: https://www.people.com.br/noticias/robotica/como-bracos-roboticos-funcionam. Acesso em: 5 abr. 2021.

DF ROBÓTICA. **Braços Robóticos Industriais.** [S. l.], 2011. Disponível em:

https://www.dfrobotica.com/bracos-roboticos-industriais. Acesso em: 5 abr. 2021.

ALMEIDA, Emília. **Tecnologia**. [S. l.], 1 mar. 2015. Disponível em: https://www.trabalhos gratuitos.com/Exatas/Engenharia/Tecnologia-598603.html. Acesso em: 25 nov. 2021.

PEREIRA, T; BARRETO, L; AMARAL, A. Network and information security challenges within Industry 4.0 paradigm. **Industry 4.0**, Spain, 28 jun. 2017. Disponível em: www.sciencedirect.com. Acesso em: 7 abr. 2021.

ZILLION CIBERSECURITY. **6 ferramentas de segurança da informação que sua empresa precisa ter!**. [S. l.], [ca. 2019]. Disponível em: https://zillion.com.br/6-ferramentas-de-seguranca-da-informacao-que-sua-empresa-precisa-ter/. Acesso em: 23 abr. 2021

BRITO, Edivaldo. **Como usar o Wireshark.** [S. l.], 14 set. 2012. Disponível em: https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2012/09/como-usar-o-wireshark.html. Acesso em: 7 abr. 2021.

LARA, Sílvio Garbes. **TCPDUMP:** CAPTURANDO TRAFEGO DE REDE COM TCPDUMP – PARTE 1 – BASICO. [S. l.], 28 maio 2013. Disponível em: https://sites.google.com /site/silviogarbes/sistemas/linux/tcpdump. Acesso em: 7 abr. 2021.

DOS REIS, Fábio. **Tcpdump – Capturar e analisar tráfego de rede no Linux**. [S. l.], 28 set. 2015. Disponível em: http://www.bosontreinamentos.com.br/redes-computadores/ tcpdump-capturar-e-analisar-trafego-de-rede-no-linux/. Acesso em: 5 jul. 2021.

NMAP. **Técnicas de Escaneamento de Portas**. [S. l.], 2020. Disponível em: https://nmap.org/ man/pt_BR/man-port-scanning-techniques.html. Acesso em: 5 jul. 2021.

FERREIRA, Kellison. **Saiba o que é SSH (Secure Shell) e pra que serve esse protocolo.** [S. l.], 17 abr. 2019. Disponível em: https://rockcontent.com/br/blog/ssh/. Acesso em: 7 abr. 2021.

JUNIOR, Celso. **Conheça a lista de comandos SSH para acesso remoto ao servidor**. [S. l.], 16 nov. 2020. Disponível em: https://www.portofacil.net/conheca-a-lista-de-comandos-ssh-para-acesso-remoto-ao-servidor.html.

Acesso em: 7 jul. 2021.

NMAP. **Nmap: the Network Mapper - Free Security Scanner**. [S. l.], 9 out. 2020. Disponível em: https://nmap.org/. Acesso em: 1 ago. 2021.

LIRA, Rodrigo. **Nmap: 30 exemplos de comandos para administradores de rede**. [S. l.], 15 jan. 2013. Disponível em: https://rodrigolira.eti.br/nmap-30-exemplos-de-comandos-para-administradores-de-rede/. Acesso em: 5 jul. 2021.

WIKIPÉDIA. **Nmap**: Recursos, Usos éticos e legalidade. [S. l.], 7 abr. 2021. Disponível em: https://pt.wikipedia.org/
wiki/Nmap. Acesso em: 7 abr. 2021.

TACIO, Paulo. **FERRAMENTA PARA DOS/DDOS T50**. [S. l.], 25 abr. 2011. Disponível em: https://www.mundodoshackers.com.br/ferramenta-para-dosddos-t50. Acesso em: 30 out. 2021.

STEFANINI. **Ataques à segurança da informação: conheça as principais ameaças.** [S. l.], 16 abr. 2019. Disponível em: https://stefanini.com/pt-br/trends/artigos/ameacas-a-seguranca-da-informacao. Acesso em: 23 abr. 2021.

BACKUP GARANTIDO. **Port scan: conheça a técnica usada pelos hackers e proteja-se.** [S. l.], 13 jul. 2020. Disponível em: https://backupgarantido.com.br/blog/port-scan-conheca-a-tecnica-usada-pelos-hackers-e-proteja-se/. Acesso em: 7 abr. 2021.

GARRETT, Filipe. **O que é uma falha zero day?**: Saiba o que significa uma falha zero-day, como essas brechas são exploradas e como se proteger.. [S. l.], 3 ago. 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/08/o-que-e-uma-falha-zero-day.ghtml. Acesso em: 15 abr. 2021.

CARDOSO, Pedro. **O que é Ransomware?**. [S. l.], 17 maio 2017. Disponível em: https://www.techtudo.com.br/
noticias/noticia/2016/06/o-que-e-ransomware.html. Acesso em: 15 abr. 2021.

KASPERSKY. **O que é um ataque de força bruta?**. [S. l.], 2021. Disponível em: https://www.kaspersky.com.br/

resource-center/definitions/brute-force-attack. Acesso em: 15 abr. 2021.

KASPERSKY. **O que é um cavalo de Troia?**. [S. l.], [20-??]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/trojans. Acesso em: 15 abr. 2021.

DIORIO, Rafael Fernando; SERAFIM, Edivaldo; ALVES, Karlan Ricomini; MEIRA, Matheus Carvalho. Ataques de Força Bruta: Um Estudo Prático. **Ataque de força bruta**, Capivari, 2019. Disponível em: https://www.lcv.fee.unicamp.br/images/BTSym-19/Papers/040.pdf. Acesso em: 15 abr. 2021.

PROFISSIONAIS TI. **Como quebrar senhas com o programa John The Ripper**. [S. l.], 2 nov. 2020. Disponível em: https://www.profissionaisti.com.br/como-quebrar-senhas-com-john-the-ripper/. Acesso em: 1 ago. 2021.

AKAMAI. **O que é UM ataque de DDoS?**. [S. l.], 2021. Disponível em: https://www.akamai.com/pt/our-thinking/ddos. Acesso em: 30 out. 2021.

REGAN, Joseph. **O que é um Cavalo de Troia? É malware ou vírus?**. [S. l.], 10 dez. 2019. Disponível em: https://www.avg.com/pt/signal/what-is-a-trojan. Acesso em: 15 abr. 2021.

NORTON. **O que é um cavalo de troia?**. [S. l.], [20-??]. Disponível em: https://br.norton.com/internetsecurity-malware-what-is-a-trojan.html. Acesso em: 15 abr. 2021.

CHHETRI, Sujit Rokka; RASHID, Na fi ul; FAEZI, Sina; AL FARUQUE, Mohammad Abdullah. **Security Trends and Advances in Manufacturing Systems in the Era of Industry 4.0.** Industry 4.0, [s. l.], 2017.

GLAVACH, Dominick; LASALLE-DESANTIS, Julia; ZIMMERMAN, Scott. **Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems**. Industry 4.0, [s. l.], 2017. Disponível em: https://researchportal.bath.ac.uk/en/publications/cybersecurity-for-industry-40-and-advanced-manufacturing-environm. Acesso em: 13 nov. 2021.

ILHAN, Ismail; KARAKÖSE, Mehmet. **Cybersecurity Framework for Requirements of Repair, Update, and Renovation in Industry 4.0**. Industry 4.0, [s. l.], 2019. Dis-

ponível em: https://ieeexplore-ieee-org.ez28.periodicos.capes.gov.br/stamp/stamp.jsp?tp=arnumber=8965488. Acesso em: 13 nov. 2021.

MERGENDAHL, Samuel; SISODIA, Devkishen; LI, Jun; CAM, Hasan. **Source-End DDoS Defense in IoT Environments**. DDoS Attack, [s. l.], p. 63-64, 3 nov. 2017. DOI https://doi.org/10.1145/3139937.3139954. Disponível em: https://dl-acm-org.ez28.periodicos.capes.gov.br/doi/10.1145/3139937.3139954. Acesso em: 24 nov. 2021.

AZZEDIN, Farag; SUWAD, Husam; ALYAFEAI, Zaid. **Countermeasureing Zero Day Attacks: Asset-Based Approach**. Zero-day Attacks, Arábia Saudita, p. 854-857, 2017. DOI 10.1109/HPCS.2017.129. Disponível em: https://ieeexplore-ieee-org.ez28.periodicos.capes.gov.br/stamp/stamp.jsp?tp=arnumber=8035168. Acesso em: 24 nov. 2021.

KASPERSKY. **O que é endereço IP – definição e explicação.** [S. l.], 2017. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address. Acesso em: 21 dez. 2021.

KAPERSKY. **O que são ataques de DDoS?**. [S. l.], 2018. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ddos-attacks. Acesso em: 5 jul. 2021.

AMIM SAB, Gabriel Augusto; FERREIRA, Rafael Cardoso; ROZENDO, Rafael Gonsalves. **Negação de Serviço, Negação de Serviço Distribuída e Botnets.** [S. l.], 2019. Disponível em: https://www.gta.ufrj.br/grad/13_1/dos/ataques.htmltop. Acesso em: 28 dez. 2021.

CBPF. **UDP – Aspectos de Segurança.** [S. l.], 28 dez. 2021. Disponível em: http://www.cbpf.br/ sun/pdf/udp.pdf. Acesso em: 28 dez. 2021.

WELIVESECURITY. **ARP spoofing: ataque às redes locais.** [S. l.], 7 nov. 2017. Disponível em: https://www.welivesecurity.com/br/2017/11/07/arp-spoofing-ataque-as-redes-locais/. Acesso em: 2 ago. 2021.

MALENKOVICH, Serge. **O que é um Ataque Man-in-the-Middle?**. [S. l.], 10 abr. 2013. Disponível em: https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/. Acesso em: 2 ago. 2021.

QUEBRANDO senhas de usuarios linux com o Estripador. Produção: Prof.Juliano Ramos. [S. l.: s. n.], 2020. Disponível em: https://www.youtube.com/watch?v=RWoNzkNTgjc. Acesso em: 15 ago. 2021.

MILLS, Matt. **Como quebrar senhas ou chaves rapidamente usando John the Ripper**. [S. l.], 15 ago. 2021. Disponível em: https://itigic.com/pt/crack-passwords-or-keys-very-fast-using-john-the-ripper/. Acesso em: 4 jan. 2022.

AWS. **O que é um ataque DDoS?**. [S. l.], 2020. Disponível em: https://aws.amazon.com/pt/shield/ddos-attack-protection/. Acesso em: 21 jan. 2022.