UNIVERSIDADE DO SUL DE SANTA CATARINA

ARTHUR DOS SANTOS

JOSIAS LAURENCE ANACLETO DE LIMA

ANÁLISE DE VULNERABILIDADES DE SEGURANÇA EM SOFTWARE DE PRODUTOS TECNOLÓGICOS DE UMA INDÚSTRIA DA GRANDE FLORIANÓPOLIS

Palhoça

2022

ARTHUR DOS SANTOS
JOSIAS LAURENCE ANACLETO DE LIMA

ANÁLISE DE VULNERABILIDADES DE SEGURANÇA EM SOFTWARE DE PRODUTOS TECNOLÓGICOS DE UMA INDÚSTRIA DA GRANDE FLORIANÓPOLIS

Projeto de Conclusão de Curso apresentado ao Curso de Sistemas de informação da Universidade do Sul de Santa Catarina, como requisito para aprovação da disciplina de Trabalho de Conclusão de Curso.

Orientador: Prof. Roberto Fabiano Fernandes, Dr.

Palhoça
2022

ARTHUR DOS SANTOS
JOSIAS LAURENCE ANACLETO DE LIMA

ANÁLISE DE VULNERABILIDADES DE SEGURANÇA EM SOFTWARE DE PRODUTOS TECNOLÓGICOS DE UMA INDÚSTRIA DA GRANDE FLORIANÓPOLIS

Projeto de Conclusão de Curso apresentado ao Curso de Sistemas de informação da Universidade do Sul de Santa Catarina, como requisito para aprovação da disciplina de Trabalho de Conclusão de Curso.

Palhoça, 20 de junho de 2022.

_____
Professor e orientador Dr. Roberto Fabiano Fernandes
Universidade do Sul de Santa Catarina

_____
Prof. Dr. Edson Rosa Gomes da Silva
Universidade do Sul de Santa Catarina

_____
Prof. Dr. Helio Ainseberg Ferenhof

_____
Prof. Dra. Viviane Brandão Miguez

Dedicamos este trabalho à Deus, responsável por nossas vidas, e por nos ajudar a vencer todos os obstáculos ~~da vida~~.

Aos nossos pais, por todo o apoio e motivação que nos motivaram nos momentos mais difíceis.

AGRADECIMENTOS

Eu, Josias, agradeço primeiramente aos meus pais Clenir Anacleto de Lima e Iranildo Lauriano de Lima por todo suporte, incentivo e companheirismo que serviram de base para minha vida e para minha carreira.

À minha irmã Clécia Anacleto de Lima por sempre me questionar nas minhas decisões e a todos os conselhos de uma irmã mais velha.

À minha namorada Giovana Cherighini Thives que está comigo em todos os momentos e me deu suporte e todo apoio técnico e mental neste trabalho.

Agradeço também aos meus amigos e colegas, em especial ao Arthur, que do começo ao fim se empenhou ao máximo no desenvolvimento deste trabalho.

Eu, Arthur, início meus agradecimentos Àquele que me orientou todos os dias e me deu forças para continuar, obrigado Deus!

Agradeço muito aos meus pais, Ana Lúcia e Adenir, minha madrasta Rosimeri e meu padrasto Euclides por me incentivarem e me apoiarem durante todo o período de faculdade.

À minha namorada, que foi fundamental desde o início.

Aos meus amigos Paulo, Luiz, Daniel, Vitor, Gabriel e Josias que me ensinaram e contribuíram muito para o meu aprendizado.

Além disso, não poderia deixar de agradecer aos meus avós que mesmo sem condições de estudos em suas épocas, sempre foram meus incentivadores durante toda a faculdade. Infelizmente não os tenho aqui para acompanhar essa conquista, mas os levo no coração para sempre.

Por fim, agradecemos aos professores que nos ajudaram a trilhar essa estrada. Em especial, ao nosso querido orientador, Profº Drº Roberto Fabiano Fernandes, que, mesmo sem apoio da universidade, continuou conosco para a finalização deste trabalho.

“A neve e as tempestades matam as flores, mas nada podem contra as sementes” (Khalil Gibran, S.d).

RESUMO

O setor denominado segurança da informação, está direcionado à proteção de dados com a intenção de preservar os conteúdos disponíveis nos suportes de informações utilizados por um indivíduo ou uma empresa. Informações sigilosas e de grande valia são procuradas por criminosos a fim de violar informações e desestruturar organizações. Diante disso, este trabalho tem como objetivo a identificação de vulnerabilidades de segurança em produtos de uma indústria da grande Florianópolis - SC. Para tanto, é apresentado um referencial teórico para embasamento do tema e após, é apresentada os resultados de uma pesquisa em campo desenvolvida. Foi realizado uma abordagem qualitativa para a coleta de dados a fim de buscar a compreensão e descrição das ocorrências encontradas na pesquisa, utilizando o embasamento bibliográfico de autores que abordam o tema sobre segurança da informação.

No desenvolvimento do trabalho foi observado quatro vulnerabilidades, sendo elas: SQL *injection*; autenticação através de *script*, em uma central telefônica; *DoS* encontrado no *switch* e senha sem criptografia encontrado em outro *switch*. Ao final da pesquisa, conclui-se que os ataques ativos detectados apontam que a empresa analisada não apresenta normas e padrões para testes de vulnerabilidades no processo de desenvolvimento de seus produtos. Sugere-se testes de vulnerabilidade como etapa obrigatória para o lançamento de novos produtos assim como a criação de um setor especializado para tal função. Isso porque mais estudos são necessários para melhor avaliação dos parâmetros de vulnerabilidades da empresa.

Palavras-chave: Vulnerabilidade. Segurança da informação. Produtos tecnológicos. Análise de software em produtos.

LISTA DE FIGURAS

Figura 1 - Ataque passivo e ativo 18
Figura 2 - Formas de segurança 22
Figura 3 - Página de primeiro acesso da central 30
Figura 4 - Realização do *SQL injection* 31
Figura 5 - Acesso realizado 31
Figura 6 - Código *PHP* para adicionar um usuário 32
Figura 7- Acesso com novo usuário 33
Figura 8 - Lista de usuários criados na central 33
Figura 9 - Código *PHP* para remover um usuário 34
Figura 10 - Página de acesso do switch 35
Figura 11 - Acesso via SSH 36
Figura 12 - Comando de varredura de senhas no hydra 36
Figura 13 - Verificando recursos de hardware do produto 37
Figura 14 - Produto sem acesso via *HTTP* e *SSH*. 37
Figura 15 - Resultado do comando “*show run*” 38
Figura 16 - Interceptação do método *GET* 39
Figura 17 - Login como usuário tipo convidado 40
Figura 18 - Criando usuário teste 40
Figura 19 - Código de validação dos dados 42

SUMÁRIO

1 INTRODUÇÃO 10
1.1 DEFINIÇÃO DO PROBLEMA 11
1.2 OBJETIVOS 11
1.2.1 Objetivo Geral 11
1.2.2 Objetivo Específicos 11
1.3 JUSTIFICATIVA 11
1.4 ESTRUTURA DO TRABALHO 12
2 FUNDAMENTAÇÃO TEÓRICA 13
2.1 SEGURANÇA DA INFORMAÇÃO 13
2.2 VULNERABILIDADE, AMEAÇA E RISCO 14
2.3 PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA DA INFORMAÇÃO 15
2.3.1 Confidencialidade 15
2.3.2 Disponibilidade 15
2.3.3 Integridade 16
2.4 TÉCNICAS DE ATAQUES À SEGURANÇA 17
2.4.1 Ataques Passivos 18
2.4.2 Ataques Ativos 19
2.5 CONTRAMEDIDAS PARA ELIMINAR, NEUTRALIZAR E MINIMIZAR AMEAÇAS 21
3 PROCEDIMENTOS METODOLÓGICOS 24
3.1 TIPO DE PESQUISA 24
3.2 PESQUISA BIBLIOGRÁFICA 25
3.3 COLETA DE DADOS PRIMÁRIOS 26
3.4 ANÁLISE E DISCUSSÃO DOS DADOS 27
3.5 DELIMITAÇÃO DA PESQUISA 27
4 DESCRIÇÃO DA EMPRESA ESTUDADA 28
4.1 PRODUTO 1 - CENTRAL TELEFÔNICA 29
4.1.1 SQL *Injection* 29
4.1.2 Autenticação 32
4.2 PRODUTO 2 - SWITCH GERENCIÁVEL 35
4.2.1 *Denial of Service* (DoS) 36
4.2.2 Senha sem Criptografia 38

4.3 PRODUTO 3 – SWITCH GERENCIÁVEL 38
4.3.1 ESCALONAMENTO DE PRIVILÉGIOS 39
5 ANÁLISE E DISCUSSÃO DE DADOS 42
5.1 RESOLUÇÃO SQL *INJECTION* CENTRAL TELEFÔNICA 42
5.1.1 Riscos e prejuízos causados por um SQL injection 43
5.2 RESOLUÇÃO DA AUTENTICAÇÃO INDEVIDA (PRODUTO 1 - CENTRAL TELEFÔNICA) 44
5.2.1 Riscos e prejuízos causados pela autenticação indevida 44
5.3 RESOLUÇÃO *DENIAL OF SERVICE* NO PRODUTO 2, *SWITCH* 45
5.3.1 Riscos e prejuízos causados pelo DoS 46
5.4 RESOLUÇÃO SENHA SEM CRIPTOGRAFIA NO PRODUTO 3, SWITCH 46
5.4.1 Riscos e prejuízos causados por senha sem criptografia 46
5.5 RESOLUÇÃO ESCALONAMENTO DE PRIVILÉGIOS 47
5.5.1 Riscos e prejuízos escalonamento de privilégios 47
6 CONCLUSÃO 49
REFERÊNCIAS 51

1 INTRODUÇÃO

O avanço tecnológico trouxe agilidade e eficiência nas atividades cotidianas, um grande exemplo disso é a evolução da comunicação que passou de cartas para mensagens instantâneas e chamadas de vídeo com o passar dos anos (ROZA, 2017).

O século XIX foi considerado como a era das máquinas a vapor. Já no século XX, a distribuição de informações se tornou destaque enquanto nos demais desenvolvimentos houve a instalação de redes de telefonia e a invenção do rádio e televisão. Após alguns anos, surgiram os lançamentos de satélites de comunicação a Internet (TANEMBAUM, 2011).

Com a constante evolução no ramo de dados, informações são geradas e compartilhadas simultaneamente com o objetivo de chegarem ao destinatário esperado. Porém, com a sobrecarga de notícias compartilhadas, o desvio de uma mensagem pode direcioná-la para um receptor indesejado utilizando dados de forma ilegal (FRAGA, 2019).

A segurança da informação é um setor direcionado à proteção de dados e como intenção preservar o conteúdo de um material para um indivíduo ou uma empresa. Tem como características principais a confidencialidade, integridade e disponibilidade, não limitando-se apenas a sistemas de computadores bem como todos os meios de proteção de informações e dados (FRAGA, 2019).

A partir da notoriedade dos dados, notícias relacionadas a crackers (praticantes de quebra de sistema de forma ilegal) foram relatadas com maior frequência. *Massachusetts Institute of Technology (MIT)* publicou no *Journal of Data and Information Quality da ACM (Association for Computing Machinery 2021)* que o vazamento de dados no Brasil aumentou em 493%.

Segundo a PSafe (2021), mais de 100 milhões de celulares brasileiros foram vazados. Esses dados são de duas operadoras não identificadas, mas que, nas informações roubadas, foram encontrados CPFs, números de celulares, contas telefônicas e dados pessoais. Segundo conta Tais materiais são encontrados na *deep web* por aproximadamente doze mil reais.

A *Kaspersky*, empresa Russa especializada em softwares de segurança, monitora os tipos de ataques que seus sistemas identificam. Segundo ela, o Brasil é o segundo país mais infectado por diferentes tipos de vírus (KASPERSKY, 2021).

1.1 DEFINIÇÃO DO PROBLEMA

Na nova era tecnológica, as empresas recebem muitas informações sigilosas e de grande valor. Isso atrai criminosos denominados crackers que conseguem capturar uma grande quantidade de dados.

Isso está associado a interesses financeiros que podem ocasionar uma enorme turbulência para empresa, que terá seus dados privados violados de forma ilegal e consequências catastróficas para as organizações.

No entanto, mesmo com a importância da segurança da informação aumentando cada vez mais, é notado um crescimento lento nesta área, que não acompanha as necessidades mercadológicas.

Assim, surge o seguinte questionamento: Quais as formas de solucionar vulnerabilidade de software encontradas em produtos tecnológicos?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Identificar vulnerabilidades de segurança nos softwares de produtos de uma indústria localizada na região da grande Florianópolis - SC.

1.2.2 Objetivo Específicos

a) identificar na literatura as principais vulnerabilidades em software;

b) analisar as vulnerabilidades em produtos de uma empresa de tecnologia;

c) sugerir adequações ao gerenciamento de vulnerabilidades para a empresa estudada;

1.3 JUSTIFICATIVA

O digital, a partir da evolução tecnológica, se tornou um meio propício a fraudes digitais por causa da troca acelerada de informações e armazenamento de dados. A segurança deve ser um dos itens essenciais de uma organização e precisa de investimentos adequados para tal demanda.

De acordo com a empresa *Canalys* (2021), comparando os anos de 2020 e 2019, os setores de Tecnologia da Informação (TI), como serviços de infraestrutura em nuvem, software para nuvem e vendas de roteadores *wi-fi* domésticos cresceram 33%, 20% e 40% respectivamente. Todavia, o setor de segurança cresceu apenas 10% no mesmo período.

Desse modo, a presente pesquisa tornará possível a observação da necessidade de tornar os produtos da empresa escolhida mais seguros conscientizando diretores, gerentes e supervisores a necessidade de implementação de normas e profissionais que atuem de forma colaborativa para uma maior segurança no desenvolvimento dos produtos para serem comercializados.

Assim, será demonstrado a importância da implementação de políticas de segurança da informação, testes de vulnerabilidades na empresa e esclarecer a importância de investimentos adequados neste segmento da empresa.

1.4 ESTRUTURA DO TRABALHO

O presente trabalho está estruturado em 6 capítulos.

O capítulo 1 é apresentada a introdução ao tema proposto, com objetivos e justificativas.

O capítulo 2 aborda a fundamentação teórica que traz os capítulos basilares da construção da dissertação e servirão como base para a compreensão dos termos de segurança da informação.

O capítulo 3 é composto pelos procedimentos metodológicos que são as diretrizes que orientam a construção de toda a dissertação, apresentando como a estratégia usada para a composição da revisão da literatura, como é a proposta de coleta de dados primários e as técnicas usadas, por fim, como foi realizada a análise dos dados. Também se propõe neste tópico explicar como a coleta e análise contribuirá para a construção de sugestões de adequações às principais normas da segurança da informação no que tange às vulnerabilidades.

No capítulo 4 é realizado a coletas de fragilidades em produtos da empresa estudada.

Como também no capítulo 5 nas quais são realizadas as análises de dados, e assim, respectivamente, apresentados os dados coletados e a sua análise.

E, finalmente, no capítulo 6 são apresentadas as conclusões do trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada a fundamentação teórica que embasou o presente trabalho, que foi realizado através do estudo da segurança da informação.

2.1 SEGURANÇA DA INFORMAÇÃO

Para Fraga (2019), a segurança da informação é um processo inerente à proteção de dados diante de possíveis ameaças relacionadas a sua integridade, confiabilidade e disponibilidade. Todas as informações processadas e guardadas por uma organização podem estar ameaçadas de algum ataque, erro, ou perigo natural, e estão sujeitas a vulnerabilidades.

O termo “segurança da informação” é constantemente relacionado a informações consideradas como um ativo de valor que necessita de uma proteção adequada. Se, porventura, a organização sofra complicações referentes a inatividade de disponibilidade, confidencialidade e integridade, é necessário combater e permitir que informações precisas estejam disponíveis rapidamente para pessoas autorizadas (ISO 27000, 2013).

A Segurança da informação procura garantir a confidencialidade, integridade e disponibilidade das informações. A segurança é alcançada a partir de um conjunto de controles, que são selecionados através do processo de gerenciamento de risco escolhido e administrado utilizando políticas, processos, estruturas organizacionais e procedimentos de software e hardware para proteção de ativos (ISO 27000, 2018).

Sendo assim, a segurança da informação não engloba apenas dados e os locais em que estão guardados, mas também sistemas de usuários não se restringindo só à estrutura da informática.

É importante entender também que nenhuma organização é totalmente livre de ameaças de segurança pois a tecnologia está sempre em evolução, assim como as pessoas mal-intencionadas, a transformação dependerá de novos tipos de estratégias para conter ataques, e cada problema deve ser tratado com sua especialidade pois é fundamental dar privilégio ao que é mais importante no momento (GARTNER, 2017).

Por conseguinte, é necessário verificar os conceitos de vulnerabilidade, ameaça e risco.

2.2 VULNERABILIDADE, AMEAÇA E RISCO

Na segurança da informação é possível encontrar vulnerabilidade, ameaça e risco.

A ameaça é um evento fortemente indesejado que pode prejudicar e danificar um ativo, causando impactos nos resultados de uma organização. Ela é classificada de três formas: naturais, intencionais e involuntária.

Os exemplos de ameaças naturais são: incêndios, enchentes, catástrofes. Por sua vez, as ameaças intencionais partem de indivíduos mal-intencionados, funcionários e vírus. Já a ameaça involuntária acontece por negligência, imprudência, imperícia, falha humana e despreparo (ISO 27000, 2013).

A vulnerabilidade é a fragilidade de um ativo ou um grupo de ativos que pode ser explorado por ameaças. De acordo com Teixeira (2020), existem sete classificações de vulnerabilidades sendo elas:

a) comunicação: afeta todo o tráfego da informação;

b) físicas: atingem as instalações;

c) hardware: afeta o equipamento;

d) ameaças Humanas: ocorrem através de pessoas de dentro e fora da organização;

e) mídias: onde as informações estão armazenadas;

f) naturais: acontecem por riscos naturais, através da região da empresa, clima e tempo e;

g) vulnerabilidade de Software: programas de computador, base de dados, sistemas operacionais, sites online.

O risco é o potencial ou possibilidade de ocorrência de uma ameaça que encontra uma vulnerabilidade. É importante ressaltar que indivíduos com má intenção analisam formas de contornar obstáculos de segurança para explorar as vulnerabilidades de uma organização (WEIDMAN, 2014).

A melhor forma para sanar as vulnerabilidades é através de medidas de segurança iniciadas a partir da classificação de ativos, de modo que identifique possíveis ameaças e preveja vulnerabilidades para averiguar aos riscos que devem ser analisados. Além disso, é necessário padronizar os procedimentos de segurança

com as normas estabelecidas pela ISO/IEC 27000, uma vez que garante maior eficiência na proteção de dados (TEIXEIRA, 2020).

Nesse sentido, se faz necessária também a análise dos princípios da segurança da informação.

2.3 PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA DA INFORMAÇÃO

Os princípios fundamentais de todos os programas de segurança são: confidencialidade, disponibilidade e integridade, que serão explanados a seguir.

2.3.1 Confidencialidade

A confidencialidade trata dos limites de quem pode obter a informação, traz qual o nível de sigilo necessário seja aplicado em cada parte de processamentos de dados e impede a divulgação não autorizada (HINTZBERGEN, 2018).

A informação deve ser acessada apenas por quem deve ter autorização para realizar o acesso. Então, a confidencialidade vai fazer o papel de garantir o sigilo da informação e impedir que pessoas indevidas acessem a informação (HINTZBERGEN, 2018).

Segundo os Fundamentos da Segurança da Informação, de Hintzbergen (2018), a confidencialidade pode ser disponibilizada através da criptografia de dados à medida que forem armazenados e transmitidos, usando o tráfego na rede, classificação de dados, e controle de acesso.

Hintzbergen (2018) também destaca que a criptografia é uma técnica que vai “embaralhar” as informações por meio de algoritmos de criptografia, fazendo com que a informação se torne algo impossível de entender.

2.3.2 Disponibilidade

A disponibilidade tem três características bem importantes: a) Oportunidade, que permite que a informação esteja disponível quando necessário; b) Continuidade, que faz com que a equipe continue trabalhando no caso de falhas; e c) Robustez a qual permite com que toda a equipe possa trabalhar no sistema (HINTZBERGEN, 2018).

Destaca-se que, caso aconteça uma falha no disco ou um super ataque de negação de serviço, no qual o sistema tenha ficado por algum tempo inativo, se enquadra como uma violação de disponibilidade (HINTZBERGEN, 2018).

Os dispositivos de backup devem ser usados para substituir rapidamente os sistemas mais importantes e é necessário ter funcionários bem capacitados para realizar os ajustes necessários para restauração do sistema. Problemas ambientais como frio, calor, eletricidade também podem atingir a disponibilidade do sistema e devem ser protegidos contra esses elementos (HINTZBERGEN, 2018).

Ataques DoS (*Denial of Service*), ataques de negação de serviço, são métodos bem comuns nas técnicas dos criminosos. Eles tiram a disponibilidade de um sistema, impedindo que os funcionários e usuários acessem o sistema (HINTZBERGEN, 2018).

Para impedir esses ataques, é necessário usar um sistema de intrusão o *IDS* (*intruder detection system*), que monitora a atividade das máquinas e o tráfego na rede. É clarividente que o *firewall* possui funcionalidade capaz de tornar a indisponibilidade ainda mais difícil, haja vista que é barreira de proteção contra-ataques que tem o objetivo de tirar um serviço de funcionamento. Por sua vez, o *backup* também é extremamente importante, pois recupera informações e as torna disponíveis novamente (HINTZBERGEN, 2018).

2.3.3 Integridade

A integridade trata-se da consistência do estado da informação pretendida, ou seja, qualquer tipo de alteração sem uma liberação, ou realizada de forma acidental é considerada uma violação a este princípio (HINTZBERGEN, 2018).

É esperado que dados armazenados dentro de um disco sejam consistentes não se espera que sejam alterados de forma aleatória, da mesma forma que sistemas guardam informações corretamente e não incluem valores diferentes dos desejados (HINTZBERGEN, 2018).

De acordo com Hintzbergen (2018), no momento que um atacante consegue implementar um vírus, ou um *backdoor* em um sistema, sua integridade está comprometida. Muitos usuários atingem a integridade de seus sistemas através de erros, inclusive, em alguns casos, um simples ato de apagar um disco, que o usuário acredita que não tenha importância, ou inserindo valores incorretos por desatenção.

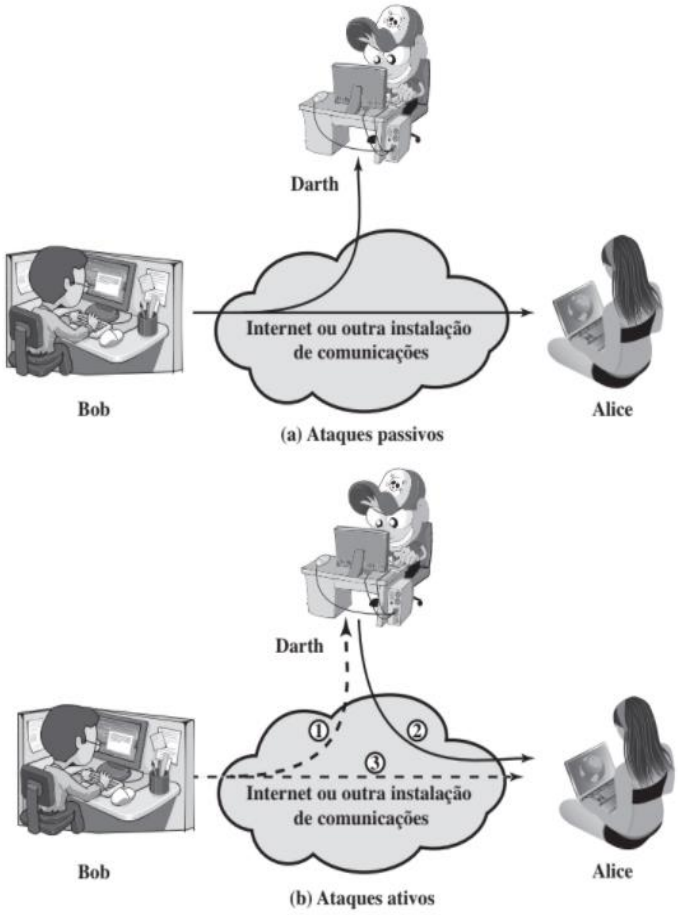
A criptografia, assim como nos demais casos, é uma grande arma a favor da integridade, pois protege a informação de acesso não autorizados e mudanças não autorizadas. Por sua vez, o *backup* também garante a integridade da informação através de restaurações (HINTZBERGEN, 2018).

Verificados, então, os princípios da segurança da informação, é necessário o estudo de um assunto igualmente importante ao presente estudo, que são as técnicas de ataques a segurança.

2.4 TÉCNICAS DE ATAQUES À SEGURANÇA

Existem diversos tipos de ataques à segurança, porém, todos esses ataques são classificados em duas modalidades: ataques passivos e ataques ativos. Enquanto o primeiro tenta utilizar dados e informações do sistema sem realizar alterações, o segundo tem o objetivo de alterar os recursos e ou afetar a operação dos sistemas (STALLINGS, 2015).

Figura 1 - Ataque passivo e ativo



Fonte: STALLINGS (2015)

2.4.1 Ataques Passivos

O ataque passivo representado na figura 01 tem a finalidade de visualizar a troca de mensagens sem realizar quaisquer alterações nas mensagens, podendo vazar as informações ou somente realizar análise do tráfego. O atacante pode copiar as mensagens que possuem dados sensíveis ou informações relevantes e realizar o compartilhamento destes dados (STALLINGS, 2015).

O segundo tipo de ataque passivo é a análise do tráfego, que, por sua vez, é mais sutil, pois caso a mensagem trocada seja encriptada o atacante não terá conhecimento do conteúdo das mensagens, mas conseguirá coletar outras

informações como a frequência das trocas de mensagens, o local e a identidade dos interlocutores e o tamanho das mensagens (STALLINGS, 2015).

Os ataques passivos são muito difíceis de serem detectados, pois não existem qualquer alteração nos dados e o sistema não tem sua operação interrompida. Tanto o emissor, quanto o receptor não percebem que outro, sem autorização, leu suas mensagens ou analisou o padrão do tráfego. Normalmente, esse tipo de ataque é evitado na prevenção ao invés da detecção (STALLINGS, 2015).

Um exemplo de ataque passivo é o *Sniffer*, um programa que monitora o tráfego de rede. Ele pode ser usado de forma desleal para roubar *logins*, senhas, cartões de crédito e demais informações (OLIVEIRA, 2003).

Os *Sniffers,* muitas vezes, são usados de forma legal para captura de dados, descrição de pacotes, soluções de problemas de rede, entre outros. Porém, quando usado de forma ilegal é uma ferramenta muito perigosa, permitindo que o atacante analise tudo que passa na rede de forma silenciosa (OLIVEIRA, 2003).

2.4.2 Ataques Ativos

Os ataques ativos, diferentemente dos ataques passivos, realizam a alteração no fluxo de dados ou criação de um fluxo não legítimo. Os ataques desse tipo podem ser subdivididos em quatro categorias: disfarce, repasse, modificação de mensagens e negação de serviços (STALLINGS, 2015).

O disfarce acontece quando uma entidade finge ser outra entidade com mais ou diferentes privilégios. Uma sequência de mensagens pode ser captada e reproduzida após a comunicação válida ser iniciada, permitindo que uma entidade com menos privilégios obtenha recursos extras que normalmente não teria (STALLINGS, 2015).

O repasse captura informações de forma passiva e retransmite para produzir um efeito não autorizado (caminhos 1,2 e 3 ativos) (STALLINGS, 2015).

A modificação da mensagem altera alguma parte legítima de uma mensagem ou as mensagens possuem sua ordem modificada, reproduzindo um efeito não autorizado (caminhos 1 e 2 ativos) (STALLINGS, 2015).

Por exemplo, uma mensagem que significa “Permitir que John Smith leia o arquivo confidencial contas” é modificada para “Permitir que Fred Brown leia o arquivo confidencial contas" (STALLINGS, 2015).

Nesse sentido, é de suma importância verificar algumas técnicas de ataques ativos.

Os ataques de negação de serviço, também chamados de *Denial-of-Service* (DoS), são métodos usados para interromper a disponibilidade e a utilização de sistemas. Esses ataques têm o objetivo de impedir que os usuários utilizem os recursos de um sistema alvo (caminho três ativo). Diferente de um ataque passivo, o ataque de negação de serviço é facilmente detectado, pois deixa o sistema inoperante ou com uma baixa performance recebendo reclamações dos usuários deste sistema. (HINTZBERGEN, 2018).

Também há a técnica *DNS Spoofing*, que ocorre quando é possível clonar o endereço DNS de um site considerado confiável. Na hipótese em que o DNS Spoofing é aplicado e faz o redirecionamento de solicitações de um endereço DNS específico da rede para um outro endereço, por exemplo, um site de esportes em que o usuário quer acessar, o atacante vai direcionar para um site que possui o mesmo endereço de URL. Isso faz com que o usuário pense que realmente está no site que gostaria de estar, mas na realidade o atacante está no controle de seu conteúdo (OLIVEIRA, 2003).

Por sua vez, a quebra de senhas é usada por diversos atacantes, muitos deles tentam descobri-las através dessa técnica, como, por exemplo, tentativas de senhas simples, nomes relacionados ao usuário, ou datas. Mas, para realizar estas tentativas, são utilizados vários programas que tentam inúmeras combinações para obter sucesso na descoberta (OLIVEIRA, 2003).

Já o *Ransomware* é um software que faz o bloqueio de acesso a todos os dados e cobra um valor para que o sistema volte ao normal. Em algumas situações em que mesmo sendo pago um resgate, os atacantes pedem um segundo resgate. Apesar de muitas organizações pagarem o resgate, os especialistas do assunto não indicam essa ação, pois a organização acaba se tornando um alvo maior e não se pode confiar nos criminosos (OLIVEIRA, 2003).

Com a pandemia em 2019 o mundo digital mudou muito, principalmente na forma em que as pessoas trabalham e o *ransomware* se tornou a principal ameaça no topo no ano de 2021 (Freitas, 2021).

Há também o *Rubber Duck,* um dispositivo USB mal-intencionado responsável por injetar comandos pré-definidos. Esses comandos são capazes de permitir acesso remoto ao computador de uma vítima e entre outras ações. Ao estar plugado no

computador da vítima, o *Rubber Duck* se “disfarça” de teclado, e dispara uma sequência de teclas pré-definidas (DIMITROVA, 2020).

Uma das ameaças mais conhecidas é o Vírus. O vírus do tipo *Worm* vem através de códigos maliciosos e executam funções não autorizadas em sistemas, implementam privilégios, obtêm informações importantes e rouba dados. São transmitidos por arquivos corrompidos em páginas suspeitas, podendo estar disfarçado de instaladores, a partir do momento em que ele acessa o alvo ele pode se espalhar de forma rápida em envios de mensagens com anexos ou links. Alguns *worms* são tão poderosos que podem fechar várias brechas de segurança do sistema para evitar infiltração de outros tipos de malwares, só para ter exclusividade no ataque (PINTO, et. al., 2020).

Outra forma de ataque é o *SQL Injection*, ao contrário da manipulação do código SQL, que é uma linguagem usada para troca de informações entre aplicativos e banco de dados relacionais, o SQL *Injection* acontece através da possibilidade de uma atacante inserir ou manipular consultas criadas pela aplicação, geralmente essas conexões são feitas em casos de um usuário com altos privilégios (CLARKE, 2012).

O SQL *Injection* é basicamente uma falha na codificação onde através de um input qualquer, é possível fazer uma manipulação SQL (CLARKE, 2012).

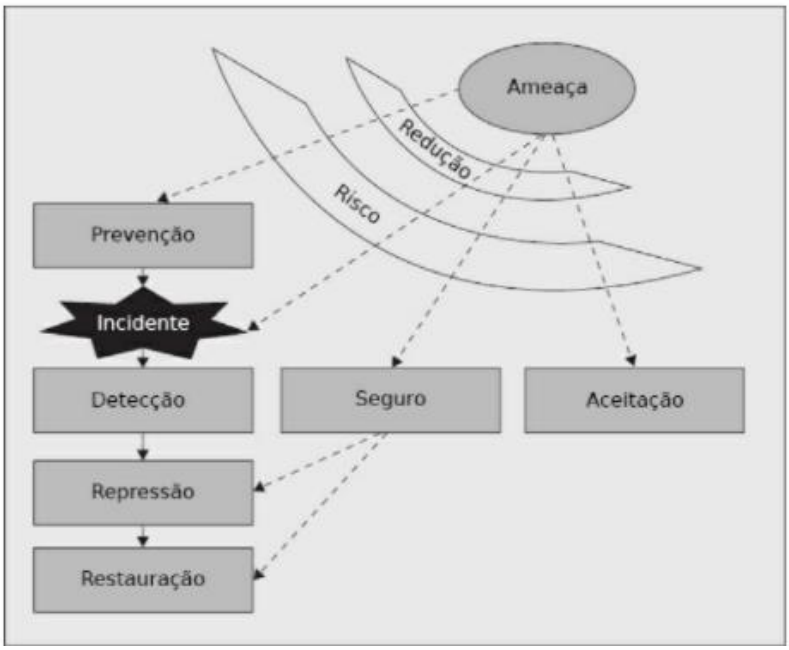
2.5 CONTRAMEDIDAS PARA ELIMINAR, NEUTRALIZAR E MINIMIZAR AMEAÇAS

Existem diversos tipos de ataques à segurança, porém, todos esses ataques são classificados em duas modalidades: ataques passivos e ataques ativos. Enquanto o primeiro tenta utilizar dados e informações do sistema sem realizar alterações, o segundo tem o objetivo de alterar os recursos e ou afetar a operação dos sistemas (STALLINGS, 2015).

As técnicas ou contramedidas administrativas evitam, neutralizam ou minimizam perdas ou indisponibilidade devido a ameaças à segurança. Caso uma organização queira mitigar as vulnerabilidades em seus serviços, ativos ou em sua rede, deve-se primeiramente, definir quais riscos podem ou não serem aceitos. Um risco pode ser aceito se, por exemplo, for acordado que determinado risco é baixo ou o custo de tratamento é demasiado. Essas técnicas podem ser divididas nas seguintes

formas: Prevenção, detecção, medidas repressivas, recuperação, seguro e aceitação (HITZBERGEN, 2015).

Figura 2 - Formas de segurança



Fonte: (HITZBERGEN e Col, 2015)

A prevenção tem como objetivo impossibilitar que a ameaça ocorra, em um ambiente físico podem ser inseridos níveis de acesso para determinados ambientes em uma organização, a fim de impedir acesso não autorizado por pessoas não autorizadas. A implementação de controles de alterações em produtos e sistemas pode garantir que alterações desnecessárias não sejam realizadas e sim implementadas de forma prevista e controlada (HITZBERGEN, 2015).

A detecção pode ser usada quando as consequências de um incidente são pequenas ou existe tempo suficiente para diminuir os danos causados. Por exemplo, apenas informar aos colaboradores de uma empresa que o acesso à *internet* é monitorado irá coibir a navegação imprópria na rede. Nesse caso, as ferramentas de monitoramento devem ser aliadas nesse tipo de contramedida, podendo detectar os padrões de comportamento de alguns usuários, além de aumentar a rastreabilidade maior na organização (HITZBERGEN, 2015).

As medidas repressivas possuem como objetivo minimizar o impacto dos danos causados por alguma vulnerabilidade. Por exemplo, caso um documento seja perdido, uma medida repressiva a ser tomada é o backup. Realizar uma cópia das informações

garante que os dados não sejam perdidos em totalidade. Neste caso, pode ser restaurada a última versão do documento salvo e ao invés de todos os dados do documento serem perdidos, somente uma parte desse documento será perdida (HITZBERGEN, 2015).

A recuperação tem atividade quando um incidente ocorre e algo deve ser recuperado, seja o dano grande ou pequeno, e está diretamente correlacionado com as medidas repressivas que foram tomadas. Caso um colaborador de uma empresa crie uma base de dados nova e sobrescreva uma outra base de dados que deveria estar ativa, a extensão desse dano depende da data do último backup, quanto mais recente menor a extensão do dano. Como medida corretiva um sistema de *stand-by* também é uma medida corretiva possibilitando o retorno imediato das atividades de uma organização (HITZBERGEN, 2015).

O seguro é cabível para eventos que não possam ser inteiramente prevenidos e que as consequências não sejam aceitáveis. Esse método busca mitigar as consequências. Por exemplo, um seguro de incêndio pode proteger uma organização de consequências financeiras de um incêndio, ao salvar dados insubstituíveis fora da organização (HITZBERGEN, 2015).

A aceitação inicia quando foram identificadas as ameaças e riscos e caso a gerência responsável decida não realizar as contramedidas necessárias de segurança, ou devido aos elevados custos ou por não haver contramedida adequada para mitigar os riscos (HITZBERGEN, 2015).

3 PROCEDIMENTOS METODOLÓGICOS

Tomando por base o tema em foco, o qual busca investigar as principais vulnerabilidades encontradas em produtos da área de tecnologia, torna-se de fundamental importância definir neste capítulo os procedimentos metodológicos utilizados e como a pesquisa é realizada em sua totalidade.

Isso se resume na observação sistemática dos fenômenos da realidade através de sucessivas etapas, sob a orientação de conhecimentos teóricos, com vistas a elucidar a causa desses fenômenos. É elaborada uma estratégia metodológica, a qual implica que os pesquisadores devam conceber a maneira prática e específica de responder às perguntas de sua pesquisa. Isso acarreta selecionar ou desenvolver um projeto de pesquisa e aplicá-lo ao contexto particular de seu estudo (VELASCO E VILLA, 2019, p. 74).

O referencial teórico discute e reflete sobre o tema em foco, para isso, motivo pelo qual é de fundamental importância o embasamento bibliográfico em produções de autores que discutem assuntos diretamente ligados ao tema, o que foi feito no capítulo 2.

A coleta de dados constitui uma das principais fases da pesquisa, já que a qualidade do material que é coletado deve afetar profundamente a qualidade do trabalho final a ser apresentado.

A necessidade de se utilizar uma abordagem qualitativa para a realização da coleta de dados tem origem na busca da compreensão e descrição do fenômeno pesquisado, e de buscar, através do estudo de caso, respostas à questão central do trabalho, isto é, os objetivos propostos.

3.1 TIPO DE PESQUISA

A caracterização do trabalho quanto a natureza se encaixa em pesquisa aplicada.

Quanto a abordagem, o tipo de pesquisa adotado para o desenvolvimento do trabalho de conclusão de curso é de abordagem qualitativa, pois, segundo os autores Sampieri, Collado e Lucio (2017 p. 376), apresentem as seguintes afirmações:

> O foco da pesquisa qualitativa é compreender e aprofundar os fenômenos, que são explorados a partir da perspectiva dos participantes em um ambiente

> natural e em relação ao contexto. O enfoque qualitativo é selecionado quando busca-se compreender a perspectiva dos participantes (indivíduos ou grupos pequenos de pessoas que serão pesquisados) sobre os fenômenos que os rodeiam, aprofundar em suas expectativas, pontos de vistas, opiniões e significados, isto é, a forma como os participantes percebem subjetivamente sua realidade. Também é recomendável selecionar o enfoque qualitativo quando o tema do estudo foi pouco explorado, ou que não tenha sido realizada pesquisa sobre ele em algum grupo social específico. O processo qualitativo começa com a ideia de pesquisa.

A pesquisa com enfoque qualitativo surgiu da necessidade de propor alternativas metodológicas para a pesquisa no campo das vulnerabilidades existentes em segurança da informação. Daí a importância da pesquisa com enfoque qualitativo (SAMPIERI, COLLADO E LÚCIO, 2017, p. 376).

Adotando-se do enfoque qualitativo, na pesquisa, é possível que o pesquisador participe e interfira na realidade pesquisada, e pode propor mudanças baseadas nos resultados do que será observado no entendimento das particularidades do comportamento dos indivíduos (SAMPIERI, COLLADO E LÚCIO, 2017, p. 376).

3.2 PESQUISA BIBLIOGRÁFICA

Segundo Ferenhof e Fernandes (2016, p. 550), “a revisão de literatura é a base para redação científica. É na revisão que o pesquisador se familiariza com os textos, identifica os autores que vêm escrevendo sobre o problema pesquisado”.

A caracterização do trabalho quanto a natureza se encaixa em pesquisa aplicada. A pesquisa, além de fundamentar nos conhecimentos teóricos já desenvolvidos a respeito do tema, na literatura especializada, fundamenta-se em referencial metodológico que permite o alcance dos objetivos do estudo. O primeiro procedimento consta de uma busca bibliográfica sistemática.

Quantos aos meios, a pesquisa bibliográfica será desenvolvida com base em materiais coletados em fontes secundárias no decorrer do desenvolvimento desta pesquisa, terá como acervo: livros e artigos científicos, sejam estes de leitura corrente ou de referência, que possibilita a obtenção de informações referentes ao tema em questão, considerando que a pesquisa a ser desenvolvida indicará a verificações diversas e análises de disposições acerca de um mesmo problema.

Como estratégia de pesquisa discorre-se que:

a) A pesquisa foi realizada para maior embasamento didático como preparação para a pesquisa estão sendo coletados dados disponíveis em plataformas online como

Google Acadêmico. O Google Acadêmico® para Creswell (2010) é uma base de dados gratuita que proporciona amplitude na busca na literatura de várias fontes, como teses, resumos e artigos, com a vantagem de poder obtê-los de forma integral. Ele também pode ser utilizado como auxílio às buscas complementares minimizando a possibilidade de que algum artigo reconhecido cientificamente e alinhado com o tema desta pesquisa não fosse incorporado ao portfólio bibliográfico (TASCA, 2013).

Também são usados livros disponíveis de forma online e exemplares físicos publicados entre os anos de 2011 - 2021, na língua portuguesa e de acesso gratuito.

b) utilizou-se as seguinte palavras-chave: “segurança da informação”; “vulnerabilidades”; “hackers”; “segurança de redes”; “segurança de TI”; “redes de computadores”; “Técnicas de invasão”; “teste de invasão”; “normas de segurança da informação”.

c) a análise de vulnerabilidade foi construída com base nos seguintes autores: Cruz (2017, p.14) e ISO 27000.

d) utilizou-se os seguintes livros e normas ISO 27.000 como o portfólio bibliográfico, por considerá-los fundamentais para a pesquisa.

Nome do Livro	Autor	Ano
Criptografia e Segurança de Redes	William Stallings	2015
Fundamentos de Segurança da Informação	Jule Hintzbergen, Kess Hintzbergen, André Smulderse Hans Baars	2018
Testes de Invasão	Georgia Weidman	2014
Gestão da Segurança da Informação	Marcos Sêmola	2013

Fonte: os autores

3.3 COLETA DE DADOS PRIMÁRIOS

A coleta de dados se dará através da realização de uma análise de vulnerabilidade com as seguintes etapas:

a) Identificação das Vulnerabilidades: realizar verificação em documentos organizacionais, como manuais de cunho sigiloso;

b) Realização de testes de intrusão;

3.4 ANÁLISE E DISCUSSÃO DOS DADOS

No que se refere ao tratamento e análise de dados, utilizou-se as etapas de tratamentos dos resultados e interpretações pertencentes a Análise de Conteúdo (Bardin, 2011). Desta forma, será possível ao final propor medidas de segurança para mitigar as vulnerabilidades em produtos tecnológicos.

3.5 DELIMITAÇÃO DA PESQUISA

Neste trabalho são realizadas generalização sobre o assunto estudado e na empresa estudada. Por outro lado, não são realizadas análises sobre todos os tipos de vulnerabilidades, somente sobre as vulnerabilidades de *softwares* abordando na forma de ataques ativos, os quais têm a intenção de realizar algum dano aos sistemas alvo. Utilizando das técnicas de força bruta para descobertas de senhas, ataques de negação de serviço (*Denial of Service*), descobertas de *backdoor, Keylogger*, ataques *man-in-the-middle*, ataques da camada TCP/IP.

Ressalta-se que devido a proteção dos dados organizacionais, o nome da empresa a ser estudada, seus documentos, manuais e especificações dos produtos serão mantidos em sigilo e nomeados como: Empresa X, Produto 1, Produto 2 e Produto 3.

4 DESCRIÇÃO DA EMPRESA ESTUDADA

A empresa X estudada neste trabalho está situada na região da grande Florianópolis, atua nas áreas de segurança, redes, comunicação e energia. Possui mais de 40 anos de experiência no mercado em desenvolvimento de equipamentos eletrônicos. Distribui suas soluções em mais de oito áreas de negócios, como: bancos, indústrias, aeroportos, saúde, escolas e universidades, construção civil, provedores, transportes e viagem e para o agronegócio.

É uma indústria eletrônica que tem especialidade em equipamentos corporativos e domésticos, conta com um portfólio bastante extenso, como telefones, centrais telefônicas, roteadores, switches entre outros produtos.

Está dividida em alguns setores tendo como seus principais setores Comunicação e redes oferecendo também algumas soluções integradas para facilitar e simplificar a vida e o trabalho das pessoas.

O setor de comunicação tem como seus principais produtos centrais telefônicas e telefones IP, oferecendo simplicidade para empresas de *call center*, e também é muito forte no setor de telefonia. Dessa forma, a central telefônica será o Produto 1 a ser analisado.

As centrais telefônicas têm o principal objetivo de facilitar a comunicação entre pessoas através de um mesmo ramal, possibilitando a realização de chamadas internas e externas, a central telefônica é fundamental para aperfeiçoar serviços de uma organização, trazendo facilidade e dinamismo ao ambiente corporativo.

As principais funcionalidades das centrais telefônicas são o recebimento e efetuação de chamadas internas e externas, centralizar todos as formas de comunicação em um único sistema, enviar informações de áudio e videoconferência, com identificador de chamadas, transferências, criação de ramais e redução de custos de telefonia.

As empresas geralmente são as principais compradoras de Centrais telefônicas, em vários setores, a central atende situações que precisam de uma comunicação constante e econômica.

No setor de redes um dos principais produtos são os switches, basicamente toda empresa precisa possuir esse produto na sua rede, pois esse aparelho é responsável por conectar computadores a rede de uma maneira que possam trocar

dados entre eles, switch irá receber dados de origem e encaminhar para uma máquina de destino, garantindo estabilidade entre máquinas da rede (TANEMBAUM, 2011).

Os switches gerenciáveis possibilitam a criação de grupos de rede através de uma VLAN, ou seja, é possível dar acesso a departamentos de uma empresa em arquivos específicos, também é possível criar redes para visitantes separando da rede corporativa.

Já os switches, serão os Produtos 2 e 3 a serem analisados.

Nos tópicos 4.1, 4.2 e 4.3 serão apresentados os produtos analisados, bem como as vulnerabilidades identificadas e as técnicas usadas para intrusão.

4.1 PRODUTO 1 - CENTRAL TELEFÔNICA

Neste tópico é abordado acerca da central telefônica, a qual possui dois ataques que obtiveram êxito: *SQL Injection* e autenticação.

4.1.1 SQL *Injection*

Os ataques ativos, diferentemente dos ataques passivos, realizam a alteração no fluxo de dados ou criação de um fluxo não legítimo. Os ataques desse tipo podem ser subdivididos em quatro categorias: disfarce, repasse, modificação de mensagens e negação de serviços (STALLINGS, 2015).

O disfarce acontece quando uma entidade finge ser outra entidade com mais ou diferentes privilégios. Uma sequência de mensagens pode ser captada e reproduzida após a comunicação válida ser iniciada, permitindo que uma entidade com menos privilégios obtenha recursos extras que normalmente não teria (STALLINGS, 2015).

Dentre os testes realizados, foi possível testar uma das principais Centrais telefônicas da empresa e obteve-se um acesso através de comando *SQL*.

Na tela de login foi inserido o nome do usuário como “admin” e no campo senha passado o comando “' OR '1'='1”, que está entre os principais comandos de *SQL Injection*. Ele faz com que o usuário e senha sejam sempre verdadeiros, permitindo acesso ao sistema sem mesmo possuir a permissão.

Neste caso, não é necessário saber a senha, pois a condição “*OR1=1”* sempre está satisfeita e todos os comandos posteriores são comentados.

Normalmente seriam informados os campos usuário e senha, os quais resultariam em uma consulta ao banco de dados da aplicação para realizar a verificação e conferência, mas sem a proteção devida no código do produto foi possível acessar sem a necessidade de uma senha.

Abaixo está a ilustração do passo-a-passo que foi utilizado para realizar a injeção *SQL* na central telefônica para realizar a intrusão na **vulnerabilidade de acesso ao login como administrador.**

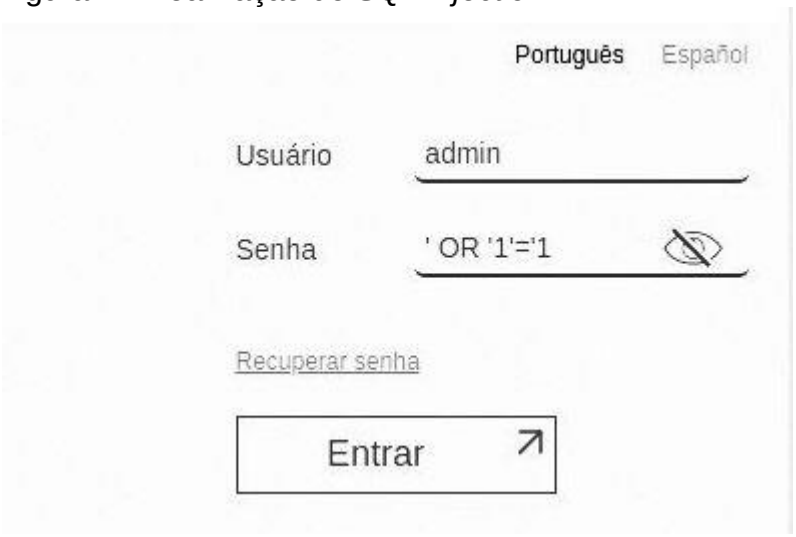
Primeiro, é realizado o acesso a interface web do produto e é inserido “admin’ que é um usuário padrão, tratando-se de um teste que foi feito dentro da empresa, então foi apenas necessário acessar a interface web estando na rede coorporativa.

Figura 3 - Página de primeiro acesso da central

Fonte: (O Autor)

Na sequência, é inserido o comando “' OR '1'='1” no campo senha e dado o click no “Entrar”.

Figura 4 - Realização do *SQL injection*



Fonte: (O Autor).

Em seguida, é possível acessar a Central com todas as opções de “admin”.

Figura 5 - Acesso realizado

Fonte: (O Autor)

A partir desse ponto, o invasor tem controle de todo o sistema da central.

4.1.2 Autenticação

Logo após, foi realizado o processo de segurança de autenticação.

Neste ponto, é observado que não é necessário estar autenticado para realizar operação de gerenciamento na Central Telefônica, uma vez que é possível trocar o usuário e senha do usuário “admin” sem nenhum tipo de autenticação.

Através de um *script* PHP, é realizada uma requisição usando o protocolo HTTPS em conjuntos com o método *POST* para URL “/sistemaUsuarios.htm”.

Abaixo na figura 6 está o passo-a-passo que foi utilizado para adicionar um usuário de sistema, explorando a **vulnerabilidade de criação de usuário de forma não autorizada, sem autenticação da central.**

Figura 6 - Código *PHP* para adicionar um usuário

Fonte: (O Autor)

No corpo da requisição é informado alguns valores e atributos “'evento=salvar&Indice=0&Usuario=arthur&Senha=arthur&Idioma=0&Perfil=1'”.

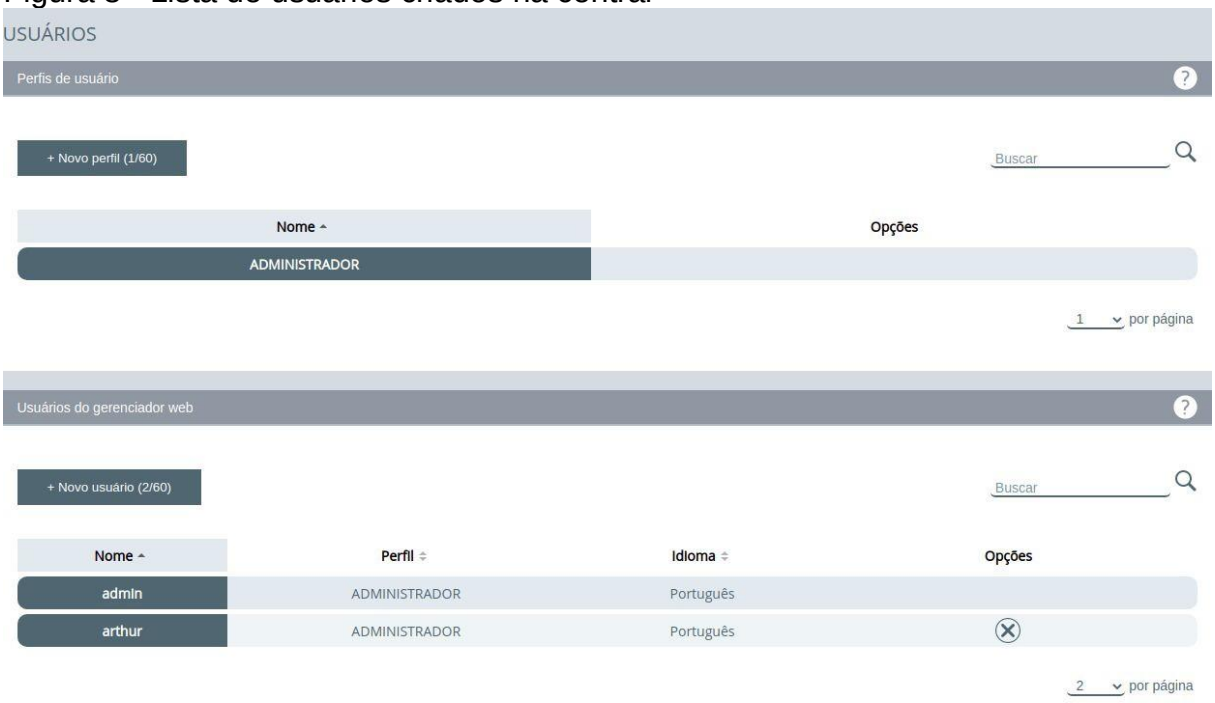
Em seguida, é possível fazer o acesso com as credenciais login: “arthur” e senha “arthur”.

Figura 7- Acesso com novo usuário

Fonte: (O Autor)

Ao clicar em “entrar”, é possível realizar o acesso a central e depois de acessar a aba “Sistemas e Usuários”, fica visível a adição do usuário “Arthur” como perfil administrador.

Figura 8 - Lista de usuários criados na central



Fonte: (O Autor)

Com esse acesso realizado pela intranet, o usuário cadastrado a partir do comando:“'evento=salvar&Indice=0&Usuario=usuario&Senha=senha&Idioma=0&Perfil=1'” pode cadastrar qualquer usuário bastando somente alterar os parâmetros de “Usuário” e “Senha”.

Além de adicionar um usuário com privilégios de administrador, também é possível excluir usuários informando o índice no *script* juntamente com o valor “excluir” no atributo “evento”, reaproveitando o *script* para adição de usuário é possível alterar o parâmetro “CURLOPT_POSTFIELDS”, passando os valores 'evento=excluir&Indice=0'.

Figura 9 - Código *PHP* para remover um usuário

exclui.php

```php
<?php

$curl = curl_init();
curl_setopt_array($curl, array(

CURLOPT_URL => 'https://172.31.11.125/sistemaUsuarios.htm',
CURLOPT_SSL_VERIFYHOST => false,
CURLOPT_SSL_VERIFYPEER => false,
CURLOPT_RETURNTRANSFER => true,
CURLOPT_ENCODING => '',
CURLOPT_MAXREDIRS => 10,
CURLOPT_TIMEOUT => 0,
CURLOPT_FOLLOWLOCATION => true,
CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
CURLOPT_CUSTOMREQUEST => 'POST',
CURLOPT_POSTFIELDS => 'evento=excluir&Indice=0',
CURLOPT_HTTPHEADER => array(
'Contet-Type: text/plain'
),
));

$response = curl_exec($curl);
curl_close($curl);

echo $response;
?>
```

Fonte: (O Autor)

Após a execução do código via terminal estando conectado na rede da empresa, basta acessar a página web do produto e tentar logar com o usuário excluído.

Verificado, portanto, o “Produto 1”, passa-se a análise do “Produto 2”.

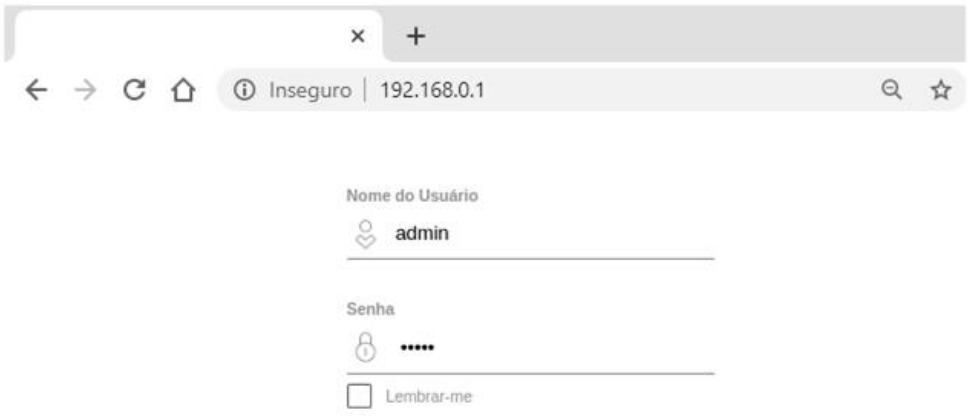
4.2 PRODUTO 2 - SWITCH GERENCIÁVEL

Todo switch gerenciável possui uma interface de gerenciamento, que possibilita a configuração de funcionalidades com o objetivo de otimizar a rede no qual o produto está instalado (CAMPOS; PAIXÃO, 2019).

As formas de realizar esses acessos, são através de uma interface web de gerenciamento, outra forma é a linha de comando chamado de CLI (*command line interface*). (CAMPOS; PAIXÃO, 2019).

A primeira utiliza um servidor web embarcado no produto, que ao digitar o endereço IP do produto o usuário é direcionado a interface de primeiro acesso, o protocolo utilizado para essa comunicação é chamado HTTP (*Hypertext Transfer Protocol).*

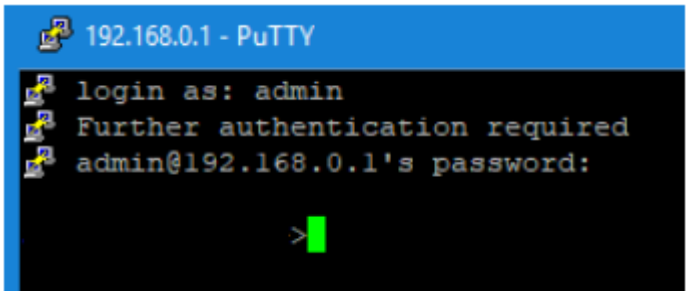
Figura 10 - Página de acesso do switch



Fonte: (O Autor)

No segundo modo, o produto pode ser acessado via uma linha de comando, no qual a interação com o produto é feita na forma de comandos escritos, que são interpretados pelo switch em uma sessão de comunicação. Esse protocolo de comunicação é chamado SSH (secure shell) (CAMPOS; PAIXÃO, 2019).

Figura 11 - Acesso via SSH



Fonte: (O Autor)

Foi utilizado duas formas de ataques para testar a segurança do produto em análise: *Denial of Service (DoS)* e senha sem criptografia.

4.2.1 *Denial of Service* (DoS)

Neste ataque é utilizado o programa Hydra, um utilitário para realizar teste de força bruta para descobrimentos de senhas, principalmente as que são fracas e configuradas em dispositivos de rede (MORENO, 2015).

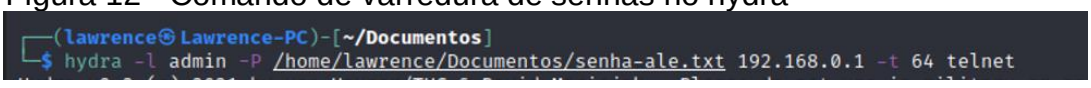
Tendo como premissa que sabemos o usuário de acesso ao produto, neste teste é utilizado um recurso no qual o programa acessa um arquivo com diversas variações de senhas.

A lista de senhas é extensa, então simula-se diversas sessões SSH simultâneas, a cada tentativa o programa repete a operação até encontrar a senha que conseguir acessar ao alvo.

Seguindo a premissa supracitada, simulou-se diversas sessões SSH simultâneas, a cada tentativa o programa repete a operação até encontrar a senha que conseguir acessar ao alvo.

Abaixo estão as figuras mostrando os detalhes de como a **vulnerabilidade de negação de serviço foi reproduzida.**

Figura 12 - Comando de varredura de senhas no hydra

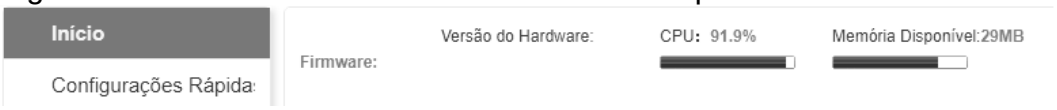


Fonte: (O Autor)

O argumento utilizado no comando “-t 64” informa ao programa que serão 64 sessões SSH abertas simultaneamente. O programa funciona até que todas as senhas salvas no arquivo “senha-ale.txt” sejam usadas.

No início desse teste, é observado que o produto fica extremamente lento. Após poucos segundos, o *switch* para de operar, ocorrendo o travamento da sua gerência, o que impossibilita o administrador de rede utilizar o dispositivo alvo.

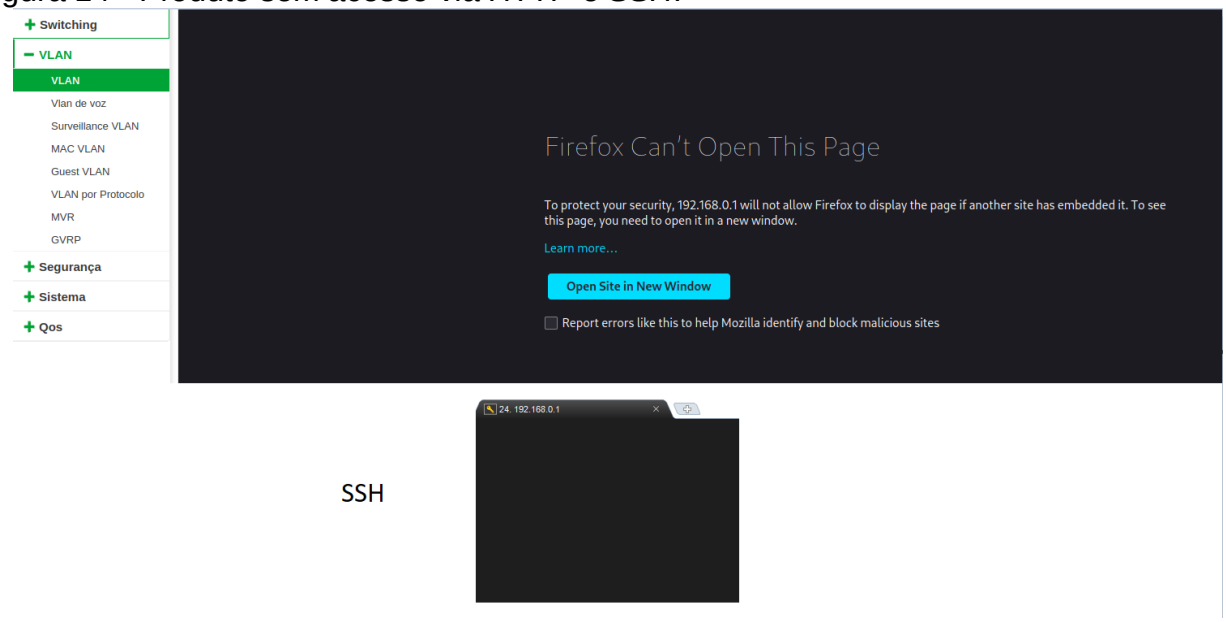
Figura 13 - Verificando recursos de hardware do produto



Fonte: (O Autor)

Após alguns segundos, não é possível realizar o acesso ao gerenciamento do produto:

Figura 14 - Produto sem acesso via *HTTP* e *SSH*.



Fonte: (O Autor)

A partir desse estágio, o ataque de negação de serviço (DoS) foi realizado com êxito.

4.2.2 Senha sem Criptografia

Um switch gerenciável possui um arquivo, chamado “*startup-config”*, que é responsável por salvar todas as configurações de rede. Caso o item seja desligado acidentalmente, ou ocorra uma eventual falha de energia, esse arquivo faz com que o produto reinicie com as mesmas configurações antes da reinicialização, evitando assim que o usuário configure o dispositivo novamente (CAMPOS; PAIXÃO, 2019).

Em uma rede de médio e grande porte, os administradores podem salvar esses arquivos de configuração em um servidor ou desktop, para eventual backup caso um switch na rede pare de funcionar e a substituição seja necessária, tirando a necessidade de realizar toda a configuração manualmente, como: endereços IPs, configuração de VLANs, modo de operação das interfaces entre outros. (CAMPOS; PAIXÃO, 2019).

No produto estudado, é constatado que no arquivo de configuração a senha de usuário para acesso da interface web não são criptografadas, de modo que ocorre uma falha de segurança, pois a senha em texto claro (totalmente legíveis) pode ser usada para acessar e configurar o produto com privilégios de administrador.

Ao entrar nas configurações do produto via conexão SSH, é possível com o comando “*show running-config*” verificar que a senha de um usuário do tipo “*web*” está em texto claro, conforme mostra a figura a baixo é possível observar a **vulnerabilidade de senha sem criptografia**.

Figura 15 - Resultado do comando “*show run*”

```
username web admin password admin
username web user password user
web-login-time 1800
web-language en
web http port 80
```

Fonte: (O Autor)

4.3 PRODUTO 3 – SWITCH GERENCIÁVEL

O equipamento em questão é um *switch* PoE (Power Over Ethernet), produto lançado há mais de 4 anos e ainda é comercializado. Ele possui 28 portas *ethernet* e pode alimentar dispositivos através do cabo de rede, neste produto verifica-se uma vulnerabilidade do tipo crítica.

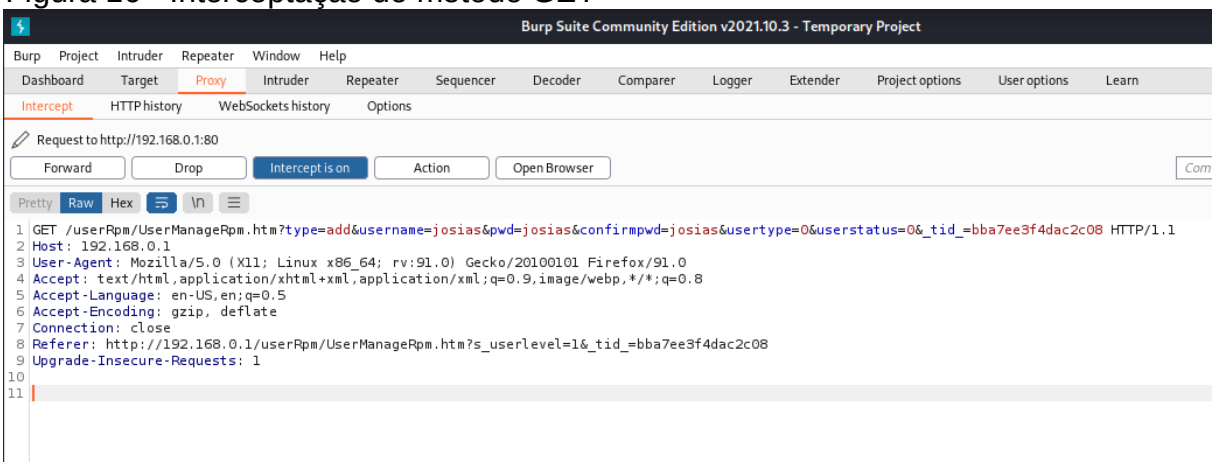
4.3.1 ESCALONAMENTO DE PRIVILÉGIOS

Neste produto existem dois tipos de usuários: o usuário administrador e o usuário convidado. O primeiro pode realizar todas as configurações possíveis no produto, já o segundo tem apenas acesso a visualizar as informações do dispositivo e não pode alterá-las.

Ao acessar o produto com um usuário administrador e criar um usuário, foi capturado a requisição que é enviada do navegador ao dispositivo para a criação deste usuário, com a utilização de um servidor proxy.

A seguir se encontra a figura com o início da exploração da **vulnerabilidade de escalonamento de privilégios**.

Figura 16 - Interceptação do método *GET*



Fonte: (O Autor)

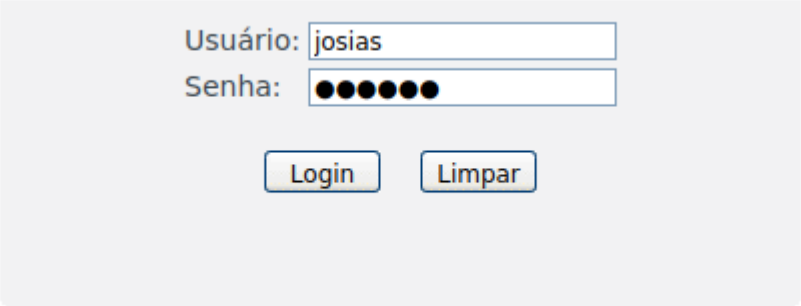
Na linha 1 da imagem acima é possível verificar o método GET enviado do navegador com destino ao switch.

Se for analisado em detalhes, verifica-se que todos os parâmetros para a criação de um usuário são fornecidos nesta etapa como: “type=add” esse parâmetro informa que será adicionado um novo usuário na lista de usuários; “username=josias” este parâmetro informa o nome do usuário que será criado; “pwd=josias” é uma abreviação de “password” e informa a senha do usuário; “confirmpwd=josias” é a confirmação da senha; “usertype=0” informa o privilégio do usuário, 0 para usuário convidado e 1 para usuário do tipo administrador e “tid= bba7ee3f4dac2c08”, valor do cookie de uma sessão logada como administrador.

Nesta análise é possível conferir que será criado o usuário “josias”, com a senha “josias” e o tipo de usuário é convidado.

O primeiro passo é realizar o login com o usuário recém-criado e coletar o cookie do navegador de uma sessão de usuário convidado.

Figura 17 - Login como usuário tipo convidado

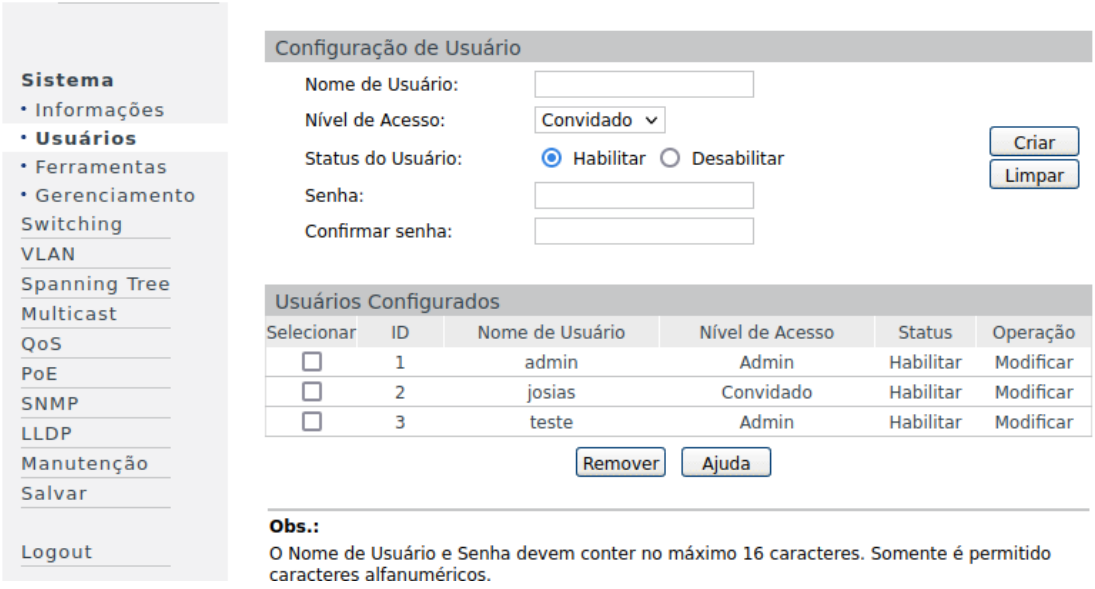


Fonte: (O Autor)

Com a sessão ativa, o segundo passo é utilizar o mesmo método GET capturado na sessão de administrador e substituir o cookie de administrador pelo cookie de convidado em uma nova aba do navegador, o seguinte código é utilizado:http://192.168.0.1/userRpm/UserManageRpm.htm?type=add&username=teste&pwd=teste&confirmpwd=teste&usertype=1&userstatus=0&_tid_=30f17fdd4091bde8”.

Neste comando pode-se verificar que é criado um usuário com o nome “teste”, “senha teste”, do tipo “administrador”. Analisa-se o resultado obtido.

Figura 18 - Criando usuário teste



Fonte: (O Autor)

A vulnerabilidade encontrada é obtida onde um usuário do tipo convidado conectado no sistema consegue criar um usuário de nível administrador. Normalmente o usuário convidado não tem permissões de configuração do produto, apenas de visualização.

A partir desse ponto, o usuário convidado pode realizar qualquer operação dentro do dispositivo.

Nesse sentido, após o estudo dos produtos, o capítulo a seguir trata da análise e discussão de resultados encontrados a partir dos testes realizados.

5 ANÁLISE E DISCUSSÃO DE DADOS

Com as vulnerabilidades apresentadas, pode-se analisar alguns riscos diante desses produtos, as pessoas e organizações relacionadas a eles.

Sendo assim, é importante relatar as causas dessas vulnerabilidades, se descobertas por pessoas maliciosas e também como solucionar essas brechas.

5.1 RESOLUÇÃO SQL *INJECTION* CENTRAL TELEFÔNICA

A melhor forma de evitar um *SQL Injection* é fazendo a validação dos dados digitados pelo usuário. Este é um dos principais motivos pelo qual o SQL é possível de ser feito. Então, é necessário que seja feita uma validação da entrada de dados no formulário e de forma alguma permitindo os caracteres indevidos: (‘), (--) e (;) evitar as palavras “*drop*”, “*insert*”, “*delete*” (CLARKE, 2012).

Outro método de tratamento é a correção e validação dos erros sem expor informações sobre a estrutura dos dados, não se deve construir instruções *SQL* diretamente na entrada de dados do usuário. Sendo assim, é necessário sempre testar as variáveis de cadeia de caracteres e somente aceitar valores esperados. Junto a isso, todas as vezes devem ser rejeitados valores binários e caracteres de comentário. Isso pode ajudar a prevenir a injeção *SQL* (CLARKE, 2012).

Para resolver a situação do *SQL Injection* da Central Telefônica, foi inserido uma validação para que quando o usuário informasse o *login* e senha. Caso esse *input* não fosse encaminhado diretamente ao banco de dados, então esses dados são armazenados por uma variável, fazendo o *select* no usuário separadamente.

Depois, é feita a comparação com a senha selecionada inserida na variável armazenada. Assim, a comparação passou a ser feita primeiro na linguagem do sistema e não diretamente dentro do banco de dados.

Fazendo os ajustes necessários para melhorar a proteção da Central, é possível evitar a quebra da confidencialidade, integridade e disponibilidade.

Verifica-se:

Figura 19 - Código de validação dos dados

sqlInjection.c

C: > Users > dime- > Documents > C sqlInjection.c

```c
char senhaSelecionada[200] = {PONTEIRO_VAZIO};
        char pchFiltroSelect[410] = {PONTEIRO_VAZIO};
        char pchResultadoSelect[3000] = {PONTEIRO_VAZIO};
        char *pchValorResultadoSelect = pchResultadoSelect;

        sprintf(pchFiltroSelect, "Usuario='%s'", paramUsuario.valor);
        if(recuperarTabela(TAB_USUARIOS, "Senha", pchFiltroSelect, pchResultadoSelect) == CONFIG_OK){
          pchValorResultadoSelect = pchResultadoSelect;
          getStringConsulta(&pchValorResultadoSelect, senhaSelecionada);
          if(STRINGS_IGUAIS(senhaSelecionada, paramSenha.valor)){
            LoginFail = FALSE;
          }else{
            LoginFail = TRUE;
          }
        }else{
          LoginFail = TRUE;
        }

```

Fonte: (O Autor)

Desse modo, é imperioso tratar sobre os riscos e prejuízos causados pela SQL *injection.*

5.1.1 Riscos e prejuízos causados por um SQL injection

Um ataque tão simples de ser feito pode causar danos extremamente prejudiciais.

No caso de um acesso por *SQL Injection* a uma central telefônica, o invasor teria acesso à telefonia da empresa, podendo registrar-se como um dos telefones com direito de receber e originar chamadas em grande quantidade para números nacionais e internacionais. Isso pode causar danos financeiros enormes, caso a invasão não seja detectada rapidamente.

Além disso, na hipótese de a central estar configurada para utilizar o *SMTP* que é um protocolo para envio de e-mail, ou seja, encaminhar a mensagem ao destino pretendido.

Com essa configuração, o invasor pode visualizar *e-mails* e senhas configurados, fazendo com que o prejuízo se torne ainda maior.

Tendo acesso a central, o invasor também poderia desconfigurá-la, de modo que toda a empresa ficaria sem receber e originar chamadas até que a central fosse restabelecida.

Ainda, através do acesso do sistema na parte de captura de tráfego de voz, o atacante poderia ouvir chamadas sigilosas e vazar informações.

Por isso, é necessário que seja feita uma correção o mais rápido possível para evitar todas essas situações indesejadas.

Um fato encontrado ao decorrer das pesquisas, foi que é possível fazer a injeção em Centrais com uma simples busca no Google usando os termos "*intitle*: Nome da Central | Manual". Existe a possibilidade de encontrar esses equipamentos que estão com a porta 443 direcionadas para internet.

Logo, ultrapassada a verificação de riscos e prejuízos à instituição, passa-se à resolução da autenticação indevida.

5.2 RESOLUÇÃO DA AUTENTICAÇÃO INDEVIDA (PRODUTO 1 - CENTRAL TELEFÔNICA)

Descobrindo o caminho certo através de uma simples investigação no navegador, é possível inserir o *script* informado e adicionar um novo usuário como administrador.

A resolução que será informada ainda está em andamento na empresa que passou pelos testes, e até o momento a ideia da implementação é ajustar a rota de criação de usuários para antes de processar a requisição, realizar a validação para verificar se o usuário está devidamente logado na Central. Somente se ele estiver logado no sistema, deve ser processada a requisição, caso contrário essa requisição deve ser bloqueada.

Realizando os devidos ajustes nesta vulnerabilidade, será evitado a quebra dos três pilares da segurança da informação (confidencialidade, integridade e disponibilidade).

5.2.1 Riscos e prejuízos causados pela autenticação indevida

Há grandes riscos com a possibilidade de trocar o nome usuário e senha de um perfil administrador em uma central telefônica.

Isso porque pode alterar uma senha de "admin" o usuário consequentemente impossibilita que o verdadeiro administrador entre na própria central, pois quando este estiver colocando suas credenciais, não estarão mais corretas.

O invasor pode acessar e alterar a central com direitos de administrador. Diante disso, pode desconfigurar a central e deixá-la impossibilitada de receber e realizar chamadas, realizando ligações e consequentemente trazendo prejuízos financeiros.

Mesmo sem acessar a central, a pessoa maliciosa pode alterar o nome e senha de todos os usuários, bastando apenas mudar o índice no *script* criado, da maneira que tornará a central inacessível a todos que antes utilizavam.

Superada esta análise, há de se destacar, ainda neste capítulo, os testes feitos com *denial of service* no produto 1.

5.3 RESOLUÇÃO *DENIAL OF SERVICE* NO PRODUTO 2, *SWITCH*

Para a resolução da vulnerabilidade de negação de serviço, se faz necessário a implementação de alguns mecanismos de defesa, o que foi verificado através dos testes realizados.

O primeiro deles se baseia em impedir diversas tentativas de acesso consecutivas.

O produto pode bloquear novas tentativas de acesso por 30 segundos, caso sejam realizadas 3 tentativas de acesso com as credenciais incorretas. Desta forma, o atacante não consegue pelo método de força bruta, utilizar infinitas combinações de credenciais a fim de obter as credenciais de acesso sem autorização.

O ataque pode ser estendido e potencializado caso sejam encontradas as credenciais de acesso. Com base nesta credencial descoberta, é possível realizar uma varredura na rede para encontrar outros dispositivos que possam ter as mesmas credenciais, ou focalizar as tentativas de força bruta em variáveis semelhantes das credenciais obtidas.

Para incremento da segurança, a segunda forma para evitar uma indisponibilidade no sistema é estipular um número máximo de sessão ativas simultaneamente, isso evita que a cada sessão aberta o switch disponibilize recursos de *hardware,* como memória, processador e armazenamento para sessões não genuínas.

Em um cenário real, nenhum *switch* na rede será operado por diferentes usuários ao mesmo tempo. No teste realizado, foi possível abrir 64 sessões simultâneas. Se o limite de sessões ativas for configurado em 4 sessões por exemplo, os recursos de *hardware* necessários serão baixos em relação a capacidade total do

dispositivo e a negação de serviço não ocorrerá. Com a implementação destas técnicas a disponibilidade e integridade do produto serão preservadas.

Então, a seguir, são vistas as conclusões acerca dos riscos e prejuízos causados pelo d*enial of service*.

5.3.1 Riscos e prejuízos causados pelo DoS

Os riscos do tipo de ataque ora analisados variam de acordo com a utilização do dispositivo, posição dele na hierarquia da rede e os dados trafegados nele. Para fim de exemplo, um *switch* de 24 portas se usado na sua totalidade pode encaminhar por um total de 48 *gigabit* por segundo de dados.

Além disso, esse produto pode conectar e interconectar diversos dispositivos na rede de uma empresa como, impressoras, computadores, servidores, roteadores, *access points,* câmeras e gravadores de imagem. Diversos serviços podem passar pelo switch em direção a internet e caso um produto desta complexidade pare, a rede de uma empresa pode ser comprometida, com lentidões, travamentos e até indisponibilidade de serviços que requerem alta largura de banda para perfeito funcionamento. A integridade e disponibilidade desse equipamento devem ser bem conservadas para a boa operação da rede de uma organização.

5.4 RESOLUÇÃO SENHA SEM CRIPTOGRAFIA NO PRODUTO 3, SWITCH

A solução desta vulnerabilidade pode ser resolvida de forma simples. A implementação consiste em adicionar um algoritmo de criptografia que possa cifrar textos curtos (senhas) no momento da criação de um usuário. É um padrão de mercado onde grandes *players* como *Cisco, HP, Dell* já realizam em seus equipamentos (CAMPOS; PAIXÃO, 2019).

5.4.1 Riscos e prejuízos causados por senha sem criptografia

A criptografia de senhas é um recurso importante em uma empresa informatizada, onde um dos recursos mais valioso de uma organização é a informação. Este tipo de produto não é acessado com frequência em uma empresa,

pois nele rodam diversos protocolos de redes que são responsáveis pela rede ficar estável e disponível.

A configuração desses protocolos é complexa e pode mudar de switch para switch dependendo da hierarquia que eles estão em uma rede, sendo assim, os administradores salvam esses arquivos de configuração como um backup, caso algum problema com o produto venha ocorrer, como uma substituição por queima, configuração aplicada de forma errônea, entre outros motivos, então esse arquivo de configurações será usado a fim de facilitar a configuração do equipamento.

Com base nessas premissas, caso esse arquivo seja aberto em um leitor de texto por uma pessoa não autorizada, esse indivíduo consegue descobrir o endereço de acesso do produto e caso as senhas não estejam criptografadas ele pode obter o total acesso ao equipamento e causar diversos danos ao ambiente no qual o produto está instalado.

5.5 RESOLUÇÃO ESCALONAMENTO DE PRIVILÉGIOS

A vulnerabilidade de escalonamento de privilégios pode ser resolvida da seguinte forma.

Não autorizar internamente no software do produto cookies de usuários do tipo convidado em nenhuma das mudanças de configuração, isso pode ser validado antes de ser aplicada as configurações no produto. Pois o equipamento não realiza a validação dos cookies de usuários, para o usuário convidado são removidos apenas os menus de configurações da interface web. Uma forma rápida de resolver o problema sem esperar uma correção de firmware, é remover os usuários convidados e somente os administradores do sistema terem acesso ao equipamento.

5.5.1 Riscos e prejuízos escalonamento de privilégios

Este escalonamento de privilégios dá poder a um operador ou convidado que já possui acesso ao produto a realizar configurações de administrador. Com a utilização de *sniffers,* é possível verificar a comunicação entre o equipamento e o navegador e capturar o método GET utilizado, com isso o usuário mal-intencionado consegue mudar o privilégio do seu usuário, ou criar e remover outros usuários. O

prejuízo causado pode depender de diversos fatores como a nível da hierarquia do produto na rede e a quantidade de equipamentos interconectados.

5.6 SUGESTÕES PARA A EMPRESA

Com o resultado das vulnerabilidades encontradas e com o objetivo de identificar e resolver fragilidades em software de produtos, sugere-se como medida de longo prazo a criação de um setor especializado em segurança da informação, que é atualmente inexistente na empresa. Além disso, como medidas de curto prazo em vulnerabilidades com altos riscos, sugerimos a contratação de uma empresa de consultoria de segurança da informação a fim de solucionar os problemas em tempo hábil.

6 CONCLUSÃO

De acordo com os dados coletados a partir da presente pesquisa pode-se analisar que há formas distintas de vulnerabilidades e ataques de segurança em produtos de tecnologia. Isso ocorre pelo crescimento gradativo do uso da tecnologia de modo que surgem cada vez mais oportunidades para invasores e criminosos.

O estudo realizado em uma indústria de tecnologia da Grande Florianópolis/SC trouxe a análise de três produtos que indicaram algumas problemáticas no que se refere ao assunto de segurança. Em resumo, em três produtos estudados foram encontradas quatro vulnerabilidades de softwares, as quais ferem os pilares da segurança da informação, sendo eles: integridade, confidencialidade e disponibilidade.

Foram identificadas, através das fragilidades encontradas na central, que o invasor pode causar prejuízos partindo de acessos não autorizados. Isso pode originar chamadas não autorizadas que causam gastos financeiros para a organização e podem gerar a indisponibilidade da infraestrutura telefônica por conta de desconfiguração. A mesma vulnerabilidade pode ocorrer com um switch que, através de um ataque de negação de serviço, pode tornar impraticável as atividades da empresa, indisponibilizando a rede e todas as aplicações em execução.

Neste sentido, sugerindo uma forma de mitigar as vulnerabilidades a longo prazo é necessário que haja adequação quanto ao gerenciamento das referidas vulnerabilidades para a organização estudada, como por exemplo, o investimento e criação de um setor especializado em segurança da informação para realização de testes de vulnerabilidade nos produtos desenvolvidos, sendo essa uma etapa obrigatória para o lançamento de novos produtos.

Para medidas de curto prazo, sugere-se que haja consultoria de uma empresa especializada em segurança da informação, abordando de forma efetiva os principais produtos da empresa.

Concluiu-se que através de estudos e testes foram identificadas vulnerabilidades em software de produtos em uma empresa de tecnologia, foi analisado como mitigar as fragilidades encontradas, sugerindo investimento na área da segurança da informação para gerenciamento das vulnerabilidades, e com essas informações coletadas é possível tornar os produtos da organização mais seguros,

sendo assim outras empresas podem se basear nessa identificação dos problemas e partir para resolução dos mesmos.

Portanto, verifica-se que mais estudos sejam necessários para melhor avaliação dos parâmetros de vulnerabilidades tanto da empresa pesquisada quanto nas demais empresas voltadas a tecnologia, visto que é de suma importância manter o controle de possíveis ataques nos sistemas e produtos da empresa assim foi realizado no presente trabalho. Além disso, após a identificação de vulnerabilidade entende-se quais os caminhos para solucionar a fragilidade em um sistema que está vulnerável.

REFERÊNCIAS

CAMPOS, Gabriel de Souza; PAIXÃO, Filipe Carvalho da. DESENVOLVIMENTO DE FERRAMENTA DE GERENCIAMENTO DE FUNCIONALIDADES DE SWITCHES, ROTEADORES E CME DA CISCO PARA OTIMIZAÇÃO DE PROCESSO DE CONFIGURAÇÃO PARA GARANTIA DE QUALIDADE COM USO DA LINGUAGEM PYTHON. **Revista Computação Aplicada - Ung-Ser**, [S.L.], v. 7, n. 1, p. 27, 3 out. 2019. Revistas Cientificas Eletronicas UNG. http://dx.doi.org/10.33947/2316-7394-v7n1-3521.

CLARKE, Justin. **SQL Injection Attacks and Defense**. 2. ed. Massachusetts: Syngress Publishing, 2012. 576 p.

CRESWELL, John W. **Projeto de pesquisa métodos qualitativo, quantitativo e misto**. In: Projeto de pesquisa métodos qualitativo, quantitativo e misto. Artmed, 2010.

DIETERLE, Daniel W. **Basic Security Testing With Kali Linux**: Third Edition. 3. ed. Estado Unidos: CyberArms, 2018. p. 1-428.

EXAME. **Novo vazamento de dados expõe 100 milhões de celulares, incluindo o de Bolsonaro**. Aparecida, 2021. Disponível em: https://exame.com/tecnologia/novo-vazamento-de-dados-expoe-100-milhoes-de-celulares-incluindo-o-de-bolsonaro/. Acesso em: 28 set. 2021.

FERENHOF, Helio Aisenberg; FERNANDES, Roberto Fabiano. Desmistificando a revisão de literatura como base para redação científica: método SSF. **Revista ACB**, v. 21, n. 3, p. 550-563, 2016.

FRAGA, Bruno. **Técnicas de invasão**: Aprenda as técnicas usadas por hackers em invasões reais. 1. ed. Brasil : Editora Labrador , 2019. p. 1-296.

GIRALDI, E. E. D. S. T. M. M. K. S. M. V. L. **Riscos, ameaças e vulnerabilidades: O impacto da segurança da informação nas organizações**. Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana) Americana – SP - Brasil, São Pulo , p. 1-13, jan./2018. *E-book.*

GU, Qijun; LIU. **Denial of Service Attacks**. Departamento de Ciência da Computação Texas State University, Texas, p. 1-28, jan./2005. Acesso em: 20 set. 2021. *E-book*.

HINTZBERGEN, Jule. **Fundamentos de Segurança da Informação**: com base na iso 27001 e na iso 27002. Rio de Janeiro: Brasport, 2018. 190 p.

ISO/IEC, Abnt Nbr. **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Brasil , v. 1, n. 3, p. 1-66, out./2019.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers Expostos 7**: Segredos e Soluções para a Segurança de Redes. 7. ed. Brasil: Bookman, 2013. p. 1-760.

MELO, Sandro. **Exploração de Vulnerabilidades Tcp/Ip Em Redes**. 3. ed. Brasil: Alta books, 2017. p. 1-640.

MORENO, Daniel. **Introdução ao Pentest**. Santa Terezinha: Novatec, 2015. 296 p.

PEREIRA, Fabio Luiz Barboza; SILVA, Cecília Alberton Coutinho. **Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT**. Rio de Janeiro, 2021. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/. Acesso em: 26 set. 2021.

ROSS, J. K. K. **Redes de computadores e a internet**. 6. ed. Brasil: Pearson Universidades, 2013. p. 1-658.

SAMPIERI, R. H., Collado, C. F., e Lucio, M. D. P. B. Metodologia da pesquisa científica (5ª ed.). Porto Alegre: Penso, 2017.

SÊMOLA, Marcos. **Gestão da segurança da informação**: Uma visão executiva. 2. ed. Brasil: Elsevier, 2013.

SHARE-ALIKE, C. C. (. A. OWASP. Top 10 - 2013: **Os dez riscos de segurança mais críticos em aplicações web**. OWASP, Brasil, p. 1-23, jan./2013.

SILVA, W. D. G. P. J. P. M. A. **Cibersegurança. Seminário De Tecnologia, Gestão E Educação**, Rio Grande do Sul, v. 1, n. 4, p. 1-8, out./2020. Disponível em: http://www.revistaneurociencias.com.br/edicoes/1998/RN%2006%2003/Pages%20from%20RN%2006%2003-6.pdf. Acesso em: 19 set. 2021.

SMULDERS, H. B. K. H. J. H. A. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 1. ed. Brasil: BRASPORT, 2018.

STALLINGS, **William. Criptografia e segurança de redes**: Princípios e práticas. 6. ed. Brasil: Pearson, 2014.

STEFANINI GROUP. **Tudo sobre segurança da informação**. Jaguariúna, 2021. Disponível em: https://stefanini.com/pt-br/trends/artigos/guia-sobre-seguranca-da-informacao. Acesso em: 20 set. 2021.

TANENBAUM, Andrew S. **Redes de Computadores**. 5. ed. Brasil: Pearson Universidades, 2011.

TASCA, Jorge Eduardo. **A contribuição da avaliação de desempenho, como um instrumento de apoio à decisão, para a prevenção ao crime baseada no ambiente**. Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós-Graduação em Engenharia de Produção, Florianópolis, 2013. 350 p.

VELASCO, C. L. R. e Villa, S. P. **Metodologia da pesquisa científica**. Barcelona: Fundação Universitária Iberoamericana, 2019.

WEIDMAN, Georgia. **Testes de Invasão**: Uma introdução prática ao hacking. 1. ed. Brasil: Novatec Editora, 2014. p. 1-576.