Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

PERIGOS DE UMA REDE DESPROTEGIDA EM PEQUENAS EMPRESAS
DANGERS OF AN UNPROTECTED NETWORK IN SMALL COMPANIES
PELIGROS DE UNA RED NO PROTEGIDA EN PEQUEÑAS EMPRESAS

Autor: Antony Gabriel Felix Garcia

Autor: Maria Eduarda Ferreira Falzoni

Orientador: Cleberson Eugenio Forte

RESUMO

O presente trabalho trata das vulnerabilidades que muitas pequenas empresas apresentam e os perigos que podem passar pela falta da segurança em sua rede de computadores. Será apresentado o conceito de pequenas empresas, as definições de segurança da informação e seus pilares, além das ameaças mais comuns que essas empresas podem enfrentar. Como resultados, oferece-se uma análise sobre as formas de proteção que podem ser adotadas pelas empresas para evitar, parcial ou totalmente, as ameaças sem a necessidade de gerar grandes custos financeiros com compra de equipamentos, de softwares ou com a contratação de serviços para a efetivação dessa proteção.
Palavras-chave: Ameaça, medidas de segurança, pequenas empresas, rede de computadores, segurança da informação.

ABSTRACT

The present work deals with the vulnerabilities that many small companies present and the dangers that they face when security is not implemented in their computer network. The concept of small businesses, the definitions of information security and their pillars, as well as the most common threats that these companies may face will be presented. As a result, an analysis is presented on the forms of protection that can be used by companies to avoid, partially or totally, threats without the need to generate large financial costs with the purchase of equipment, software or with the contracting of services for effective protection.
Key-words: *Threat, security measures, small businesses, computer networks, information security.*

INTRODUÇÃO

O uso de elementos da tecnologia da informação se tornou essencial para as empresas, ajudando no seu gerenciamento e facilitando diversas tarefas, fazendo-as economizar tempo e, com isso, aumentar sua produtividade e seus lucros. No entanto, o uso dessas tecnologias sem os devidos

cuidados pode trazer diversos problemas, como roubo, perda ou vazamento de informações, danos causados por efeito de algum vírus ou a presença de algum intruso na rede que esteja verificando tudo o que acontece.

Muitos gestores dessas empresas acreditam que nunca serão alvos desse tipo de situação, ou que é algo extremamente difícil de ser feito, mas no cenário atual, com o compartilhamento de informações e conhecimento, em teoria, qualquer um pode ter acesso às informações sobre como causar algum problema para uma rede de computadores, principalmente se estiver conectada a *internet*. Caso uma rede não tenha as proteções necessárias, ela pode facilmente ser alvo de um ataque cibernético, pois seu endereço de *Internet Protocol* (IP), a principal identificação do seu computador na *internet*, estará suscetível a ser encontrado por outras pessoas assim que estiver acessando algum *website* e, a partir do ponto que for encontrado, receberá tentativas de conexão de diversas formas, como por *Packet Internet Network Groper* (PING) onde pode-se saber se o computador está respondendo ao protocolo Internet Control Message Protocol (ICMP), sendo usado em redes internas, com ou sem a conexão com a internet, ou em redes externas desde que o computador esteja na *internet*, pois só assim pode responder a esse comando de fora da rede e, caso o resultado do comando vindo de fora seja positivo, algum serviço de escaneamento pode ser usado para verificar as vulnerabilidades no seu computador, abrindo caminho para o ataque. Outra possibilidade é a pessoa possuir informações privilegiadas sobre a rede, sendo descoberta por conhecer a pessoa que a fez ou até mesmo sendo essa pessoa, agindo assim como o problema e a solução para a empresa, visando obter um lucro maior com suas ações.

Existem varias formas de se achar uma rede mesmo não estando conectado fisicamente a ela, o que torna o fato da rede estar sem proteção ainda mais preocupante. O objetivo deste trabalho é mostrar como algumas vulnerabiliades podem ser exploradas e os riscos que uma rede desprotegida possui. Em seguida, através de um estudo de caso, será demonstrado como evitar esses ataques, mostrando como pode ser feita a proteção e prevenir esses problemas de forma simples, sem gastos para a empresa com relação a contratação de serviços terceirizados ou a compra de softwares, sempre pensando em seguir e proteger os pilares da segurança da informação.

1-PEQUENAS EMPRESAS

A definição do que é uma empresa de pequeno porte (ou EPP) pode alterar de acordo com os critérios utilizados por cada órgão em sua avaliação. De acordo com a Lei Complementar nº 123/200, a classificação do porte de uma empresa é definida pelo seu faturamento anual. Seguindo essa Lei, uma EPP deve obter a receita anual superior a R$ 360 mil e inferior ou igual a R$ 3,6 milhões. Já de acordo com o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas, o SEBRAE, essa classificação varia conforme o número de funcionários. Sendo, essa contagem variável entre 10 e 19 nas EPPs do setor de comércio e serviços e entre 20 e 99 para a indústria. (SILVA, 2016).

As empresas de pequeno porte exercem um papel de suma importância na economia do Brasil. Os dados divulgados nessa matéria do SEBRAE demonstram que 99% dos estabelecimentos no país são micro e pequenas empresas (MPEs). Ainda de acordo com os estudos realizados por essa mesma entidade em parceria com a FGV projetos, as MPEs representam cerca de 30% do PIB nacional, além de serem responsáveis por uma alta quantidade de geração de empregos formais. Essas informações comprovam quão fundamental é a participação dos pequenos negócios dentro do cenário brasileiro. (SEBRAE, 2020, p. 6)

1.1-A tecnologia nas EPP

Com o passar dos anos o uso da tecnologia se tornou cada vez mais importante dentro das organizações, e com as vastas marcas, modelos, atualizações e evoluções tecnológicas esses recursos tornaram-se mais presentes em organizações pequenas, deixando de ser um privilégio somente das grandes empresas.

Segundo uma pesquisa realizada nas 5 regiões do país em 2016 pelo Sebrae, cerca de 24% das empresas ainda não utilizavam computadores (MARTINS, 2016). Infelizmente, ainda que o uso da tecnologia venha crescendo no mundo dos negócios, esse cenário não teve grandes mudanças.

Profissionais de Tecnologia da Informação afirmam que empresas já adeptas ao uso da tecnologia em seus negócios fazem atualizações desses PCs a cada 3 anos, mas existem medições que comprovam a troca desses equipamentos como sendo superior a 5 anos. A Microsoft revela, ainda, que os maiores motivos que levarão as empresas a fazer a troca desses equipamentos são: melhorias de desempenho, maior segurança (cerca de 50% das pessoas entrevistadas passaram por algum problema de segurança no ano anterior) e facilidade de gerenciamento (MICROSOFT, 2019).

Ainda que invista em equipamentos mais novos e com sistemas operacionais mais atualizados, tem-se a necessidade de aplicar simples regras e configurações de segurança como firewall, controle de acesso e monitoramento de rede, *proxy* e regras de senhas, a fim de evitar ataques cibernéticos ou diminuir seus impactos caso ocorra. Por isso é importante as empresas estarem alinhadas com uma política de segurança (PSI) e seguir os princípios básicos de Segurança da Informação.

2-SEGURANÇA DA INFORMAÇÃO

Há alguns anos, pensava-se que os ativos das empresas eram somente bens materiais que possuíam e poderiam ser convertidos em dinheiro. Atualmente, a informação já é considerada um ativo, se não o mais importante deles. Infelizmente, mesmo com a grande inclusão de tecnologias, muitas das instituições não dão a devida importância a essas informações, deixando-as totalmente desprotegidas, e só enxergando o quanto a informação é valiosa quando ela é perdida, destruída ou vazada, causando assim grandes prejuízos a empresa, como a reputação marcada ou a falta de confiança para seus parceiros. "O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir" (DAVIS, 1997 APUD BLUEPHOENIX, 2008). Por isso, é importante que haja a implementação da Segurança das Informações, visto que passou a ser um recurso essencial nas empresas, com a finalidade de proteger seus ativos e manter a continuidade do negócio.

A segurança da Informação é um conjunto de medidas que ajudam a manter a confidencialidade, integridade e disponibilidade (CID) da informação de uma organização ou de um indivíduo, a fim de preservar essas informações de acordo com a sua necessidade e diminuir os impactos caso haja uma perda ou vazamento dessas informações, passou a ser também uma forma de gestão. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos." (BLUEPHOENIX, 2008).

A segurança da informação se baseia em três pilares fundamentais para o seu bom funcionamento, sendo eles, de acordo com Ian Ramone (2018):

- **Confidencialidade:** A informação só poderá ser acessada por pessoas autorizadas.
- **Integridade:** Garante a completude da informação e que ela só será alterada por pessoas autorizadas.
- **Disponibilidade:** A informação estará disponível sempre que requisitada.

3-PERIGOS NO MUNDO VIRTUAL

Uma ameaça virtual pode ser definida como:

> “Uma chance de violação da segurança que existe quando há uma circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos. ou seja, uma ameaça é um possível perigo a explorar uma vulnerabilidade.” (STALLINGS, 2015, p. 10)

enquanto um ataque virtual é:

> “Um ataque à segurança do sistema, derivado de uma ameaça inteligente; ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de fugir dos serviços de segurança e violar a política de segurança de um sistema.” (STALLINGS, 2015, p. 10)

Como pode ser visto nas duas definições, a principal diferença entre uma ameaça e um ataque virtual é que, enquanto a ameaça pode ter sido criada de forma acidental, o ataque só acontece de forma intencional, nunca acontecendo por acidente, mas embora as suas definições sejam diferentes, ambos fazem parte do mesmo conjunto de problemas para a segurança da informação pois, para haver um ataque, tem que existir uma vulnerabilidade, ou seja, uma ameaça.

3.1-Hackers e Crackers

Na área da computação, principalmente em segurança da informação, somos apresentados à dois tipos de pessoas que utilizam essas vulnerabilidades, os *hackers* e os *crackers*. O *cracker* é considerado o pior dos dois sujeitos, tendo apenas a intenção de invadir e destruir um sistema, simplesmente porque pode fazer isso. Já os *hackers*, muitas vezes são considerados o lado bom dos dois, tendo o conhecimento para fazer o mesmo que o *cracker*, mas escolhendo outro caminho, com outros motivos e intenções. (ASSUNÇÃO, 2002, p. 9)

O *hacker* pode ser tanto um agente malicioso na rede, como pode ser um agente benéfico, tudo dependendo das suas intenções com o ataque. De acordo com o site da empresa McAfee (2019), mundialmente conhecida por seu sistema de antivírus, existem 9 tipos de *hackers*, cada um se diferenciando no objetivo e como o alcançará. Dentre esses 9 tipos, temos 3 definições principais e 6 que podem se encaixar dentro delas. De forma resumida, temos:

- *Hackers White Hat*: São os conhecidos como “*hacker* do bem”, são especializados em segurança computacional e fazer testes de penetração para garantir que o sistema está seguro. Agem de forma legal, pois são contratados pelas empresas para esses ataques de teste nos seus próprios sistemas.
- *Hackers Grey Hat*: São o meio termo entre os *black* e *White hackers*. Eles não usam o conhecimento para benefício próprio, mas agem de forma ilegal, como no exemplo citado no site, onde o *hacker* acha uma vulnerabilidade em um sistema e avisa os usuários dele sobre o risco, sendo algo bom, mas como está invadindo algo privado, o sistema de uma empresa, é considerado ilegal e criminoso.
- *Hackers Black Hat*: Eles são focados em objetivos ilegais, como ataques a sistemas para roubo de informações, criação e distribuição de vírus, encontrar vulnerabilidades e expor elas para outros que tenham interesse de explorá-las, etc. Eles se diferem dos crackers pois, enquanto os *crackers* fazem só para destruir, esses *hackers* têm objetivos de vingança contra a organização alvo ou interesses financeiros com os ataques, como ocorre no sequestro de informações.
- *Script Kiddies*: São uma variante dos *Hackers black hat*, são os *hackers* que só usam ferramentas prontas da internet para seus ataques, geralmente são iniciantes na área de *hacking* ou apenas são curiosos e estão testando algo.

Diferente das 3 primeiras definições, o termo “*Script Kiddies*” é importante para a compreensão do trabalho pois será o estilo de *hacker* do nosso invasor. Como dito acima, os “*Script Kiddies*” utilizam programas para fazer seus ataques, sendo algo fácil de se aprender na internet e causando pouco ou nenhum dano a empresas com um sistema seguro, mas a história é diferente com as pequenas empresas, visto que, como não investem muito em segurança e muito menos possuem formas de identificar o local que o invasor se encontra, são um alvo fácil para testar a curiosidade de quem está iniciando como *hacker*.

4-ATAQUES TESTADOS

Os ataques escolhidos para serem testados serão feitos utilizando ferramentas prontas, muito conhecidas no meio da área de teste de penetração em redes e sistemas. Eles foram escolhidos, dentre os diversos tipos de ataques que existem, por serem muito comuns e por atacarem os 3 pilares principais da segurança da informação, sendo eles disponibilidade com o ataque *Denial of Service* (*DoS*), autenticidade com o ataque de força bruta e o ataque *Man-in-the-middle* (MITM) irá afetar a integridade e a autenticidade.

4.1-DoS

Ataque DoS, ou ataque de negação de serviço em português, tem o objetivo de interromper um determinado serviço que está funcionando, por exemplo um site, fazendo com que ele fique fora de funcionamento enquanto o problema não for resolvido. Esse ataque funciona de uma forma bem simples, enviando diversas solicitações para o alvo, fazendo com que os recursos do serviço se esgotem e parem de funcionar.

No ataque DoS, apenas um computador envia as solicitações para o serviço, sendo mais fácil, mas ao mesmo tempo mais ineficaz em grandes empresas, pois podem simplesmente pegar o endereço do *Internet Protocol* (IP) do atacante e bloquear de uma vez. Já no ataque *Distributed Denial of Servisse* (DDoS), ou serviço de negação de serviço distribuído em português, outra versão do DoS, vários computadores de diversos lugares do mundo são usados, tornando a proteção muito mais complicada.

4.2-Força Bruta

O ataque de força bruta consiste na ideia básica de tentativa e erro, o atacante faz com que o programa fique enviando tentativas de senha para o endereço alvo, usando o nome de login da vítima, até que consiga acertar a senha. Estes testes podem ser feitos usando senhas sequenciais, passando por todas as combinações entre letras, números e caracteres especiais, também pode ser usado uma lista de palavras pronta que pode ser achada na internet e irá conter as senhas mais comuns de acordo com estudos anteriormente realizados, como Senha@123 e, como outra alternativa, mas levando a um trabalho maior, dados pessoais da vítima, como data de nascimento, nome de parentes, idade, próprio nome da pessoa e etc.

Existem duas grandes dificuldades com relação a eficiência desse ataque, sendo o primeiro o fato de empresas grandes, se a pessoa errar a senha algumas vezes, ela é bloqueada por um determinado tempo, como em e-mails e caso continue, pode ser bloqueada definitivamente até que a vítima perceba e siga os passos do serviço para desbloquear, como em sites bancários. A segunda dificuldade é o tempo, senhas muito complexas tendem a demorar muito mais para serem descobertas, por isso é importante que a senha siga as medidas de segurança para a senha, como as indicadas pela *Threat Intelligence Team* (Time de inteligência contra ameaças) do site da empresa Avast (2018), com ela possuindo no mínimo 8 caracteres, não ser sequencial, possuir todos os tipos de caracteres, evitar senhas padrões.

4.3- MITM

Um ataque MITM ou “homem do meio” se caracteriza quando uma informação, que tem um destino determinado, é mandada para outro lugar antes de chegar ao destino. Por exemplo, se eu mandar uma mensagem para uma pessoa, sendo minha intenção que só essa pessoa veja isso, mas se esse ataque estiver sendo feito, a mensagem passara primeiro pelo invasor, podendo ver e fazer as alterações que quiser, para depois ela ser mandada ao destino original. Para isso acontecer, o invasor precisa saber quem são as vítimas, por onde a informação será passada e estar dentro da rede em que as vítimas estão, por exemplo, invadindo o roteador do local, para então ele se passar por ambas as partes para entregar a mensagem sem que ninguém desconfie.

Um dos jeitos de fazer esse ataque é se aproveitando da vulnerabilidade de sites sem criptografia, os sites que usam *Hypertext Transfer Protocol* (HTTP ou protocolo de transferência de hipertexto) em vez de *Hyper Text Transfer Protocol Secure* (HTTPS ou protocolo de transferência de hipertexto seguro). Nesses sites, todas as informações são mandadas sem criptografia e podem ser vistas caso o ataque esteja em execução. Outro jeito é, depois de estar dentro da rede das vítimas, fazer com que todos os arquivos sejam mandados para você primeiro, podendo alterar e depois enviar para a outra parte.

5-CENÁRIOS

Para realizarmos os testes de vulnerabilidade, foram montados cenários próprios e controlados usando máquinas virtuais, a fim de não prejudicar os computadores dos participantes deste trabalho ou não infringir nenhuma lei usando algum sistema pronto, de alguma empresa, para nossos testes.
Os computadores usados serão:

- O computador do funcionário, podendo haver mais deles na rede mas, para os testes, apenas um é necessário. O sistema operacional usado é o Linux Slax, por ser um sistema simples, sem necessitar de um equipamento muito avançado e atingindo as necessidades de uso da empresa.
- Um Servidor, sendo um computador simples que foi designado como servidor de arquivos, também utiliza o sistema operacional Linux Slax.
- Um *Hub*, fazendo a conexão entre funcionário, servidor e *gateway*, permitindo a comunicação entre elas.
- O *gateway*, sendo um computador que, no início, está sendo usado apenas para estar conectado à internet via cabo e transmitir para os outros equipamentos dentro da rede. Possui o sistema operacional Linux CentOS, por ser um sistema que também precisa de poucos recursos para funcionar, além de servir para as funções necessárias no segundo cenário.
- A conexão de internet, sendo um contrato com uma provedora de internet.
- O invasor, uma pessoa de fora da rede que tentará ter acesso aos computadores e arquivos da empresa. Está utilizando um sistema operacional Linux Kali, pois ele possui muitos recursos para testes de invasão.

Informações referentes ao hardware das máquinas não serão dadas, visto que, esses dados não farão diferença para a execução dos testes, assim como informações sobre a empresa de internet, como nome dela, a velocidade ou como o sinal chega até a empresa.

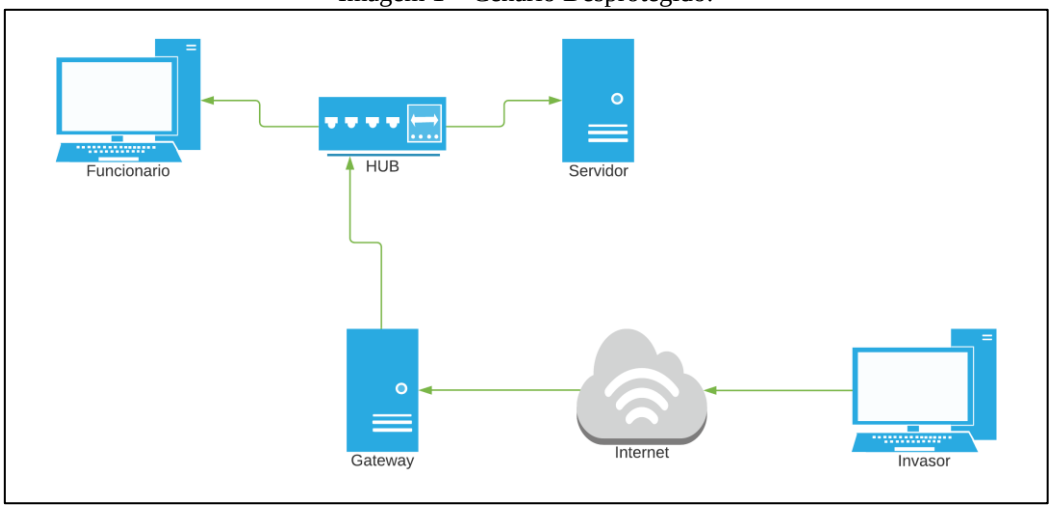
5.1-Cenário Base

Para o cenario base, as unicas configurações feitas foram as necessarias para que os computadores possam funcionar dentro da rede, com o compartilhamento de arquivos e acesso a *internet*, mas nenhuma outra configuração, como proteção, foi realizada, levando em consideração que a empresa não se preocupou com isso ou não possuia conhecimento dos riscos que pode estar passando.

Como foi dito na introdução deste trabalho, existem diversas formas do invasor conseguir ter um tipo de conexão com algum computador que está conectada na internet, como é caso do *gateway*. Resumindo, ele pode ter feito tentativas de ping aleatorias na internet até achar a rede, saber qual o endereço de IP por alguem que sabia e falou pra ele ou até ele mesmo ter feito a rede e saber tudo o que precisa para o ataque.

Já estando com conexão ao *gateway*, o invasor terá acesso a todos os outros componentes da rede, conforme a imagem 1, podendo ver o que é feito, obter senhas e usar isso para se conectar remotamente a esses computadores e se passar por algum funcionario para fazer algum ato.

Imagem 1 – Cenário Desprotegido.



Autoria Própria. Setas verdes indicam onde o "Invasor" pode se conectar.

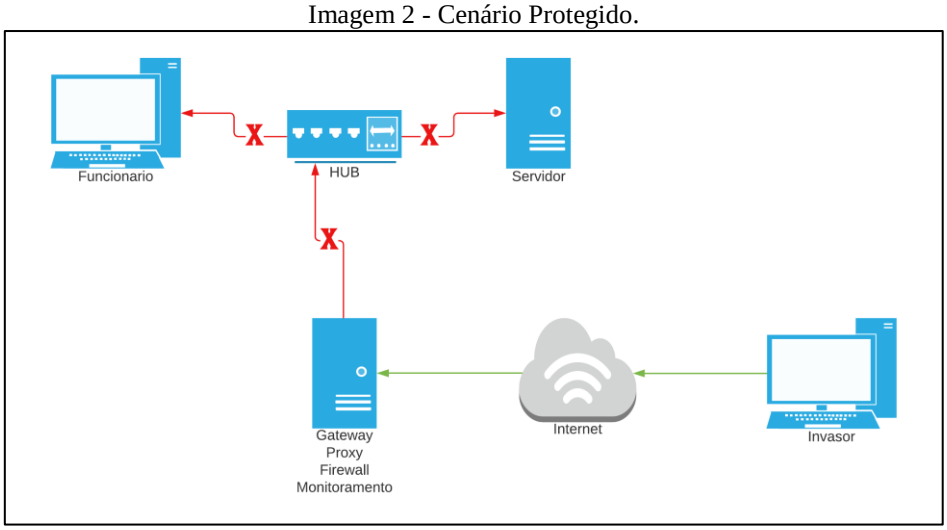
5.2-Cenário Protegido

No segundo cenario, o protegido, serão implementadas algumas medidas de segurança que irão servir como bareirras para que os ataques testados não sejam concretizados ou para que, mesmo que outros ocorram, a empresa tenha um jeito de encontrar a vulnerablidade e bloquea-la.

Agora o invasor ainda conseguirá ver o *gateway*, pois ele está conectado na *internet* e isso já o torna um pouco vulneravel, mas o acesso aos outros computadores da rede está bloqueado, como pode ser visto na imagem 2. Alem disso, as medidas de segurança foram implementadas, sendo elas:

- *Proxy;*
- *Firewall*, sendo o IPtables, com o Fail2Ban e algumas regras relacionadas a passagem e resposta de pacotes;
- Politica de senha;
- Politica de uso da *Internet*;
- Serviço de prevenção a ataques de força bruta e DoS.

Imagem 2 - Cenário Protegido.



Autoria Própria. Setas verdes indicam onde o “Invasor” pode se conectar e setas vermelhas indicam onde não pode se conectar.

As medidas irão impedir os ataques bloqueando as vulnerabilidades que seriam exploradas e, para ser de melhor entendimento, suas funções serão explicadas melhor durante o teste de cada ataque, mas assim como não serão mostrados o passo a passo da realização de cada ataque, as configurações de cada serviço não serão passadas, devido ao fato de que este ambiente é controlado, com máquinas virtuais e não tendo o risco de prejudicar um computador real, tanto na implementação das medidas, quanto no resultado dos ataques. Configurações de segurança em computadores devem ser feitas de acordo com cada situação, observando a capacidade da equipamento, quais funções elas desempenham e quais serviços já estão sendo usados, para que uma medida de segurança não acabe bloqueando um serviço que já estava sendo executado e traga prejuizos a empresa até o concerto do problema.

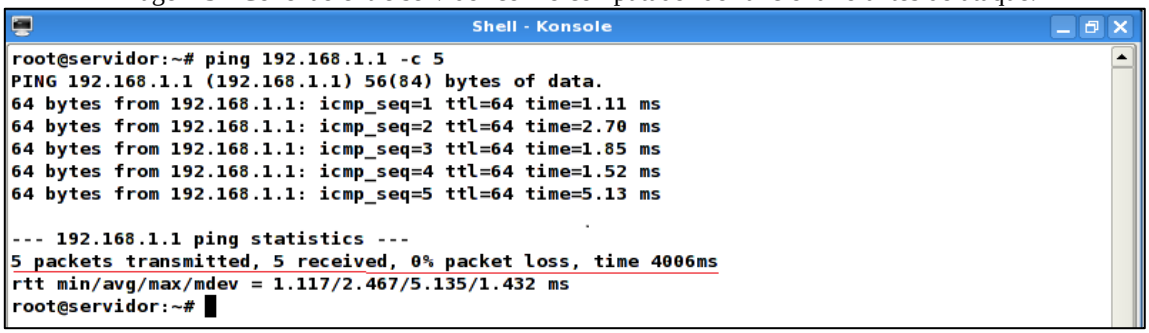
6-TESTES

6.1-Primeiro Teste: DoS

Como o objetivo de um ataque DoS é fazer com que um serviço do alvo pare de funcionar, nosso alvo será o *gateway* pois, mesmo podendo fazer como alvo direto o servidor, os pacotes de dados que serão enviados irão passar pelo *gateway*, fazendo ele parar de responder primeiro e não deixando o servidor parar, afinal a conexão do servidor com o invasor, que está fora da rede, será cortada.

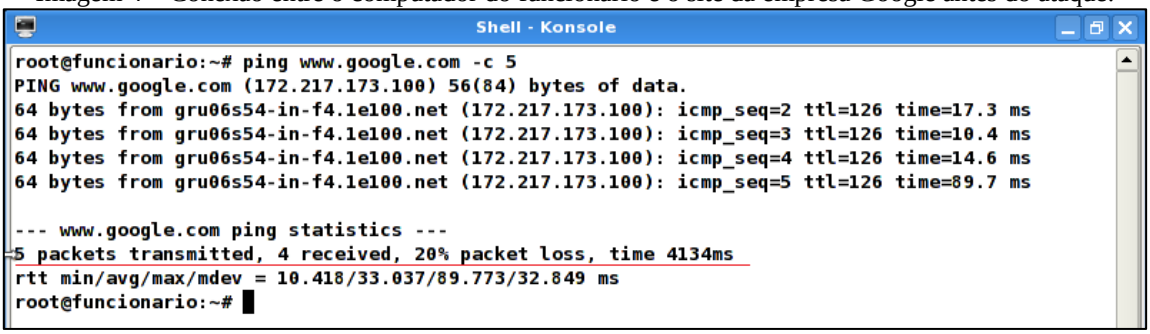
Para demonstrar as conexões antes do ataque, foram tirados alguns *prints* com os computadores executando o comando *ping* do servidor para o *gateway*, representado na imagem 3, e do computador do funcionário para o site da Google, demostrando a conexão com a *internet*, representado na imagem 4.

Imagem 3 - Conexão entre servidor com o computador do funcionário antes do ataque.



Autoria Própria. Execução do comando “ping” para verificar se o computador está respondendo.

Imagem 4 – Conexão entre o computador do funcionário e o site da empresa Google antes do ataque.

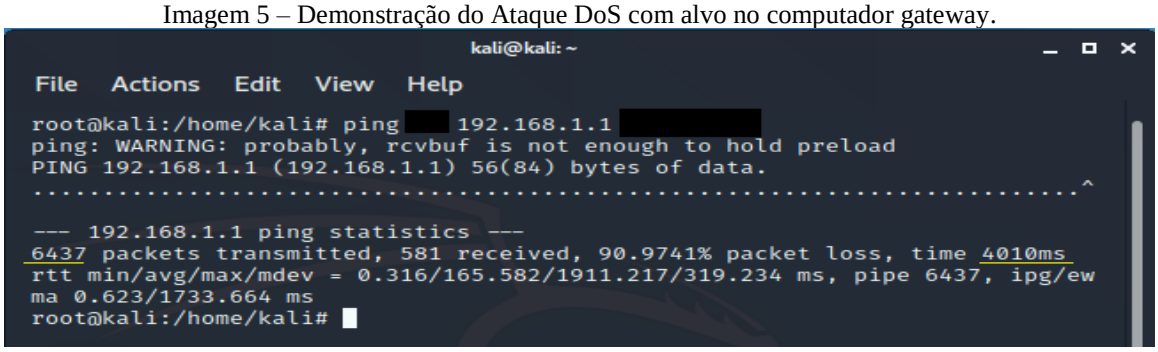


Autoria Própria. Execução do comando “ping” para verificar se o computador está respondendo.

Como pode ser visto, nas duas situações, 5 pacotes de dados foram enviados, sendo todos respondidos com sucesso, no tempo de 4,006 segundos e 4,134 segundos, respectivamente.

Agora, o invasor irá iniciar o ataque, mandando solicitações para o *gateway* utilizando o comando *ping*, como visto na imagem 5.

Imagem 5 – Demonstração do Ataque DoS com alvo no computador gateway.

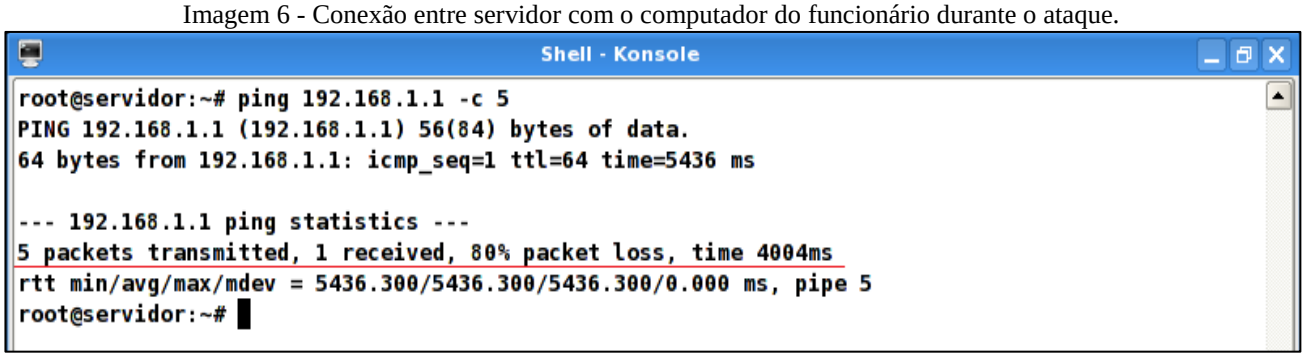


Autoria Própria. Ataque DoS utilizando o sistema operacional Kali Linux

Na primeira linha desta imagem está o comando do ataque, mas os atributos do comando *ping*, que tornam possível utilizá-lo como meio para este teste, foram tampados visto que, não temos a intenção de ensinar como fazer um ataque que pode prejudicar o site ou sistema de uma empresa. O endereço de IP alvo, 192.168.1.1, se refere ao gateway e, assim como nas imagens anteriores, o ataque aconteceu no tempo médio de 4 segundos, mas com a diferença de que, enquanto antes foram mandados 5 pacotes, agora foram mandados 6437, como demarcado em amarelo na imagem acima.

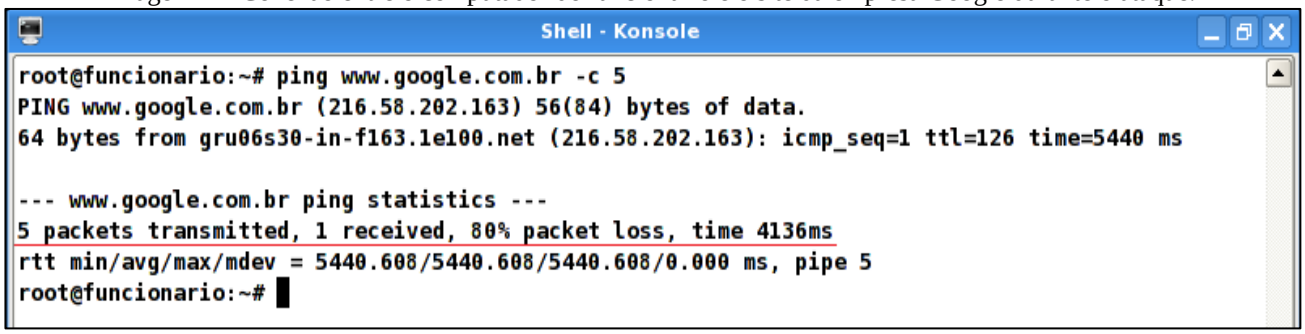
Com a grande quantidade de pacotes recebidos pelo gateway, ele parou de funcionar e, com isso, o servidor não consegue mais se comunicar com o ele, como visto na imagem 6, e o computador do funcionário não pode mais se conectar na internet, como demonstrado na imagem 7, então o ataque obteve sucesso, ele parou o serviço.

Imagem 6 - Conexão entre servidor com o computador do funcionário durante o ataque.



Autoria Própria. Execução do comando “ping” para verificar se o computador está respondendo.

Imagem 7 – Conexão entre o computador do funcionário e o site da empresa Google durante o ataque.



Autoria Própria. Execução do comando “ping” para verificar se o computador está respondendo.

Esse ataque é um dos mais comuns e mais difíceis de se proteger, pois pode vir de vários jeitos, como pela internet, por tentativas de conexão remota ou por tentativas de acesso a um serviço, como foi o teste acima. Cada um destes tipos irá atingir um serviço diferente dentro de um computador.

A proteção pode ser feita através de um *Firewall*, onde geralmente possuem um sistema de monitoramento e que podem bloquear automaticamente o ataque. No nosso caso, estamos usando o *IPtables* como *o software para filtro dos pacotes*, um serviço simples para *Linux*, um serviço de monitoramento separado, como o *Fail2Ban* e regras nesses serviços para impedir os ataques, sendo esse o nosso *Firewall*.

Na imagem 8 está sendo mostrado o serviço já em execução. Como dito antes, o *fail2ban* age em conjunto com o *IPtables* e as suas regras podem ser vistas com o comando marcado em azul, na primeira linha. Marcado em amarelo, está o nome da função, dentro do fail2ban, que irá bloquear esse tipo de ataque que, nesse caso, é via o protocolo ICMP e, marcado em vermelho, está o IP do atacante sendo bloqueado.

Imagem 8 – Regra *IPtables* para bloqueio do ataque DoS.

```
[root@gateway fail2ban]# iptables -nvL
Chain fail2ban-ICMP(1 references)
 pkts bytes target     prot opt in     out     source               destination
   42  25202 DROP       all  --  *      *       192.168.1.15         0.0.0.0/0

    0     0 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0

[root@gateway fail2ban]#
```

Autoria Própria. Regra de bloqueio no *IPtables* colocada pelo programa de monitoramento *Fail2ban*.

A partir desse ponto, nenhum pacote que o atacante mandar será respondido pelo alvo dentro do limite de tempo estipulado nas regras do firewall, como demonstrado na imagem 9, onde suas partes demarcadas em amarelo mostram que 35717 foram enviados, mas houve 100% de perda, e o limite de tempo de bloqueio pode ser alguns segundos ou ser indeterminado, sendo preciso que técnicos de informática retirem manualmente o IP do invasor do bloqueio, se for necessário.

Imagem 9 – Ataque do Invasor sendo bloqueado.

```
kali@kali: ~
File  Actions  Edit  View  Help
root@kali:/home/kali# ping [redacted] 192.168.1.1 [redacted]
ping: WARNING: probably, rcvbuf is not enough to hold preload
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
.....
.....^
C
--- 192.168.1.1 ping statistics ---
35717 packets transmitted, 0 received, 100% packet loss, time 5292ms
```

Autoria Própria. Todos os pacotes de dados do invasor são perdidos depois de bloqueado pelo *Firewall*.

É importante ressaltar que as configurações do *IPtables* e do *fail2ban* devem ser feitas pensando na empresa em questão pois, para reconhecer o ataque, os serviços definem um limite aceitável de recebimento de pacotes naquele computador dentro de um tempo e se o limite for baixo, um funcionário pode acabar sendo bloqueado por atingir esse limite naturalmente ou se o limite for muito alto, a proteção pode se tornar ineficaz e o ataque ainda poderá acontecer.

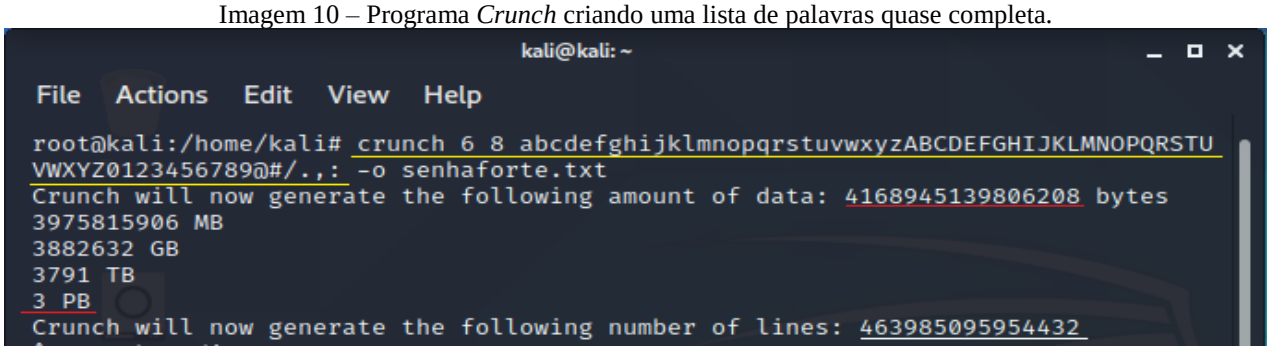
6.2-Segundo Teste: Força bruta

Para realizar o ataque de força bruta, é necessário possuir o nome de usuário naquele serviço, e precisa ter de um arquivo de texto contendo as palavras que serão testadas no alvo, como citado

anteriormente na explicação deste ataque. Para este teste, iremos usar uma lista de palavras sequenciais, feita utilizando um programa apropriado para essa tarefa, o software *Crunch*.

Na imagem 10, o programa está sendo executado para criar as combinações de senha com base nos padrões básicos de hoje em dia, sendo uma senha de 6 a 8 caracteres, possuindo letras maiúsculas, letras minúsculas, números e caracteres especiais, que nesse caso foram colocados apenas 6 deles, sendo eles: "@", "#", "/", ".", ",", ":".

Imagem 10 – Programa *Crunch* criando uma lista de palavras quase completa.

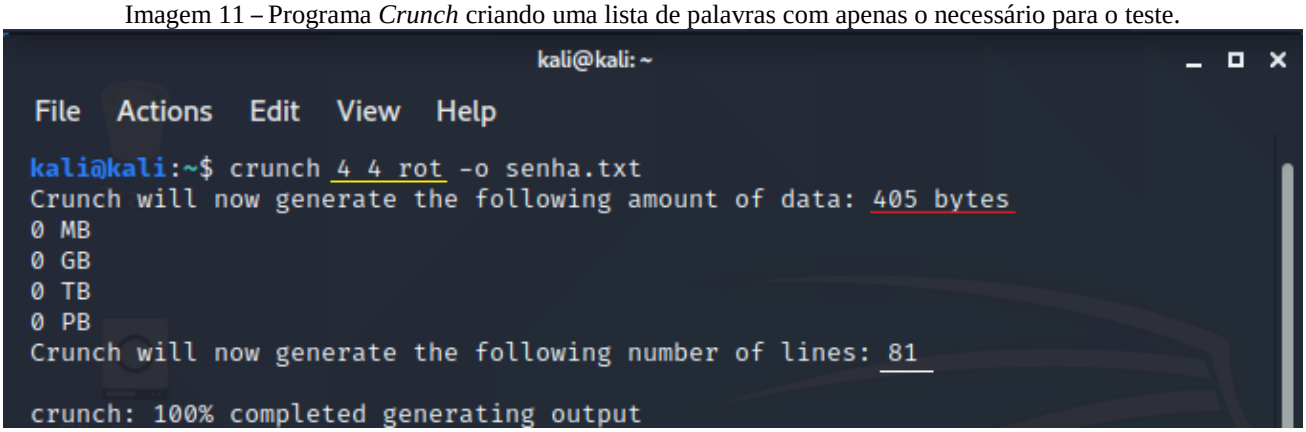


Autoria Própria. Imagem de execução inicial do programa de criação de lista de palavras.

O resultado desse comando iria gerar um arquivo de 3 Petabytes com 463.985.095.954.432 combinações, quase 464 trilhões de combinações diferentes. Em um teste que foi feito para calcular o tempo de envio das combinações nesse cenário, foi constatado que, por hora, são enviadas em média de 1800 tentativas de senha, então caso a senha certa fosse a última dessa lista, tendo que passar pelas quase 464 trilhões de combinações, levaria 257.769.497.752,4 horas, ou aproximadamente 29.425.741,752 anos, quase 29,5 milhões de anos, para descobrir a senha.

Existe a chance de acertar na primeira tentativa, mas como o ataque envolve tentativa e erro, deve-se pensar em todas as situações. Em computadores melhores, esse tempo pode ser reduzido, mas ainda sendo uma quantia fora do que é humanamente possível de realizar, por isso geralmente são usadas as outras opções para a lista de palavras, pegando uma pronta ou fazendo a própria com base no alvo. Como não possuímos os recursos necessários para tal tarefa, tanto em relação ao necessário para o armazenamento, os 3 Petabytes, quanto o tempo para realizar esse ataque, utilizando a lista de palavras explicada acima, e como já sabemos qual a senha do alvo, sendo ela a palavra "toor", foi feita outra lista de palavras com possíveis senhas para demonstrar o ataque funcionando. Desta vez, as combinações serão de 4 caracteres, possuindo apenas as letras "rot" em minúsculo, fazendo um arquivo de apenas 405 *bytes*, com 81 linhas, como pode ser visto na imagem 11.

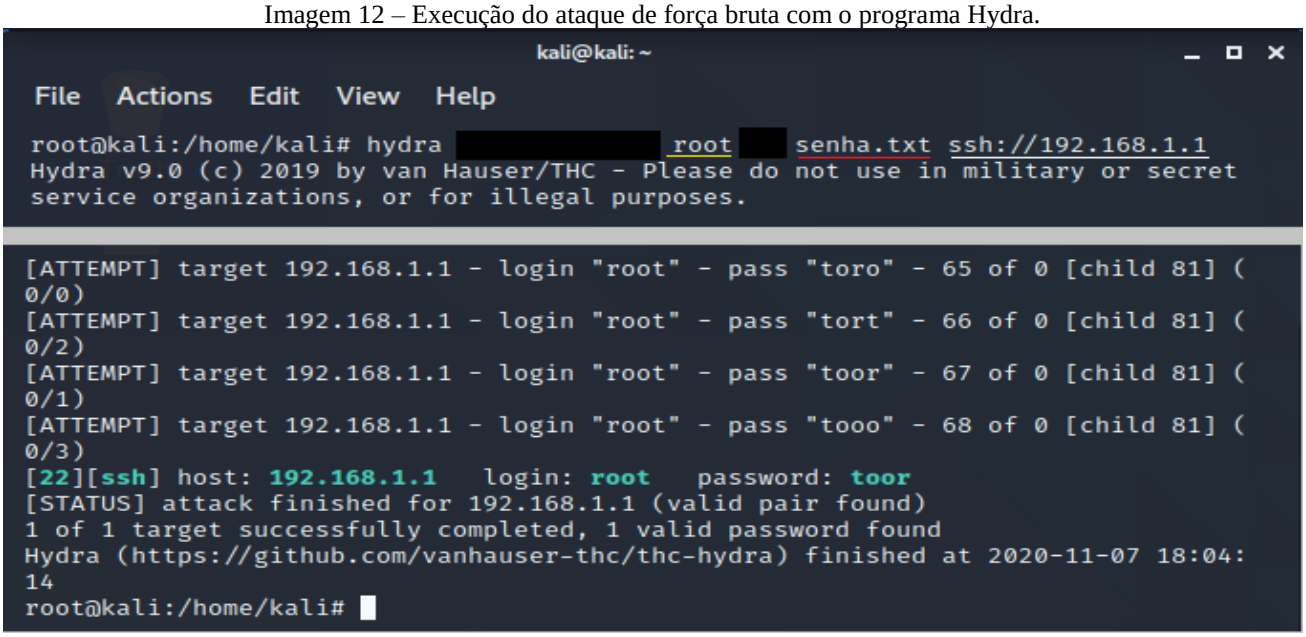
Imagem 11 – Programa *Crunch* criando uma lista de palavras com apenas o necessário para o teste.



Autoria Própria. Execução completa do programa de criação de lista de palavras.

Com a lista pronta, podemos realmente iniciar o ataque, utilizando o programa *Hydra*, conforme pode ser visto na imagem 12.

Imagem 12 – Execução do ataque de força bruta com o programa Hydra.



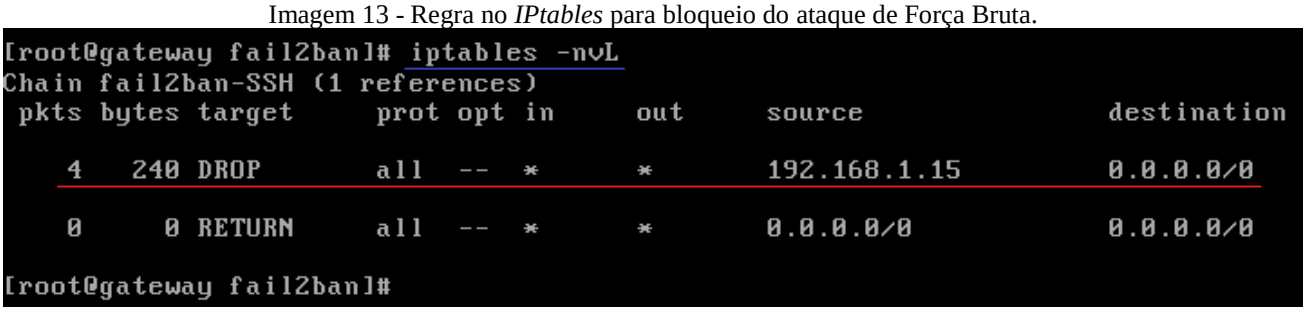
Autoria Própria. Parte inicial e final do ataque de força bruta.

Este são os dados para o ataque e o resultado dele. As imagens foram cortadas pois foram 68 tentativas até chegar ao resultado, não sendo necessário colocar todas aqui. No início do ataque estão os parâmetros que ele irá seguir, sendo mostrado apenas o que é necessário para os testes. Grifado em amarelo, está o nome de usuário alvo, “root”, em vermelho está sendo indicado qual arquivo será usado para os testes, no caso o que foi criado na imagem anterior e, em branco, está o tipo de conexão que será feita para o ataque, sendo *Secure Shell* (ssh) pois é uma tentativa de conexão remota para acesso no computador. Na parte final do ataque, ele mostra, em azul, o resultado que deu certo, a combinação que funcionou para o usuário “root” que foi denominado no começo e, como citado anteriormente, a senha “toor” foi encontrada.

Este ataque, além de ter o objetivo de achar a senha de um usuário, também pode servir como ataque DDoS se mais computadores forem utilizados para agilizar o trabalho, visto que ficará enviando diversas requisições ao alvo para um serviço e pode acabar sobrecarregando-o e o fazendo parar de funcionar. Por essa similaridade com os ataques DoS e DDoS, a forma de bloqueio é parecida, e irá utilizar o mesmo serviço de *firewall*.

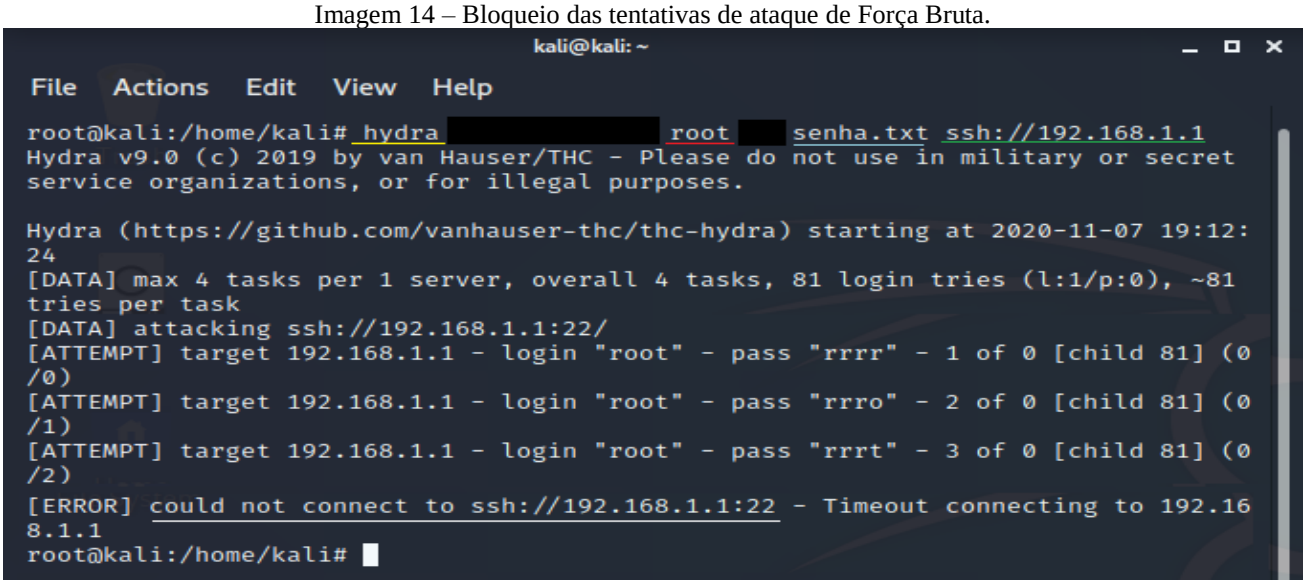
Diferente do ataque anterior, o DoS, as configurações para bloquear esse ataque serão mais rígidas, visto que o usuário não ficará errando a própria senha tantas vezes, então será definido como 3 tentativas máximas erradas para o usuário ser bloqueado. Depois de 3 tentativas erradas, o IP do invasor é bloqueado no firewall, como mostrado na imagem 13 e, na imagem 14, é visto que o invasor recebe a mensagem de falha de conexão com o alvo, causada por esse bloqueio.

Imagem 13 - Regra no *IPtables* para bloqueio do ataque de Força Bruta.



Autoria Própria. Regra de bloqueio no *IPtabels* colocada pelo programa de monitoramento *Fail2ban*.

Imagem 14 – Bloqueio das tentativas de ataque de Força Bruta.



Autoria Própria. Depois de 3 tentativas com senha errada, a conexão foi bloqueada.

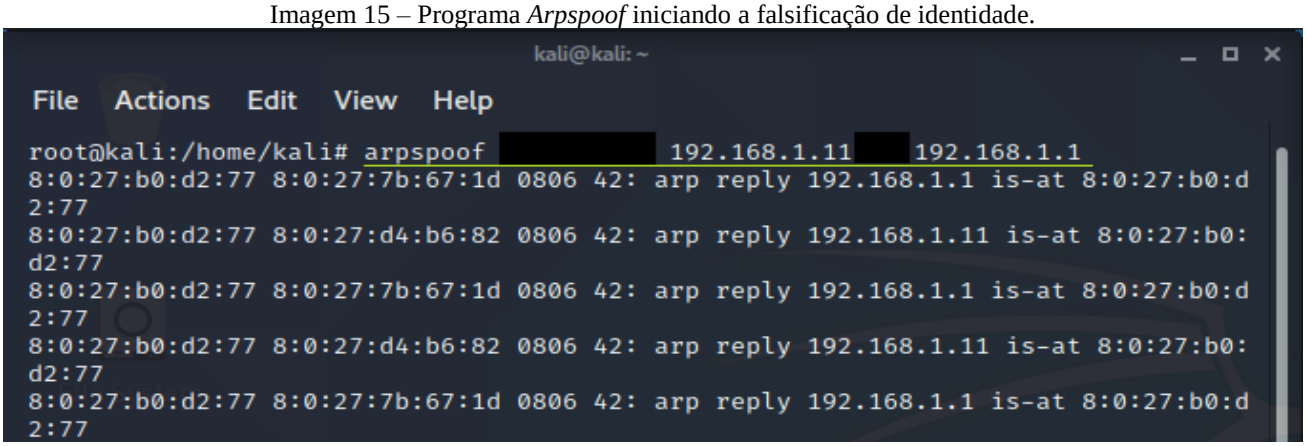
Como nesse caso é possível que os próprios funcionários da empresa errem a senha e sejam bloqueados, então o tempo de bloqueio será breve, mas é de extrema importância que haja um monitoramento mais rígido nessa situação, pois o atacante pode ficar esperando o tempo acabar para tentar de novo, fazendo o ataque levar mais tempo, mas ainda sendo possível. É aconselhável que, assim que seja verificado as várias tentativas erradas do mesmo IP, ele seja bloqueado de vez no *firewall*, mas isso deve ser definido por regras de acordo com os profissionais que estão encarregados da rede da empresa.

6.3-Terceito Teste: Man-in-the-middle

Este ataque possui diversas formas de acontecer, além de precisar de várias ferramentas, dependendo do objetivo do atacante. Nesse teste, nosso objetivo será verificar o que é transmitido entre o computador do funcionário, quando está acessando a internet, com o *gateway*, que está sendo o caminho para a internet. Primeiramente, para o ataque funcionar, o invasor deve estar dentro da rede do alvo, ou seja, já fez outros testes e ataques para chegar nesse ponto e, depois de concluído, tem liberdade para acessar o servidor, as configurações do *gateway*, os dados dos funcionários e etc.

Depois de já estar na rede, será usado o programa "*arpspoof*" para o invasor se passar por ambos os alvos, onde necessita-se saber qual interface de rede está sendo usada, qual é o IP do alvo que será simulado e qual seria o destino das informações dele, que agora irão primeiro para o invasor. Na imagem 15, o invasor está recebendo os dados do computador do funcionário enquanto finge ser o *gateway*, já na imagem 16 ele está fingindo ser o computador do funcionário e mandando os dados que pegou para o *gateway*, recebendo as respostas do mesmo e depois as enviando novamente ao computador do funcionário.

Imagem 15 – Programa *Arpspoof* iniciando a falsificação de identidade.



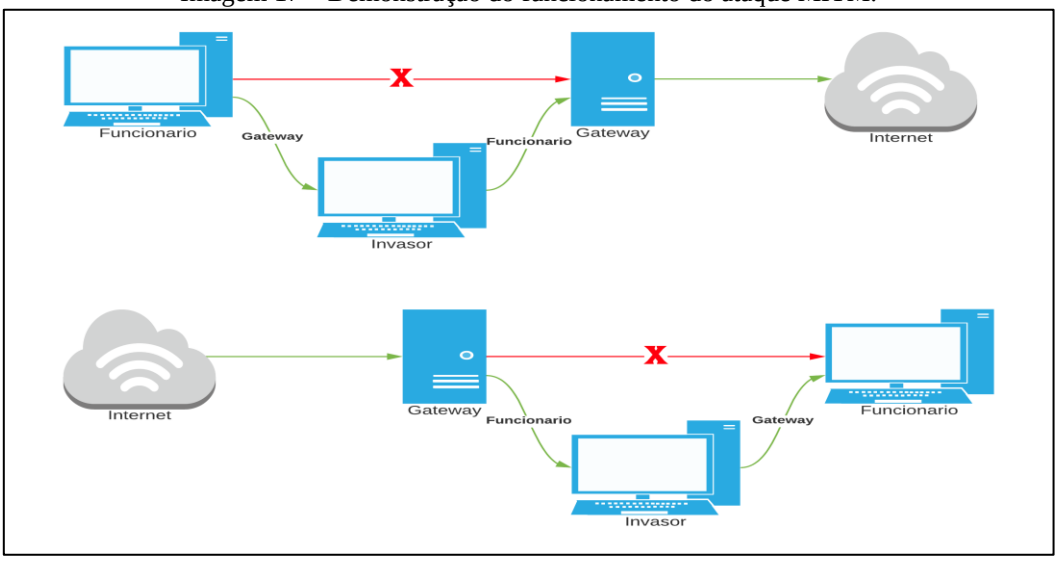
Autoria Própria. O invasor está se passando pelo *gateway* e recebendo os dados do computador do funcionário.

Imagem 16 – Programa *Arpspoof* terminando a falsificação de identidade.

Autoria Própria. O invasor está se passando pelo computador do funcionário e mandando os dados para o *gateway*.

A imagem 17 demonstra, visualmente, o processo do ataque, com o invasor se passando pelo *gateway* para enganar o computador do funcionário e se passando pelo funcionário para enganar o *gateway*. Os dois cenários presentes na imagem servem para demostrar a solicitação de uma informação na internet, como visto no de cima, e a resposta da internet sendo recebida pelas partes do sistema até chegar no solicitante, conforme é mostrado no cenário de baixo.

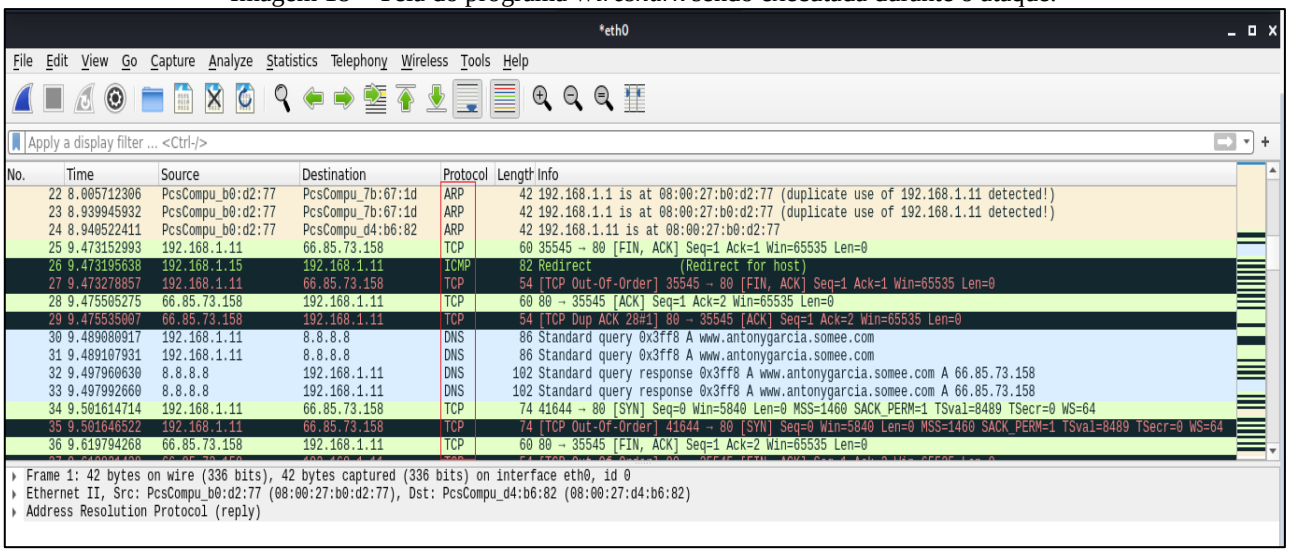
Imagem 17 – Demonstração do funcionamento do ataque MITM.



Autoria Própria. Demonstração gráfica da operação que acontece nas duas imagens anteriores.

Com os dois comandos do *arpspoof* sendo executados simultaneamente, o ataque está completo e permite ao invasor visualizar ou alterar todos os dados passados. Como dito antes, serão verificados os dados de acesso à internet do funcionário, então utilizaremos uma ferramenta chamada "*Wireshark"* para capturar esses dados. Assim que o funcionário acessa algum site, a comunicação entre o servidor do site e o cliente, quem o está acessando, é capturada pelo programa e podendo ser separada por alguns filtros, como marcado na imagem 18.

Imagem 18 – Tela do programa *Wireshark* sendo executada durante o ataque.



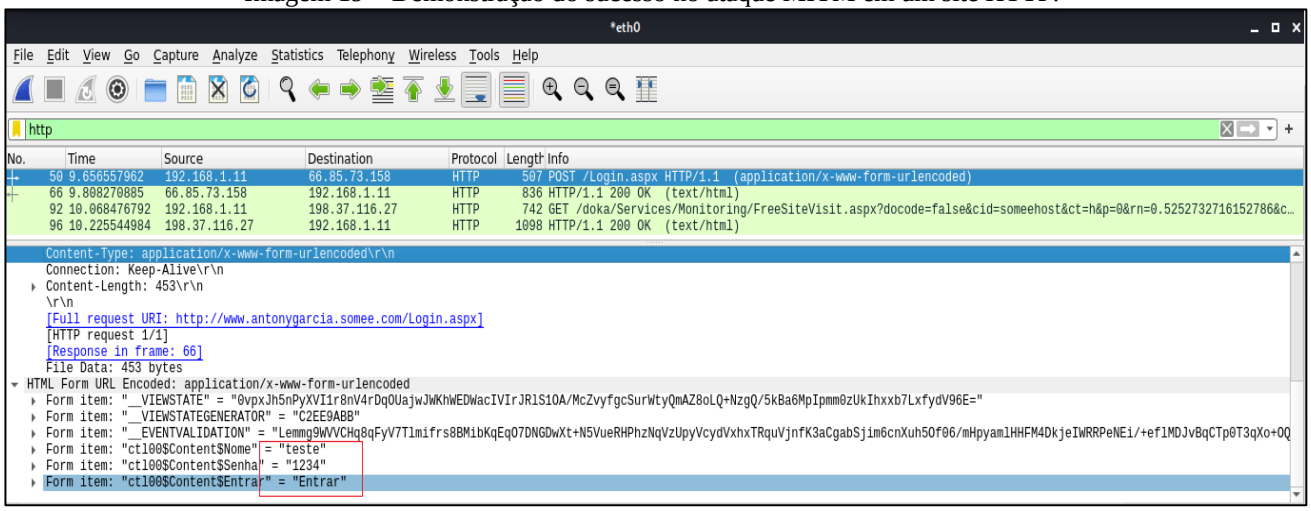
Autoria Própria. Pacotes de dados capturados pelo programa durante o ataque e especificados por tipo.

Existe uma proteção usada nos próprios sites para impedir, ou ao menos dificultar, esse tipo de ataque, usada quando o *site* possui a característica "HTTPS" onde todos os dados da comunicação são criptografados para impedir essa falha de segurança. Enquanto alguns sites utilizam esse tipo de segurança adicional, nos *sites* que não a utilizam, os *sites* em "HTTP", todos os dados estão disponíveis para o invasor.

O *site* escolhido para acesso é de autoria própria, evitando problemas judiciais que possam ocorrer ao explorar e expor uma vulnerabilidade do *site* de alguma empresa. Ele possui um formulário de login e senha onde, depois de colocar os dados corretos, ocorre o redirecionamento para uma página

vazia. Na imagem 19 é possível perceber que, se o filtro dos pacotes for definido para “HTTP” no *Wireshark* e procuramos nos itens que aparecerem, pode-se encontrar os dados de login utilizados, como o nome de usuário “teste”, a senha “1234”. Com isso, o invasor já possui esses dados da vítima, podendo utilizá-los nesse mesmo site ou tentar em outros para acessar dados pessoais dela ou se passar por ela para realizar alguma tarefa.

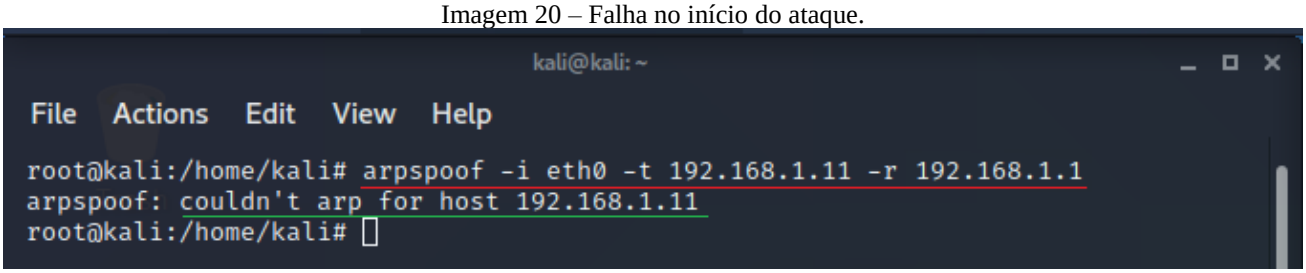
Imagem 19 – Demonstração do sucesso no ataque MITM em um site HTTP.



Autoria Própria. Nome de usuário e senha encontrados durante o ataque.

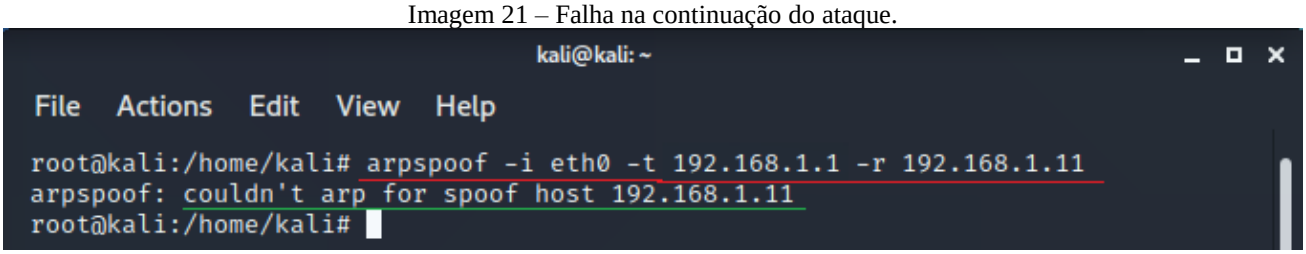
Já com relação a proteção, o *gateway* no segundo cenário está com um serviço de *Proxy* funcionando, o que impede o invasor de ter acesso aos outros equipamentos na rede, já parando o ataque no início, como mostrado na imagem 20 e na imagem 21.

Imagem 20 – Falha no início do ataque.



Autoria Própria. O invasor não pode fingir ser o computador do funcionário pois não “enxerga” ele na rede.

Imagem 21 – Falha na continuação do ataque.



Autoria Própria. O invasor não pode fingir ser o computador do funcionário pois não “enxerga” ele na rede.

Além do uso do *Proxy*, é necessário que algumas medidas sejam tomadas na rede, pois outra vulnerabilidade pode ser explorada para realizar esse ataque mesmo com o *Proxy* funcionando. Primeiro, para evitar que o invasor entre na rede, é aconselhável que conexões remotas de fora da rede sejam bloqueadas, ou que seja necessário o uso de uma medida de identificação a mais, como usar um par de chaves pública e privada. Outra medida serve para caso a rede possua algum roteador, onde é

necessário que sua senha seja muito boa ou que seja configurado para aceitar conexões apenas para computadores autorizados através de alguma identificação, como o endereço de *Media Access Control* (MAC), fazendo com que, mesmo que o invasor descubra a senha, ele não conseguira se conectar. A última dica é em relação ao uso da internet na rede da empresa pois, como dito antes, alguns sites possuem essa vulnerabilidade enquanto outros já não a possuem, então bloquear acesso a sites não seguros é uma ótima alternativa para evitar esse e outros tipos de ataques cibernéticos.

7-CONSIDERAÇÕES FINAIS

As medidas de proteção implementadas ao longo do trabalho foram poucas, simples, mas suficientes para impedir que o ataque de negação de serviço (DoS), o ataque de força bruta e o ataque MITM aconteçam e, assim, evitar problemas relacionados aos prejuízos que poderiam se ocasionar desses atos contra a empresa. Isso mostra que o uso de softwares gratuitos pode ser suficiente para manter a segurança da empresa contra os ataques virtuais se ela não possuir uma necessidade alta de proteção. Para a proteção básica, essas pequenas medidas são suficientes e todos os programas utilizados são gratuitos para uso, fazendo com que não seja necessário ter um gasto mensal ou anual com sua licença de uso ou ter a chance de gerar problemas jurídicos com o uso de softwares falsos, sendo que o único gasto necessário para a implementação e proteção da rede será a contratação de um profissional para implementar essas medidas e monitorar sua rede, algo essencial para empresas que possuem e utilizam computadores para alguma tarefa.

Essas medidas implementadas para a proteção da rede de computadores foram pensadas de acordo com o que é necessário para manter a segurança de qualquer sistema e rede, sendo elas: o uso de um sistema de *Proxy* para garantir que seus computadores internos não estejam totalmente expostos na internet, fazendo com que as medias seguintes possam ser configuradas apenas em um computador, facilitando o serviço e diminuindo o tempo necessário para resolver um problema. Após a implementação do *Proxy*, o *Firewall* deve ser colocado para existir uma forma de bloqueio do invasor no caso de um ataque e automatizar essa operação para que possa ocorrer mesmo se o técnico de informática não estiver presente no local monitorando a rede por algum motivo. Para finalizar, a definição de criação de senhas complexas para uso no sistema, tornando mais difícil sua descoberta por tentativas sequenciais, como demostrado no segundo teste.

Obtendo os resultados dos testes e provando a eficácia dessas medidas de proteção, podemos afirmar que uma rede segura não é exclusividade de grandes empresas, com contratos de softwares pagos e empresas terceirizadas para monitorar e cuidar de sua rede. Pequenas configurações na rede já a tornam mais segura e podem impedir muitos problemas futuros e prejuízos derivados dos ataques. Claro que o uso de softwares mais estruturados, com mais funções e de uma equipe de profissionais capacitados seria a melhor opção para todas as empresas, mas muitas não possuem recursos para isso, principalmente em pequenas empresas que utilizam computadores, mas suas atividades não são focadas no uso dessa tecnologia e seus recursos disponíveis são escassos.

8-REFERENCIAS

ASSUNÇÃO, M. F. A. **Guia do Hacker Brasileiro**. Visual Books, 2002. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=lang_pt&id=s2ZZAwAAQBAJ&oi=fnd&pg=PA5&dq=hacker+e+cracker&ots=6rmC6zGrtI&sig=SgmbjUepvmn4PAXw57jni6Xufhk#v=onepage&q&f=false>. Acesso em: 3 de out. de 2020.

BUSCA por mais segurança é um dos principais motivos que levam pequenas e médias empresas a investir em novos PCS. **Microsoft**, 2019. Disponível em: <https://news.microsoft.com/pt-br/busca-por-mais-seguranca-e-um-dos-principais-motivos-que-levam-pequenas-e-medias-empresas-a-investir-em-novos-pcs/>. Acesso em: 19 de out. de 2020.

ECONOMIA NACIONAL. **Sebrae**, 2020. Disponível em: <https://datasebrae.com.br/wp-content/uploads/2020/04/Relatório-Participação-mpe-pib-Na.pdf>. Acesso em: 26 de set. de 2020.

MARTINS, Ana Cláudia. Pequenas empresas ainda não utilizam computadores. **Jornal Cruzeiro do Sul**, Sorocaba, 04 de abr. de 2016. Disponível em: <https://www2.jornalcruzeiro.com.br/materia/689025/pequenas-empresas-ainda-nao-utilizam-computadores>. Acesso dia: 19 de out. de 2020.

MCAFEE. 9 Tipos de hackers e suas motivações. **McAfee**, 2019. Disponível em: <https://www.mcafee.com/blogs/languages/portugues/9-tipos-de-hackers-e-suas-motivacoes/>. Acesso em: 26 de set. de 2020.

RAMONE, Ian. Os pilares da Segurança da Informação**. N&DC**, 2018. Disponível em: <https://www.ndc.com.br/os-pilares-da-seguranca-da-informacao/#:~:text=São%20os%20três%20principais%20critérios,Integridade%20e%20Disponibilidade%20(CID).&text=A%20propriedade%20de%20que%20a,entidades%20ou%20processos%20não%20autorizados>. Acesso em: 22 de out. de 2020.

SEBRAE. ATUALIZAÇÃO DE ESTUDO SOBRE PARTICIPAÇÃO DE MICRO E PEQUENAS EMPRESAS NA SEGURANÇA da Informação. **Tecnews.net**, 2017. Disponível em: <https://www.tecnews.net.br/hello-world/>. Acesso em: 15 de set. de 2020.

SILVA, Cassiano Gabriel de Oliveira. Qual a diferença entre micro e pequena empresa?. **Contábeis**, 2016. Disponível em: <https://www.contabeis.com.br/noticias/30432/qual-a-diferenca-entre-micro-e-pequena-empresa/#:~:text=Pequena%20empresa%3A%20é%20a%20sociedade,%24%203.600.000%2C00>. Acesso em: 19 de out. de 2020.

STALLINGS, W. **Criptografia e Segurança de Redes:** Princípios e Práticas. 6. Campinas: Pearson Education do Brasil Ltda, 2014.

TEAM, Threat Intelligence. Vazamento de senhas na deepweb: 7 dicas para fortalecer a segurança das suas senhas**. Avast**, 2018. Disponível em: <https://blog.avast.com/pt-br/vazamento-de-senhas-na-deepweb-7-dicas-para-fortalecer-a-seguranca-das-suas-senhas>. Acesso em: 10 de dez. de 2020.

Antony Gabriel Felix Garcia

Maria Eduarda Ferreira Falzoni

PERIGOS DE UMA REDE DESPROTEGIDA EM PEQUENAS EMPRESAS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.

Área de concentração: Segurança da Informação

Americana, 15 de Dezembro de 2020.

Banca Examinadora:

_____

Cleberson Eugenio Forte (Presidente)

Doutor

Fatec Americana

_____

Rossano Pablo Pinto (Membro)

Mestre

Fatec Americana

_____

Wellington Aires Da Cruz Pereira (Membro)

Mestre

Fatec Americana