CENTRO UNIVERSITÁRIO DO CERRADO PATROCÍNIO UNICERP
Graduação em Sistemas de Informação

ANDRÉ LUIZ DE LIMA

PENTEST: TÉCNICAS DE PENETRAÇÃO EM REDES *WIRELESS*

PATROCÍNIO/MG
2018

ANDRÉ LUIZ DE LIMA

PENTEST: TÉCNICAS DE PENETRAÇÃO EM REDES *WIRELESS*

Trabalho Monográfico de Conclusão de Curso apresentado como exigência parcial para obtenção do grau de bacharel em Sistemas de Informação, pelo Centro Universitário do Cerrado Patrocínio – UNICERP.

Orientador: Prof. Esp. Célio Rafael Martins Júnior

Patrocínio/MG

2018

Centro Universitário do Cerrado Patrocínio

Curso de Graduação em Sistemas de Informação

Trabalho de conclusão de curso intitulado **"Pentest: técnicas de penetração em redes Wireless"**, de autoria do graduando André Luiz de Lima, aprovado pela banca examinadora constituída pelos seguintes professores:

BANCA EXAMINADORA

Orientador Prof. Célio Rafael Martins Júnior

Instituição: UNICERP

Leonard Vieira Martins

Avaliador 1 – Prof. Leonard Vieira Martins

Instituição: UNICERP

Avaliador 2 – Prof. José Côrtes de Castro Neto

Instituição: UNICERP

Data de aprovação: 07/12/2018

Patrocínio, 07 de Dezembro de 2018

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus por até aqui me ter dado forças para as batalhas diárias que temos e por nunca ter me desamparado.

Gostaria de agradecer em especial a minha esposa Vanessa Fortunato M. de Lima, que sempre me apoiou, nos momentos em que pensei em desanimar ou desistir, ela sempre me deu forças e sempre me incentivou a continuar e a não desistir dos meus objetivos.

Aos meus pais e familiares que me deram suporte para chegar até aqui e todo apoio incondicional.

Ao meu orientador Célio Rafael por todo o suporte e dedicação para que eu conseguisse concluir e finalizar mais uma etapa em minha vida, sem ele isso não seria possível.

RESUMO

Introdução: Com o aumento exponencial das informações e a evolução tecnológica com a disseminação da internet, surgem novos processos e oportunidades de negócio, de modo consequente, novas vulnerabilidades. Infraestruturas *Wi-Fi* tornaram-se comuns em ambientes domésticos e corporativos, principalmente pelo benefício da mobilidade, mas requerendo atenção na parte de segurança evitando prejuízos e danos. Neste sentido, o teste de penetração(*pentest*) é um método eficiente para a detecção e correção de riscos e ameaças referentes a segurança da informação. Por essa razão, o trabalho trouxe como objetivo a análise sob a perspectiva teórica e prática a segurança da informação e as técnicas de teste de penetração direcionadas a sistemas de redes *Wi-Fi* **Materiais e Métodos:** Para esse fim, foi utilizada a pesquisa bibliográfica e foi executado um estudo de caso com o intuído de exemplificar os testes de penetração introduzidos em uma rede de computadores *Wi-Fi*, contribuindo de forma expressiva no desenvolvimento do trabalho. **Resultados:** Com ênfase expõe-se o pensamento crítico a respeito do gerenciamento da segurança da informação em redes *Wi-Fi*, através da execução de testes de penetração e com seus diversos benefícios que é o enfoque da presente pesquisa. E como citado acima, houve estudos de caso, artigos, livros, sites especializados, que contribuíram de forma primordial. **Conclusão:** Neste sentido o trabalho demonstra ao final que, a utilização de técnicas de *pentes*t aliado a métodos de boas práticas em relação a segurança da informação, traz inúmeros benefícios, proporcionando confiabilidade, integridade, autenticidade, e reduzindo danos e prejuízos em relação a informação.

Palavras-chave: Segurança da Informação, *Pentest*, Tecnologia.

LISTA DE FIGURAS

“Estou convencido que nem a ciência nem a tecnologia podem satisfazer as necessidades espirituais a que todas as possíveis religiões procuram atender.”

Arnold Toynbee

LISTA DE SIGLAS E ABREVIAÇÕES

DOS **-** Denial of Service, ataque de negação de serviço.

S.O – Sistema Operacional

WAN **-** Wide Área Network

LAN **–** Local Area Network

WLAN **–** Wireless LAN

PENTESTER **–** Profissional especializado em segurança ofensiva.

IEEE -Institute of Electrical and Eletronics Engineers

WI-FI **-** Wireless Fidelity, tecnologia de comunicação que não faz uso de cabos.

SUMÁRIO

1. INTRODUÇÃO

Com a crescente globalização e a expansão da Internet e da inclusão digital, a necessidade de implementação de medidas de segurança da informação tem crescido e se tornado cada vez mais expressiva. No mundo contemporâneo, o valor da informação é inestimável. Empresas, que grande parte das vezes tem o seu ramo de negócio e diferencial competitivo baseado unicamente em informações, e o próprio Governo, que contém documentos, dados e registros sigilosos, precisam adotar práticas que promovam a preservação e segurança de tais informações. Infelizmente, boa parte das empresas só deixa para agir 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.

A Internet e a Tecnologia da Informação (TI) se difundiram de forma crescente e permanente através da globalização, expansão das conexões e da inclusão digital, em corporações de todos os tamanhos e segmentos e de usuário domésticos.

Empresas de pequeno porte e usuários domésticos já desfrutam de conexões de internet via banda larga, utilizando-se de um modem para recebimento e envio do sinal da internet, podendo ser ela cabeada ou via *wireless*
, também conhecida como *wi-fi*. A rede *Wi-fi* recebe sinal da internet via cabos de redes e reenvia este mesmo sinal sem a necessidade de cabos, através de ondas de radiofrequência, similares aos que são usados em rádio comunicadores.

Nos anos 2000 aconteceu a consolidação e expansão da internet, com o surgimento da internet de banda larga, a conexão com a internet através do próprio celular via dados móveis (3g, 4g e 5g) através da popularização dos *smartphones*, o surgimento das redes sociais, entre outros (BARROS, 2013).

No mundo contemporâneo a informação tem um valor inestimável, e é em grande parte das oportunidades o diferencial de negócio da organização em um mercado tão competitivo, este bem tão precioso é manipulado, armazenado e processado através da tecnologia. A velocidade e quantidade de acontecimentos e informações internos e externos força as organizações a enfrentar novas circunstâncias no qual se exige agilidade na tomada de decisão, introduzir novos métodos e tecnologias e em alguns casos ela própria descobrir e produzir sua tecnologia.

A crescente concorrência obriga as empresas a reterem os melhores recursos, a terem capacidade de inovação. Tudo isso passa pelas informações que as empresas possuem, na técnica de extrair, captar e aplicar esses dados em conhecimento real para a empresa é de vital importância. O propósito mais simples da informação é de possibilitar o uso efetivo e ágil dos dados acessíveis, utilizando-se ao máximo dos resultados colhidos, definindo o futuro da empresa, este é bem mais precioso de uma empresa (BRUM, 2018).

O país registrou entre Abril de 2016 e Abril de 2017 cerca de 6 golpes envolvendo criminosos cibernéticos a cada segundo no Brasil, e a grande maioria dos alvos foram a pequenas empresas. Isso ocorre devido essas empresas não se preocuparem com a segurança de seus dados internos, talvez por pensarem que não há informações que os invasores queiram, por negligência ou até mesmo por pensarem que isso nunca acontecerá com sua empresa (LISBOA e RIBEIRO, 2017).

Com o que foi exposto tem-se a noção da importância da informação, é necessário e imprescindível adotar práticas que promovam a preservação e segurança de tais elementos.

Segurança da informação consiste em proteger a empresa de muitos e distintos perigos para assegurar a continuidade do negócio, reduzir a ameaça ao negócio, potencializar o retorno sobre o que foi investido e aumentar as possibilidades negócio. O analista de segurança da informação é o profissional da área de TI responsável por garantir que as empresas adotem medidas de segurança tanto tecnológicas quanto humanas, e para que os funcionários entendam e sigam as respectivas normas para que os dados estejam o mais seguro possível (DAQUINO, 2018).

Infelizmente, grande parcela das organizações só agem em relação a essa segurança da informação quando os problemas decorrentes de ataques e invasões já estão instaurados, não compreendendo a relevância e necessidade de criar e manter métodos e procedimentos proativos na segurança. Esses processos são baseados em testes de segurança regulares que identificam e solucionam possíveis vulnerabilidades, tornando, assim as redes de comunicação e os sistemas de informação mais robustos, resguardados e confiáveis, minimizando futuros danos e falhas.

Para uma maior didática será exposto um caso de teste que foi realizado em uma pequena empresa na sua rede *wi-fi* para garantir acesso interno a rede, no qual irá utilizar o S.O Kali Linux e algumas ferramentas nativas no mesmo nativamente e que são utilizadas por *Pentesters*.

2. OBJETIVOS

2.1. Geral:

Analisar sob a perspectiva teórica e prática os conceitos de segurança da informação e as técnicas de teste de penetração direcionadas a sistemas de redes *Wi-Fi*

2.2. Específicos:

- Apresentar uma revisão bibliográfica sobre os princípios básicos da segurança da informação e rede sem fio.
- Analisar tipos de ataques comuns ao tópico em questão, no caso invasão de sistemas de redes sem fios.
- Identificar as vulnerabilidades usuais nas redes sem fios de pequenas organizações.
- Descrever a estrutura, implantação e execução das técnicas de teste de invasão em redes corporativas.
- Evidenciar sobre os benefícios da implantação de testes de penetração de forma proativa nas redes de comunicação.

3. DESENVOLVIMENTO

PENTEST: TÉCNICAS DE PENETRAÇÃO EM REDES *WIRELESS*.

ANDRÉ LUIZ DE LIMA[1]

ESP. CÉLIO RAFAEL MARTINS JÚNIOR[2]

RESUMO

Introdução: Com o aumento exponencial das informações e a evolução tecnológica com a disseminação da internet, surgem novos processos e oportunidades de negócio, de modo consequente, novas vulnerabilidades. Infraestruturas *Wi-Fi* tornaram-se comuns em ambientes domésticos e corporativos, principalmente pelo benefício da mobilidade, mas requerendo atenção na parte de segurança evitando prejuízos e danos. Neste sentido, o teste de penetração(*pentest*) é um método eficiente para a detecção e correção de riscos e ameaças referentes a segurança da informação. Por essa razão, o trabalho trouxe como objetivo a análise sob a perspectiva teórica e prática a segurança da informação e as técnicas de teste de penetração direcionadas a sistemas de redes *Wi-Fi* **Materiais e Métodos:** Para esse fim, foi utilizada a pesquisa bibliográfica e foi executado um estudo de caso com o intuído de exemplificar os testes de penetração introduzidos em uma rede de computadores *Wi-Fi*, contribuindo de forma expressiva no desenvolvimento do trabalho. **Resultados:** Com ênfase expõe-se o pensamento crítico a respeito do gerenciamento da segurança da informação em redes *Wi-Fi*, através da execução de testes de penetração e com seus diversos benefícios que é o enfoque da presente pesquisa. E como citado acima, houve estudos de caso, artigos, livros, sites especializados, que contribuíram de forma primordial. **Conclusão:** Neste sentido o trabalho demonstra ao final que, a utilização de técnicas de *pentest* aliado a métodos de boas práticas em relação a segurança da informação, traz inúmeros benefícios, proporcionando confiabilidade, integridade, autenticidade, e reduzindo danos e prejuízos em relação a informação.

Palavras-chave: Segurança da Informação, *Pentest*, Tecnologia.

ABSTRACT

Introduction: With the exponential increase of information and technological evolution with the spread of the Internet, new processes and business opportunities arise, consequently, new vulnerabilities. *Wi-Fi* infrastructures have become commonplace in home and corporate environments, mainly for the benefit of mobility, but requiring attention in the security part avoiding damages and damages. In this sense, *pentest* is an efficient method for the detection

[1] Autor, Graduando em Sistemas de Informação pelo UNICERP.

[2] Professor orientador. Especialista e docente do Curso de Sistemas de Informação e outros cursos UNICERP.

and correction of information security risks and threats. For this reason, the objective of the work was to analyze the information security and penetration test techniques directed to *Wi-Fi* networks from a theoretical and practical perspective **Materials and Methods:** To this end, bibliographical research was used. a case study was carried out with the aim of exemplifying the penetration tests introduced in a network of *Wi-Fi* computers, contributing significantly to the development of the work. **Results:** The critical thinking about the management of information security in *Wi-Fi* networks, through the performance of penetration tests and its various benefits is the focus of the present research. And as mentioned above, there were case studies, articles, books, specialized websites, which contributed in a primordial way. **Conclusion:** In this sense, the work demonstrates that the use of p*entest* techniques combined with good practice methods in relation to information security brings innumerable benefits, providing reliability, integrity, authenticity, and reducing damages and losses in relation to information

Keywords: Information Security, *Pentes*t, Technology

3.1. INTRODUÇÃO

Com a multinacionalização e o aumento da inclusão digital, tem crescido a necessidade de implementar medidas de segurança. Atualmente o valor das informações são inestimáveis. Corporações, que no mercado atual tão competitivo e dinâmico, tem suas informações como diferenciais em relação aos concorrentes, necessitam adotar medidas e boas práticas no quesito segurança para que esses dados não sejam quebrados.

A consolidação da internet e sua expansão aconteceu nos anos 2000, com os vários tipos de internet, dados móveis, banda larga, internet via satélite, entre outros (BARROS, Thiago 2013).

O progressivo aumento na concorrência implica as companhias a manterem os melhores recursos, para se ter uma vantagem ao concorrente e ter a capacidade de inovar. Tudo isso é possível através das informações que as empresas possuem, por isso ter essas informações para uso eficiente e tê-los de modo acessível quando necessário, maximizando os resultados é vital (BRUM,2018).

O principal objetivo da segurança da informação é proteger a empresas das diferentes ameaças tecnológicas para garantir a continuidade do negócio, aumentar as possibilidades de negócios, minimizar as ameaças ao negócio. Com tudo isso há uma necessidade de se ter um profissional especializado nessa área que pode assegurar que a empresa e os funcionários adotem medidas esses quesitos sejam atendidos, esse profissional é o Analista de Segurança (DAQUINO, 2018).

A despeito dos vários benefícios da evolução tecnológica e com a disseminação da rede sem fio *Wi-Fi*, também crescem exponencialmente as vulnerabilidades inerentes a segurança da informação. A necessidade de avaliar o nível de segurança do ambiente das redes de comunicação de forma eficiente e eficaz ocorre com a implementação de testes de penetração simulando ataques e danos buscando vulnerabilidades, falhas e ameaças, otimizando e maximizando de forma proativa a segurança de todo o ambiente testado.

Destarte, constata-se que a pesquisa é justificada por abordar aspectos teóricos e práticos através dos estudos bibliográficos realizados em concomitâncias com teste de penetração realizados em uma rede *wireless*, utilizando o Kali Linux como sistema operacional e algumas ferramentas especificas contidas no mesmo.

3.2. MATERIAL E MÉTODOS

A elaboração deste trabalho se desenvolve através de pesquisa bibliográfica e documental de natureza exploratória, a organização da pesquisa foi realizada pelo método descritivo, com os principais estudos baseados em artigos e livros da área de segurança da informação, a fim de fundamentar a proposta idealizada pelo o autor do projeto.

O trabalho está organizado em três sessões, que se apresentam de forma sequencial na seguinte estrutura: primeiramente se realiza um estudo histórico e conceitual sobre os princípios da segurança da informação, testes de penetração, redes *wireless* e *cyber* segurança. Em um segundo momento, o trabalho apresenta os métodos, ferramentas e procedimentos utilizados no teste de penetração. E por fim, o trabalho descreve testes práticos em uma rede *wireless* de uma pequena organização, analisa os resultados e apresenta as perspectivas adotas no trabalho.

3.3. RESULTADOS E DISCUSÃO

3.3.1. Segurança da Informação

A informação é o diferencial primordial no cenário competitivo de mercado, é um recurso de vital importância nas organizações de todos os tamanhos. Justamente por esse valor carece de proteção, permeando assim a segurança da informação.

Segurança da Informação é a área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas e sua disponibilidade. (SÊMOLA, 2003)

Esses conceitos são parte integrante e garantem uma maior proteção e acesso quando necessário aos dados das corporações. A consequência do extravio ou violação de informações para as corporações é enorme e pode, em algumas situações, levá-la a falência. Existem casos em que empresas perderam seu valor de mercado na bolsa de valores devido a invasões que sofreram. (DAQUINO, 2018)

3.3.2. Redes *Wireless*

A introdução da rede de computadores em grande escala revolucionou a forma em que as pessoas e empresas se comunicam.

Desde meados da década de 60 com o surgimento da ARPANET nos Estados Unidos, passando pela década de 70 com a criação da internet tornando-se uma rede pública, com o passar dos anos o crescimento progressivo do número de computadores e acessos a rede de internet popularizam o acesso a usuários comuns e pequenas empresas a rede mundial de computadores.

Segundo Franciscatto, Cristo e Perlin(2014) incialmente as redes de comunicações eram interligadas através de cabos e divididos em quatro tipos de acordo com a extensão geográfica:

• **PAN (*Personal Area Network*) -** Rede de área pessoal formada por dispositivos muito próximos uns dos outros;

• **LAN (*Local Area Network*)** - Rede local de computadores formada por dispositivos que estão normalmente no mesmo espaço físico;

• **MAN (*Metropolian Area Network*) -** Rede de área metropolitana, corresponde a uma rede de dispositivos que compreende um espaço de média dimensão como uma região ou cidade;

• **WAN (*Wide Area Network*) -** Rede de longa distância, representa um rede de dispositivos que abrange uma grande área geográfica como um país ou até continente. (MIRANDA JEFERSON, 2014)

As redes de computadores como qualquer tecnologia evoluiram até o surgimento das redes sem fios ou *wireless* WLANs(Wirelles Local Aera Nertwork), é comumente utilizada para interligar dispositivos eletrônicos fisicamente próximos. Esta rede encerra a necessidade de cabos que interliguem os dispositivos, tem aplicações variadas pelo fato da mobilidade como característica principal. (BUSCH, 2008)

Em relação aos padrões utilizados nas redes sem fio diversos foram usados até meados da década de 90, quando o IEEE(Institute of Eletrical and Eletroinc Engineers) desenvolveu o padrão 802.11, conhecido como *Wi-Fi*(*Wireless* Fidelity ou fidelidade sem fio) o padrão mais utilizado em redes domesticas e coorporativas.

3.3.2.1. Segurança Redes *Wireless*

A evolução nos meios de transmissão de dados nos últimos anos possibilitaram o aparecimento de várias tecnologias, que a partir de então buscam atender a real necessidade de seus usuários, com a melhor qualidade possível. Nos últimos anos a comunicação *wireless* ganhou um espaço considerável nas tecnologias de transmissão de dados. Essa tendência foi ficando maior movido pelos investimentos de instituições e empresas no sentido de aplicar a transmissão sem fio em redes de computadores. Referência: Redes locais sem fio que atendem ao padrão IEEE 802.11. (UZEDA, 2012)

Por padrão as redes *wireless* utilizam o protocolo 802.11, O padrão IEEE 802.11 original possibilita a transmissão de dados numa velocidade de 1 (obrigatório) à 2Mbps (opcional), e especifica uma arquitetura comum, métodos de transmissão, e outros aspectos de transferência de dados sem fio, permitindo a interoperabilidade entre os diversos produtos WLAN (SOARES, 2010).

Atualmente com padrão 802.11g que foi disponibilizado em 2003, teve-se uma grande melhoria no quesito taxa de transmissão, hoje esse padrão consegue trabalhar com taxas até 54 Mb/s, fazendo com nos dias atuais seja o mais utilizado por sua velocidade de transmissão. Até o momento estão sendo feitos pesquisas para desenvolver a tecnologia 802.11i. (DERMATINI, 2013)

3.3.2.2. Criptografias

Por sua vez uma vez que esses padrões de transferência foram adotas, teve a necessidade de se ter uma certa segurança para acesso a essa rede, foi então que surgiram as criptografias para as redes *wireless*. Para o uso nas redes *wireless* são mais comumente utilizadas as criptografias WEP, WPA e WPA2: (MIRANDA, 2013)

- **WEP** (***Wired Equivalent Privacy)*** **-** O WEP foi criado para redes *wi-fi* e aceito como modelo de segurança *wireless* em setembro de 1999. O WEP era atribuído a disponibilizar o mesmo grau de segurança das redes cabeadas, porém, encontram-se alguns problemas de segurança relacionado a criptografia WEP e, além disso, ele é mais simples de ser quebrado. Apesar de todo o empenho que tem sido feito para aprimorar o sistema WEP, ele ainda é uma solução altamente vulnerável. Os sistemas que se baseiam deste protocolo necessitam ser atualizados ou substituídos por outros dispositivos, caso o upgrade da segurança não esteja disponível. O WEP foi oficialmente abandonado pela *Wi-Fi* Alliance em 2004.
- **WPA (*Wi-Fi Protected Access)*** **-** O WPA foi uma evolução significante sobre o WEP, porém como os itens essenciais foram feitos para que eles pudessem ser implementados através de upgrades de firmware em aparelhos habilitados para WEP, ele ainda se fundamentava em elementos vulneráveis. O WPA, assim como WEP, após ter se submetido a uma prova de conceito e aplicado a demonstrações públicas acabou, por sua vez, sendo muito vulnerável a invasões. As tentativas de invasão que representavam boa parte da ameaça para o protocolo, eram feitos indiretamente, através do sistema *Wi-Fi* Protected Setup (WPS) - sistema auxiliar desenvolvido para facilitar a conexão dos dispositivos aos pontos de acesso modernos.
- **WPA2 (*Wi-Fi Protected Access version 2)* –** O avanço mais significativo do WPA2 em comparação ao WPA foi o uso do Advanced Encryption Standard (AES) para criptografia, este podendo chegar a blocos de até 256 bits. O AES foi aprovado pelo governo dos EUA para ser utilizado como modelo para a criptografia dados confidenciais, por este motivo utilizá-lo em sua rede empresarial deverá ser suficiente para protege-la. (MIRANDA, 2013)

Além da segurança das redes *wireless* a criptografia é um dos principais itens para a segurança da rede, com ela é possível esconder dados embaralhando os seus conteúdo, que quando interceptados, sua compreensão será difícil. De tal maneira, pode se dizer que as informações não passam de forma clara e legível ao olho nu, e quando chega ao ponto final é feito o processo reverso.

Além do seu uso ser bastante comum para criptografar as conexões sem fio são comuns para conversas online, e-mails, transporte de arquivos, na compactação de dados, entre outros.

Segundo Castelló e Vaz (2012), existem 4 tipos de criptografias:

- Criptografia Hash;
- Chaves Simétricas;
- Chaves Assimétrica;
- Combinação dos Tipos:
- Cada um dos tipos de criptografia seguem uma sequência/padrão distinta pra que seu conteúdo seja embaralhado, aproveitando o que cada um tem de melhor para que as informações estejam mais protegidas possível.

Existem alguns tipos de chaves simétricas, como o DES, o IDEA, e o RC. (ALECRIM, 2009):

- DES (Data Encryption Standard): criado pela IBM em 1977, ele cifra através de substituição/transposição e recombinação e que possui 19 estágios. Faz uso de chaves de 56 bits. Primeiro ela é dividida em 64bits onde múltiplos de 8 são desprezados, ficam com apenas 54 bits acima citado. Isso corresponde a 72 quadrilhões de combinações. Em 1997, o algoritmo foi quebrado por técnicas de tentativa e erro em um desafio promovido na Internet;
- IDEA (International Data Encryption Algorithm): criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo que usa blocos fixos com 64 bits (8 bytes) e usa chaves com 128 bits (16 bytes). Sua implementação em software é mais utilizado devido a sua facilidade de uso do que a chave DES;
- RC (Ron's Code ou Rivest Cipher): criado por Ron Rivest na empresa RSA Data Security, esse algoritmo é muito utilizado em e- mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões: RC2, RC4, RC5 e RC6, cada versão difere da outra por trabalhar com chaves maiores. Esses algoritmos são mais utilizados, pois são mais seguros e rápidos do que os citados anteriormente;

As chaves de combinação, como o próprio nome sugere, faz a combinação da chave Assimétrica e da chave Simétrica. Surgiu para que fosse tirado o que cada uma tem de vantagem, eliminando a suas desvantagens. (CASTELLÓ E VAZ, 2012).

De acordo com PEDROSO (2016) *firewall* é um programa no qual a sua função é proteger o dispositivo contra acessos não autorizados, tráfego indesejado, defender serviços que estão sendo executados nas máquinas e impedir a passagem de dados que você não deseja receber.

3.3.3. Testes de Penetração

Os procedimentos de segurança da informação não garantem total eficácia e eficiência contra todos os tipos de ameaças e ataques. Adotar processos específicos em busca de vulnerabilidades e falhas é primordial para se alcançar um nível de segurança minimamente aceitável. Entre esses métodos podemos destacar o teste de penetração.

O conceito de teste de penetração ou *pentest* refere-se de um método ou procedimento com o intuito de verificar, avaliar e descobrir vulnerabilidades em uma rede ou sistema operacional. (GIVAROTO e SANTOS, 2013)

Deste modo, dentre os principais objetivos de um teste de penetração temos a melhoria da segurança física e logica, identificar vulnerabilidades e registrar possíveis ameaças em busca de maximizar a infraestrutura organizacional e pessoal do ambiente testado.

Durante o processo do teste de penetração são feitas simulações de ataques de maneira controlada tal como esses atos fossem feitos por pessoal má intencionadas tentando invadir o sistema ou ambiente testado. Levantando dados e informações pertinentes para o desenvolvimento de mecanismos de defesa, atuando na prevenção de riscos e danos aos dados do local testado.

Os testes de penetração são classificados em três tipos como caixa preta (*Black Box*), caixa branca (*White Box*) e caixa cinza(*Gray Box*).

- **Caixa preta (*Black Box*):** procedimento mais comum, que define que o profissional que executa o teste não tem qualquer conhecimento prévio da infraestrutura a ser testada, simula varreduras e possibilita a definição de estratégias para aperfeiçoamento do ambiente testado. (COUTINHO, 2011)

.

- **Caixa branca (*White Box*):** procedimento em que o profissional que executa o teste possui conhecimento prévio sobre toda a infraestrutura a ser testada: tipos de redes, diagrama de rede e IPs de rede. Simula varreduras e ataques com o sistema em estágio de produção tendo informações de estruturas como endereços, roteadores, modens, senhas de administradores e usuários do sistema.(SHAKEEL e HERIYANTO, 2011)

- **Caixa cinza (*Gray Box*):** procedimento em que o profissional que executa o teste mescla os dois tipos de teste citado acima, tendo um conhecimento parcial da infraestrutura a ser testada. (MORENO, 2014)

De acordo com Senna (2011) podemos dividir o teste de penetração em três grandes fases: Planejamento e Preparação, Reconhecimento e Execução e Conclusões. A figura 1 apresenta a abordagem de cada fase em concomitância com a documentação redigida especifica.

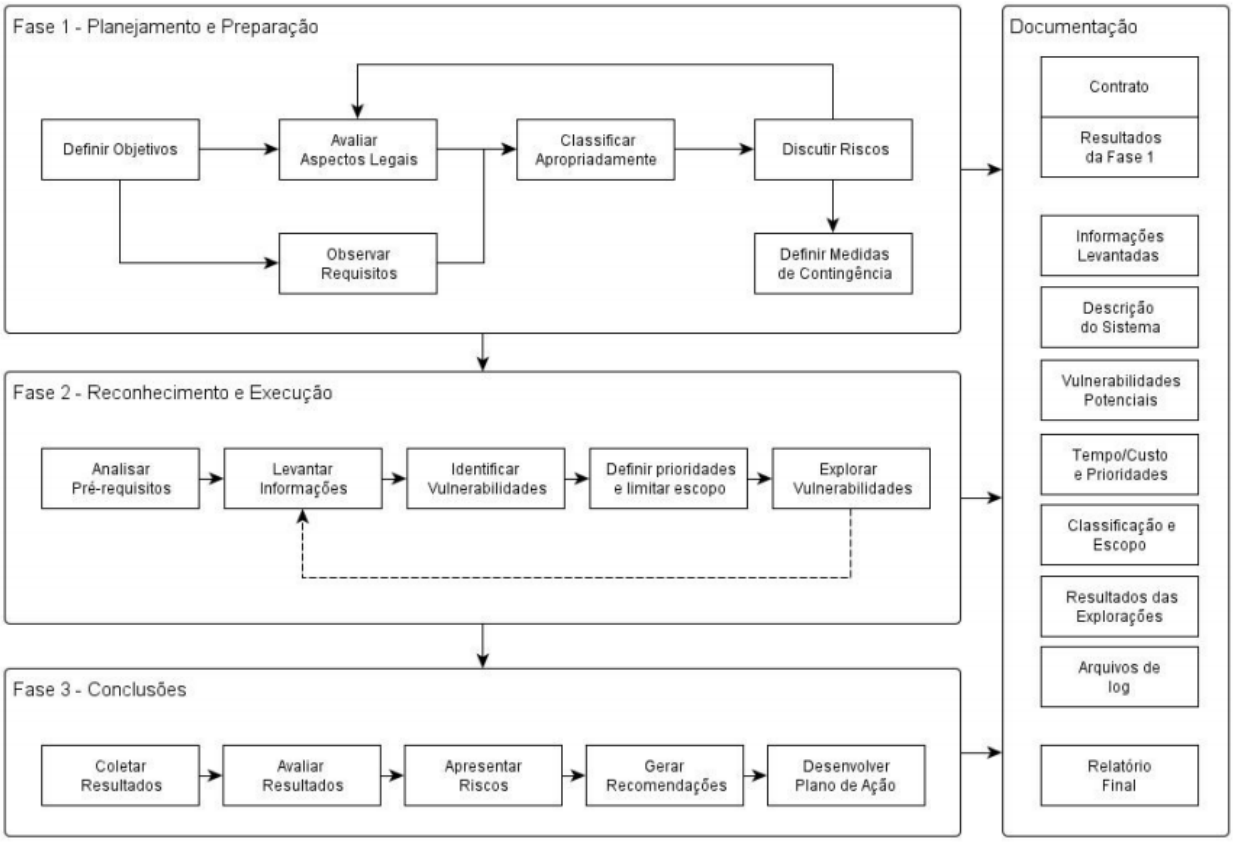

Figura 1. Fases do Teste de Penetração e o Processo de Documentação
Fonte: SENNA, 2011

Baseado na figura 1 acima podemos analisar que na fase 1 Planejamento e Preparação o escopo do teste de penetração é definido em contrato entre o prestador do teste e o cliente que o requisita, na fase 2 Reconhecimento e Execução o teste é aplicado de forma efetiva seguindo a sequência dos módulos e procedimentos e por fim a fase 3 Conclusões em que é redigido um relatório final com o detalhamento de todas as atividades, ameaças, vulnerabilidades e falhas encontradas contíguo com as recomendações e soluções para aperfeiçoamento do ambiente ou sistema testado.

3.3.4. Tipos de Ataques

Segundo Senna (2012), dentre vários tipos de ataque que existem, tem alguns que são mais comumente praticados, neste momento saber como o seu inimigo age, lhe dará uma vantagem, saber como se defender e por onde se defender,são exemplos de ataques cibernéticos: (GRIMES, 2018)

- **BruteForce –** É bastante utilizado para testes de penetração e quebras criptografias de senhas, no nosso caso de teste utilizaremos esta técnica. Ela consiste em fazer sem criar uma lista de palavras e fazer com que o programa teste essas palavras até quebrar a senha.
- **DDoS (Distributed Denial of Service)** – Este tipo de ataque tem como fim sobrecarregar a rede de uma empresa, fazendo os seus servidores ou site fiquem indisponíveis para acesso. Normalmente o hacker faz uso de bots que são computadores "zumbis" controlados por ele, e que enviam várias requisições ao mesmo tempo, fazendo com que se acabe o processamento e a memória do servidor.
- **Ransomware -** Por sua vez o *ransomware* tem o objetivo de criptografar todos os dados que os usuários possuem no seu computador, no qual somente o invasor tem a chave para desincriptar, em boa parte esse ataque acontece através de e-mail malicioso ou algum site falso.
- **Cavalo de Troia –** Esse ataque pode ser considerado o mais comum, funciona da seguinte maneira. O usuário instalar um programa ou algum *plugin* e dentro dessa instalação tem uma parte do código que tem como função ficar espionando o dispositivo ele se une ao sistema do computador, podendo assim apagar ou capturar dados, dependendo do nível de acesso do usuário até mesmo parar toda rede da empresa.

3.3.5. Tipos de Testes

Segundo Senna (2011), dentre os principais testes utilizados no *pentest* podemos destacar e citar os mais significativos e relevantes como:

• **Análise de Informações Públicas:** levantar e analisar informações preliminares sobre a organização e o ambiente a ser testado como estrutura funcional, estrutura organizacionais, estrutura de comunicações e estrutura física;

• **Identificação da Estrutura de Rede:** identificar a estrutura de rede como servidores ativos e mapeamento e monitoramento do tráfego de redes e envio e recebimentos de pacotes;

• **Varredura de portas:** identificar e analisar as portas e seus protocolos de redes e da camada de transporte normalmente utilizando o modelo TCP/IP;

• **Análise e Verificação de Vulnerabilidades:** avaliar as informações dos servidores e seus atributos, reconhecer softwares desatualizados, falhas de configuração, correções não instaladas e verificar o cumprimento das politicas de segurança da organização;

• **Testes de Aplicações e Serviços**: testar e conhecer as aplicações e serviços trabalhados pela a organização a ser testada;

• **Captura e Quebra de Senhas:** processo de obter senhas através da identificação de suas hashes podendo usar a implementação de um algoritmo de criptografia;

• **Teste de Firewall:** é recomendado o envio de pacotes de dados de uma ferramenta localizada fora do ambiente para outra ferramenta localizada dentro da rede analisando os pacotes que chegaram e os que foram bloqueados**;**

• **Teste do Sistema de Detecção de Intrusos:** verifica o desempenho do Sistema de Detecção de Intrusos(IDS-Intrusion Detection System) analisando os arquivos de log;

• **Teste de Dispositivos Sem-fio:** examinar as informações trafegadas através do espectro eletromagnético estão seguras e protegidas e seus pontos de acesso a rede;

• **Teste de Segurança Física:** analisar aspectos de segurança físicas das instalações, monitoramento, controle de acesso, perímetro, respostas a alarmes e localização;

• **Engenharia Social:** investigar informações através de funcionários e prestadores de serviço visando obter informações sigilosas sobre a empresa.

3.3.6. Vantagens e desvantagens do teste de penetração

Segundo Souza (2018) analisando a implementação e resultados do teste de penetração podemos destacar as principais vantagens e benefícios, tendo como principais:

- Colaborar com as empresas a testarem a competência de sua cibersegurança;
- Encontrar fraquezas no sistema de segurança antes que um cibercriminoso descubra;

- Possibilitar que companhias acolham novas posturas em relação à Segurança da Informação, assim como apresentar argumentos para investimentos na área;
- Proteger o nome da sua empresa, uma vez que um teste de intrusão revela o empenho em garantir a continuidade do negócio e manter uma relação efetiva com a segurança corporativa.

Mas como qualquer outro procedimento, existem algumas desvantagens e dificuldades que podem ocorrer durante o teste, sendo os principais:

- Contratar empresa que não tem boas práticas de conduta;
- O *Pentest* não ser feito da maneira deveria ser feita e comprometer a infraestrutura da empresa;
- O profissional não ser ético e capturar ou vazar informações da empresa ou não revelar totalmente toda as falhas de segurança.

3.3.7. Implementação do Teste de Penetração

Para uma maior elucidação de metodologias e ferramentas utilizadas por *Pentesters*, foi realizado um pequeno e básico caso de teste de penetração em uma rede *wireless* em uma pequena empresa, teste no qual foi efetuado com autorização prévia de seu dono.

Para os testes utilizaremos o *bruteforce* como metodologia de ataque e *aircrack*-ng, *airodump*, crunch, *aireplay-ng* e *airmon-ng* como ferramentas auxiliares para ganho de acesso ao *wireless* da empresa.

Para iniciarmos os testes foi criado um wordlist, na qual serão as palavras/números utilizados para tentar o acesso a empresa. Como demonstrado na imagem do *anexo1* foi criado uma wordlist com combinações de 8 (oito) números de 0(zero) a 9(nove).

Inicialmente utilizaremos o *airmon-ng* que serve para habilitar o modo Monitor da sua placa de rede *wireless*, após habilitado iremos escolher a rede que será alvo do ataque usando o *airodump-ng* que é utilizado para captura de pacotes.

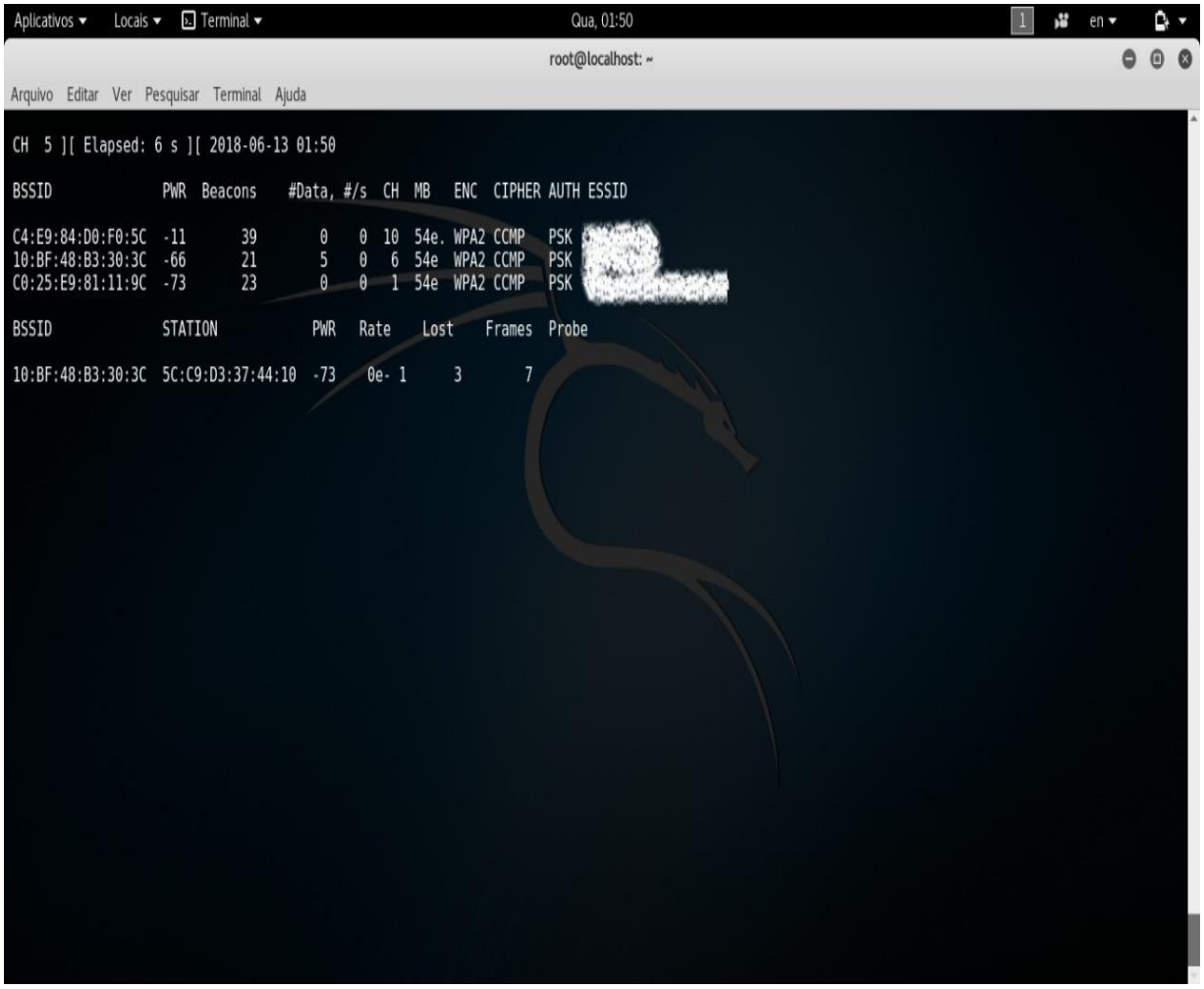

Figura 2 - Verificação de dados da rede alvo
Fonte: Elaborada pelo autor

Após ser escolhido a rede alvo iremos escolher uma uma conexão que esteja ativa nesta rede que será alvo do ataque para forçarmos a sua conexão novamente.

Após forçarmos a sua conexão na rede novamente temos a *Handshake* ou aperto de mão que é o processo pelo qual duas máquinas afirmam uma a outra que a reconheceu e está pronta para iniciar a comunicação

Chegou-se a última etapa onde utilizaremos os dados colhidos pelo *Handshake* através do *airodump-ng* e a wordlist criada no primeiro passo para tentar ganhar o acesso. Na figura 3 mostra o resultado do teste, tal como a senha e o tempo de duração do teste.

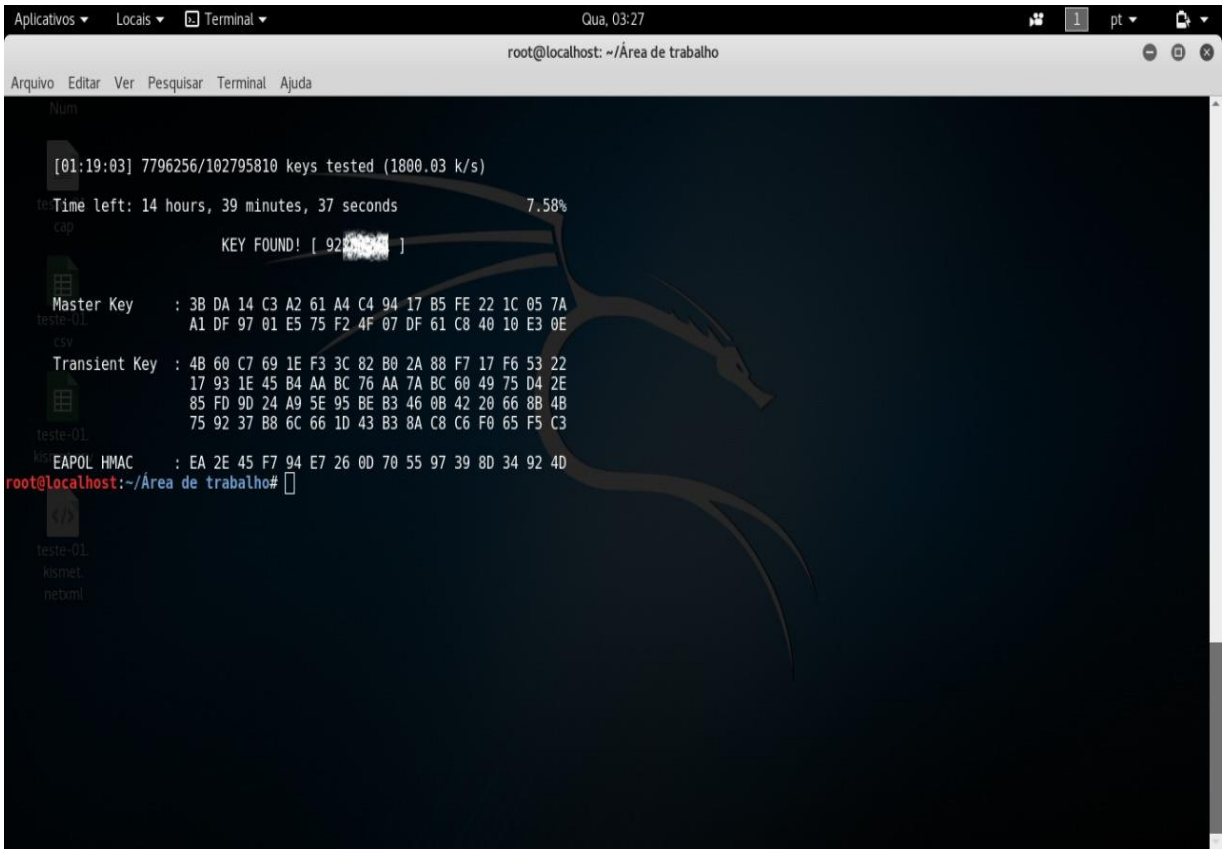

Figura 3 - Senha descoberta
Fonte: Elaborada pelo autor

Esse ataque simples poderia ser evitado se tivessem tomado alguma medidas de segurança, como por exemplo, colocado uma senha mais forte, com letras, números e caracteres especiais.

Algumas tecnologias também podem ser adotadas para a prevenção de ataques, tecnologias essas simples que podem integradas, envolvem:

- **Antivírus -** é um programa no qual o seu propósito é detectar e eliminar os vírus existentes tanto em programas na hora da sua instalação e pós-instalação quanto em arquivos infectados;
- **Filtragem de Conteúdo –** Programa que faz a filtragem de entrada e saída de dados de sua rede. Programa no qual se pode configurar o que p usuário pode ter acesso na internet e o que ele pode fazer download, fazendo com que os riscos sejam minimizados. Um exemplo é o Pfsense;

- **Detecção de Intrusão** – Como o próprio nome sugere, esse programa detecta acesso não autorizado e permite enviar notificações e gerar relatórios que podem ser analisados pela equipe de analistas de segurança. (Pinheiro, José 2007)

3.4. CONSIDERAÇÕES FINAIS.

A partir do que foi demonstrado no artigo, foi possível demonstrar importância de se fazer um teste penetração ou mesmo manter um profissional dessa área em sua empresa, pensando proteção dos seus ativos e a segurança da corporação em sim. Como podemos ver no caso de teste, um simples ataque sem muita complexidade um invasor pode ter acesso a sua rede.

Testes de invasão devem fazer parte do programa de segurança da informação das empresas. Existem maneiras diferentes de tratar a segurança de uma rede, sistema ou aplicação, e o *pentest* é somente uma das várias ferramentas e metodologias, entretanto é a que apresenta resultados com maior esclarecimento sobre as falhas de segurança, com menos índices de falsos positivos/negativos. É necessário se atentar para as auditorias preventivas, além de compreender a necessidade da percepção da exposição dos ativos de TI aos possíveis riscos.

Sendo assim, uma das qualidades fundamentais de um auditor de testes de segurança é o senso ético e moral, já que vai ter acesso a informações cruciais para a vida da organização testada. Pode-se dizer que sem uma postura ética é impossível realizar *pentest* e ser bem sucedido

Diante do que foi exposto as empresas precisam repensar no que se refere a segurança do seu bem mais valioso, que são os seus ativos. Precisam avaliar sua segurança, suas metodologias e suas ações no que se refere a sua segurança tanto interna quando externa.

3.5 REFERÊNCIAS

BERTOGLIO, Dalalana, D.; ZORZO Francisco, A. (2015). **Um Mapeamento Sistemático sobre Testes de Penetração**. - Disponível em < http://www.pucrs.br/facin-prov/wp-content/uploads/sites/19/2016/03/tr084.pdf> Acessado em 16/11/2018

CASTELLÓ, T. C.; VAZ, V. T. Assinatura Digital. 2012a. Disponível em <http://www.gta.ufrj.br/grad/07_1/ass-dig/index.html> - Acessado em 14/10/2018.

COUTINHO, J.C.P. **Processo de Testes de Vulnerabilidades em Componentes MVC para CMS** JOOMLA. Monografia – Engenharia de Sistemas, ESAB, 2011

DAQUINO, Fernando. **Profissão especialista em segurança da informação**. Disponível em<https://www.tecmundo.com.br/seguranca/5366-profissao-especialista-em-seguranca-da-informacao.htm> - Acessado em 02/11/2018

ELENARA, Geraldo. **Transmissão de dados de forma inteligente em uma rede**. Disponível em <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/413/1/CT_GESER_1_2011_11.pdf> Acessado em 0311/2018

FELIPE DEMARTINI **WEP, WPA, WPA2: o que as siglas significam para o seu WiFi**? – Disponivel em <https://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm>Acessado em 10/11/2018

FRANCISCATTO, Roberto; CRISTO, Fernando de; PERLIN, Tiago. **Redes de Computadores.2014.**Disponívelem:http://estudio01.proj.ufsm.br/cadernos/cafw/tecnico_informatica/redes_computadores>. Acessado em 22/08/2018.

GIAVAROTO, Silvio César Roxo. SANTOS, Gerson Raimundo dos. **Backtratrack Linux: auditoria e teste de invasão em redes de computadores**. Rio de Janeiro, Ciência Moderna Ltda., (2013).

GRIMES**,** Roger A. **Tipos de ataques cibernéticos e como detectar cada um deles** https://computerworld.com.br/2018/07/25/8-tipos-de-ataques-ciberneticos-e-como-detectar-cada-um-deles. Acessado em 18/11/2018

LISBOA, D; RIBEIRO V. **64% dos ataques de hackers miram pequenas empresa**. Disponível em<https://pme.estadao.com.br/noticias/pme,65-dos-ataques-de-hackers-miram-pequenas-empresas-diz-estudo,70001746157,0.htm> Acessado em 13/10/2018

MIRANDA, Jeferson Luiz Ferreira- **SEGURANÇA EM REDES SEM FIO** (2013)http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2412/1/CT_GESER_IV_2014_03.pdf

MORENO, D. **Tipos de *PenTest***. Disponível em: < http://www.100security.com.br/tipos-de-*pentes*t/ >. Acessado em: 18 outrubro de 2018

RASMUSSE, Bruna. **LAN,WAN,WLAN, PAN: conheça os principais tipos de redes**. Disponível em <https://canaltech.com.br/infra/lan-wlan-man-wan-pan-conheca-os-principais-tipos-de-redes//> Acessado em 03/11/2018

SÊMOLA, Marcos**. Gestão da Segurança da Informação**: Uma visão Executiva. Rio de Janeiro: Campus, 2003

SENNA, Vinícius; MAIA Delgado. **Estudos de Teste de Penetração**. Rio de Janeiro. 2011. Disponível em: <http://www.defesacibernetica.ime.eb.br/pub/repositorio/2011-Senna_Macambira.pdf>. Acesso em: 28 de agosto de 2018

SHAKEEL, Ali; HERIYANTO Tedi. **Backtrack 4: GARANTINDO SEGURANÇA PELO TESTE DE INVASÃO**. Packt Publishing, 2011.

SOARES ,Rafael. Auditoria Teste de Invasão(*Pentest*) – **Planejamento, Preparação e Execução** –Disponível em <https://seginfo.com.br/2010/09/07/auditoria-teste-de-invasaopentest-planejamento-preparacao-e-execucao-2/> Acessado em 15/10/2018

SOUZA, Állison 2018 -***Pentest*: o que é e quais são os principais tipos?** Disponivel em https://ostec.blog/geral/pentest-conceito-tipos

UZEDA, Luis Guilherme Garcia https://www.gta.ufrj.br/grad/01_2/802-mac/index.html

4. CONSIDERAÇÕES FINAIS / CONCLUSÃO

A partir do que foi demonstrado no artigo, foi possível demonstrar importância de se fazer um teste penetração ou mesmo manter um profissional dessa área em sua empresa, pensando proteção dos seus ativos e a segurança da corporação em sim. Como podemos ver no caso de teste, um simples ataque sem muita complexidade um invasor pode ter acesso a sua rede.

Testes de invasão devem fazer parte do programa de segurança da informação das empresas. Existem maneiras diferentes de tratar a segurança de uma rede, sistema ou aplicação, e o *pentest* é somente uma das várias ferramentas e metodologias, entretanto é a que apresenta resultados com maior esclarecimento sobre as falhas de segurança, com menos índices de falsos positivos/negativos. É necessário olhar com outros olhos para as auditorias preventivas, além de compreender a necessidade da percepção da exposição dos ativos de TI aos possíveis riscos

Diante do que foi exposto as empresas precisam repensar no que se refere a segurança do seu bem mais valioso, que são os seus ativos. Precisam avaliar sua segurança, suas metodologias e suas ações no que se refere a sua segurança tanto interna quando externa.

5. REFERÊNCIAS

BARROS, Thiago. **Internet completa 44 anos – Relembre a história**. Disponível em <http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html> - Acessado em 25/05/2018

BERTOGLIO, Dalalana, D.; ZORZO Francisco, A. (2015). **Um Mapeamento Sistemático sobre Testes de Penetração**. - Disponível em < http://www.pucrs.br/facin-prov/wp-content/uploads/sites/19/2016/03/tr084.pdf> Acessado em 16/11/2018

CASTELLÓ, T. C.; VAZ, V. T. Assinatura Digital. 2012a. Disponível em <http://www.gta.ufrj.br/grad/07_1/ass-dig/index.html> - Acessado em 14/10/2018.

COUTINHO, J.C.P. **Processo de Testes de Vulnerabilidades em Componentes MVC para CMS** JOOMLA. Monografia – Engenharia de Sistemas, ESAB, 2011

D. LISBOA; V. RIBEIRO. **64% dos ataques de hackers miram pequenas empresa**. Disponível em<https://pme.estadao.com.br/noticias/pme,65-dos-ataques-de-hackers-miram-pequenas-empresas-diz-estudo,70001746157,0.htm> Acessado dia 13/10/2018

DAQUINO, Fernando. **Profissão especialista em segurança da informação**. Disponível em<https://www.tecmundo.com.br/seguranca/5366-profissao-especialista-em-seguranca-da-informacao.htm> - Acessado em 02/11/2018

ELENARA, Geraldo. **Transmissão de dados de forma inteligente em uma rede**. Disponível em <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/413/1/CT_GESER_1_2011_11.pdf> Acessado em 0311/2018

FELIPE DEMARTINI **WEP, WPA, WPA2: o que as siglas significam para o seu *WiFi*?** – Disponivel em <https://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm>Acessado em 10/11/2018

FRANCISCATTO, Roberto; CRISTO, Fernando de; PERLIN, Tiago. **Redes de Computadores.2014.**Disponívelem:http://estudio01.proj.ufsm.br/cadernos/cafw/tecnico_informatica/redes_computadores>. Acessado em 22/08/2018.

GIAVAROTO, Silvio César Roxo. SANTOS, Gerson Raimundo dos. **Backtratrack Linux: auditoria e teste de invasão em redes de computadores**. Rio de Janeiro, Ciência Moderna Ltda., (2013).

GRIMES**,** Roger A. **Tipos de ataques cibernéticos e como detectar cada um deles** https://computerworld.com.br/2018/07/25/8-tipos-de-ataques-ciberneticos-e-como-detectar-cada-um-deles. Acessado em 18/11/2018

MIRANDA, Jeferson Luiz Ferreira- **SEGURANÇA EM REDES SEM FIO** (2013)http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2412/1/CT_GESER_IV_2014_03.pdf

MORENO, D. **Tipos de *PenTest***. Disponível em: < http://www.100security.com.br/tipos-de-*pentes*t/ >. Acessado em: 18 outrubro de 2018

RASMUSSE, Bruna. **LAN, WAN, WLAN, PAN: conheça os principais tipos de redes**. Disponível em <https://canaltech.com.br/infra/lan-wlan-man-wan-pan-conheca-os-principais-tipos-de-redes//> Acessado em 03/11/2018

SÊMOLA, Marcos**. Gestão da Segurança da Informação**: Uma visão Executiva. Rio de Janeiro: Campus, 2003

SENNA, Vinícius; MAIA Delgado. **Estudos de Teste de Penetração**. Rio de Janeiro. 2011. Disponível em: <http://www.defesacibernetica.ime.eb.br/pub/repositorio/2011-Senna_Macambira.pdf>. Acesso em: 28 de agosto de 2018

SHAKEEL, Ali; HERIYANTO Tedi. **Backtrack 4: GARANTINDO SEGURANÇA PELO TESTE DE INVASÃO**. Packt Publishing, 2011.

SOARES,Rafael. Auditoria Teste de Invasão(*Pentest*) – **Planejamento, Preparação e Execução** –Disponível em <https://seginfo.com.br/2010/09/07/auditoria-teste-de-invasaopentest-planejamento-preparacao-e-execucao-2/> Acessado em 15/10/2018

SOUZA, Állison 2018 -***Pentest*: o que é e quais são os principais tipos?** Disponivel em https://ostec.blog/geral/pentest-conceito-tipos

UZEDA, Luis Guilherme Garcia https://www.gta.ufrj.br/grad/01_2/802-mac/index.html