ANTONIO MENEGHETTI FACULDADE - AMF
CURSO DE SISTEMAS DE INFORMAÇÃO

SEGURANÇA DE REDES: MITIGAÇÃO E ANÁLISE DE VULNERABILIDADES

VANDERLEI DARLEI KOBS

RESTINGA SECA/RS
2017

VANDERLEI DARLEI KOBS

SEGURANÇA DE REDES: MITIGAÇÃO E ANÁLISE DE VULNERABILIDADES

Trabalho de Conclusão de Curso-Monografia, apresentado como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação, Faculdade Antonio Meneghetti-AMF.

Orientação: Profª Drª Ana Marli Bulegon

RESTINGA SECA/RS

2017

AGRADECIMENTOS

À Antonio Meneghetti Faculdade (AMF), seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior.

A minha orientadora Ana Marli Bulegon, pelo suporte, incentivos e pelo empenho dedicado à elaboração deste trabalho.

Agradeço a todos os professores por me proporcionar o conhecimento. Os seus ensinamentos foram muito além dos conteúdos do currículo, são conhecimentos para toda vida. Muito obrigado pela sua dedicação, esforço, paciência e carinho ao lecionar.

Agradeço a meus pais Sírio lírio kobs e Tarcila plate kobs, minha namorada Cristina Gonçalves e em especial a professora Josele delazeri de oliveira, pelo incentivo nas horas difíceis, de desânimo e cansaço.

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

“Na base da vida, em primeiro lugar, deve existir o trabalho, a ação e a realização”.

Professor Antonio Meneghetti

FACULDADE ANTONIO MENEGHETTI

Vanderlei Darlei Kobs

SEGURANÇA DE REDES: MITIGAÇÃO E ANÁLISE DE VULNERABILIDADES.

Trabalho de Conclusão de Curso-Monografia, apresentado como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação, Curso de Graduação em Sistemas de Informação, Faculdade Antonio Meneghetti-AMF.

Orientadora: Profª Drª Ana Marli Bulegon

Profª Drª Ana Marli Bulegon

Orientador do Trabalho de Conclusão de Curso

Antonio Meneghetti Faculdade

Prof. Esp. José Luiz Rodrigues Filho

Membro da Banca Examinadora

Antonio Meneghetti Faculdade

Profª Ms. Vanice Hentges

Membro da Banca Examinadora

Antonio Meneghetti Faculdade

Restinga Sêca, RS, 04 de dezembro de 2017.

RESUMO

Os testes de penetração nos sistemas de Tecnologia de Informação (TI) das empresas são recursos para a identificação de fragilidades de segurança; potencialmente exploráveis e componente importante de uma auditoria de segurança. Fornecer uma avaliação de segurança holística para redes constituído de centenas de hosts é dificilmente viável, embora sem algum tipo de mecanismo. Para minimizar essa dificuldade, a mitigação do sistema é uma alternativa que proporciona uma avaliação de segurança, priorizando contramedidas sujeitas a um determinado orçamento. Diante disso, este trabalho teve por objetivo verificar como os Teste de Intrusão (TIn) e a Análise de Vulnerabilidades (AV) podem contribuir para a segurança de dados de uma empresa. Para isso, realizou-se uma pesquisa exploratória-descritiva de abordagem qualitativa, com busca de dados na literatura sobre o tema segurança de redes. Os resultados dessa busca apontam que o pentest é uma possibilidade para fazer a detecção de ataques e proporcionar mais segurança das redes nas empresas.-

Palavras-chave: Pentest, vulnerabilidade, análise e mitigação

ABSTRACT

The penetration tests in the Information Technology (IT) systems of the companies are resources for the identification of security fragilities; and an important component of a security audit. Providing a holistic security assessment for networks consisting of hundreds of hosts is hardly feasible, though without some sort of mechanism. To minimize this difficulty, system mitigation is an alternative that provides a safety assessment, prioritizing countermeasures subject to a specific budget. Therefore, this work aimed to verify how Intrusion Testing (TIn) and Vulnerability Analysis (AV) can contribute to the data security of a company. For this, an exploratory-descriptive research of qualitative approach was carried out, with search of data in the literature on the topic of network security. The results of this quest point out that pentest is a possibility to do attack detection and provide more network security in companies.

Keywords: Pentest, vulnerability, analysis and mitigation

LISTA DE ABREVIATURAS

TI – Tecnologia da Informação
TIn – Teste de intrusão
AV – Análise de vulnerabilidade

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Você já tentou calcular o prejuízo de sua empresa ser invadida e seus dados serem excluídos, roubados ou divulgados na internet? Com a insegurança global que existe em constantes sites muitas empresas necessitam proteger-se e recorrem a profissionais da área de Tecnologia de Informação (TI) para este serviço. Onde falamos em ataques podem surgir vários problemas, pois a tecnologia vem crescendo. Com isso, há muitas vulnerabilidades nos sistemas de dados das empresas, pois muitas vezes pode haver falhas na elaboração de grandes sistemas feitos para suprir suas necessidades. Entretanto, muitas empresas submetem seu sistema há profissionais com conhecimento hacker[1], que irão usar ferramentas e técnicas possíveis para invadir o sistema e apontar pontos fracos e tentar corrigir as falhas antes que pessoas mal-intencionadas façam algum mal ao seu sistema. (LEPESQUEUR; OLIVEIRA, 2012).

Os profissionais de TI que fazem esse trabalho são chamados de "**Pentest".** Esses profissionais são aqueles que fazem diversos testes de vulnerabilidades realizados em uma rede ou em um sistema. Eles determinam a postura de segurança de uma empresa, identificam potenciais problemas em processos e ativos críticos de seu negócio. Com isso, a empresa poderá tomar medidas e alocar decisões de segurança baseado em situações reais de seus sistemas e processos, que posam estar infectados e muitas vezes não estarem expostos aos riscos (MACÊDO, 2012).

Se isso não for feito, muitas vezes, as empresas podem perder documentos que são importantes, ficarem lesionadas e, em última instância, irem à falência. Um exemplo disso foi o ataque com o *ransomware*[2]*,* que foi devastador onde o mundo inteiro, como mostra a Figura 1, foi alvo desse ataque. Nesse ataque muitas empresas tiveram seus dados sequestrados e algumas empresas não conseguiram sobreviver, pois eram de pequeno porte e tiveram que fechar para se prevenir de novos ataques (segurança de dados) (TANENBAUM, 2011).

---

1 Hacker: Hacker são indivíduos que modificam softwares e hardwares de computadores, desenvolvendo funcionalidades novas ou adaptando as antigas. Eles normalmente possuem um grande conhecimento sobre softwares livres, como a elaboram e linguagem Linux.

2 Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

Figura 1. Imagem representativa do ataque do ransomware.

Fonte: http://www.midiamax.com.br/sites/default/files/destaque/20170512173859_660_420.jpg

Neste sentido, questiona-se: Em que medida os Teste de Intrusão (TIn) e a Análise de Vulnerabilidades (AV) podem contribuir para a segurança de dados de sua empresa?

1.2- OBJETIVO GERAL

Verificar como os Teste de Intrusão (TIn) e a Análise de Vulnerabilidades (AV) podem contribuir para a segurança de dados de uma empresa.-

1.2.1 - OBJETIVOS ESPECÍFICOS

- Identificar os fatores de vulnerabilidade em TI.
- Analisar a viabilidade de uso dos Testes de Intrusão para a segurança dos dados de uma empresa.
- Verificar a atuação dos profissionais de TI que fazem os testes de intrusão (Pentest).
- Investigar as contribuições de testes de segurança, aplicados pelos Pentests, para a segurança desses dados.

1.3 - JUSTIFICATIVA

Em geral, as empresas só deixam para agir com relação a segurança de dados quando os problemas decorrentes de ataques e invasões já estão instaurados, não percebendo a importância de se manter uma defesa proativa. Tal defesa é baseada em testes de segurança regulares que identificam e solucionam possíveis vulnerabilidades, tornando, assim os sistemas de segurança mais confiáveis e robustos. Empresas que mantém o hábito de avaliarem sua segurança se tornam mais competitivas no mercado, mas muitas empresas cogitam essa possibilidade e não sentem a necessidade de provar se sua segurança é realmente eficaz. (MACÊDO, 2012)

Com a intenção de contribuir com as soluções para as questões de segurança de dados nas empresas, este trabalho buscou investigar as contribuições de testes de segurança, aplicados pelos Pentests para a segurança desses dados.

Para dar conta de atingir os objetivos e encontrar uma solução para o problema de pesquisa o texto a seguir apresenta a abordagem teórica que embasa o trabalho, a metodologia de pesquisa utilizada, além do cronograma e referências (TANENBAUM, 2011).

2- ABORDAGEM METODOLÓGICA

Nesta seção, apresentamos a metodologia de pesquisa utilizada. Trata-se de uma pesquisa exploratória e descritiva, com abordagem qualitativa. Fez-se uma busca de dados em livros e artigos, disponíveis na WEB, a partir do ano de 2010. A escolha dos materiais ocorreu a partir das palavras-chave "segurança de redes". A seleção dos trabalhos encontrados sobre esse tema nos levou a procurar trabalhos sobre os temas: mitigação, pentest, análise de vulnerabilidade.

A seleção desses trabalhos deu-se por afinidade com o escopo do nosso problema de pesquisa que era a segurança de redes e vulnerabilidades de sistemas.

Nos artigos selecionados, analisamos as referências bibliográficas e buscamos novas leituras sobre os temas descritos acima. A partir da análise desses materiais, realizou-se uma síntese e compôs-se o texto deste trabalho.

Optou-se por uma pesquisa exploratório-descritiva a fim de compreender melhor o que tem sido desenvolvido acerca do tema "Segurança de redes" e descrever suas características, vantagens e desvantagens, condições de ocorrência, entre outros. Neste sentido, a pesquisa teve cunho qualitativo, pois investiga os processos de segurança de redes; os equipamentos e profissionais envolvidos neste tipo de trabalho (MACÊDO, 2012).

3- INFORMAÇÕES COLETADAS

Nessa seção apresentamos os dados teóricos pesquisados e que embasaram o presente trabalho de pesquisa. Os temas apresentados referem-se à Segurança de Redes, suas ferramentas e vulnerabilidades.

3.1 - REDES

De acordo com Plinio (2011) uma rede são vários caminhos para a comunicação entre dois ou mais hosts[3], pois sua importância crescente, já que os computadores estão cada vez mais sendo usados como dispositivos da mídia do que para a computação. A Figura 2 ilustra o modelo de cabeamento de rede utilizado.

Figura 2: Modelo de cabeamento de rede

Fonte: http://codigofonte.uol.com.br

Os cabos de redes são emaranhados de fios e podem parecer caóticos, mas cada um deles tem uma função. Neste modelo de rede, os dados empacotados são recebidos e anexados ao endereço virtual (IP[4]) do computador remetente e do destinatário, onde existem camadas de

3 Host - é qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos. Essas máquinas são responsáveis por oferecer recursos, informações e serviços aos usuários ou clientes. Por essa abrangência, a palavra pode ser utilizada como designação para diversos casos que envolvam uma máquina e uma rede, desde computadores pessoais à roteadores.

4 IP - O IP (Internet Protocol) é o principal protocolo de comunicação da Internet. Ele é o responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores.

comunicação ou protocolos TCP/IP [5]que são utilizadas para garantir a integralidade dos dados que trafegam na rede. De acordo com Nakamura; Geus (2007), essas camadas são:

- Camada de vínculo de dados: a camada proporciona uma transferência de quadros de dados sem erros de um nó para outro, permitindo que as demais camadas assumam a transmissão praticamente sem erros através do vínculo.

- Camada de rede: controla a operação da sub-rede, decidindo que caminho físico os dados devem seguir com base nas condições da rede, na prioridade do serviço e em outros fatores.

- **Camada de transporte**: esta camada garante que as mensagens sejam entregues sem erros, em sequência e sem perdas ou duplicações. Ela elimina para os protocolos de camadas superiores qualquer preocupação a respeito da transferência de dados entre eles e seus pares.

- **Camada de sessão:** a camada permite o estabelecimento da sessão entre processos em execução em estações diversas.

- Camada de apresentação: está camada formata os dados a serem executados na camada de aplicativo. Ela é considerada o tradutor da rede. Essa camada pode converter dados de um formato usado pela camada de aplicativo em um formato comum na estação de envio e, em seguida, converter esse formato comum em um formato conhecido pela camada de aplicativo na estação de recepção.

- **Camada de aplicativo**: ela serve de janela, onde os processos de aplicativos e usuários podem acessar serviços de rede.

Com as redes de internet sem fio, acessos remotos e com o aumento do desenvolvimento da tecnologia, que produzem dispositivos móveis cada vez mais sofisticados, hoje em dia muitas pessoas nem se dão conta que muitas vezes estamos vulneráveis a falha de segurança. Ao acessar redes de internet em locais abertos, sem se dar conta da segurança pessoal de seus dados, estamos vulneráveis a ter nossos dados copiados sem deixar rastros. Isso implica, muitas vezes, em danos irreparáveis, pois podem estar utilizando nossos dados sem nossa autorização (NAKAMURA; GEUS, 2007).

5 TCP/IP - TCP/IP é o principal protocolo de envio e recebimento de dados MS internet.

3.1.2- SEGURANÇA DE REDES

Na área de segurança de rede consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados.

De acordo com Tanenbaum (2011) a segurança de rede é uma parte essencial para a proteção da informação, porém uma boa estratégia deve ser levada em consideração, além dos aspectos humanos e processuais de uma organização.

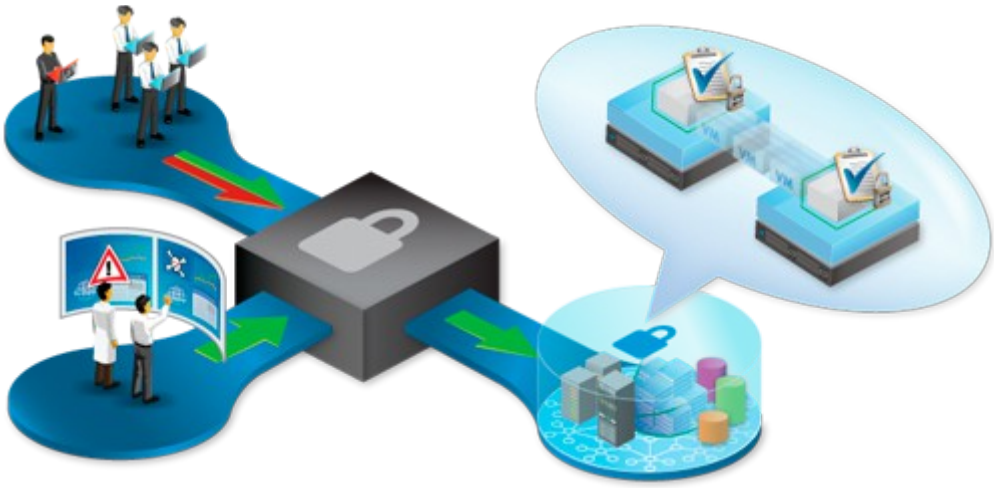
A segurança de redes, nas primeiras décadas de sua existência foram usadas principalmente por pesquisadores universitários e funcionais de empresas para compartilhar impressoras onde nestas condições não tinha muitas preocupações com a segurança. Atualmente há milhões de pessoas usando as redes e executando operações bancárias, fazendo compras na web e muitas outras coisas que envolvem a rede, porém temos que ter um cuidado com a segurança e se protegendo de pessoas mal-intencionadas que possam modificar os destinatários dos arquivos.

Os maiores problemas de segurança podem ser divididos em áreas interligadas ao sigilo, autenticação, não repudio e controle de integralidade. Algumas empresas de TI, por medida de segurança, orientam seus funcionários a não usarem seus equipamentos pessoais dentro da empresa, pois caso o equipamento esteja infectado com algum vírus este não se propague na rede da empresa. Em muitos casos as pessoas mal-intencionadas buscam informações de pessoas ligadas a empresa que possam estar vulneráveis e através deste jeito chegar ao que procura (TANENBAUM, 2011).

A fim de evitar o ataque de vírus[6], recomenda-se que as empresas tenham filtros em seus bancos de dados, ou seja, uma camada que verifica as informações e pede cerificação do conteúdo. A figura 3 ilustra como funciona este filtro da informação que são passadas ao destinatário.

6 Vírus - é um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

Figura 3: Segurança de rede



Fonte : Oesteline (http://www.oesteline.com.br)

O filtro da informação opera no sistema de entrada de rede por meio de firewall[7] que controla a entrada de conteúdos da rede ou os conteúdos acessados. Posteriormente, analisa os dados e refuta aqueles que possam danificar o sistema (MACÊDO, 2012).

3.1.3- ANÁLISE DE VULNERABILIDADES

É o processo de identificar e quantificar as vulnerabilidades existentes em um ambiente. (MACÊDO, 2012) A análise de vulnerabilidade, de acordo com Macêdo, (2012) é uma avaliação ampla sobre sua postura de segurança, indicando fraquezas e provendo os processos adequados para mitigação. O intuito dessa análise é eliminar ou reduzir a níveis aceitáveis esses riscos. Sua principal atividade é o processo de identificação de falhas e vulnerabilidades conhecidas que o expõem a ameaças. Essas falhas podem ser causadas por erros de programação, má configuração ou simplesmente falha humana (MACÊDO, 2012).

A análise de vulnerabilidade mapeia todos os sistemas que possam conter falhas e vulnerabilidades, reportando esses resultados através de um relatório conclusivo. A partir destas informações podemos tratar e mitigar as vulnerabilidades encontradas, tentando garantir maior

7 Firewall - é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, proxy de aplicações, etc. Os firewalls são geralmente associados a redes TCP/IP

segurança ao ambiente. O processo de Análise de Vulnerabilidade é suportado por diversas Ferramentas capazes de auxiliá-lo na identificação de vulnerabilidades (MACÊDO, 2012).

A análise de vulnerabilidade alimenta os sistemas sobre informações, muitas vezes desconhecidas, de sua rede com relação aos ataques de vírus que podem acontecer, com que frequência esses ataques ocorrem e quão crítica é a consequência deles, somada a um relatório técnico detalhando de quais serviços e sistemas estão sujeitos a quais tipos de ameaça. De posse dessas informações o usuário será capaz de tirar conclusões sobre seu estado atual de exposição a ameaças. Além da análise de vulnerabilidade temos a mitigação de dados.

3.1.4 - MITIGAÇÃO

A mitigação de dados consiste no ato de diminuir a intensidade de algo, fazer com que fique mais brando, calmo ou relaxado.

O processo de mitigar riscos está relacionado à priorização, avaliação e implementação dos controles de segurança recomendados na avaliação de risco. Normalmente, a estratégia selecionada para minimizar riscos leva em consideração a seguinte premissa: o controle de segurança a ser implantado deverá ser o mais adequado para conseguir reduzir o risco ao nível aceitável, com o menor custo e proporcionando o menor impacto negativo aos recursos e funcionalidades da organização. De acordo com Macêdo, (2012) o processo de mitigação de riscos pode ser tratado de seis formas, a saber:

- Assunção do risco – aceita o risco e continua a operar o sistema ou a implementar controles para manter o risco dentro de um nível aceitável.

- Evitação do risco – o risco é evitado, eliminando a sua causa ou consequência (evitar a reinicialização do servidor, usando Ctrl Alt Del).

- Limitação do risco – é realizado, implementando controles que reduzam o impacto negativo do ataque (controles de detecção).

- Planejamento de Riscos – gerencia o risco através do desenvolvimento de um plano de mitigação de risco que priorize, implemente e mantenha os controles de segurança.

- Pesquisa e Reconhecimento – visa reduzir o risco de perda do reconhecimento da vulnerabilidade ou falha, e pesquisa controles de segurança para corrigir a vulnerabilidade.

- Transferência de risco – transfere o risco, usando outras opções com o objetivo de compensar a perda (por exemplo: aquisição de seguro).

A escolha de uma dessas formas tem de levar em consideração os objetivos e as tarefas da organização. Outra questão a ser pensada para essa escolha é quais riscos serão tratados pela organização. Tratar todos eles são quase inviáveis, mas um processo de avaliação, priorizando aqueles que trarão um maior impacto negativo sobre a organização seria uma estratégia interessante para determinar que riscos devem ser tratados pela mesma. Esse processo passa por utilizar testes de segurança (MACÊDO, 2012) descritos a seguir:

3.1.5- TESTE DE SEGURANÇA

O Teste de Segurança tem como meta garantir que o funcionamento da aplicação esteja exatamente como especificado. É muito comum que as aplicações se tornem alvo de sujeitos que buscam provocar ações que possam prejudicar ou, até mesmo, beneficiar pessoas. Em função de situações como estas, o Teste de Segurança propõe demonstrar se a aplicação faz exatamente o que deve fazer ou se a aplicação não faz o que não deve ser feito. A execução do Teste de Segurança possibilita que dúvidas sobre prováveis vulnerabilidades do software sejam sanadas. Pode auxiliar também na definição de um plano de contingência, visando determinar qual precaução será tomada contra os possíveis ataques, como os de hackers ou crackers (MACÊDO, 2012).

3.1.6 - HACKER E CRACKER

Os Crackers têm a intenção de violar a segurança do computador e da rede para explorar essas mesmas falhas para seu próprio ganho **(**CHAPIN, 2016).

De acordo com Chapin (2016) Hacker é um indivíduo que usa computador, rede ou outras habilidades para superar um problema técnico. O termo hacker pode se referir a qualquer pessoa com habilidades técnicas, mas muitas vezes se refere a uma pessoa que usa suas habilidades para obter acesso não autorizado a sistemas ou redes para cometer crimes. Um hacker pode, por exemplo, roubar informações para ferir as pessoas por roubo de identidade,

danos ou derrubar sistemas e, muitas vezes, mantêm esses sistemas rejeitados para colecionar resgate. Eles são identificados por chapéus que são:

- O chapéu branco: é o Hacker que segue o lado da segurança, ele invade dentro da lei e da ética hacker. Normalmente achando uma vulnerabilidade em um sistema ou programa, ele avisa o administrador para que tal falha seja corrigida. Eles agem livremente e dão até palestras sobre segurança, e prestam consultorias a empresas, tem até empresas que contratam esses hackers para cuidar da segurança de seus sistemas e dados. Por haver ainda um certo receio entre a sociedade e a mídia com o Hacker, onde muitas vezes não se apresentam como hacker, e sim como um profissional na área de TI ou um analista e desenvolvedor de sistemas. Outros exemplos de hackers éticos são peritos e investigadores digitais. Lembrando que nem todo profissional em TI ou analista de sistemas são hackers (TACIO, 2010).

- O Hacker de chapéu preto: é aquele Hacker que não segue de nenhuma forma a ética hacker ou a lei, ele age da forma que quer para fazer o que quiser com sistemas vulneráveis, esses são os verdadeiros criminosos cibernéticos, eles usam o seu conhecimento para roubar pessoas, para invadir computadores e para destruir sistemas. As pessoas que age dentro do lado negro de, não é tido como um **Hacker** e sim como um **Cracker** (TACIO, 2010).

- Hacker de chapéu cinza: são Hackers que ficam no meio do muro, eles agem de forma legal, mas em certos casos usam justificam os seus atos que ferem a ética hacker, só que também não avisa os administradores do sistema sobre a falha e nem toma atitude para corrigi-la. É bom deixar claro que os de chapéu cinza concordando ou não com alguns pontos da lei ou da ética hacker, se agirem de forma ilícita, serão considerados criminosos e responderão por isso independente de seu ponto de vista. (TACIO, 2010).

Um dos temas de preferência dos hackers é o conhecimento da engenharia social.

3.1.7- ENGENHARIA SOCIAL

De acordo com Macêdo (2012) Engenharia Social é um termo que se refere ao processo de persuadir pessoas a realizarem determinadas ações ou fornecer informações de cunho confidencial. Do ponto de vista de segurança da informação, é definida como uma coleção de técnicas e ferramentas que podem englobar negociações, psicologia, além de técnicas para

enganar, objetivando a utilização do fator humano para burlar mecanismos de segurança de sistemas.

Engenharia social é algo presente no dia-a-dia das pessoas, podendo ser utilizada desde um *hacker* até uma criança quando faz isso para conseguir o que quer. É uma técnica amplamente utilizada durante os ataques, pois não existe "*patches* de correção para a estupidez humana", ou dizendo de outra forma, as maiores vulnerabilidades de qualquer sistema são seus próprios usuários. Por tais motivos, a engenharia social constitui uma das formas de ataque mais perigosas e bem-sucedidas na atualidade (MACÊDO, 2012; CHAPIN, 2016).

Para contrapor ao ataque dos hackers e crackers há diversos testes. Esses testes são executados por profissionais mais conhecidos por Pentest, que fazem a segurança de dados.

3.1.8 - PENTEST

Pentest são basicamente um conjunto de diversos testes de vulnerabilidades realizados em uma rede ou em um sistema, onde hackers ou crackers procuram por vulnerabilidades que lhes forneçam informações que possibilitem a realização de ataques que lhes garantam acesso ao alvo almejado (CHAPIN, 2016). Esses testes são executados por profissionais de TI, especialistas em segurança de dados na rede. Por associação, esses profissionais são chamados de Pentest.

Um Pentest simula as ações de um criminoso que visa infiltrar a infraestrutura de TI de uma empresa e roubar dados, informações sigilosas ou causar problemas derrubando o sistema. Atualmente existem diversas ferramentas e scripts que automatizam e facilitam a vida do invasor. Por isso, o profissional Pentest faz uso de ferramentas do próprio sistema operacional para realização dos testes de vulnerabilidade de um sistema operacional. Com isso, ele pode detectar as fragilidades e vulnerabilidades do sistema operacional que podem vir a ser alvos de ataques.

Dentre os testes de vulnerabilidade, utilizados pelos Pentests para prevenir a invasão de vírus no sistema de rede, temos os testes Whitebox e Blackbox como os mais utilizados (CHAPIN, 2016; MACÊDO, 2012).

O **Whitebox** é um teste realizado com o Pentest sabendo todas as informações sobre a rede como topografia, IPs, senhas, níveis de usuários e logins. Esse é o mais amplo de todos os

testes e é capaz de encontrar qualquer vulnerabilidade, porém não é muito requisitado pelas empresas por não estar muito próximo de uma situação real (CHAPIN, 2016).

O **Blackbox** é um teste mais voltado para situações reais onde o testador não terá nenhuma informação sobre o sistema, quase como um teste cego. Esse teste é muito próximo do que acontece na vida real quando um cracker tenta quebrar a segurança de uma rede e é atualmente o mais requisitado pelas empresas. As invasões "reais" são realizadas por pessoas com alto nível de conhecimento técnico, com focos específicos em determinadas instalações ou empresas.

Existe também uma categoria de profissionais que são contratados pelas empresas para testar seus próprios sistemas de segurança, essa atividade se chama de *PenTest* (*Penetration Test* ou Teste de Penetração).

Segundo Junqueira (2016) esse tipo de invasão é uma atividade coordenada e cuidadosamente planejada, que passa por diversas etapas. Essas etapas são descritas a seguir.

Etapa 1: Coleta de informações

Antes de iniciar qualquer tentativa de invasão, devemos coletar o máximo de informações a respeito da empresa atacada. Uma pesquisa no *Google*, por exemplo, pode ser um bom começo para saber o que existe de informação disponível na internet, a respeito do tema estudado/analisado ou de uma empresa, entre outros. Ainda nessa fase, considerando que se pesquise uma empresa, pode-se verificar se a empresa possui um *site* na internet, podemos coletar as informações sobre endereços de servidores DNS (*Domain Name Service* ou Serviço de Nome de Domínio), nome do responsável técnico, endereço, outros.

Toda e qualquer informação deve ser considerada para que possamos ter uma visão global e um bom nível de entendimento sobre a empresa. Nomes de sócios, diretores, funcionários e parceiros comerciais podem ser utilizados para ataques de *Engenharia Social*. A existência de filiais e coligadas pode significar a existência de conexões VPN (*Virtual Private Network* ou Rede Privada Virtual), que a princípio é uma forma segura de interconectar redes pela internet. Endereços web servem para descobrir os endereços IP por onde a rede corporativa geralmente se conecta na internet.

Etapa 2: Mapeamento do ambiente

O objetivo dessa fase é tentar descobrir a topologia da rede: quantos computadores existem e como estão interligados. Para isso, podemos iniciar com uma pesquisa nos servidores de DNS da empresa. Um servidor DNS é responsável pelo mapeamento dos nomes de domínio (ex: servidor.empresa.com) para endereços IP (ex: 200.100.200.50). Ele é naturalmente acessível pela internet para determinados tipos de consultas, entretanto, existe um recurso, chamado de *Transferência de Zona*, que serve para sincronização de registros entre servidores primários e secundários. De acordo com Chapin (2016) alguns administradores de rede permitem que esse tipo de consulta seja feito de qualquer lugar da internet, por descuido ou desconhecimento, e simplesmente fornece o "mapa da mina" para um atacante, porque esse tipo de consulta permite que se obtenha todo os nomes e endereços de todos os servidores da rede. Se esse servidor DNS também for responsável pela resolução de nomes da rede interna, pode ser que o atacante obtenha não só os endereços dos computadores acessíveis pela internet, mas simplesmente de TODOS os computadores da rede interna da empresa (CHAPIN, 2016).

Uma outra possibilidade para descobrir os computadores que existem no domínio da empresa, é através de consultas de DNS "reverso", quando informamos o endereço IP e o servidor retorna o nome da máquina que responde por aquele endereço. Sabendo o endereço de um servidor, é possível inferir a faixa de endereços possivelmente destinados à empresa e limitar a pesquisa reversa nessa faixa.

Existe inclusive uma técnica sofisticada de mapeamento, chamada de *firewalking*, que permite "enxergar" quais são as máquinas que estão por trás do firewall. Seria mais ou menos como se pudéssemos ver através das paredes (CHAPIN, 2016; JUNQUEIRA, 2016).

Etapa 3: Enumeração de serviços

Umas feitas já foram descobertas as máquinas existentes na rede, procuramos descobrir quais os serviços que estão sendo executados em cada uma delas. Um serviço não é nada mais do que um programa que fica aguardando conexões numa determinada "porta". Por exemplo, todas as conexões de páginas web são feitas para a porta de número 80. Quem responde às solicitações de conexão nessa porta é um software servidor web como por exemplo, Apache, IIS (Internet Information Service) da Microsoft ou qualquer outro software com a mesma finalidade (JUNQUEIRA, 2016).

As portas de numeração 1 à 1024 (de um total de 65.535) são padronizadas de acordo com o tipo de serviço. Assim, se encontramos a porta 22 aberta, podemos ter quase certeza que existe um serviço SSH (terminal remoto), assim como a porta 25 implicaria num serviço de e-mail. Só não podemos ter certeza sobre o serviço que está "escutando" uma determinada porta porque essas numerações são padronizadas, mas não obrigatórias. Nada impede que o administrador disponibilize um serviço SSH na porta 25, por exemplo (JUNQUEIRA, 2016).

Etapa 4: Busca por vulnerabilidades

Uma vulnerabilidade de um software é decorrente de um projeto deficiente ou erro de programação. Quando uma vulnerabilidade é descoberta por incontáveis pesquisadores (os verdadeiros *Hackers*) ao redor do mundo, o fabricante do software é notificado e a vulnerabilidade é divulgada em *sites* especializados para que todos tomem conhecimento da sua existência e tomem as providências necessárias para eliminar esse risco. Isso geralmente é atingido com a aplicação de uma *Correção* ou *Patch* (traduzindo literalmente: remendo), disponibilizado pelo fabricante do software (JUNQUEIRA, 2016).

Se o administrador da rede não aplicou as devidas correções num determinado software, pode ser que ele possa ser explorado para a invasão. Para isso, basta uma pesquisa na internet para descobrir se aquela versão de software que está sendo usada, possui alguma vulnerabilidade e como ela é explorável.

Algumas ferramentas já automatizam todo o processo de identificação dos softwares, suas versões, assim como a vulnerabilidades existentes para aquelas versões específicas, simplificando o trabalho do atacante (JUNQUEIRA, 2016).

Etapa 5: Exploração das vulnerabilidades

Essa é a etapa onde efetivamente ocorre a invasão. Dependendo do tipo de vulnerabilidade encontrada, a invasão será mais ou menos efetiva. Algumas vulnerabilidades permitem apenas a interrupção do serviço, ao qual damos o nome de ataque *DOS* (*Denial of Service* ou Negação de Serviço).

As vulnerabilidades mais perigosas são as que permitem a execução de programas e comandos no computador remoto. O *Buffer Overflow* (estouro de memória) é um exemplo de vulnerabilidade que pode permitir que o atacante obtenha acesso à uma tela de terminal remoto,

podendo executar os comandos que desejar, como se estivesse sentado diante do computador atacado e geralmente com privilégios de administrador (JUNQUEIRA, 2016).

Outro exemplo de ataque perigoso é o do tipo *SQL Injection*, feito em aplicações web mal feitas, permite desde a consulta direta à um banco de dados (onde o atacante pode obter informações sigilosas como números de cartões de crédito) à execução comando do sistema operacional. Muitos desses ataques podem ser feitos com uso de programas ou *scripts* prontos, chamados de *sploits*.

Etapa 6: Implantação de Backdoors e Rootkits

Uma vez que o invasor tenha obtido sucesso na sua investida, é comum que ele implante programas que facilitem o seu retorno. São os chamados *Backdoors*, ou literalmente "porta dos fundos". Além disso ele pode implantar os chamados *Rootkits*, que são programas que se agregam ao núcleo do sistema operacional, dificultando a sua localização (JUNQUEIRA, 2016).

Etapa 7: Eliminação de Vestígios

Toda invasão deixa rastros no computador atacado, seja nos *logs* (históricos) do sistema seja em forma de arquivos temporários. Para dificultar a identificação da sua presença, o bom atacante procura eliminar esses vestígios, requerendo uma intervenção muito mais minuciosa na investigação do incidente e muitas vezes impossibilitando rastrear sua origem (JUNQUEIRA, 2016).

3.2 - FORMAS DE PREVENÇÃO

Existe várias formas de proteção que é da nossa responsabilidade de tomar medidas preventivas necessária.

Uso de firewall, IDS e IPS: o firewall é um elemento indispensável na sua rede, para controlar e impedir os acessos indesejáveis. Hoje é simplesmente inaceitável que se tenha uma rede conectada na internet sem um firewall. O uso de *IDS* (*Intrusion Detection System* ou

Sistema de Detecção de Intrusão) e um *IPS* (*Intrusion Prevention System* ou Sistema de Prevenção de Intrusão), são elementos desejáveis para uma defesa efetiva (CHAPIN, 2016; JUNQUEIRA, 2016).

- **Serviços desnecessários**: todos os serviços que não estiverem sendo efetivamente usados, devem ser desabilitados. Além de serem itens adicionais para atualizações de segurança, são pontos adicionais em potencial para serem explorados.

- **Atualização e Configuração**: é indispensável que todos os serviços disponíveis para internet estejam com as últimas atualizações de segurança aplicadas e, principalmente, corretamente configurados. Falhas de configurações são grandes causas de incidentes de segurança.

- **Monitoração constante**: a monitoração das atividades da rede devem fazer parte da rotina diária de um administrador de redes. Só assim você poderá perceber anomalias no seu funcionamento. Deve ser incluída nessa rotina, a monitoração dos *logs*, também para detectar registros de ocorrências anormais. O uso de ferramentas que detectem modificações nos arquivos do sistema também é uma medida desejável. Uma ferramenta gratuita que pode ser utilizada para esse fim, é o *tripwire* (CHAPIN, 2016; JUNQUEIRA, 2016).

A melhor forma de defesa, entretanto, é o conhecimento. Fique sempre atualizado quanto as novas formas de ataque e vulnerabilidades descobertas para poder agir de forma proativa, antecipando-se aos movimentos dos invasores.

4- RESULTADOS E DISCUSSÕES

O Brasil é o país que mais recebe ataques cibernéticos na América Latina e ocupa a 9ª posição no mundo. Apenas em 2016, o número de ataques cibernéticos no nosso país aumentou 274% de acordo com relatório da PWC[8]. Por causa de dados alarmantes como esses, a preocupação com a segurança de dados e a confiabilidade em parceiros que agregam tecnologia em suas soluções, têm tirado o sono de muitos gestores Brasil afora.

As grandes empresas vêm sofrendo tentativas de roubo de informação ao longo dos últimos tempos e por isso estão investindo em segurança de redes de internet. Cerca de 85% dos problemas de Segurança da Informação, vem de dentro das empresas. Estas são causadas, muitas vezes, por falhas internas da estrutura das redes; por erro dos próprios funcionários, que não tem conhecimento sobre a infraestrutura da segurança das redes da empresa (MACÊDO, 2012; TANENBAUM, 2011). Àquelas empresas que não investem na segurança de redes de internet, deixam seus dados muito expostos e vulneráveis aos ataques de hackers (criminosos virtuais), que capturam os dados das empresas e pedem recompensas pelos mesmos ou os vendem para a concorrência.

Por conta disso, atualmente, as empresas tem feito grandes investimentos nas suas estruturas de rede externas e internas. Esses investimentos têm por objetivo reduzir a vulnerabilidade dos dados (são aplicados testes de Vulnerabilidade), no caso das estruturas internas, e evitar que vírus possam ser instalados nas redes, por ataques externos (Testes de Intrusão). Estes testes são aplicados por profissionais de auditoria de segurança de TI. A vantagem deste investimento é a possibilidade de ter um profissional, altamente treinamento e qualificado, testando todos os seus controles e regras de segurança.

Os testes de Vulnerabilidade (TV) detectam problemas na infraestrutura interna das redes locais da empresa, enquanto que os testes de intrusão (TIn), validam se o caminho da infraestrutura interna e a segurança das redes, que estamos tomando e assumindo na empresa, está correto e se está cumprindo a sua função que é "barrar" as tentativas de acesso indevido vindos, geralmente, do lado externo de nossa rede. Este tipo de teste pode ser executado de

8 PWC: A PWC é uma empresa que faz análise de ataques cibernético no mundo e mostrar como vem aumentando os ataques no mundo inteiro.

diversas formas, podendo ser executado totalmente do lado externo, ou também ser executado dentro da estrutura da empresa.

Os profissionais que realizam esses testes são chamados de Pentests. Porém não há uma função regulamentada dessa profissão. Eles são mais conhecidos nos Estados Unidos, Alemanha e Rússia. Por serem mais conhecidos nestes países a literatura sobre esse tema está escrita, basicamente, em inglês. Poucas publicações foram encontradas em Português sobre esse tema.

5- PROPOSTA PARA SEGURANÇA EM REDES.

Diante da pesquisa sobre o tema “Segurança em redes”, descritas nas páginas anteriores, nossa proposta de aplicação desse conhecimento seria a de realizar, antes da aquisição de um sistema operacional, os testes de conhecimento para a detecção de prováveis tentativas inesperadas de hacker, com testes e analises de segurança de seus negócios. Esses testes tem por objetivo identificar e explorar vulnerabilidades de softwares, infraestrutura de TI , segurança logica e física, antes da aquisição e uso de um sistema operacional, processos e comportamentais da organização para oferecermos recomendações de correção, mitigação e prevenção. Além disso, evitam causar impacto no negócio, onde a simulações de ataques em tempo real possam chegar em tempo real as tentativas de ataques de hacker de chapéu preto ou crackers que pretendem comprometer os ambientes de TI e aplicações, ativos tecnológicos e ambientes físicos e pessoas.

Eles devem usar ferramentas para identificar vulnerabilidades, auxiliando na avaliação de riscos em si, testando aplicações e tecnologias antes de serem adquiridas ou colocados em produção, testando e melhorando processos de segurança e aumentando o nível de conscientização e capacitação de colaboradores de sua organização. Onde temos que implantar os seguir aos seguintes passou para obtemos uma boa segurança.

1. Verificação de Segurança existente.
2. As necessidades.
3. Equipamentos de prevenção.
4. Testes de vulnerabilidades.

6- CONSIDERAÇÕES FINAIS

Ao concluirmos a busca de dados acerca de nosso problema de pesquisa, que visava investigar o tema “Segurança de Redes”, destacamos que as informações encontradas são, em geral, escritas na língua inglesa. Os textos encontrados em língua portuguesa descreviam, em sua maioria, aspectos de gestão de segurança de redes pelas empresas. O modo de fazer a segurança de redes era pouco explorado pelos autores encontrados.

Com o aumento da insegurança no tratamento de dados, cada vez estamos mais expostos a ataques cibernéticos, como aconteceu há pouco tempo em que houve um grande ataque de um *Ransoware* nas empresas. Este ataque afetou uma grande parte do mundo e grandes empresas como a Microsoft tiveram que fazer atualizações de emergências para proteger seus clientes.

Os técnicos de segurança e auditoria de segurança (Pentest) são peças fundamentais para segurança de dados sigilosos que não podem sair de dentro das empresas, pois são documento que muitas empresas fiquem competitivas.

Essa pesquisa nos mostrou que com o trabalho dos pentests e o uso de ferramentas adequadas para análise de vulnerabilidade no sistema de uma empresa pode-se evitar os ataques e roubo de informações nos sistemas de TI, evitando perdas físicas e virtuais. Infelizmente, dada a falta de informação e ao custo desse processo muitas empresas de pequeno porte não investem em segurança de Redes (CHAPIN, 2016).

7- TRABALHOS FUTUROS

Com a evolução da tecnologia onde cada dia está se aprimorando a TI, pretendo continuar estudando as fragilidades de segurança, pois a cada dia tem alguém testando jeito novo de derrubar os sistemas e testando os sistemas para achar alguma vulnerabilidade.

8- REFERÊNCIAS:

BACKES, Michael, HOFFMANN, Jörg, KÜNNEMANN, Robert, SPEICHER, Patrick, STEINMETZ, Marcel, **Simulated Penetration Testing and Mitigation Analysis**. Disponível em: https://arxiv.org/abs/1705.05088 acessado em 28/05/2017.

BERTOGLIO, Dalalana; ZORZO, Daniel , FRANCISCO, Avelino. Overview and open issues on penetration test. In.**: Journal of the Brazilian Computer Society**, 2017, Vol.23(1), pp.1-16 , Disponível em: https://journal-bcs.springeropen.com/articles/10.1186/s13173-017-0051-1 Acessado em: 22/05/2017.

BRODEUR, Vincent. **Porque o Pentest É Importante Para Sua Empresa**. Disponível em http://www.bwg.com.br/4bee-rede-social-corporativa/pentest-importante-sua-empresa/ acessado em: 23/10/2017.

CHAPIN, Doug. **Hacker Breached EAC Website Sought To Sell Passwords**, disponível em: http://editions.lib.umn.edu/electionacademy/2016/12/16/hacker-breached-eac-website-sought-to-sell-passwords/ acessado em: 15/10/2017.

JUNQUEIRA, Guilherme ; **introdução ao hacking e pentest** disponível em https://solyd.com.br/treinamentos/introducao-ao-hacking-e-pentest Acessado em: 31/10/2017.

LEPESQUEUR, Alexandre Mendes Alvim; OLIVEIRA, Ítalo Diego Rodrigues. Pentest, análise e mitigação de vulnerabilidades. 2012. XVI, 74 f., il. **Monografia** (Bacharelado em Engenharia de Redes de Comunicação) Universidade de Brasília, Brasília, 2012. Disponível em: http://bdm.unb.br Acessado em: 15 /05/2017 .

MACEDO, Diego; **Gestão de Riscos** Disponível em http://www.diegomacedo.com.br/gestao-de-riscos/ acessado em:15/10/2017.

MARTINS**,** Elaine. **O que é tcp/ip?** Disponível em https://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm acessado em:31/10/2017.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. Ed. Novatec, 2007.

PLINIO, Ventura; **O modelo OSI e suas 7 camadas** disponível em: https://imasters.com.br/artigo/882/redes-e-servidores/o-modelo-osi-e-suas-7-camadas?trace=1519021197&source=single acessado em:16/10/2017.

ROUSE Margaret; **hacker**; http://searchsecurity.techtarget.com/definition/hacker acessado em: 01/09/2017.

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

TACIO, Paulo; **Termos hacker os chapéus.** Disponível em http://www.mundodoshackers.com.br/termos-hacker-os-chapeus acessado em:25/11/2017.