FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Alexander Torette Salandin

Exploração de Vulnerabilidades em Pequenas Empresas

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Alexander Torette Salandin

Exploração de Vulnerabilidades em Pequenas Empresas

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do (a) Prof.(a) Marcus Vinícius Lahr Geraldi.

Área de concentração: Segurança em Sistemas Operacionais e Redes de Computadores II.

Americana, SP.

2017

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

S153e SALANDIN, Alexander Torette

Exploração de Vulnerabilidades em Pequenas Empresas. / Alexander Torette Salandin. – Americana, 2017.

34f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinicius Lahr Giraldi

1 Segurança em sistemas de Informação. I. GIRALDI, Marcus Vinicius Lahr II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Alexander Torette Salandin

Exploração de Vulnerabilidades em Pequenas Empresas

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

Americana, 12 de dezembro de 2017.

Banca Examinadora:

Marcus Vinicius Lahr Giraldi
Especialista
Fatec Americana

Benedito Aparecido Cruz
Mestre
Fatec Americana

Ricardo Kiyoshi Batori
Especialista
Fatec Americana

AGRADECIMENTOS

Agradeço de forma simplória e única, a todos aqueles que separam sequer o mínimo tempo possível para esclarecer minhas dúvidas, que se tornaram responsáveis para a conclusão deste trabalho, todos são, em conjunto, culpados por me ajudarem a alcançar meus objetivos recorrentes e quando deixo explícito de forma geral, estou selecionando apenas aqueles que fazem parte da minha vida, seja essa parte como professor, orientador, amigo, ou melhor dizendo, agradeço à essa família que se fez presente.

DEDICATÓRIA

Aos meus pais e amigos que se esforçaram em me fazer ter esforços para a conclusão deste.

RESUMO

Com o incrível avanço e o crescimento da tecnologia atual, há de crescer também a preocupação com a informação que essa tecnologia armazena em sua memória, principalmente se tratando de empresas. As grandes empresas têm um espaço maior no mundo dos negócios, e isso faz com que estas procurem e estudem meios de se proteger. Já as pequenas empresas, utilizam meios de transferência de arquivos não mais utilizados, senhas de complexidade simples para acessos rápidos e conexões via serviços por portas padrões, assim como configurações padrões ou a falta de configurações do sistema operacional. Buscam a agilidade e esquecem que, há muito a perder quando se trata de informação. Lidamos com um mundo empreendedor, no qual os empresários estão preocupados com seus negócios e se dispersam da proteção devida de sua empresa, a segurança da informação. O presente monólogo irá apresentar algumas vulnerabilidades presentes em um cenário empresarial de pequeno porte, tais como teste de acesso e força bruta através de uma ferramenta presente na distribuição Kali Linux utilizada na realização de *Pentests.* O *Pentest* consiste em um método para avaliação de segurança em um sistema de computador ou uma rede, que validam acessos através de uma verificação de vulnerabilidade com a possibilidade de ser evitada, ou melhor elaborada, em questão presente, a senha de acesso. Para garantir melhor o tripé da segurança, sem perder o uso da utilidade em si, deve-se usufruir de ferramentas que possa trazer benefícios ao negócio quando se trata de empresas, sem deixar de lado a importância e o valor da informação. O método científico utilizado é o hipotético-dedutivo. Foi realizado em um ambiente virtual, simulando configurações genéricas de uma rede em um determinado campo organizacional, denominado de pequena empresa. Partindo dessas análises, são apresentadas sugestões e correções para garantir a segurança da informação.

Palavras Chave: Exploração de Vulnerabilidades; Pequenas Empresas; Segurança da Informação.

ABSTRACT

Through the incredible advance and growth of the current technology, there is also a growing concern with the information that this technology stores in your memory, especially when it comes to companies. Big companies have a bigger place in the business world, and that makes them look for ways to protect themselves. Small businesses, however, use file transfer media that are no longer used, simple complexity passwords for fast access, and connections via standard port services, as well as default settings or the lack of operating system configurations. They look for agility and forget that there is much to lose when it comes to information. We deal with an entrepreneurial world in which business owners are concerned about their business and disperse from the due protection of their company, information security. The present monologue will present some vulnerabilities present in a small business scenario, such as access testing and brute force through a tool present in the Kali Linux distribution used in the realization of Pentests. Pentest consists of a method for evaluating security in a computer system or a network, which validates accesses through a vulnerability check with the possibility of being avoided, or better elaborated, in this present, the access password. In order to better guarantee the safety tripod, without losing the use of the utility itself, it is necessary to use tools that can bring benefits to the business when it comes to companies, without leaving aside the importance and value of information. The scientific method used is hypothetical-deductive. It was performed in a virtual environment, simulating generic configurations of a network in a given organizational field, called a small business. From these analyzes, suggestions and corrections are presented to guarantee information security.

Keywords: Vulnerability Exploration; Small Business; Information Security.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

AP	Access Point
DNS	Domain Name System
FTP	File Transfer Protocol
GPO	Group Policy
IP	Internet Protocol
RDP	Remote Desktop Protocol
TTL	Time To Live
VLAN	Virtual LAN
VPN	Virtual Private Network

LISTA DE FIGURAS

1 INTRODUÇÃO

Para melhor compreensão do tema ao longo deste monólogo no que se refere à Segurança da Informação (SI), com foco nas vulnerabilidades existentes em um ambiente empresarial de pequeno porte, é necessário a clareza de alguns conceitos presentes, separadas em blocos de informação.

Segundo a norma Brasileira ABNT NBR ISO/IEC 27002 (2005, p.10), “a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida”, no entanto, algumas organizações sofrem com a falta de conhecimento ou de preparo adequado para ter essa proteção necessária.

Empresas de pequeno porte que, consistem em um número pequeno de colaboradores, se preocupam pouco, ou não se preocupam com seus dados, suas informações, a troca de suas senhas periodicamente, e o compartilhamento de sua autenticação com outros colaboradores do mesmo ambiente, quando, na verdade, todos esses atos deveriam ser o oposto, para garantir um melhor conforto e segurança das informações (CERT.br, 2012, p.63).

Para tanto, o estudo **justifica-se** para uma outra visão das configurações presentes a fim de colaborar com a segurança, no que se refere à conscientização de um ambiente organizacional pequeno, necessitado de proteção.

Já o **Problema** consistiu em falta de conhecimento, interesse e investimento, uma vez que, pessoas de frente de um ambiente organizacional pequeno buscam crescimento no mercado, com foco em qualidade e venda bruta dos produtos oferecidos.

Como **Pergunta** que se buscou responder foi: Há necessidade de investimento e maior conhecimento por parte das pequenas empresas no que se refere ao quesito Segurança da Informação?

As **Hipóteses** foram: a) Não existem pessoas interessadas em explorar vulnerabilidades de pequenas empresas; b) A vulnerabilidade só irá ser explorada por colaboradores desligados com conhecimento em informática; e, c) A exploração de vulnerabilidades pode acontecer com todos que se encontram desprotegidos.

O **objetivo geral** consistiu em analisar a importância das configurações de computadores, não deixando de lado a elaboração de um manual de boas práticas

em um ambiente organizacional, uma vez que, este, tem grande fluxo e circulação de informações relevantes para a concorrência no mercado de trabalho.

Os **objetivos específicos** foram: a) Realizar um levantamento bibliográfico sobre os conceitos de: pequenas empresas, informação, Segurança da Informação, exploração de vulnerabilidades e ameaças; b) Fazer uma análise de vulnerabilidades expostas em um determinado ambiente organizacional; e, c) Sugerir correções e aplicar testes para realizar uma nova análise do quesito Segurança da Informação em um ambiente empresarial específico.

O **método científico** de pesquisa utilizado foi o Hipotético-dedutivo que para Karl R. Popper é um método que parte de um problema, no qual se oferece uma solução provisória, vindo a criticar a solução dada, com vista a eliminar erros e, como na dialética, tal processo se renovaria a si, com surgimento de novos problemas (LAKATOS; MARCONI, 2003, p.95)

A **pesquisa** foi classificada, por sua natureza, como aplicada, que: “Objetiva gerar conhecimentos novos, úteis para o avanço da Ciência, sem aplicação prática prevista. Envolve verdades e interesses universais” (GERHARDT; SILVEIRA, 2009, p.34).

Para a abordagem do problema foi utilizada a pesquisa qualitativa pois segundo Polit, Becker e Hungler tem a característica de “salientar os aspectos dinâmicos, holísticos e individuais da experiência humana, para apreender a totalidade no contexto daqueles que estão vivenciando o fenômeno” (2004, p.201, apud GERHARDT; SILVEIRA, 2009, p.33)

Para que os objetivos fossem atingidos, foram utilizadas as pesquisas descritiva e explicativa. Para Gil (2002, p.42), a pesquisa descritiva é:

> As pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática.

A pesquisa explicativa:

> “[...] têm como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão, o porquê das coisas. Por isso

> mesmo, é o tipo mais complexo e delicado, já que o risco de cometer erros aumenta consideravelmente" (GIL, 2002, p.42).

Já para os procedimentos técnicos, foram utilizadas as pesquisas bibliográficas e experimental. A pesquisa bibliográfica para Gil (2002, p.44): "[...] é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos".

A pesquisa experimental:

> "[...] constitui o delineamento mais prestigiado nos meios científicos. Consiste essencialmente em determinar um objeto de estudo, selecionar as variáveis capazes de influenciá-lo e definir as formas de controle e de observação dos efeitos que a variável produz no objeto. Trata-se, portanto, de uma pesquisa em que o pesquisador é um agente ativo, e não um observador passivo" (GIL, 2002, p.48).

O trabalho foi estruturado em cinco capítulos, sendo que o **primeiro** é responsável pela introdução do tema tratado, o **segundo** apresenta o estudo bibliográfico conceituando a importância de proteção da informação nas pequenas empresas. No **terceiro** capítulo foram realizados uma análise e o levantamento de vulnerabilidades existentes em um ambiente organizacional. O **quarto** sugere propostas de soluções para as vulnerabilidades listadas, assim como apresenta o resultado de uma nova análise a partir da aplicação soluções previamente sugeridas.

Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o capítulo **cinco** se reserva às considerações finais.

2 PEQUENAS EMPRESAS E A SEGURANÇA DA INFORMAÇÃO

A fins de esclarecimento e melhor compreensão dos próximos capítulos, o capítulo presente se tratará de conceitos e definições de pequena empresa, informação, Segurança da Informação e também a atuação da mesma no ambiente empresarial.

2.1 O CONCEITO DE PEQUENA EMPRESA

Para compreensão de alguns conceitos envolvidos, primeiramente é necessário a explanação dos mesmos. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE) as características gerais das micros e pequenas empresas são: (IBGE, 2005, p.20)

> a) baixa intensidade de capital; b)altas taxas de natalidade e de mortalidade: demografia elevada; c) forte presença de proprietários, sócios e membros da família como mão-de-obra ocupada nos negócios; d) poder decisório centralizado; e) estreito vínculo entre os proprietários e as empresas, não se distinguindo, principalmente em termos contábeis e financeiros, pessoa física e jurídica; f) registros contábeis pouco adequados; g) contratação direta de mão-de-obra; h) utilização de mão-de-obra não qualificada ou semiqualificada; i) baixo investimento em inovação tecnológica; j) maior dificuldade de acesso ao financiamento de capital de giro; e, k) relação de complementaridade e subordinação com as empresas de grande porte.

Por outro lado, em uma perspectiva quantitativa, os comentários referentes à demografia de empresas foram baseados no critério de pessoa: (IBGE, 2005, p.21)

> a) microempresas - empresas com até 5 pessoas ocupadas; b) pequenas empresas – empresas com 6 a 19 pessoas ocupadas; e, c) médias e grandes empresas - empresas com 20 ou mais pessoas ocupadas.

2.2 O CONCEITO DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é a proteção da informação em relação à diversas ameaças existentes, para a garantia de um negócio sem paradas, com riscos mínimos e um retorno maximizado diante ao investimento e oportunidades. Quando se pensa em segurança da informação não deve deixar de lado a consideração sobre as qualidades da informação, uma vez que, qualquer ação que possa vir a comprometer essas qualidades, atentará contra sua segurança (DANTAS, 2011, p.11).

Devido a tal quesito, existem os responsáveis pela Segurança da Informação (SI) que irão mitigar os riscos e cuidar para que os dados devidamente protegidos com cada grau de necessidade correspondente.

2.2.1 Os Pilares da Segurança da Informação

Os pilares da segurança da informação são como bases que sustentam a garantia de que os dados não foram violados, roubados ou invadidos. Quando utilizada a informação, necessita-se de pelo menos três pilares. Os principais pilares que se mantidos intactos, garantem a segurança da informação e são definidos por Dantas (2011, p.11-14):

Integridade como a garantia de que a informação é completa, assim como outros métodos de processamento;

Disponibilidade como o que garante ao usuário autenticado, o acesso à informação sempre que necessário e solicitado; e

Confidencialidade como o pilar que assegura o acesso da informação apenas para aqueles usuários que são autenticados, que contém acessos autorizados à informação.

2.2.2 Vulnerabilidades, Ameaças e Riscos

Vulnerabilidades são pontos frágeis ou falhas que podem resultar em um dano irreversível, dependendo da gravidade do problema causado. A cartilha do CERT.br (2012) define vulnerabilidade como “uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança”.

Dantas (2011) concorda com o raciocínio apresentado anteriormente, afirmando que as vulnerabilidades podem de algumas formas vir a provocar danos, pois são fragilidades em um ativo ou grupo de ativos. Silva, Carvalo e Torres (2003) dizem que a vulnerabilidade “visa permitir aproximar o cálculo da probabilidade de concretização das ameaças inerentes à realidade da empresa”.

Dadas as definições de vulnerabilidade, conclui-se que estas podem estar presentes nos softwares, nos hardwares e principalmente nas pessoas. Não obstante, para exploração dessa vulnerabilidade é preciso uma ameaça, que seja capaz de enfrentar os limites da organização e obter as informações sobre as falhas presentes na empresa ou em seu alvo de ataque.

Mas o que são ameaças? **Ameaça** é tudo que, ao explorar uma ou mais vulnerabilidades, podem acarretar em danos e perdas.

Para Silva, Carvalo e Torres (2003) pode-se identificar ameaças através de cenários produzidos ou por listagem de tipificação. No entanto, no cenário atual do mercado das pequenas empresas, os diretores, ou linhas de frente da organização, tem como pensamento de que a segurança da informação se trata de um ponto de vista técnico e não de negócios, colocando a própria organização em risco.

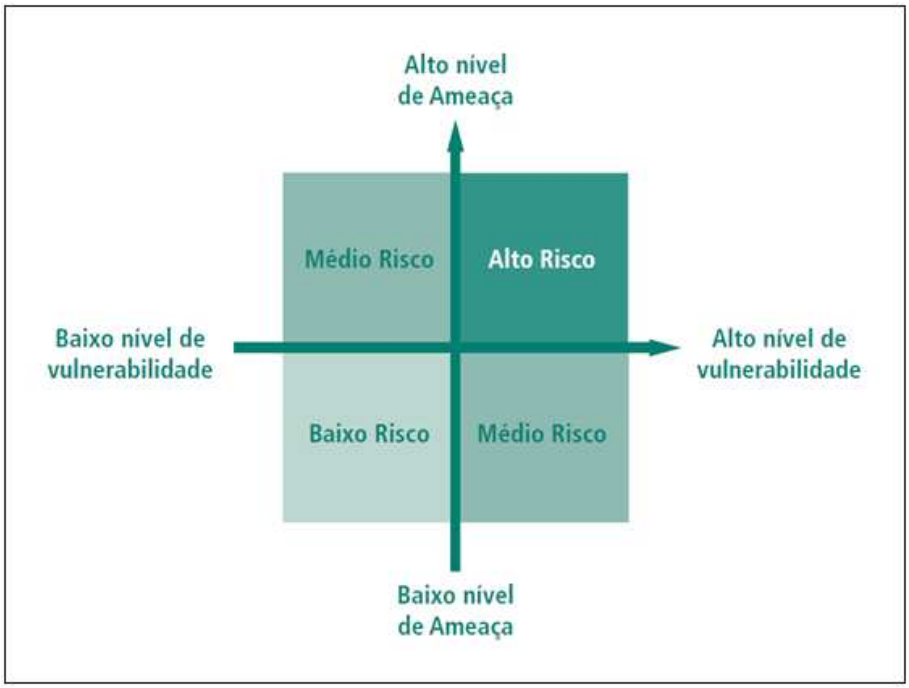
Uma vez que a empresa se encontra ameaçada por algo, ou algum indivíduo malicioso, corre-se o risco de perda de dados, imagem, informação e tudo o que é de posse da organização (DANTAS, 2011, p.41-42).

O conceito de **risco** é visto como algo que usa da probabilidade de um evento junto com suas consequências. Dantas (2011, p.41-42) apresenta uma ideia semelhante dizendo que:

> O risco é compreendido como algo que cria oportunidades ou produz perdas. Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Novo (2010, p.32) também concorda afirmando que “os riscos são a probabilidade de uma ameaça se concretizar, provocando danos aos ativos de uma informação”. O valor do risco se dá conforme a vulnerabilidade e ao nível de ameaça como pode ser vista em um exemplo simplificado na Figura 1 – Medida do grau de risco.

Figura 1 – Medida do grau de risco



Fonte: (NOVO, 2010)

2.3 A SEGURANÇA DA INFORMAÇÃO NO MUNDO ORGANIZACIONAL

O mercado de trabalho pode ter, muitas das vezes o foco direcionado a outros segmentos comerciais, o que faz a tecnologia atuar de forma inteligente, com uma participação importante para o crescimento da empresa, seja na agilidade de entrega, na disponibilidade de produto ou na segurança dos dados registrados em sistema (IBGE, 2005, p.27).

Pelo motivo de a Segurança da Informação (SI) não ser o foco das pequenas empresas devido à escassez de recursos e escala de operações, existe a possibilidade de haver uma grande vulnerabilidade em suas configurações de redes e computadores, que, de maneira genérica, são ativados serviços, portas e protocolos como *Telnet*, *File Transfer Protocol* (FTP) e *Remote Desktop Protocol* (RDP) com senhas de complexidade simples, deixando uma grande janela aberta para um invasor mal-intencionado.

O cenário atual do mundo dos negócios é repleto de informações nas quais as empresas detentoras esperam acontecer algo negativo para buscar auxilio para proteção. Nesse ambiente competitivo, é preciso um certo cuidado para que a imagem da empresa diante à uma invasão não seja totalmente denegrida. Pois segundo Dantas (2011, p.30):

> No ambiente atual, bastante competitivo, as empresas devem estar sempre atentas para as ameaças aos negócios corporativos, que, se concretizadas poderão tirá-las desse cenário, encerrando suas atividades para sempre.

É muito provável que o mesmo computador que usuários acessam para usufruir de *e-mails*, redes sociais ou até transações bancárias é também utilizado para armazenar dados relativos, e se utilizados de alguma forma maliciosa, trará consequências ao responsável dos mesmos (CERT.br, 2012).

No entanto, nem todo dado deve ser protegido da mesma maneira, tanto em um ambiente empresarial quanto em um ambiente escolar, por exemplo, existem dados com diferentes prioridades e necessidades de proteção. Os dados referentes à empresa vão de lucros a prejuízos, gastos e investimentos. Já em um ambiente acadêmico os dados são referentes a alunos, despesas e outros registros. Logo deve-se definir as necessidades de segurança de cada organização para que evite medidas indevidas em toda a informação.

Silva, Carvalo e Torres (2003, p.58) defendem que:

> Um passo essencial na definição e implementação de medidas eficazes de salvaguarda é a existência de uma clara identificação dos proprietários da informação da organização. Ao determinar os responsáveis pelos dados existentes nos SI da Empresa, o responsável pela segurança terá interlocutores claramente identificados com quem poderá definir as necessidades reais de segurança, evitando aplicar medidas genéricas a toda a informação da Empresa, medidas essas muitas vezes desajustadas da realidade.

Todos procuram velocidade em acessar seus dados e por isso, usam uma senha de acesso fácil de se digitar ou memorizar, para facilitar ainda mais, o seu acesso particular. De acordo com a cartilha do CERT.br (2012, p.51):

> “Contas e senhas são atualmente o mecanismo de autenticação mais usado para o controle de acesso a sites e serviços oferecidos pela Internet. É por meio das suas contas e senhas que os sistemas conseguem saber quem você é e definir as ações que você pode realizar [...]”

Atualmente, em todo tipo de tecnologia utilizada no mundo é feita a utilização do quesito autenticação, não somente na internet e sites conforme descrito pela cartilha em sua respectiva época de publicação. No próximo capítulo, será possível perceber que as pequenas organizações contêm muita coisa em comum nesse quesito abordado.

3 ANÁLISE DE VULNERABILIDADES EM AMBIENTE ORGANIZACIONAL

Por questões éticas e com o intuito de garantir a integridade e confidencialidade da empresa citada, darás um nome fictício à esta de Empresa Anônima (EA), e todos os testes de exploração serão realizados em um ambiente virtual, montado ao que mais se aproxima da realidade estudada.

Este capítulo retratará o cenário existente antes de algumas implementações de segurança da informação, e também depois destas implementações terem sido feitas nessa pequena empresa, que não possui seus objetivos voltados à tecnologia, e sim ao comércio comum.

No início de 2015, a EA se encontrava com diversas vulnerabilidades, tais como:

- Falta de *Group Policy* (GPO) locais e acesso de administrador;
- Roteadores e Access Points (AP) sem restrições;
- Computadores com senhas padrões;
- Falta de gerenciamento do servidor *firewall*;
- *Firewall* das máquinas locais desativado;
- Servidor de banco de dados atuando como servidor de *login* também;
- Infraestrutura de rede da Empresa Anônima (EA) desprotegida;
- Máquinas em versões antigas de sistemas operacionais e sem atualizações periódicas;
- Falta de política de segurança.

Partindo de tais fragilidades, de modo respectivo, houve uma análise para entender quais riscos a empresa EA estava enfrentando, com a intenção de mitigar estes riscos ou dificultar o livre acesso do usuário mal-intencionado. No entanto, para ocorrer a mitigação dos riscos, deve-se primeiro listá-los para facilitar a compreensão e ordem de execução dos processos de segurança realizados para proteção das informações.

3.1 FALTA DE *GROUP POLICY* (GPO) LOCAIS E ACESSO DE ADMINISTRADOR

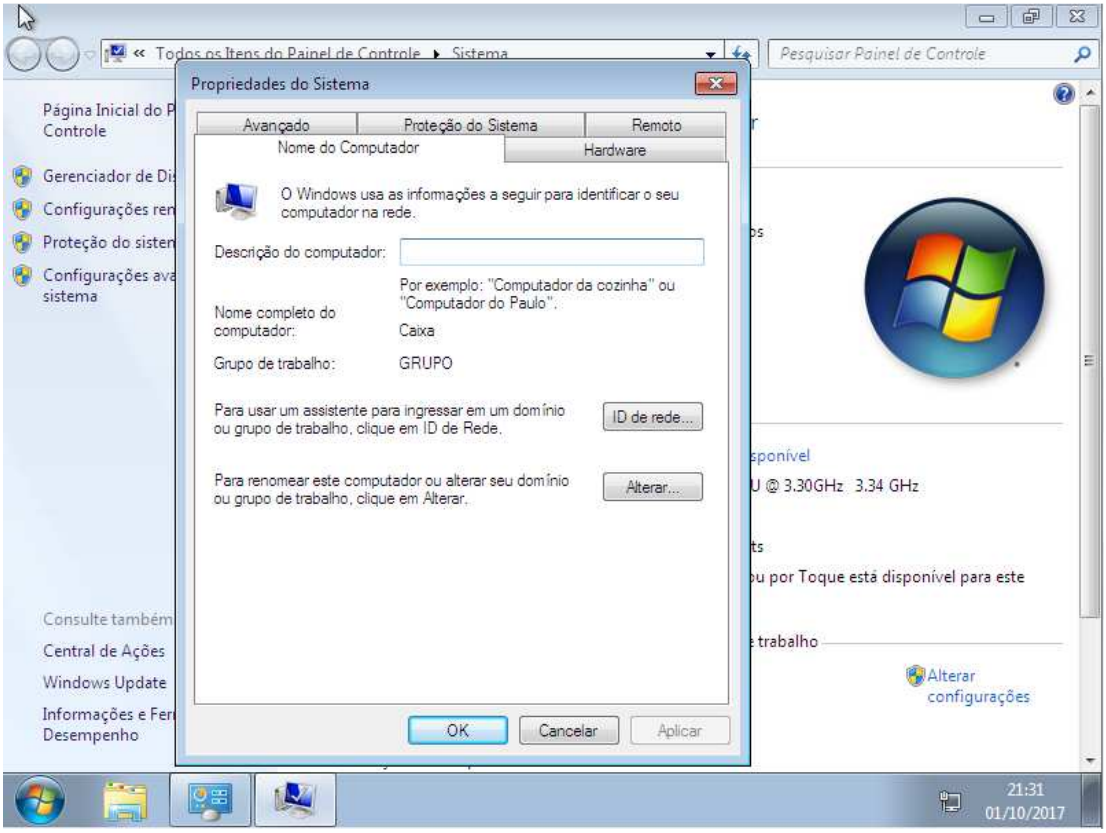
Com a falta de GPOs locais, o usuário tem acesso e permissão de alteração a todo tipo de configuração do sistema operacional, propiciando a existência de um

enorme risco à integridade das informações que estão contidas no computador e também às informações que passam por aquele computador.

3.1.1 Propriedades do Sistema

Nas propriedades, ou configurações do sistema operacional conforme Figura 2 – Propriedades do Sistema, é exibida toda informação de *hardware*, *hostname (tradução livre: nome do hospedeiro)* e até qual grupo está acoplado a máquina operante.

Figura 2 – Propriedades do Sistema



Fonte: Captura de tela retirada pelo próprio autor.

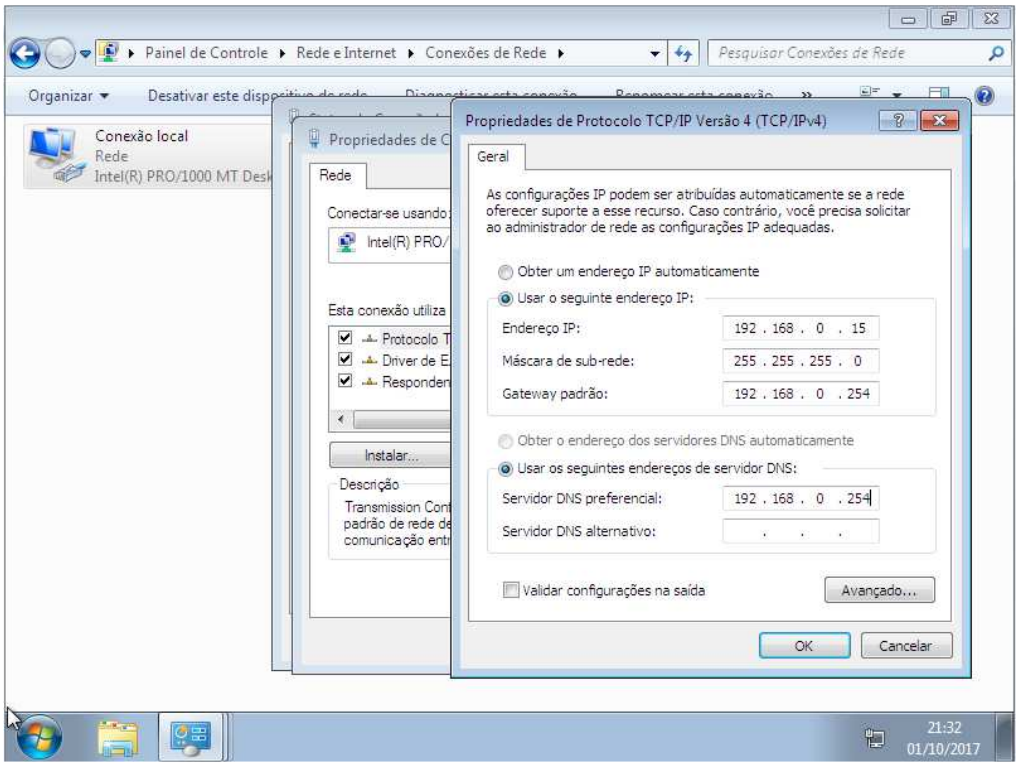
3.1.2 Configurações de rede

Com a permissão de acesso e alteração das configurações de rede, o usuário, ou o invasor mal-intencionado obtém as informações de DNS, *Gateway* e IP conforme Figura 3.

Desse modo, torna-se possível estimar o alcance da rede toda e também quais endereços de IP são aceitos na rede, ou também, se for o caso, usar o

endereço da máquina em outra máquina para adentrar à rede e efetuar o ataque com sucesso.

Figura 3 – Configurações de Rede

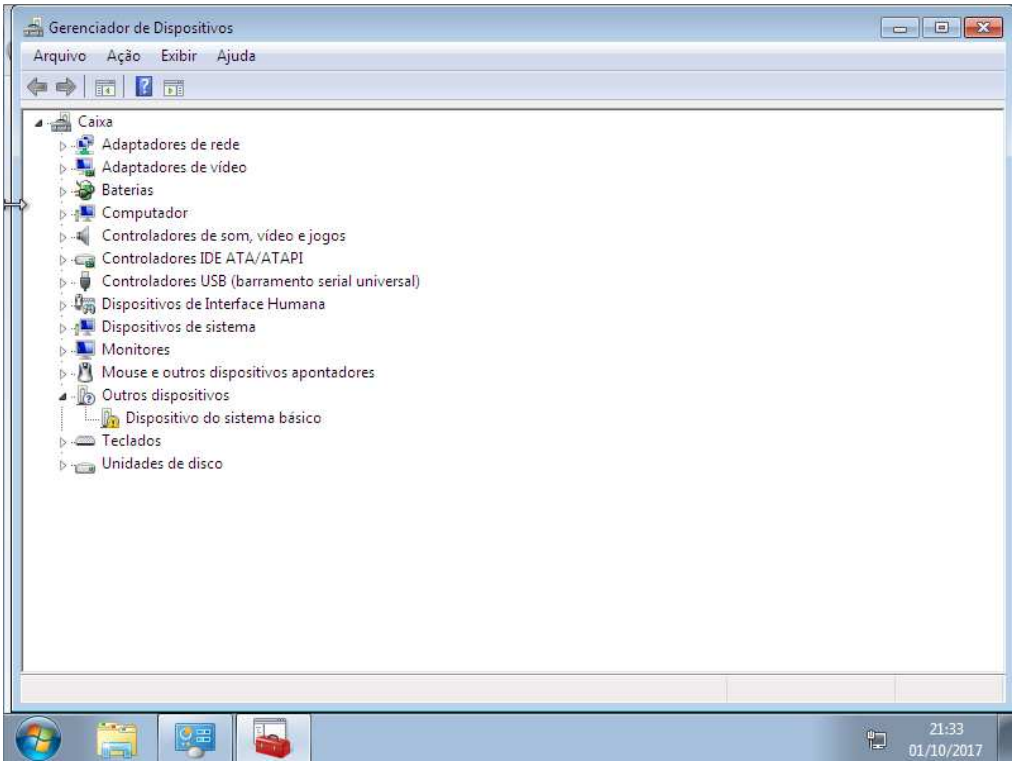


Fonte: Captura de tela retirada pelo próprio autor.

3.1.3 Configurações e informações dos drivers para funcionamento do hardware

Com as configurações dos dispositivos liberadas, o usuário, ou invasor mal-intencionado tem a ciência de todos equipamentos conectados diretamente no computador conforme retrata a Figura 4, tal como quais dispositivos estão à disposição da máquina a ser acessada.

Figura 4 – Dispositivos da Máquina

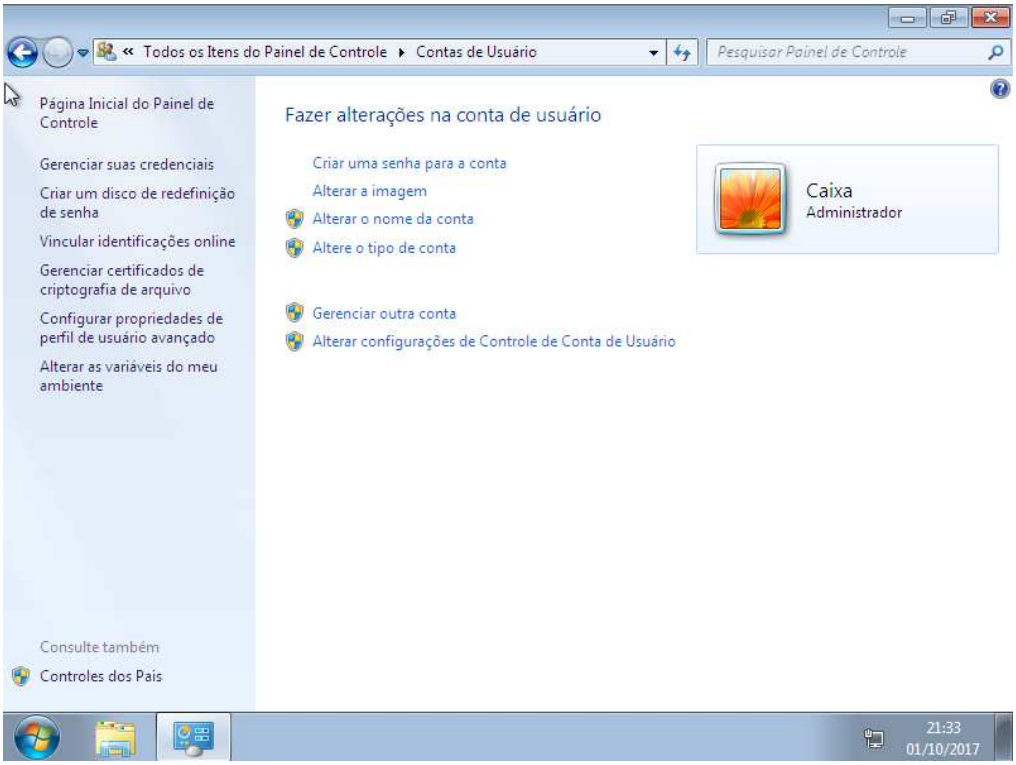


Fonte: Captura de tela retirada pelo próprio autor.

3.1.4 Configurações de usuários

O usuário tem a opção não só de alteração da senha, como também de exclusão, gerir credenciais, certificados, criar novos usuários, e é capaz de ter todo acesso como administrador do sistema operacional conforme Figura 5, que é o nível de maior permissão usada hoje nesse ambiente de sistema operacional.

Figura 5 – Configurações de Contas de Usuários



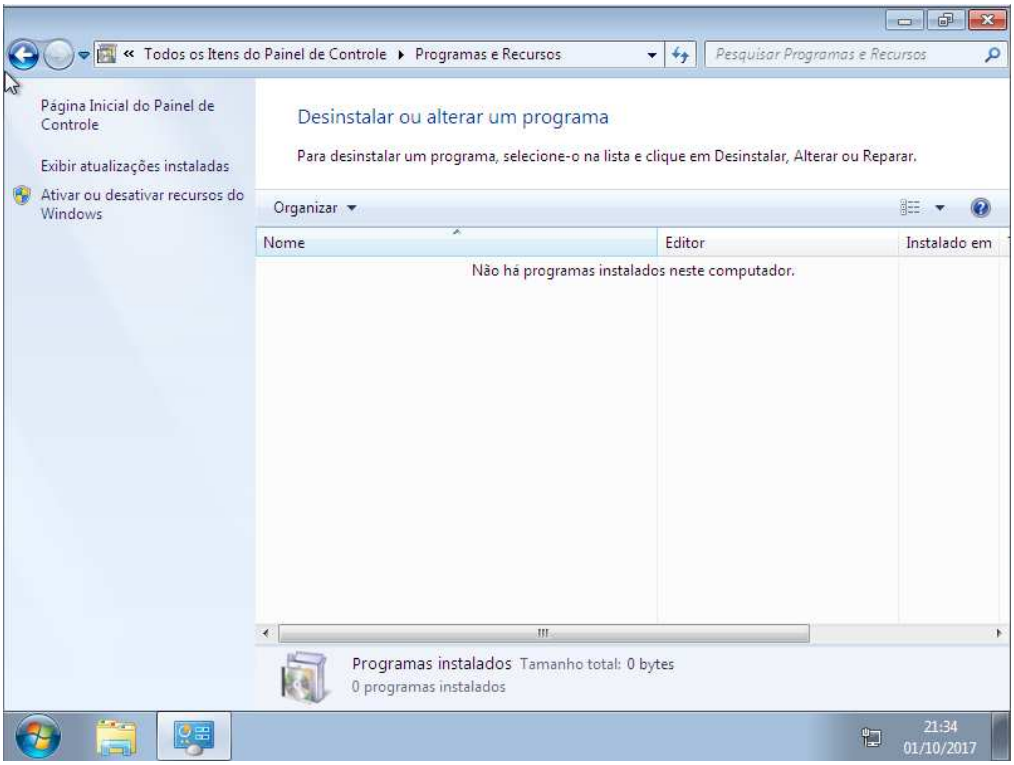
Fonte: Captura de tela retirada pelo próprio autor.

3.1.5 Instalação e remoção de programas

Com a permissão de instalar e remover programas explícita na Figura 6, o usuário pode, por engano, desinstalar algum programa dependente dos processos cotidianos da empresa, causando um desconforto e a distração das pessoas responsáveis para a reinstalação do software.

Já no caso do invasor mal-intencionado, este pode instalar programas maliciosos, *Keyloggers*, *Malwares,* e outros vírus comuns que atingem os usuários leigos com frequência.

Figura 6 – Tela de Programas e Recursos



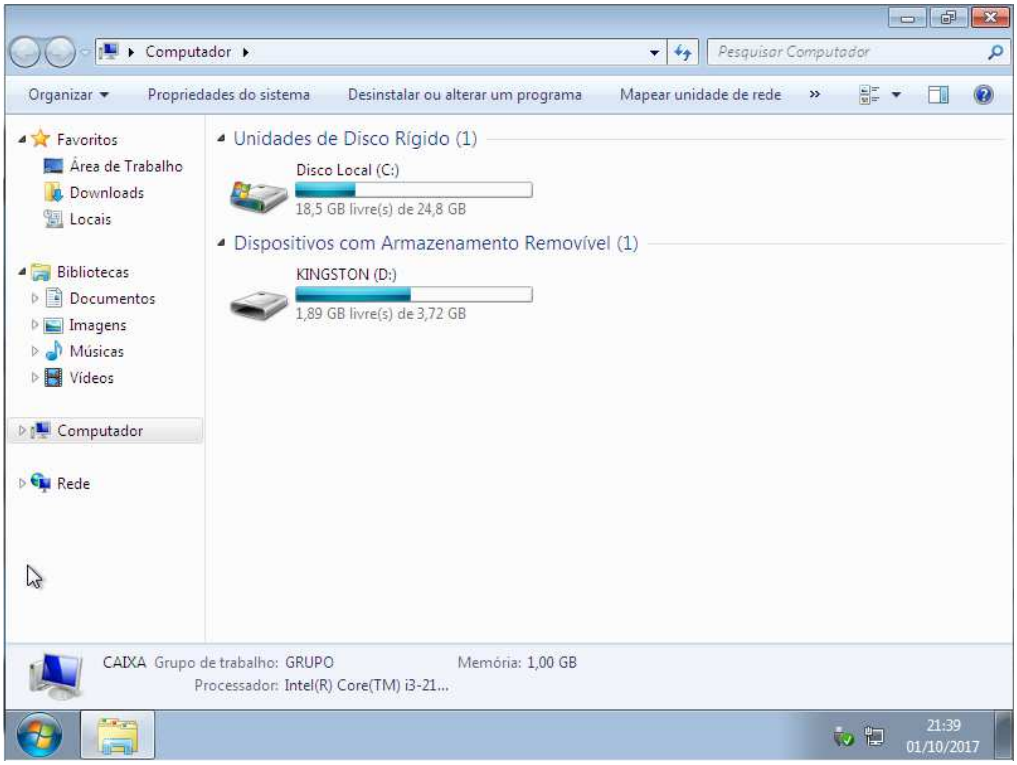
Fonte: Captura de tela retirada pelo próprio autor.

3.1.6 Penetração e ejeção de dispositivos removíveis (*Pen Drives)*

Os *Pen drives* foram, durante uma época, um dos maiores responsáveis pela propagação de vírus nas máquinas pessoais e em empresas. Atualmente, esse tipo de incidente não é causado com frequência, mas nada impede que algum dispositivo removível como o *pen drive* esteja contaminado com um *Malware ou Cryptor Locker* de risco.

Em uma simples tentativa de apenas plugar um pen drive qualquer na máquina alvo, a leitura do disco removível demonstrou-se um sucesso, como descreve Figura 7.

Figura 7 – Dispositivos removíveis



Fonte: Captura de tela retirada pelo próprio autor.

3.2 ROTEADORES E ACCESS POINTS (AP) SEM RESTRIÇÕES

Na organização EA, todo ponto de acesso à internet era completamente aberto à intranet inteira, que facilitaria, para um mal-intencionado, acessar computadores e informações locais simplesmente pelos pontos Wi-Fi. Havia, também, roteadores espalhados em cantos aleatórios com portas acessíveis para qualquer um que plugasse o cabo, fazendo com que houvesse a possibilidade deste indivíduo, se conectar à rede interna com imensa facilidade.

A conexão Wi-Fi era “protegida” somente por senhas comuns, não consideradas fortes segundo a cartilha de segurança do CERT.br (2012, p. 61), ou seja, uma senha mal elaborada, e fácil de ser descoberta como: a) o nome do estabelecimento e o piso onde se encontra o dispositivo roteador; b) o telefone do estabelecimento; ou até mesmo c) o nome do estabelecimento seguido do ano presente. Estas senhas, são completamente fáceis de quebrar por um simples ataque bruto feito por ferramentas como Hydra, que tem a intenção de fazer testes de penetração em portas e protocolos indicados por parâmetros na linha de comando.

3.3 COMPUTADORES COM SENHAS PADRÕES

Em algumas empresas, mais visar, pequenas empresas, usualmente atribui-se uma configuração em seus computadores, semelhante ou idêntica a que usuários utilizam em suas casas. Os usuários são orientados à usarem a senha com o mesmo nome referente ao *login,* ou seja, usuário e senha iguais. Essas orientações, defendidas por um argumento de que facilita o acesso remoto para auxilio técnico, também facilita a entrada de um invasor, ou de vírus conhecidos por epidemias de ataques atuais, o *Ransomware*.

O *Ransomware* tem como princípio próprio, criptografar todos os dados do computador e pedir uma quantia em dinheiro, em troca do resgate das informações que era então, contidas na máquina presente (CERT.br).

3.4 FALTA DE GERENCIAMENTO DO SERVIDOR *FIREWALL*

Na EA, havia um servidor Linux na distribuição CentOS 6.7 trabalhando com serviços de: Squid, FTP, SARG, Apache, VPN e Iptables.

Apesar da existência de tantos serviços disponíveis, nem todos estavam sendo utilizados, tampouco gerenciado por alguém. Não havia tal tarefa sob responsabilidade de algum empregado da empresa. O serviço de transferência de dados através do protocolo FTP, por se tratar de uma conexão feita sem qualquer tipo de criptografia, pode ser facilmente capturada por um software interceptador de pacotes para identificação e autenticação do acesso ao serviço.

Analisando hipoteticamente um indivíduo mal-intencionado dentro da rede, suas chances de ataque bem-sucedido se encontram em alta quando o assunto se trata de serviços inutilizados sem criptografia na “cabeça” da rede interna da empresa – sendo no caso em questão -, o *Firewall*.

3.5 *FIREWALL* DAS MÁQUINAS LOCAIS DESATIVADO

Na análise feita na Empresa Anônima (EA), foi constatado que todos os serviços de firewall local presentes no sistema operacional, fora desativado pela presença de um servidor Linux existente, e também, para a utilização de programas de serviços remotos auxiliares. Com o serviço desativado, todo serviço instalado na máquina tem o livre acesso para executar processos e utilizar portas existentes no sistema operacional. No entanto, em uma propagação interna, o dano que a

instalação de um serviço mal-intencionado faz para os dados da máquina, ou da rede, tem a possibilidade de se tornar irreversível futuramente.

3.6 SERVIDOR DE BANCO DE DADOS ATUANDO COMO SERVIDOR DE *LOGIN* TAMBÉM

O servidor responsável pelo “cérebro” da empresa, que tem como finalidade executar serviços para auxílios de softwares e alocar em seu espaço todos os dados da empresa, tais como suas vendas, lucros, despesas e contas a pagar, era também utilizado como um servidor de acesso remoto.

O protocolo de acesso via *terminal service, Remote Desktop Protocol* (RDP), era utilidade do servidor mais importante da empresa, e continha usuário e senha para todos os colaboradores, sendo elas, respectivamente, o próprio nome de cada colaborador.

Sendo assim, todo usuário que abrisse uma conexão para o servidor, autenticava seu acesso com o próprio nome, mesmo que para fins de mapeamento. Logo, o caminho para o indivíduo mal-intencionado fica ainda mais fácil, pois sem esforço, a senha seria quebrada via ataque de força bruta em poucas horas para acesso e violação dos dados.

3.7 INFRAESTRUTURA DE REDE DA EMPRESA ANÔNIMA (EA) DESPROTEGIDA

Apesar de ser uma empresa privada, a Empresa Anônima (EA) não tratava parte de sua infraestrutura de rede como importante, conforme Figura 8. Diversas portas e cabos estavam soltos, sem utilidade, até mesmo acessíveis para qualquer pessoa que entrasse no local, que se encontrava em uma sala comum, usada para fins financeiros da empresa e que não tinha sequer gerenciamento do setor de Tecnologia da Informação (TI), sem segurança e qualquer fator de proteção.

Figura 8 – Infraestrutura de Rede Interna

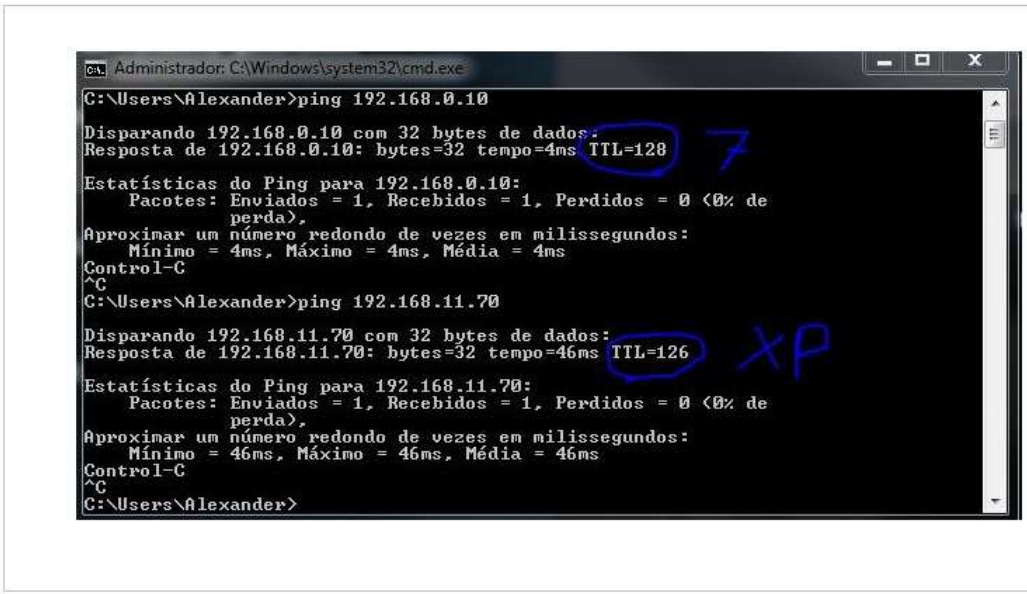
Fonte: Foto retirada pelo próprio autor.

Através destas portas ativadas e sem uso, qualquer pessoa que introduzisse um cabo de rede na infraestrutura de rede, teria acesso à toda rede interna e externa da empresa, pois não havia *VLANs* para restringir acessos, nem tampouco monitoramento e gerenciamento da rede interna.

3.8 COMPUTADORES COM SISTEMAS OPERACIONAIS ANTIGOS E SEM ATUALIZAÇÕES PERIÓDICAS

Foi encontrado na rede interna da EA, através de testes simples como o envio de *pings* à algumas máquinas e, como indica a Figura 9, existem máquinas em versões antigas de sistemas operacionais, como, no caso citado, o Windows XP. A identificação foi feita através da sigla TTL do *prompt* de comando que significa *Time To Live*, em tradução livre “tempo de vida” que o pacote enviado tem.

Figura 9 – TTL das Maquinas na Rede



Fonte: Captura de tela retirada pelo próprio autor.

O TTL de cada máquina varia de acordo com seu sistema operacional instalado, que vem, como padrão, em suma, Windows 7 com um TTL= 128 e o Windows XP com um TTL= 126, um valor configurado para que aquele pacote em específico, tenha o seu tempo de vida definido.

Por conseguinte, aqueles que não efetuavam atualizações periódicas nas máquinas utilizadas em um ambiente, tiveram uma surpresa quando sofreram ataques direcionados a esse tipo de vulnerabilidade, no qual todo e qualquer dado, era criptografado a pedido de um resgate em dinheiro.

3.9 FALTA DE POLÍTICA DE SEGURANÇA

Dentro do ambiente profissional, não havia sequer alguém responsável para determinar políticas de segurança e conscientização da importância da informação e suas trajetórias. Através disso, e-mails eram enviados para dentro e fora da empresa com informações internas, usuários locais abriam links suspeitos em ambiente de trabalho na máquina que utilizava todos os dias, não trocava senhas pessoais periodicamente, fazendo com que, a descoberta e dedução delas fossem premeditadas.

De certo, um simples ataque de força bruta rodando todos os dias, teria tempo suficiente para quebrar a senha, levando em conta dados básicos do usuário, como o nome, data de nascimento, o ano atual, animal de estimação, nome da mãe ou dos filhos.

No quarto capítulo, serão realizadas as correções de algumas configurações incorretas existentes e apresentadas no terceiro capítulo, a fim de facilitar e clarear a ideia de que, pequenas alterações podem garantir a defesa de ataques em massa que miram os desprevenidos.

4 TESTE DE PENETRAÇÃO E APLICAÇÕES DAS CORREÇÕES

Nesse capítulo serão abordadas as aplicações feitas no ambiente virtual criado para representar a empresa citada no capítulo anterior. Sendo assim, com a intenção de facilitar o entendimento claro da ordem de execução, tratará das vulnerabilidades seguindo uma ordem respectiva dos tópicos no capítulo anterior.

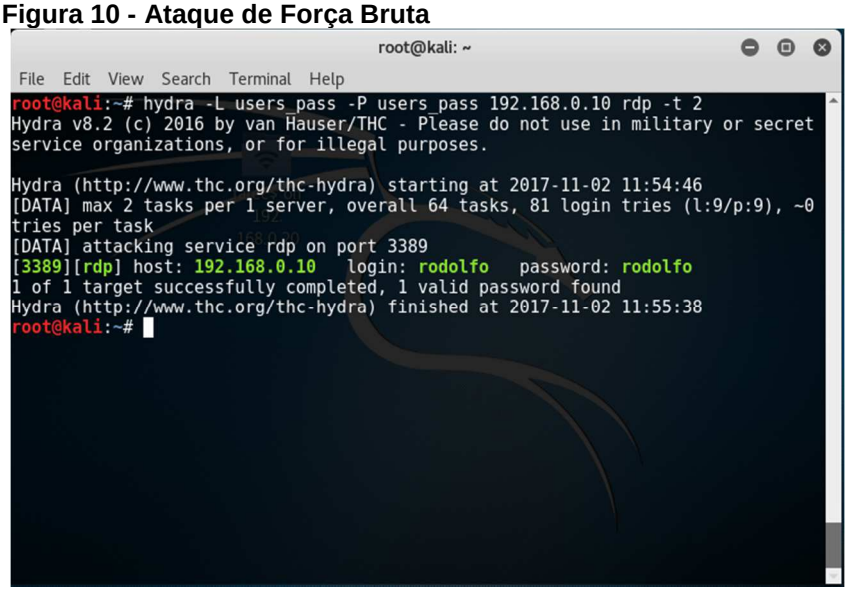
4.1 ATAQUE DE FORÇA BRUTA

No entanto, a fim de explicitar a facilidade de conseguir acesso a informações secretas e conter privilégio sobre as máquinas invadidas, como introdução deste capítulo, será realizado um teste de penetração (do inglês: *Penetration Test*), mais conhecido por *Pentest*.

O *Pentest* tem como uma das finalidades, fazer análises de vulnerabilidades expostas em um ambiente, ou uma rede, porém este não é seu único propósito. O teste de penetração vai além de uma avaliação, ele também avalia as vulnerabilidades identificadas para verificar se esta é real ou falsa positiva. Como por exemplo, uma auditoria pode rodar softwares para listar vulnerabilidades, já o teste de penetração irá além de listar, iniciar ataques direcionados à estas para provar uma vulnerabilidade mais concreta (MUNIZ e LAKHANI, 2013, p. 7).

Dadas as explicações, foi realizado um teste de penetração através de uma das diversas ferramentas da distribuição Kali Linux, a Hydra, que executa ataques de força bruta direcionados a um endereço de IP, através de uma porta, ou serviços específicos, com um dicionário criado em um arquivo de texto, conforme a Figura 10.

Figura 10 - Ataque de Força Bruta

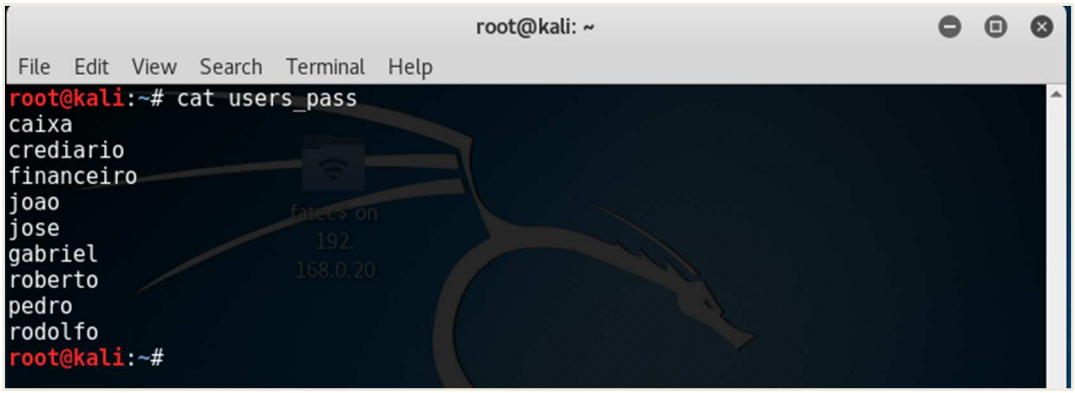


Fonte: Captura de tela retirada pelo próprio autor.

Através da Figura 10, pode se comprovar que o ataque foi um sucesso e o acesso foi obtido através do usuário de *login* “Rodolfo” com a senha “rodolfo”, conforme situação previamente informada, tratando-se da vulnerabilidade existente em ambientes que utilizam a senha semelhante ao nome de usuário.

Neste ataque de força bruta, foi utilizado um arquivo conforme Figura 11, com alguns nomes direcionados ao alvo, uma vez que, necessita de algum conhecimento ou informação para o ataque ser efetivo, pois, um ataque de força bruta com um dicionário muito amplo se resultará em uma quantidade enorme de horas para quebrar a senha do alvo.

Figura 11 - Arquivo de Texto

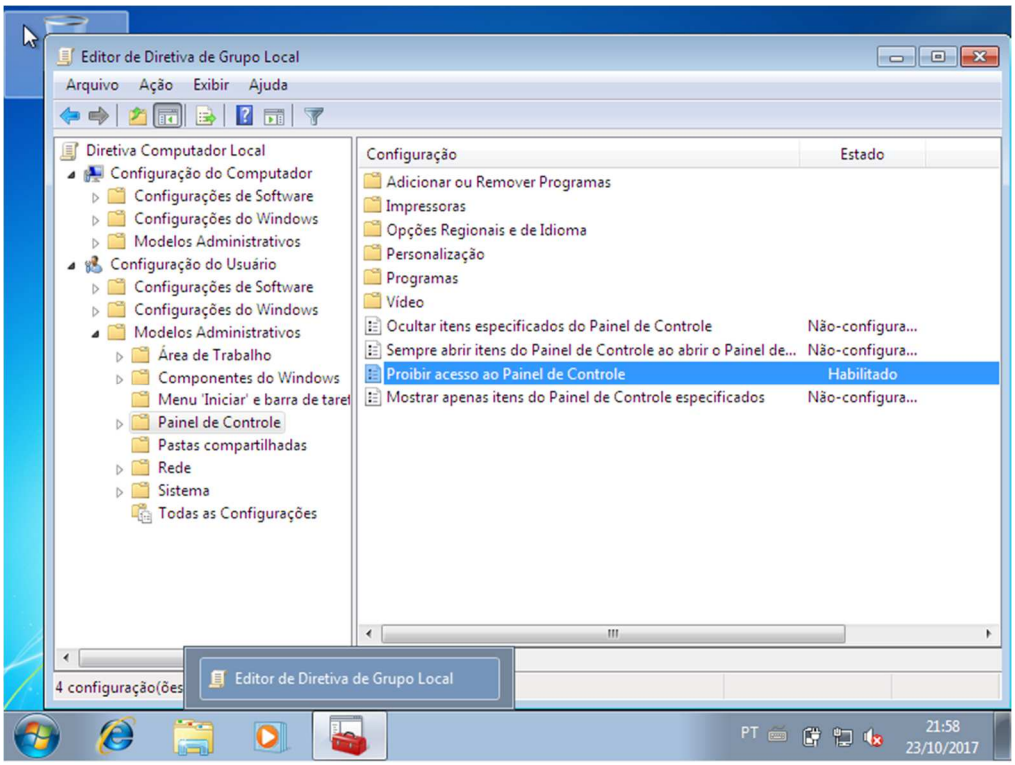


Fonte: Captura de tela retirada pelo próprio autor.

4.2 GROUP POLICY (GPO) LOCAIS E CONTROLE DE ACESSO

Em um ambiente empresarial, no qual não existe a utilização de um servidor *Active Directory* (AD), a aplicação de GPOs, pode ser realizada localmente conforme Figura 12, para dificultar acessos indevidos e mudanças nas configurações que dificultam reparos futuros.

Figura 12 - Editor de Diretiva de Grupo Local



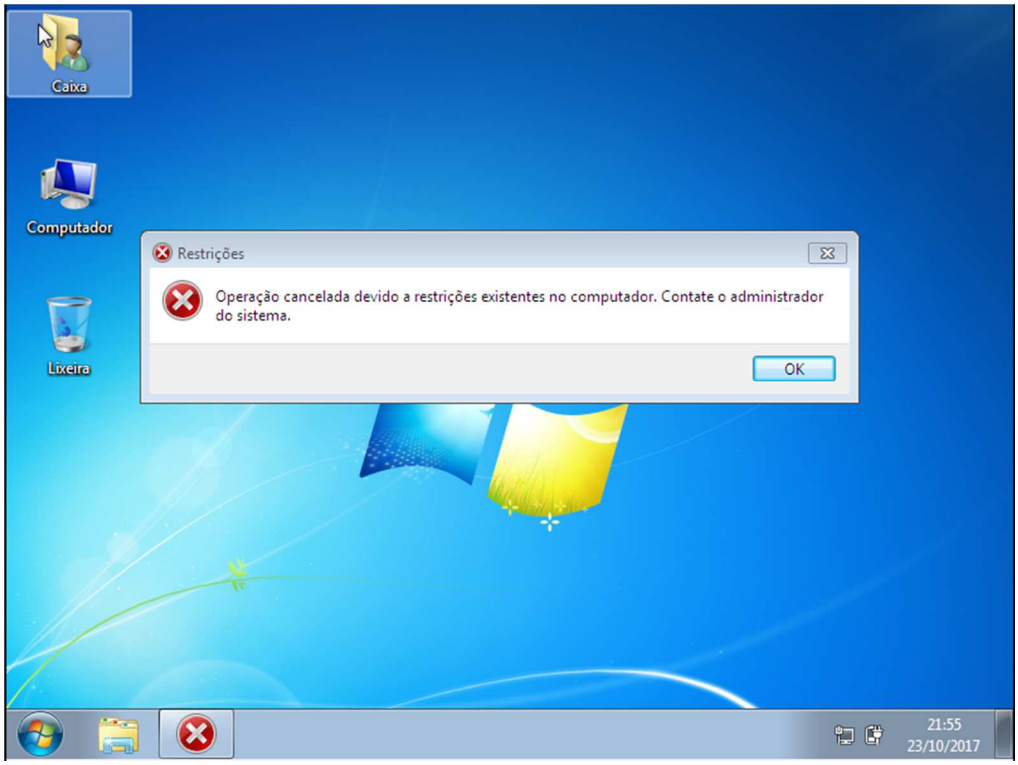
Fonte: Captura de tela retirada pelo próprio autor.

No editor de diretivas do Windows, aberto através do comando “gpedit.msc”, escrito no Executar do Menu Iniciar, é possível restringir e até mesmo proibir acessos indevidos de usuários curiosos. Para uma primeira visão, será feito o bloqueio local do acesso ao Painel de Controle, visto que, é um link repleto de informações e configurações responsáveis pelo controle completo do sistema operacional.

Uma vez que as configurações do sistema fazem parte do painel de controle, as mesmas serão totalmente restringidas à serem acessadas por qualquer usuário a partir da habilitação desta regra.

A fins de conferência, tentou-se acessar tanto o Painel de Controle, quanto as configurações do sistema que podem ser encontradas nas propriedades do computador. Em resposta, foi retornada uma mensagem de alerta avisando ao usuário de que o acesso estava restrito ao tipo de informação solicitada conforme Figura 13.

Figura 13 – Mensagem de Restrição



Fonte: Captura de tela retirada pelo próprio autor.

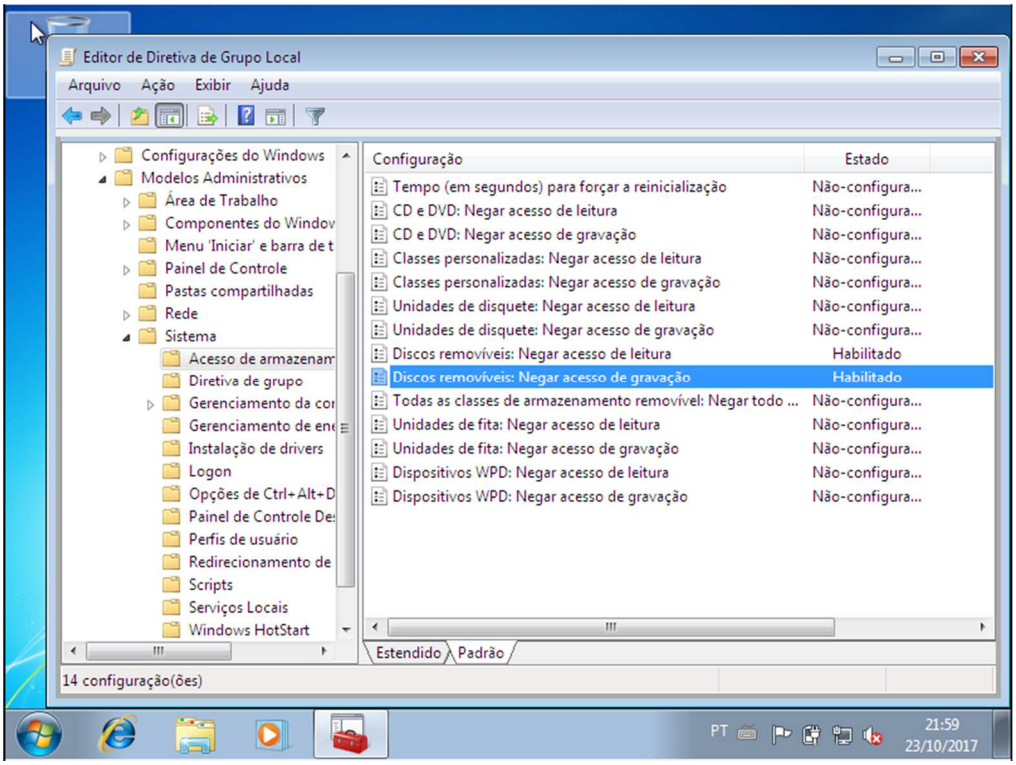
A mensagem de restrição é apresentada sempre que o usuário tenta acessar alguma configuração proibida pelo administrador, assim como as configurações de rede, de dispositivos, de usuários e até de instalações e remoções de programas.

4.2.1 Discos Removíveis

Para restringir a leitura e/ou a gravação de discos removíveis na máquina, existe uma regra situada no editor de diretivas que aplica devidas correções, como mostra na Figura 14.

.

Figura 14 - Configurações de Discos Removíveis



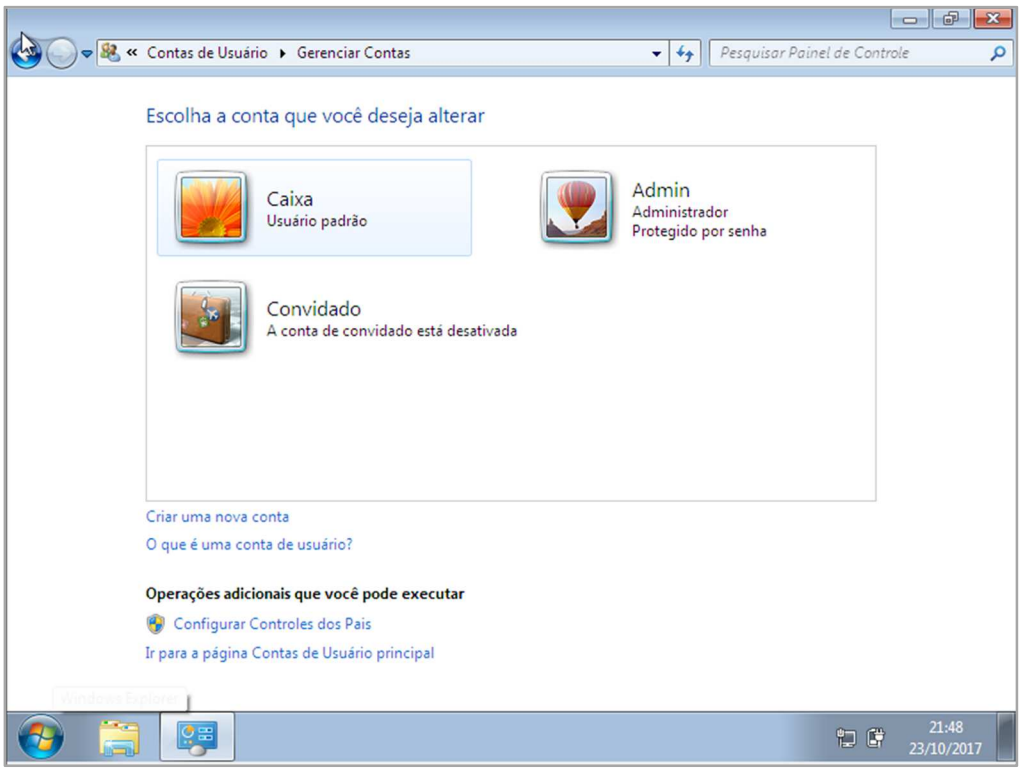
Fonte: Captura de tela retirada pelo próprio autor.

Para validar todas as configurações aplicadas no editor de diretivas, basta fazer *logoff* do usuário, ou executar o comando simples denominado de “gpupdate” que também deve ser executado através do Menu Iniciar do Windows.

4.2.2 Controle de Acesso

Todas as configurações não valeriam de nada se o usuário diário estivesse com poderes de administrador. Assim, o correto e mais adequado, é retirar o controle de acesso como administrador e substituir por acesso de usuário padrão. No entanto, é recomendado que, para fins de manutenção ou recuperação de dados locais da máquina, seja criado um usuário novo e em poder da pessoa responsável na organização pela parte de informática que terá acesso como administrador das máquinas conforme Figura 15, não esquecendo de escolher a senha de modo seguro e considerado forte (CERT.br, p. 51).

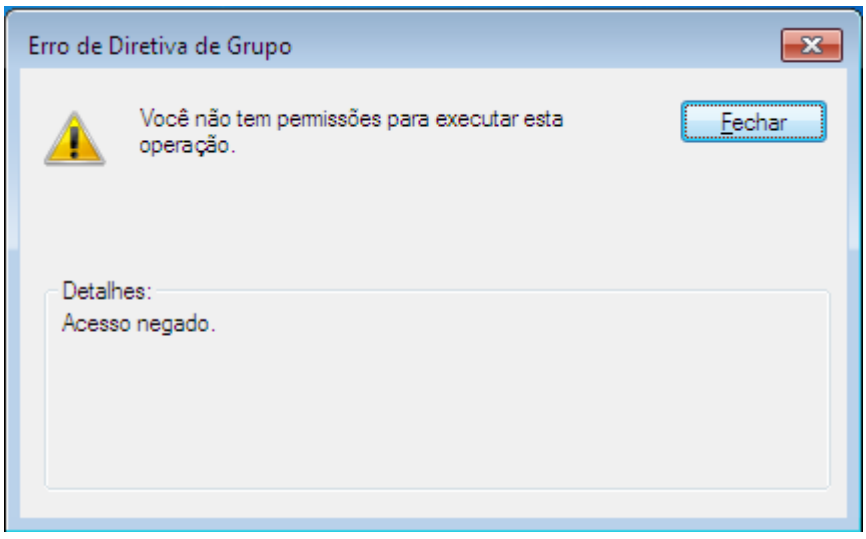
Figura 15 - Gerenciador de Contas



Fonte: Captura de tela retirada pelo próprio autor.

Com as configurações finalizadas e completas, o usuário passou a não ter mais acesso ao editor de diretivas. Conforme Figura 16, foi executado um teste para validar a integridade das configurações aplicadas e em retorno, obtiveu-se a mensagem: “Você não tem permissões para executar esta operação”.

Figura 16 - Permissão Bloqueada no Editor



Fonte: Captura de tela retirada pelo próprio autor.

No entanto, com a senha de administrador, é possível acessar tais configurações para manutenção ou retirar alguma restrição específica, portanto, é necessário escolher a senha de autenticação da maneira mais adequada, tendo como sugestão: **caracteres maiúsculos, caracteres minúsculos, números** e de preferência, **caracteres especiais.**

4.3 ROTEADORES E ACCESS POINTS (AP)

Assim como explicado anteriormente, os roteadores e *Access Points* (AP) utilizados na organização, devem conter uma senha considerada forte, mas além deste quesito, não se deve acessar a intranet, uma vez que, os roteadores e APs são usados para apenas o acesso à internet, geralmente por convidados, representantes de futuras parcerias ou reuniões semanais.

Logo, se o roteador for de modelo recente, deve se criar uma “Rede Convidado” que terá opções para limitação de acesso e também de banda utilizada, mitigando o risco de acesso direto à senha do roteador ou AP e também o risco de acesso direto à intranet da empresa, que contém toda informação da organização.

4.4 COMPUTADORES E SUAS SENHAS

Seguindo o raciocínio anterior, manuseando as senhas de maneira adequada, dificilmente ocorreria um ataque bem-sucedido de força bruta para obter acesso, até porque, caso ocorresse, com uma senha utilizando **três** das quatro sugestões de criação de senha, demoraria anos, mesmo com um supercomputador, para quebrar a senha declarada.

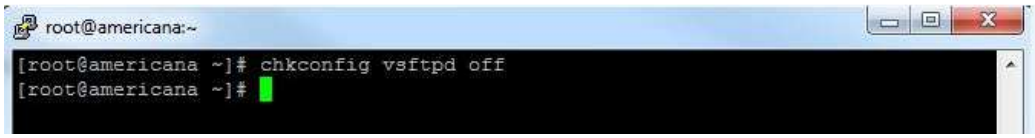
4.5 O SERVIDOR FIREWALL

O primeiro passo para melhorar a situação de um Firewall que contém serviços ativos inutilizados, é desinstalar, ou desativar tais serviços. O serviço de transferência de arquivos através do protocolo *File Transfer Protocol* (FTP) é totalmente ultrapassado em questão de segurança, uma vez que, o protocolo em questão não utiliza qualquer tipo de criptografia para firmar a conexão em ambas as pontas.

Para desativar o serviço que utiliza o protocolo FTP do servidor Firewall com a distribuição do CentOS 6.7 Linux, basta executar duas linhas de comando, primeiro deve-se parar o serviço ativado com a linha “service vsftpd stop” e em seguida,

desativar o serviço da inicialização do sistema com a linha “chkconfig vsftpd off”, como sugere na Figura 17.

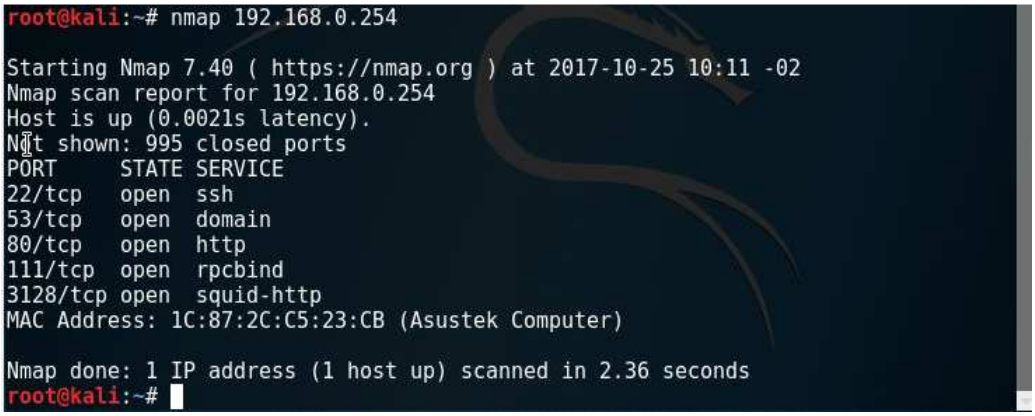
Figura 17 - Comando CentOS



Fonte: Captura de tela retirada pelo próprio autor.

A fim de conferência do comando, pode-se consultar através de uma ferramenta de *pentest* da distribuição Kali Linux, se o serviço está efetivamente desativado, conforme Figura 18.

Figura 18 - NMAP para Checagem de FTP



Fonte: Captura de tela retirada pelo próprio autor.

Uma vez que o serviço está desativado, não há mais a vulnerabilidade do FTP para um usuário malicioso usufruir das brechas deste serviço em questão e este ser, de fato, uma ameaça.

4.6 O FIREWALL DAS MÁQUINAS LOCAIS

Iniciando o raciocínio em um contexto de ataque interno (na intranet) da organização EA, todas as máquinas não hesitariam em aceitar a execução de qualquer serviço, devido à não existência, ou a desativação do firewall padrão do sistema operacional.

No entanto, para não prejudicar auxiliares remotos, utilizados para manutenção por parte do setor de Tecnologia da Informação (TI), há possibilidades de criar-se regras de permissões no firewall do sistema operacional, mantendo assim, a segurança, também, interna do ambiente empresarial.

4.7 O SERVIDOR DE BANCO DE DADOS

O acesso ao servidor de banco de dados deve ser restrito apenas ao *software* utilitário das informações da empresa. Uma vez que o acesso é liberado à usuários leigos, abre-se uma nova porta para o mundo dos usuários maliciosos, sendo assim, não se torna necessária, um usuário RDP para cada colaborador da organização, e sim somente aos responsáveis pelo setor de Tecnologia da Informação.

4.8 INFRAESTRUTURA DE REDE

Uma reestruturação da infraestrutura de rede certamente não é uma tarefa básica, no entanto, mapear pontos utilizados em toda organização é obrigação do responsável pela parte informática da empresa.

Utilizando pontos ativos, mas não utilizados, era possível o acesso totalmente livre da rede interna da empresa, assim como o acesso total externo se escolhesse um alcance de endereço IP válido ao servidor firewall. Cada ponto foi mapeado e todos os pontos ativos foram organizados ao rack principal da matriz da EA conforme Figura 19.

Figura 19 - Rack Reestruturado

Fonte: Foto retirada pelo próprio autor

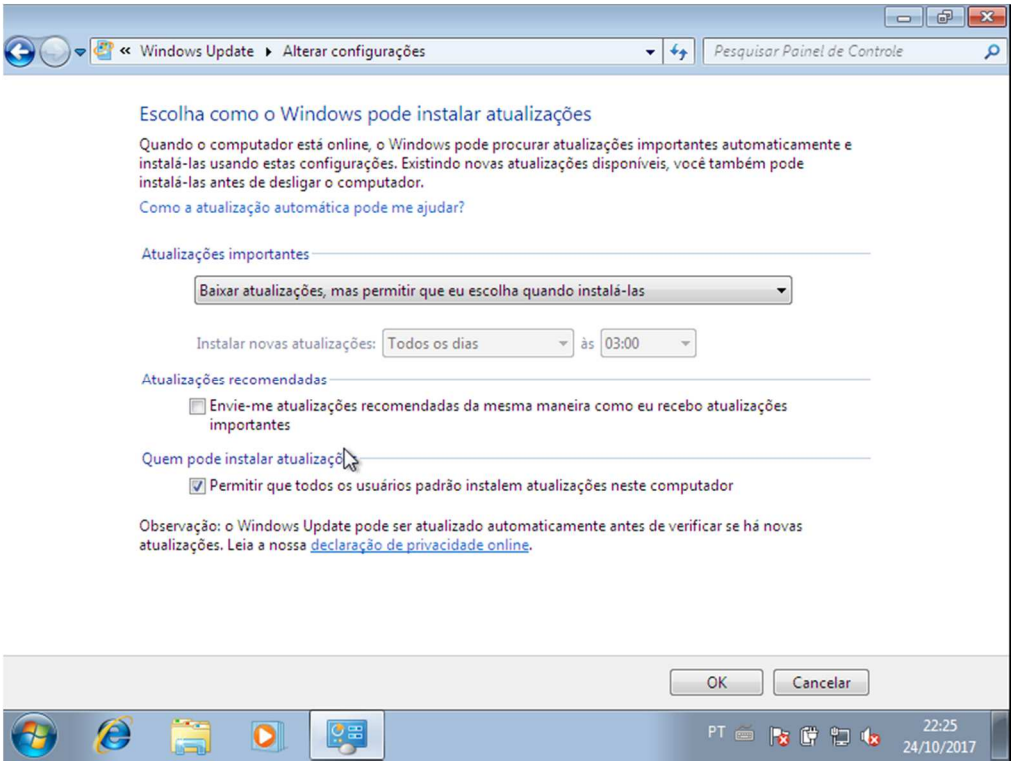
Além da organização dos pontos e mapeamento do que estava ativo, fora documentado e conectado todo e cada ponto existente na empresa, para que se um dia precisasse ser utilizado, a pessoa responsável pelo setor informático faria a conexão do ponto em comunicação com os demais via *patch cord*.

4.9 MÁQUINAS: SISTEMAS OPERACIONAIS E ATUALIZAÇÕES PERIÓDICAS

Por ser uma empresa, ainda que de pequeno porte, a EA deveria estar em dia com atualizações e mantendo suas máquinas com sistemas operacionais atuais, ou não tão antigos.

A informação que trafega de máquina a máquina na organização de pequeno porte é intensa e necessita de cuidados básicos, mas que não atrapalhe aos afazeres do dia a dia. Portanto, para atualizar os computadores operacionais, é recomendado utilizar o tipo: “Baixar atualizações, mas permitir que eu escolha quando instalá-las” conforme Figura 20.

Figura 20 - Configurações de Atualizações



Fonte: Captura de tela retirada pelo próprio autor.

Já para os computadores que estão fora da zona de atualização e suporte fornecido pelo autor do sistema operacional utilizado, é recomendado que seja

realizada uma nova instalação de sistema operacional, para garantir melhor suporte e menos riscos diante das vulnerabilidades.

4.10 IMPLANTANDO UMA POLÍTICA DE SEGURANÇA

Após todas as correções e sugestões apresentadas no decorrer deste capítulo, a segurança da informação da pequena empresa em questão necessita ser gerenciada. Assim, pelo fato de o quadro de colaboradores estar sujeito a sofrer mudanças decorrentes, uma política de segurança ou manual de boas práticas para garantir a integridade, confidencialidade e disponibilidade das informações não é um assunto a se dispensar.

Para a elaboração desta, deve-se procurar melhores informações e dicas em cartilhas de segurança e normas específicas, uma vez que, atualmente a grande maioria de pessoas, são usuários da internet e estão acessíveis a futuras vulnerabilidades, pois a tecnologia sofre rápidas mudanças e atualizações.

É importante também para toda organização de pequeno porte saber sobre a importância da segurança da informação para o negócio, pois segundo a norma Brasileira ABNT NBR ISO/IEC 27002 (2005, p.10):

> “A Informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.”

Delegar a alguém a responsabilidade de se certificar das mais básicas técnicas de segurança da informação também é essencial para que não seja alvo de ataques em massas e tenha o seus dados e todas informações da empresa destruídos.

5 CONSIDERAÇÕES FINAIS

Com base nas configurações realizadas visando mitigar os riscos presentes no ambiente organizacional citado, percebe-se que algumas vulnerabilidades nas quais o usuário se encontra a ponto de violá-las com facilidade, foram protegidas de invasores mal-intencionados. Vulnerabilidades que, além de serem baseadas em configurações, podem, também, causar um enorme prejuízo à empresa responsável pelas informações violadas.

Este experimento atual, deixa explícito a facilidade de identificar fragilidades nas configurações padrão de instalação de um sistema operacional com a clareza das correções e sugestões aplicadas, uma vez que, não são soluções complexas e com necessidade de muita técnica. Assim, fica claro a importância da Segurança da Informação e de uma política de segurança presente, independente do porte empresarial. Uma organização sem proteção, está vulnerável a todo tipo de ataque, sendo ele por força bruta, abuso de serviços e até mesmo através de um protocolo sem qualquer criptografia de senhas ativo, mas não utilizado. É importante também ter a clareza de que não são só serviços e configurações que tornam um ambiente vulnerável, mas sim os atos e as decisões de pessoas. Escolher uma senha fraca, é pôr em risco não só os seus dados presentes em sua máquina local de trabalho, como à toda rede conectada ao seu computador.

Considerando os resultados dos testes aplicados no ambiente após algumas correções, pode-se supor que o ambiente se tornou mais seguro, mas deve ser mantido e gerenciado, com futuras atualizações para “tapar” novos buracos nos riscos existentes no ambiente empresarial. Através das soluções propostas, o esclarecimento da dúvida de proteção da informação é nítido, pois com pequenas informações, é possível gerar um interesse pelo conhecimento da segurança, e não só pelo crescimento da organização no mercado. Pode-se, também, conhecer outras ferramentas presentes e que dão suporte à Segurança da Informação, além da Hydra, que foi responsável pelo *Pentest* aplicado para descobrir senhas a partir de informações coletadas e conhecidas do ambiente empresarial citado.

Assim, para o estudo, a hipótese (c) se mostrou correta. Nessa hipótese, se afirmou que a exploração de vulnerabilidades pode acontecer com todos que se encontram desprotegidos.

Pesquisas futuras, aplicadas previamente, sobre as sugestões e configurações realizadas, podem contribuir para um ambiente mais seguro e com significativamente menor risco para a informações valiosas do ambiente empresarial. A implantação de uma política de segurança também pode ser de importante contribuição, bem como o uso de ferramentas de *Pentest* que dão apoio à Segurança da Informação no quesito invasão de vulnerabilidades.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **Tecnologia da Informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas - ABNT, 2005. 120 p.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet, versão 4.0.** 2. ed. São Paulo: Equipe do Cert.br, 2012. 126 p.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet:** Ransomware. São Paulo: Equipe do Cert.br, 2017. Disponível em: <https://cartilha.cert.br/ransomware/>. Acesso em: 02 nov. 2017.

DANTAS, Marcus Leal. **Segurança da Informação:** Uma Abordagem Focada em Gestão de Riscos. Olinda: Livro Rápido, 2011. 150 p.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa.** Porto Alegre: Universidade Federal do Rio Grande do Sul, 2009. 114 p. (Educação a Distância).

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa.** 4. ed. São Paulo: Editora Atlas S.A., 2002. 175 p.

Instituto Brasileiro de Geografia e Estatística - IBGE . **As Micro e Pequenas Empresas Comerciais e de Serviços no Brasil 2001.** Rio de Janeiro: Instituto Brasileiro de Geografia e Estatística - IBGE, 2003. 100 p.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica.** 5. ed. São Paulo: Editora Atlas S.A., 2003. 311 p.

MUNIZ, Joseph; LAKHANI, Aamir. **Web Penetration Testing with Kali Linux:** A pratical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux. Birmingham: Packt Publishing, 2013. 325 p

NOVO, Jorge Procópio da Costa. **Softwares de Segurança da Informação.** Manaus: Centro de Educação Tecnológica do Amazonas - Cetam, 2010. 115 p.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. **Segurança dos Sistemas de Informação:** Gestão Estratégica da Segurança Empresarial. Lisboa: Centro Atlantico, 2003. 256 p.