SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO

ANDRÉIA ALVES DOS SANTOS

ANÁLISE DE VULNERABILIDADE EM REDE, COM TESTE DE INTRUSÃO, UTILIZANDO A DISTRIBUIÇÃO *KALI LINUX*

PETROLINA/PE

2015

SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO

ANDRÉIA ALVES DOS SANTOS

ANÁLISE DE VULNERABILIDADE EM REDE, COM TESTE DE INTRUSÃO, UTILIZANDO A DISTRIBUIÇÃO *KALI LINUX*

Monografia apresentada à banca avaliadora do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - *Campus* Petrolina como exigência final para conclusão do curso de Licenciatura em Computação.

Orientador: Fábio Cristiano de Oliveira.

PETROLINA/PE

2015

ANDRÉIA ALVES DOS SANTOS

ANÁLISE DE VULNERABILIDADE EM REDE, COM TESTE DE INTRUSÃO, UTILIZANDO A DISTRIBUIÇÃO *KALI LINUX*

Trabalho de conclusão de curso submetido ao Colegiado de Computação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - *Campus* Petrolina como parte dos requisitos necessários para obtenção do grau de Licenciada em Licenciatura Plena em Computação.

Aprovado em:___/___/_____.

BANCA EXAMINADORA

_____

Professor Mestre Fábio Cristiano

Instituto Federal de Educação Ciência e Tecnologia do Sertão Pernambucano

Orientador

_____

Professor Mestre Laécio Araújo Costa

Instituto Federal de Educação Ciência e Tecnologia do Sertão Pernambucano

_____

Professor Especialista Ubirajara Santos Nogueira

Instituto Federal de Educação Ciência e Tecnologia do Sertão Pernambucano

Dedico este trabalho aos meus pais que foram e
São meu alicerce nessa caminhada.

AGRADECIMENTOS

Quero começar meus agradecimentos rendendo a Deus toda honra e glória para sempre. Se não fosse por cada oportunidade que Ele me concedeu todos os dias de estar viva e poder lutar mais uma batalha e vencer, eu não estaria aqui. Reconheço que sem Ele eu não sou nada e nada posso fazer. Bendito seja o Senhor Jesus para sempre!

Agradeço aos meus pais, Maria da Glória e José de Arimatea, meu alicerce. Sem vocês não teria conseguido chegar até aqui. Obrigada por seu amor incondicional, por terem investido em minha vida, mas acima de tudo por não desistirem de mim. Amo muito vocês!

Agradeço aos meus irmãos Filipe e Gabriela por fazerem parte da minha vida e história. Vocês contribuíram muito em minha formação. A minha amiga que se tornou minha irmã mais velha, Aline Bezerra, pelas palavras de encorajamento e por me impulsionar a seguir em frente. Anália que me ajudou muito compartilhando seus conhecimentos durante a minha caminhada acadêmica.

Não posso esquecer-me do meu orientador professor mestre Fábio Cristiano que com paciência me suportou durante toda a execução deste trabalho, suas orientações me fizeram chegar até aqui! Aos meus professores do curso de Licenciatura em Computação, em especial as professoras Danielle Martins e Josilene Brito que através do PIBID me mostraram o quão lindo é ser docente. Meus sogros Aureliano e Marciana que abriram as portas de sua casa para que por um período de tempo eu pudesse descansar e retornar aos estudos.

Enfim, por último mas não menos importante, quero agradecer ao meu noivo amado, Leandro que com muita paciência me tratou quando eu só tinha olhos para este projeto ou para as atividades acadêmicas. Meus sinceros sentimentos de gratidão por cada palavra, por cada empurrão para que eu não desistisse, por cada reclamação quando eu estava desanimada, por cada gesto de carinho quando eu me sentia cansada, por me sustentar em oração. Amo muito você!

Obrigada a todos que contribuíram para que eu me tornasse uma profissional de excelência!

“Se você conhece o inimigo e a si mesmo, não
Precisa temer o resultado de cem batalhas. Se você se
Conhece, mas não o inimigo, para cada vitória sofrerá
Uma derrota. Se você não conhece o inimigo nem a você
Mesmo, perderá todas as batalhas.”
Sun Tzu

RESUMO

As informações são o bem mais precioso em qualquer tipo de organização, por isso, sabe-se que a necessidade de mantê-las protegidas é de suma importância para um bom andamento e sucesso da empresa. Com o advento dos avanços tecnológicos na área de Segurança da Informação (tanto na defesa como no ataque), manter suas informações seguras se tornou um fator que necessita de grandes recursos (sejam humanos ou ferramentas tecnológicas). Contudo, são por meio destes mesmos instrumentos que pessoas mal intencionadas podem chegar a obter o ativo mais importante para a instituição, suas informações. Diante disto, este trabalho visa mostrar como a distribuição *Kali Linux*, software de código livre, utilizado para testes de intrusão e auditoria, pode auxiliar empresas de pequeno e médio porte na segurança de seus ativos, verificando se seus dados estão seguros ou não em suas redes de comunicações. Para alcançar tal objetivo realizou-se um experimento utilizando sistemas operacionais virtuais, simulando uma invasão na estação de trabalho para demostrar eficiência do *Kali Linux* em testes de intrusão e auditoria dentro de um sistema de rede de computadores. Portanto foram colhidos resultados bem peculiares nos testes realizados, gerando resultados diferenciados bem satisfatórios.

Palavras-chaves: Testes de Intrusão; *Kali Linux*; Auditoria; Segurança da Informação;

ABSTRACT

The information is the most valuable asset in any organization, so it is known that the need to keep them protected is of paramount importance for a smooth running and success of the company. With the advent of technological advances in the field of Information Security (both in defense and attack), keep your information secure has become a factor that requires large resources (whether human or technological tools). However, it is through these same tools that bad guys can get to get the most important asset for the institution, its information. In view of this, this paper shows how the Kali Linux distribution, open source software, used for intrusion and audit tests, can help small and medium sized companies in the safety of their assets, making sure that your data is safe or not their communication networks. To achieve this goal held up an experiment using virtual operating systems, simulating an invasion on the workstation to demonstrate Kali Linux efficiency of intrusion and audit tests within a computer network system. So very peculiar results in the tests were collected, generating well differentiated satisfactory results.

Keywords: Penetration Testing; Kali Linux; Audit; Information Security;

LISTAS DE FIGURAS

LISTAS DE TABELA

SUMÁRIO

CAPÍTULO I – Introdução

1.1 Apresentação

A segurança da informação tem sido fator de grande importância e preocupação para as empresas, principalmente para as equipes de Tecnologia da Informação ou TI, responsáveis pelo bom andamento do sistema utilizado na organização. Os profissionais precisam estar sempre um passo à frente de pessoas com intenções maldosas que desejam invadir o sistema e coletar informações que lhes tragam algum retorno favorável, isto é, seus adversários (BORGES, 2011).

Sem dúvidas, a internet é a maior rede de compartilhamentos e facilita a comunicação entre pessoas, bem como de organizações. A necessidade de compartilhamento de dados através da internet para filiais ou servidores locais, exige um cuidado maior, principalmente quando se trata de um ativo tão importante para a organização, como dados comerciais e financeiros por exemplo. No entanto, tais cuidados só são postos em prática quando a ameaça de vulnerabilidade no sistema já se tornou uma realidade.

Portais governamentais brasileiros como, por exemplo, o da Presidência da República, Ministério do Esporte, e o sitio da Universidade de Brasília (UnB) foram invadidos por hackers e retirados do ar. No dia 18 de junho de 2011 o grupo Fatal Error Crew invadiu o site do Exército Brasileiro coletando dados confidenciais tais como, nome, cpf e e-mail de aproximadamente mil militares (COSTA, 2011). De acordo com Coleman (2010), "Os hackers são pessoas que possuem conhecimentos avançados em informática". Estes são os responsáveis pelas invasões em sistemas virtuais causando danos às empresas, provando que um bom programa antimalware[1] e um firewall[2] não são considerados suficientes para sanar o problema. Diante desse contexto, alguns conceitos para melhor entendimento são citados:

[1] **Antimalware** é todo o programa de segurança que combate pragas digitais como vírus, spam, rootkits, etc (MORAES, 2011).

[2] ***Firewalls*** podem ser definidos como pontos de conexão entre duas redes não confiáveis que permitem que a comunicação entre elas seja monitorada e segura (GONÇALVES, 1997).

- **Ameaça:** qualquer circunstância ou evento com o potencial intencional ou acidental de explorar uma vulnerabilidade específica em qualquer sistema computacional, resultando na perda de confidencialidade, integridade ou disponibilidade (KIOSKEIA, 2015).
- **Ataque:** é a exploração de uma falha de um sistema informático (KIOSKERA, 2015).
- **Vulnerabilidade:** É uma condição de risco, falha existente no sistema que, ao ser explorado pode trazer danos à organização (KIOSKEIA, 2015).

Perante os fatos que foram apresentados, torna-se imprescindível o uso de técnicas que possibilitem Testes de Intrusão nos sistemas das empresas que desejam aumentar a segurança das informações. Estes são responsáveis por detectar as vulnerabilidades do sistema, contribuindo para sua segurança e consequentemente auxiliando na diminuição de perdas financeiras e de ativos importantes para a empresa, impedindo a quebra de confiança nos sistemas e processos (BORGES, 2011).

Assim, ressalta-se a importância da aplicação dos Testes de Intrusão a fim de garantir maior segurança na transação de informações evitando perdas e danos, através de auditoria.

Segundo a ISO/IEC 17799:2005, que “estabelece diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização, esses testes também podem garantir a funcionalidade dos três aspectos fundamentais que regem a segurança de um sistema” e que são descritos a seguir:

- **Integridade** assegura que os dados não possam ser alterados por usuários não autorizados;
- **Confidencialidade** é a propriedade de que a informação não esteja disponível, ou seja, revelada a indivíduos, entidades ou processos não autorizados, sendo assim, é a garantia de que as informações não possam ser acessadas por usuários não autorizados;

- **Disponibilidade** é a propriedade de estar acessível e utilizável, sob demanda, por uma entidade autorizada, ou seja, garante que os recursos estejam disponíveis aos usuários autorizados.

Existem técnicas e ferramentas de software que auxiliam na segurança de rede. Estes contribuem no auxílio a medidas futuras que podem tornar um sistema mais seguro contra ataques e invasões, possibilitando maior segurança e menos vulnerabilidade no sistema, permitindo a qualificação do problema diante da importância da mesma para a organização. A norma aponta como uma boa prática a realização de testes de intrusão ao menos uma vez por ano (ISO/IEC 17799:2005).

Nesse contexto, surge a motivação em buscar alternativas apropriadas com técnicas e ferramentas de software que possam favorecer as empresas de pequeno porte, na detecção de intrusão e que ao mesmo tempo possuam baixo custo.

As ferramentas de software podem ser baseadas em licenças de proprietário e livre. Esta última apresenta vantagem competitiva uma vez que, além de ser um utilitário gratuito, oferece, em suma, os mesmos serviços que um software proprietário. As ferramentas proprietárias como, por exemplo, o *WebInspect*[3] que permite "testar os aplicativos da Web desde o desenvolvimento até a produção, gerenciando com eficiência os resultados dos testes e distribuindo informações de segurança em sua organização", e WPA Cracker[4] que permite a quebra de senhas online bem como a quebra de criptografia de documentos; estes são produtos que possuem algum custo financeiro em sua aquisição, em contrapartida ferramentas como Netfilter[5] que filtra o conteúdo na rede com o objetivo de gerar segurança na mesma. Outro exemplo a ser citado é o *Kali Linux*[6] que oferece muitas outras opções de Testes de Intrusão e Auditoria, tais como quebra de senhas e escaneamentos no sistema. O Netfilter assim como o *Kali Linux* pode ser adquirido gratuitamente.

Desta forma, esse trabalho analisará como a distribuição *Kali Linux* pode ser utilizada a favor de pequenas e médias empresas a fim de verificar a eficiência da

[3]**WebInspect:** http://www8.hp.com/br/pt/software-solutions/software.html?

[4]**WPA Cracker:** https://www.cloudcracker.com/

[5]**Netfilter:** http://www.netfilter.com.br/

[6]**Kali Linux:** http://www.kali.org/

ferramenta para a realização de testes de intrusão com baixo custo, através de um experimento. De acordo com Nakamura (2003), os softwares de varreduras de vulnerabilidades fazem vários tipos de testes, buscando encontrar brechas e furos de segurança nos sistemas e serviços da rede corporativa.

1.2 Objetivos:

1.2.1Objetivo Geral

Avaliar como a distribuição *Kali Linux* pode contribuir na segurança em rede, em empresas de pequeno e médio porte, com baixo custo, verificando sua eficiência na busca por vulnerabilidades no sistema.

1.2.2 Objetivos Específicos:

- Identificar testes de intrusão disponíveis no *Kali Linux*;
- Investigar a eficiência do *Kali Linux* enquanto sistema de intrusão;
- Definir um cenário de Teste de Intrusão para empresas de pequeno porte.

1.3 Metodologia

Para a execução deste trabalho, foi realizado uma simulação de um Teste de Intrusão onde duas máquinas virtuais, inicialmente, são interligadas entre si. Essas máquinas são Windows XP e a distribuição livre *Kali Linux*. As mesmas estão sendo utilizadas dentro do software denominado de Virtual Box[7] que, permite instalar e executar diferentes sistemas operacionais de uma única vez.

Antes de partir para a fase da experiência propriamente dita, é importante levantar alguns conhecimentos referentes ao sistema que será utilizado para estudo, tais como seu funcionamento, recursos que oferece para atender as necessidades de Testes de Intrusão e Auditoria, bem como o sistema de rede de computadores da empresa a qual se deseja realizar o teste a fim de *Kali Linux* atingir os objetivos propostos para este trabalho.

[7]**Virtual Box:**https://www.virtualbox.org/.

Após a instalação dessas máquinas, parte-se para o processo de pesquisa, aqui será utilizada a pesquisa exploratória que, segundo Kauark (2010), tem como objetivo possuir “maior familiaridade com o problema, tornando-o explícito, ou construindo hipóteses.” Diante disso, é levantado um estudo sobre o sistema operacional a ser utilizado, *Kali Linux*, e como ele pode auxiliar empresas de pequeno e médio porte, com baixo custo, a manter seus sistemas seguros de vulnerabilidades. São observados os tipos de testes que o sistema oferece e qual deles é mais conveniente ser utilizado durante a execução deste trabalho.

É importante ressaltar que, o Teste de Intrusão demonstrado aqui é realizado por um profissional de Tecnologia da Informação que se encontra dentro da empresa, ou seja, é utilizado máquinas na mesma faixa de endereço IP.

Feito isso, é descrito os resultados, conclusões obtidas no decorrer do experimento.

1.4 Estrutura do Trabalho

O primeiro capítulo consistiu na introdução do trabalho onde foram relatados alguns conceitos breves do que será visto no decorrer deste projeto. Os demais capítulos serão descritos a seguir.

- **Capítulo 2:** Será apresentada a Revisão da Literatura, onde alguns conceitos importantes para a compreensão deste trabalho serão descritos. São eles: software livre, testes de intrusão bem como seus tipos e as metodologias utilizadas para a realização desses testes. Também serão definidas algumas concepções de vulnerabilidade finalizando com a explicação da distribuição *Kali Linux*.
- **Capítulo 3:** Será descrito uma análise de competidores mostrando ao final a relação positiva e negativa, das três ferramentas mais utilizadas em testes de intrusão e auditoria de segurança.
- **Capítulo 4:** Será descrito a metodologia utilizada para a investigação deste estudo. Ocorrerá a preparação do laboratório de testes para a realização dos experimentos utilizando o *Kali Linux*.
- **Capítulo 5:** Após a realização do experimento proposto, neste capítulo é exposto os resultados obtidos e as discussões dos dados analisados durante a atividade descrita no capítulo anterior.

- **Capítulo 6:** após a realização de toda a proposta transcrita neste trabalho, esta última seção consistirá das conclusões obtidas a partir dos resultados.

CAPÍTULO II – Referencial Teórico

O crescente avanço da tecnologia e consequentemente a sua utilização alteram as formas de comunicação entre organizações e indivíduos, causando alterações no elenco social e gerando dependências quanto ao uso dessas tecnologias e os dados neles veiculados.

Diante disso, alguns conceitos serão esclarecidos neste capítulo, a fim de trazer uma melhor compreensão no que é proposto para este trabalho.

2.1 Software Livre

De acordo com Iwata “o movimento do software livre surge como um processo de compartilhamento do conhecimento” (IWATA, 2009). Diferente dos sistemas proprietários como o Windows, por exemplo, o *free software* ou *software* livre é um sistema OSS (*Open Source Software*), isto é, de código e aberto, que pode ser copiado, modificado e redistribuído sem custo para qualquer usuário. Esse tipo de programa surgiu na década de 60 com a primeira versão do *Unix*, utilizado para fins acadêmicos, nos primeiros computadores denominados mainframes. A partir daí, foram desenvolvidas novas versões do Unix e posteriormente outros programas também de código aberto.

Em 1984 surge o Projeto GNU[8], hoje chamado de *GNU/Linux*, uma versão similar ao Unix, criado pela *Free Software Foundation*. Por se tratar de um sistema livre, o seu desenvolvimento é realizado por voluntários não pagos. Qualquer indivíduo com conhecimentos em computação, em especial na área de programação, pode contribuir para a expansão do sistema.

O software precisa possuir quatro tipos de liberdade para ser considerado livre. São eles:

1. A liberdade de executar o programa que quiser para qualquer propósito.
2. A liberdade de estudar como o programa funciona, e adaptá-lo às suas necessidades. Acesso ao código-fonte é um pré-requisito para isso.
3. A liberdade de redistribuir cópias para ajudar os outros

[8]*GNU* vem do inglês *General Public License*, no português quer dizer Licença Pública Geral. É um sistema operacional que é software livre, ou seja, respeita a liberdade dos usuários. (gnu.org)

4. A liberdade de melhorar o programa e publicar restaurado, de modo que toda a comunidade tenha os benefícios. O acesso ao código-fonte é um pré-requisito para esta liberdade;

É importante ressaltar que, software livre não pode ser confundido com software de código aberto, uma vez que, o software pode possuir código aberto, mas não atender as liberdades citadas acima. Assim, todo e qualquer software considerado livre terá que possuir seu código fonte aberto a fim de garantir seu estudo e aperfeiçoamento, mas nem todo software de código aberto será livre (FALCÃO, 1997).

Diante disso, algumas empresas de grande e médio porte estão migrando de softwares proprietários para sistemas livres, uma vez que diminuem os gastos e encontram alternativas para suprir as necessidades de sua organização. Dentre estas alternativas, encontram-se os programas que auxiliam nos testes de intrusão responsáveis por verificar as vulnerabilidades em um sistema de rede. Este tema será descrito a diante.

2.2 Teste de Intrusão

Como já citado acima, testes de intrusão permitem verificar vulnerabilidades em sistemas eletrônicos. Segundo Soares (2014): a finalidades dos testes de intrusão é verificar a resistência de redes, sistemas ou aplicações em relação aos atuais métodos de ataque.

Com o objetivo de encontrar esses erros o profissional, chamado de *Pentester*, precisa analisar com precisão as informações para ter um teste de intrusão bem-sucedido. Grande parte dessas informações pode ser coletada na Internet em sites de busca e mídias sociais (BROAD, 2014).

Um teste de intrusão para ser bem sucedido, precisa percorrer algumas etapas que serão á descritas a seguir.

- **Planejamento e Preparação:** É levantado todo material necessário para a realização dos testes, tais como: detalhes da infraestrutura contemplada, equipamentos e recursos financeiros bem como os tipos de ataques que serão utilizados na invasão.

Toda organização que se submete a esses testes para avaliarem o nível de segurança de seus sistemas, assinam um termo de confidencialidade que garantem o sigilo das informações acessadas pelos analistas de sistemas durante a execução dos testes. Prazos também são estabelecidos para efetivar os testes e para resolve problemas que, por ventura venham a aparecer. Nesta fase também é escolhido o tipo de teste que será realizado, isto dependerá da quantidade de informações que o analista poderá ter acesso (SOARES, 2014).

- **Avaliação:** Nesta fase são utilizadas técnicas que possibilitam avaliar de que maneira o sistema pode ser invadido com maior facilidade. Aqui se iniciam os testes que são divididos em fases. Estes são descritos a seguir.

    - **Obtenção de Informação:** Algumas informações referentes à empresa precisam ser coletadas. Estes dados podem ser pesquisadas em diversos tipos de sites de buscas na Internet, bem como outras fontes. Uma pesquisa detalhada sobre o funcionamento da empresa ajuda, a saber, quanto de informação existe espalhado na rede, ajudando a modelar os ataques e determinar quais áreas podem ser explorados mais facilmente.

      Analistas buscam informações também sobre servidores de DNS (*Domain Name Service*), quando as organizações possuem sites em funcionamento na internet. Buscam CNPJ, nome do técnico responsável, endereço, etc. Utilizam-se de Engenharia Social, que segundo Cipoli (2014), “é a habilidade de conseguir acesso a informações confidenciais ou a áreas importantes de uma instituição através de habilidades de persuasão” e também de *Dumpster Diving*[9] em suas buscas.
    - **Sondagem e Mapeamento:** Nessa fase objetiva-se descobrir a topologia de rede, quantos computadores existem e como estão

[9]Consiste na busca por informações contidas em lixos corporativos como documentos impressos descartados sem cuidados.

interligados entre si. Existe também uma técnica denominada de *firewalking*, que possibilita identificar outras máquinas interligadas ao sistema que não pertencem à empresa. Outras etapas também se destacam. São elas:

- Identificação de hosts ativos;
- Portas e serviços abertos;
- Mapeamento da rede;
- Identificação de sistemas operacionais;
- Identificação de rotas.

- **Identificação de Vulnerabilidades:** identificação das vulnerabilidades é o próximo passo após mapeamento da rede. Em cada serviço oferecido é analisado qual deles oferece algum tipo de risco de invasão. Após ter conhecimento de cada vulnerabilidade e documentá-las, as mesmas são enumeradas e classificadas quanto ao impacto que elas podem causar dentro da organização.

- **Exploração:** A exploração é a fase em que são liberados os ataques no sistema. Tal ação tem como objetivo obter acesso não autorizado através das vulnerabilidades encontradas, alcançando o maior nível de privilégios possível. Segundo Soares (2010), busca-se para cada vulnerabilidade detectada:
  - Encontrar ou desenvolver código/ferramenta para prova de conceito (é recomendado que tais provas sejam testadas em ambiente controlado, principalmente se forem desenvolvidas por terceiros);
  - Confirmar ou refutar a existência de vulnerabilidades;
  - Documentar o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;
  - Obter acesso e, se possível, escalar privilégios.

- **Documentação e Relatório:** O objetivo principal é manter de forma transparente os registros de todas as etapas realizadas nos testes de intrusão. Informações importantes como escopo do projeto, ferramentas utilizadas, datas e horas dos testes, lista de todas as vulnerabilidades identificadas e

exploradas, assim como recomendações para execução de melhorias devem conter nos relatórios, a fim de orientar a empresa na melhor solução para combater os riscos em seus sistemas organizacionais. Assim, reforça-se mais uma vez o que diz a norma que “estabelece diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização”, ISO/IEC 17799:2005, é importante realizar ao menos uma vez por ano os testes de intrusão nos sistemas de rede das empresas, uma vez que isso possibilitará a proteção de suas informações e perdas irrefutáveis para os negócios. Existem três tipos de Testes de Intrusão: *BlackBox, GrayBox e WhiteBox*. Estes serão definidos mais adiante.

2.3 Vulnerabilidades

Muitos e diferentes são os caminhos que podem ser utilizados pelos adversários para invadir um sistema de uma organização. Cada vulnerabilidade é uma fraqueza e permite que o invasor obtenha informações de determinado sistema.

Segundo a *Modulo Security Solution* as vulnerabilidades podem ser causadas por:

- ***Erros de programação*** – Grande parte das vulnerabilidades surge do erro de tamanho do buffer, uma região da memória reservada para escrita e leitura dos dados.
- ***Configuração* Inadequada** – Aplicativos de segurança como o firewall, devem ser corretamente configurados, ou podem ser brechas para ataques maliciosos.
- ***Falha humana*** – Execução de arquivos maliciosos manualmente.

Portanto, as vulnerabilidades "são os portais através dos quais ameaças são reveladas" (UMRAO, 2012). Diante dessas ameaças, algumas empresas têm optado por invadir seus próprios sistemas a fim de encontrar pontos vulneráveis, constatando soluções para a problemática.

Diante disso, organizações buscam testes de intrusão que permite encontrar nos processos, nos recursos e nos sistemas dos negócios, “portais” que, podem se tornar ameaças, pondo em risco o ativo mais importante da empresa, a informação.

2.4 Tipos de Testes de Intrusão

Três são os tipos de testes de invasão que podem ser utilizados para encontrar vulnerabilidades no sistema. São eles: BlackBox (Caixa Preta), GryBox (Caixa Cinza) e WhiteBox (Caixa Branca). Estes são conceituados abaixo (TESTE DE INVASÃO, 2014).

- **BlackBox:** a característica principal deste tipo de teste é ser as cegas. Não é preciso conhecimento prévio do ambiente de TI ou de credenciais de acesso a sistemas e aplicações. Apenas o endereço de domínio que deverá ser avaliado será informado ao pentester. Este tipo é o mais solicitado porque simula a ação de um harcker, que tenta invadir o sistema da empresa sem nenhuma informação prévia, buscando dados que possam ser usados de forma prejudicial à organização.
- **GrayBox:** este tipo serve para descobrir se existe incoerência nas permissões de acesso. O pentester entrará como funcionário da empresa para avaliar esses riscos, ou seja, identificar se as permissões de acesso e autorização de transações estão em conformidade com a especificação ou necessidade do negócio.
- **WhiteBox:** nesse tipo de teste o pentester recebe todas as informações, tais como topologia de rede, o domínio que deverá ser testado bem como credenciais de acesso a sistemas e aplicações.

Para auxiliar nos testes de intrusão, existem alguns programas proprietários e livres, como já citado no capítulo anterior, que realizam esses processos encontrando vulnerabilidade assessorando no combate aos riscos.

Neste trabalho será focado a utilização do sistema livre *Kali Linux*.

2.5 Kali Linux

Com o constante avanço da tecnologia algumas medidas vêm sendo tomadas a fim de garantir a segurança na rede de computadores. Empresas de pequeno, médio e principalmente grande porte tem procurado investir em sistemas que lhe

tragam segurança no armazenamento e compartilhamento de seus dados, que para elas são considerados ativos de grande importância para seus negócios.

Dentre as medidas executadas para este fim, está a utilização de softwares que possibilitam realizar testes de intrusão no sistema, a fim de encontrar vulnerabilidades que tragam algum risco para a organização. Diante dos sistemas operacionais que se encontram no mercado, está o *Kali Linux*, uma distribuição Linux que realiza testes de intrusão e auditoria de segurança. Para alcançar esse objetivo, o usuário deve estar logado como administrador do sistema. Pode-se considerar como uma versão avançada da distribuição BackTrack Linux, também utilizado para o mesmo fim.

Depois de algumas mudanças em sua infraestrutura, o *Kali Linux* passou a ter mais de 300 ferramentas de testes de intrusão, além de, ser totalmente gratuito para o consumidor e *Open Source*, ou seja, possui seu código fonte aberto para ver e modificar, a fim de ser melhorado e estudado por indivíduos que possuam algum conhecimento em programação.

Dentre as 300 ferramentas pode-se destacar:

- ***Metasploit***
    - metasploitcommunity / pro
    - metasploitdiagnostic logs
    - metasploitdiagnosticshell
    - metasploit framework
    - updatemetasploit

O *metasploit* permite verificar o nível de segurança nos computadores existentes em determinada rede possibilitando o ataque às vulnerabilidades existentes.

- ***Network Exploitation***
    - Armitrage
    - exploit6
    - ikat
    - jboss-autopwn-linux
    - jboss-autopwn-win
    - termineter

O *network exploitation* permite a infiltração em sistemas de rede a fim de coletar dados que não estão visíveis ao público geral. Permite a exploração de computadores individuais e redes de computadores externas.

Por ser um programa de segurança Linux, o Kali foi criado para ser compatível com o *File System Hierarchy Standard*[10], onde os usuários do sistema poderão encontrar tranquilamente arquivos, pacotes, e outros. Com isso, o sistema oferece um ambiente seguro quanto ao seu desenvolvimento. Os desenvolvedores responsáveis utilizam-se de protocolos seguros para fazerem interação com os repositórios.

Dentre outros múltiplos fatores que existem para incentivar o uso do *Kali Linux*, está o fato dele possuir versão em vários idiomas, os seja, possui não apenas no inglês, mas em português, espanhol e muitas outras línguas. Também é totalmente personalizável, onde permite que o usuário tenha total liberdade de personalizar o software como queira. A utilização do *Kali Linux* é recomendada para pessoas que já possuam algum conhecimento do sistema operacional Linux, uma vez que o Kali adere padrões do sistema Debian.

Para realizar as atualizações não é preciso reinstalar o software, apenas digitar alguns comandos no terminal Linux para aderir às novas propostas. Além disso, é permitido criar uma versão USB da distribuição *Kali Linux* e utilizá-lo através do mesmo, podendo assegurá-la através da criptografia.

[10] Padrão utilizado para sistemas hierárquicos. Define os principais diretórios, bem como seu conteúdo nos sistemas operacionais Unix.

CAPÍTULO III - TIPOS DE SISTEMAS DE INTRUSÃO

Neste capítulo será descrito a análise de competidores com o levantamento de alguns sistemas que realizam diferentes tipos de testes de intrusão. Estes determinam o nível de segurança em um sistema. Portanto, serão classificados de acordo com sua respectiva função.

3.1 Footprinting e Fingerprinting:

Sistemas que realizam este tipo de atividade buscam informações a fim de criar um perfil detalhado do alvo que deve ser atacado.

3.1.1 Nmap:

Utilizado para exploração e segurança em rede, mostra aos usuários os sistemas operacionais disponíveis em rede bem como os serviços que oferecem, como tipo de filtros de pacotes ou firewalls que estão sendo utilizados, além de dezenas de outros recursos. Os sistemas de firewall que existem hoje são avançados e por isso restringem o acesso a redes externas. Utilizando o Nmap camufla-se o endereço IP tentando assim confundir o firewall. Pode ser utilizado em forma textual, através de um terminal de comandos ou de forma gráfica denominada de Zenmap(figura 1) (NMAP.ORG).

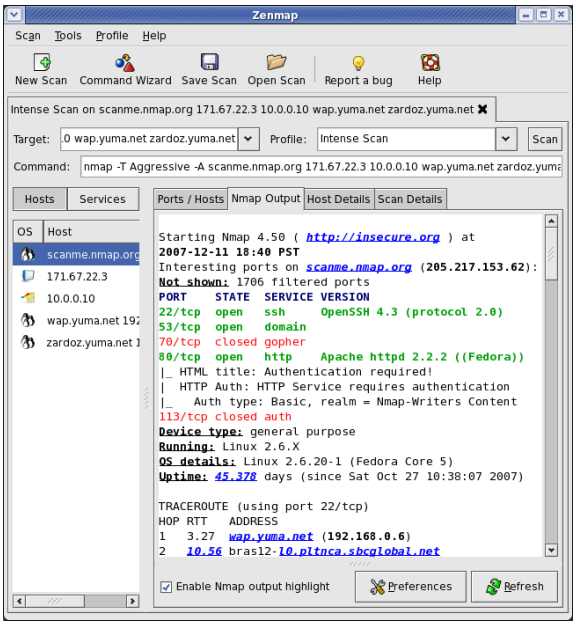

Figura 1Tela do Zenmap

Fonte site oficial nmap.org

3.1.2 Anubis

É uma ferramenta de código aberto, utilizado para criptografar e assinar *emails* que saem, como também na descriptografia automática de *emails* que chegam. Permite que os administradores configurem uma infraestrutura PGP *(Pretty Good Privacy)* centralizada. Concebido para anexar às ferramentas necessárias para os processos de auditorias de segurança e testes de intrusão dedicados a encontrar informações, denominado *Footprinting* que levanta informações detalhadas sobre o alvo e *Fingerprinting* encontra a oportunidade de invasão através de uma informação fundamental coletada (HAISCHT, 2006).

3.1.3 FOCA (Fingerprinting Organizations with Collected Archives):

Utilizado principalmente para encontrar através de varreduras, dados ocultos e informações constantes. Essas informações podem se encontrar em páginas da internet e podem ser baixados e analisados pelo Foca. Possui a capacidade de analisar grandes quantidades de documentos que são pesquisados no *google* por exemplo. Faz também uma análise completa das informações descoberto através da URL é conduzida até mesmo antes de baixar o arquivo. Com as informações extraídas, Foca busca fazer o levantamento de quais equipes e quais servidores e clientes pode ser inferida a partir deles (ELEVEN PATHS).

3.2 Exploits (Exploração de Vulnerabilidades)

Os exploits tem a finalidade de explorar as vulnerabilidades encontradas durante as varreduras nos sistemas de rede.

3.2.1 WinAUTOPWN

Uma das poucas ferramentas criadas para o Windows funcionando também em Linux e *Apple MAC* OSX. A WinAUTOPWN é considerada uma das melhores ferramentas de testes de intrusão para Windows e seus vários tipos de testes podem

ser realizados em url de forma automática, em hosts e redes. Utiliza a exploração de vulnerabilidades para conduzir a execução remota de comando. Contém um banco de dados enorme de *Shell* Carregar Vulnerabilidade, inclusão remota de arquivos remotos e execução de comandos, exploits e é atualizado quase todos os dias.

WinAUTOPWN explora *Framework* sem pedir nenhuma informação complementar além do mínimo de detalhes sobre o seu destino. Pode ser utilizado tanto para ataques “cegos”, ou seja, onde não há informações sobre o invasor, como para invasões onde todas as informações necessárias já são conhecidas (GENERAL SECURITY, 2011).

3.2.2 Metasploit

Uma das ferramentas mais populares já utilizadas para testes de intrusão e mais úteis para os profissionais de Tecnologia da Informação (TI). *Metasploit* realiza testes 45% mais rápido que outras ferramentas de forma mais eficiente, acelerando tarefas comuns, como a descoberta, exploração e relatórios, fornecem métodos de evasão avançada e pós-exploração e gerencia de forma eficiente as vastas quantidades de dados gerados em grandes avaliações. Essa ferramenta também ajuda a profissionais que estão iniciando em testes de intrusão por se tratar de uma ferramenta simples (METASPLOIT).

3.2.3 Exploit-DB - Base de dados de exploits

Recurso utilizado por profissionais de TI, pesquisadores de vulnerabilidades entre outros. Tem o objetivo de servir como a mais completa coleção de *exploits* recolhidos através de apresentações diretas, ordenando em listas de discussão apresentando-os em um banco de dados livremente disponível e de fácil navegação. Realiza explorações remotas, locais, em aplicações web entre outras atividades. Está disponível para *Windows, Linux* e *Mac*. É um repositório para *exploits* e prova-de-conceitos em vez de avisos, tornando-se um recurso valioso para aqueles que precisam de dados acionáveis imediatamente. (EXPLOIT DATABASE).

3.3Sniffers

Responsável por analisar os protocolos de rede que são coletados durante o tráfego.

3.3.1 Wireshark

É um analisador de pacotes de rede que mostra os dados o mais detalhado possível (SHARP,2014).É um analisador de protocolo para *Windows* e *Mac*, que permite a captura e navegação interativamente no tráfego de uma rede de computadores em tempo real. Além de verificar os pacotes transmitidos pelos dispositivos de comunicação, como placa de rede, placa de fax modem, entre outros, do aparelho. Comumente utilizado por administradores de rede para detectar problemas, conexões suspeitas, auxiliar no desenvolvimento de aplicativos e inúmeras outras atividades relacionadas. Criado sob a licença *GNU General Public License*, também é chamado de *Sniffer* (ou farejador, em português).

O aplicativo tem interface agradável facilitando seu entendimento, é multi plataforma, funcionando nos Sistemas operacionais *Windows*, *Mac* OS X e nas distribuições *Linux* entre outros, porem, é um pouco difícil de instalar e não tem uma rede suporte formal.

3.3.2 Tshark

Analisa os protocolos de rede. Permite a captura de dados por pacotes a partir de uma rede, ou ler os pacotes a partir de um arquivo de captura salvo anteriormente, imprimindo uma forma decodificada desses pacotes para a saída padrão ou escrevendo os pacotes em um arquivo. O formato de arquivo de captura nativa *tshark 's* é *pcap*, que também é o formato usado pelo *tcpdump* e várias outras ferramentas.

É capaz de detectar, ler e escrever os mesmos arquivos de captura que são suportados pelo *Wiresha*rk. Sem qualquer conjunto de opções, *tshark* vai funcionar muito como *tcpdump*. Ele vai usar a biblioteca *pcap* para capturar o tráfego a partir da primeira interface de rede disponível e exibe uma linha de resumo para cada pacote recebido (TSHARK).

3.4 Distribuições de Linux orientadas a auditoria

São sistemas operacionais Linux utilizados para auxiliar em testes de intrusão e auditoria com a finalidade de encontrar vulnerabilidades no sistema.

3.4.1 Helix3

Permite a visibilidade em toda a infraestrutura de rede revelando atividades maliciosas, tais como o abuso de Internet e compartilhamento de dados. Também permite isolar e responder a incidentes ou ameaças de forma rápida e sem detecção do usuário por meio de uma ferramenta de administração central. Permite detectar rapidamente, identificar, analisar vulnerabilidades preenchendo relatório dando-lhe os elementos de prova para revelar a verdade e proteger o seu sistema.

Helix3 é controlada através de uma interface gráfica de fácil manuseio e que funciona com qualquer sistema operacional. É tão fácil que exige o mínimo de experiência. É de fácil implementação (E-EFENSE).

3.4.2 Caine (Computer Aided INvestigative Environment)

É uma distribuição GNU / Linux italiano de código aberto. CAINE oferece um ambiente completo que é organizado para integrar ferramentas de software existentes como módulos de software e para fornecer uma interface gráfica amigável além de ferramentas de fácil utilização. Foi criado a partir do Ubuntu (CAINE).

Após descrever algumas ferramentas utilizadas para buscas de vulnerabilidades e testes de intrusão, segue-se uma tabela com as vantagens e desvantagens das três ferramentas mais utilizadas.

Ferramentas	Pontos Negativos	Pontos Positivos
Nmap	Nem todos os sistemas seguem a RFC 793; não conseguem diferenciar portas abertas de alguns tipos de portas filtradas,	Podem bisbilhotar através de alguns firewalls não orientados à conexão e de roteadores que filtram pacotes; esses tipos de scan são um pouco mais camuflados do que o scan SYN;

	deixando você com a resposta aberta.	
Metasploit	Não encontrado	É o único caminho de acesso com suporte para a maioria dos recursos no Metasploit; Fornece uma interface baseada em console para o quadro; Contém a maioria dos recursos e é a mais estável interface MSF; Suporte completo readline, tabulação e conclusão de comando.
Wireshark	O programa pode ser usado de forma maliciosa para obter informações não autorizadas; Ainda não é um programa simples que pode ser usado por qualquer pessoa.	É um software livre, captura e observa as mensagens que estão sendo enviadas/recebidas pelo seu computador; Captura de pacotes de dados em tempo real; Mostra os dados dos pacotes de forma detalhada.

Tabela 1. Pós e Contras de Competidores

CAPÍTULO IV – Experimento / Preparação do Laboratório de Teste

A distribuição *Kali Linux* oferece algumas alternativas que auxiliam nos testes de intrusão e auditoria. Dentre estes, pode-se citar o xHydra ou Hidra-GTK que é uma ótima opção quando se trata em quebra de senhas online, pois trabalha de forma gráfica, não apresentando muitas dificuldades em sua utilização. Em contra partida, o Medusa que ataca de forma bruta para ter acesso remoto através da descoberta também de senhas do sistema atacado. Este não se utiliza de interface gráfica, mas ainda assim desenvolve seu papel de forma satisfatória.

Uma outra opção é o *Metasploit*, uma ferramenta de intrusão muito utilizada para testes de segurança. Foi desenvolvido por HD Moore, especialista em segurança, e lançada em 2003 (GIAVAROTO, 2013). Quando se trata de acesso a sistemas, Metasploit ainda é uma das opções mais utilizadas para este fim, pois é capaz de realizar simples scans até uma invasão completa em sistemas operacionais ou em programas que façam parte do alvo, explorando suas vulnerabilidades.

A fim de trazer entendimento sobre alguns comandos que são descritos aqui, torna-se relevante mencionar alguns conceitos, tais como:

- ***Exploit:*** objetiva explorar vulnerabilidades através de códigos de programação em sistemas computacionais.
- ***Payload:*** é o que permite a abertura de comunicação entre o atacante e o alvo.

O Metasploit possui uma interface gráfica recentemente implementada denominada de Armitage, possibilitando um caminho mais amigável para que o usuário possa atacar seu alvo (GIAVAROTO, 2013). Neste trabalho será utilizado o Metasploit, porém não será utilizado o armitage. O experimento será realizado no terminal do *Kali Linux* de forma textual, o MSFCONSOLE. Isto não implicará na eficiência do Metasploit.

4.1 Descrição do teste de intrusão

Para este teste de intrusão, o cenário utilizado foram duas máquinas interligadas entre si através de uma rede local, aqui simbolizando a rede da empresa.

Uma máquina hospedando o sistema operacional Windows XP, e outra com a distribuição *Kali Linux* que detectará as vulnerabilidades existentes no sistema. É importante relembrar que os sistemas operacionais Windows XP e *Kali Linux* estão sendo executados no VirtualBox.

Os endereços IPs utilizados foram:

- KaliLinnux:
  - Eth0: 192.168.0.110
- Windows XP:
  - Eth0: 192.168.0.103

Levando em consideração que as informações prévias do sistema já são conhecidas, pois a proposta é que a empresa invada seu próprio sistema a fim de verificar o quanto ele está vulnerável. O tipo de teste utilizado foi o White Box ou Caixa Branca. Este teste é considerado um teste simples, pois o objetivo deste trabalho é verificar como o software *Kali Linux* pode auxiliar empresas de pequeno e médio porte a manterem seus sistemas livres de vulnerabilidades ou menos acessível a ataques.

O metasploit oferece algumas opções de como invadir determinado sistema, dentre elas está à alternativa de criar um executável e enviar ao usuário por algum meio de comunicação como e-mail, por exemplo, ou ainda através de engenharia social, conseguindo informações sobre o sistema que possam ser uteis para a invasão.

Diante disso, descreve-se a seguir as etapas do teste de intrusão.

4.2 Passo a passo do Teste de Intrusão

Antes de iniciar o Teste de Intrusão utiliza-se o terminal do *Kali Linux* para fazer um escaneamento na rede interna, utilizando *NMAP*[11], a fim de encontrar vulnerabilidades conhecidas para que possam ser exploradas. Isto é demonstrado

[11] O Nmap ("*Network Mapper*") é uma ferramenta de código aberto desenhado para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. (Guia de Referência do Nmap. Disponível em: <http://nmap.org/man/pt_BR/index.html#man-description>. Acesso em 19 jan. 2014.)

na figura*2* como, por exemplo, o *MS06-025* que é uma vulnerabilidade em roteamento e acesso remoto, ou o *MS07-029* que é vulnerabilidade no Windows interface RPC (*Remote Procedure Call*) DNS (*Domain Name System*).

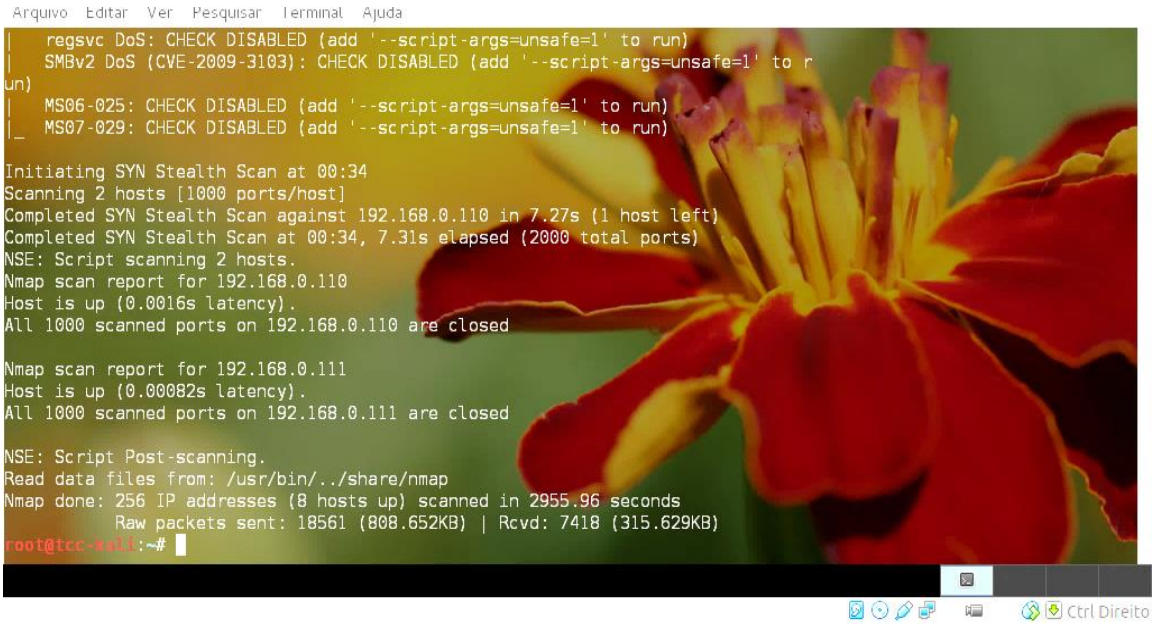

Figura 2. Scanning utilizando NMAP

Fonte (Print screen gerado pela autora)

Para efetuar esse *scanner* foi utilizado o comando demostrado na tabela 2.

nmap –v –script=smb-check-vulns 192.168.0.0/24

Tabela 2. Comandos do scanner

Como já citado acima, esse comando busca vulnerabilidades conhecidas. Outro exemplo a ser citado é o *MS08-067*[12] *e o CONFICKER*[13]dentro do ranger de IP utilizado nesse experimento. O *MS08-067* é explorado neste projeto.

[12] ***MS08-067***- é uma vulnerabilidade no serviço do servidor e pode permitir execução remota de código se um usuário receber uma solicitação de RPC especialmente criada em um sistema afetado

[13] ***CONFICKER*** é um vírus de computador criado com o objetivo de afetar sistemas operacionais Windows. Também conhecido como *Downup*, *Downadup* e *Kido*.

Após a realização do *scanner*, e com as vulnerabilidades conhecidas, parte-se para o teste de intrusão utilizando *Metasploit*. Para entrar no console, basta digitar o comando #*msfconsole*.

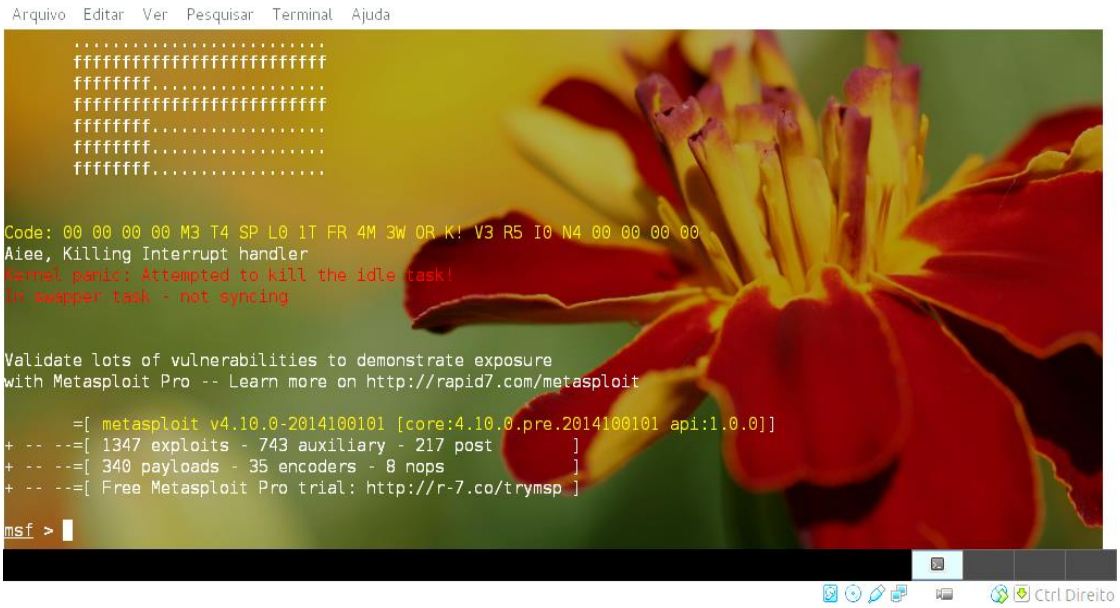

Figura 3. Tela inicial do console Metasploit

*Fonte (Print screen*gerado pela autora*)*

A figura 3 mostra que já se tem acesso ao *metasploit,* o que é identificado através da sigla *msf (metasploit).* Algumas informações sobre o mesmo é gerado, tais como sua versão, a quantidade de *exploits* disponíveis e de *payloads*. Após entrar no console, o próximo passo é informar alguns comandos simples necessários para a intrusão. Inicia-se citando como devem ser buscadas as vulnerabilidades. Aqui será utilizada a forma exploratória, exploit, já descrita acima.

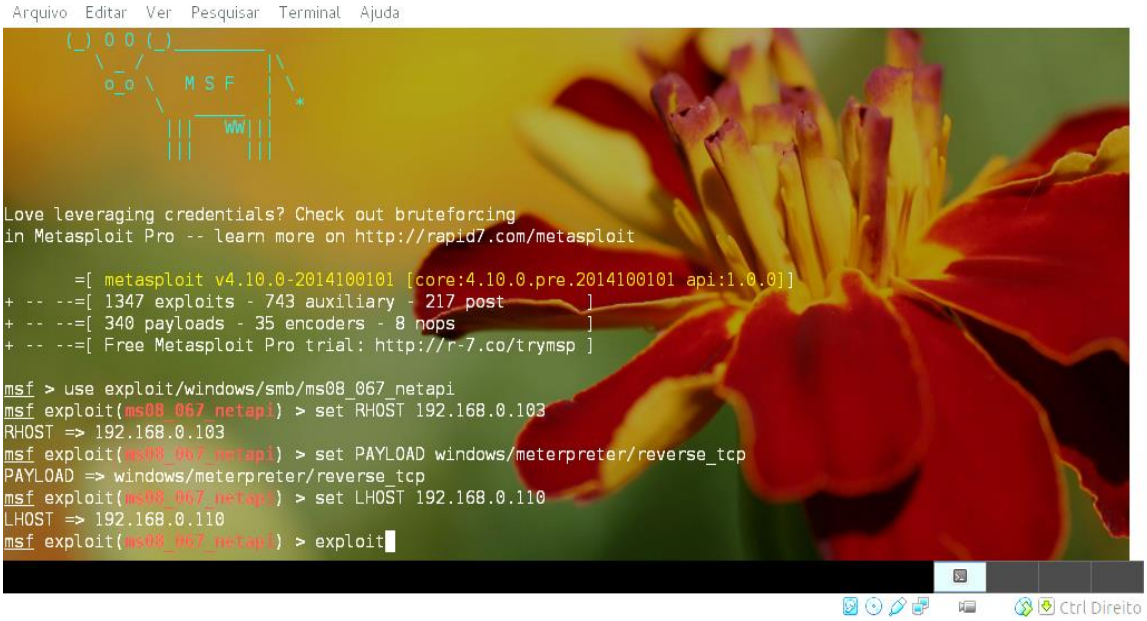

Figura 4. Comandos utilizados para a intrusão

Fonte (Print screen gerado pela autora)

Na figura 4 é mostrado a sequência de comandos utilizados para invadir o sistema proposto. Esses comandos são descritos adiante.

O primeiro comando da tabela 3 informa que se deseja explorar a vulnerabilidade *ms08_067_netapi.*

#use exploit/Windows/smb/ms08_067_netapi

Tabela 3. Primeiro comando para explorar a vulnerabilidade

Após ser explorada, a vulnerabilidade se destaca entre parênteses e em vermelho (demonstrado na figura 3).

O próximo comando já é inserido dentro da vulnerabilidade explorada, o mesmo informa que se deseja utilizar o explorar a vulnerabilidade *ms08_067_netapi.*

Para isso é preciso setar o host remoto da máquina alvo, no caso o Windows XP.

set RHOST 192.168.0.103

Tabela 4. Comandos para utilizar ou explorar a vulnerabilidade

O *Payload* utilizado para criar a comunicação entre o *RHOST* e o *LHOSTE* forma-se a partir do comando abaixo, que, gerando um meterpreter, gera comunicação entre o invasor e o alvo.

set PAYLOAD Windows/meterpreter/reverse_tcp

Tabela 5. Comando para para criar a comunicação entre o RHOST e o LHOSTE

Para setar o endereço IP da máquina atacante, utiliza-se o seguinte comando:

set LHOST 192.168.0.110

Tabela 6. Comando setar o endereço IP da máquina atacante

*Kali Linux*Por fim, executa-se a operação com o comando:

exploit

Tabela 7. Comando de execução

Após digitar o comando *#exploit,* o console entrou em meterpreter, isso significa que o alvo foi atingido. Para confirmar isso foram inseridos os comandos *ipconfig*e *sysinfo*para mostrar as informações da máquina invadida. Essas informações podem ser visualizadas na Figura 5.

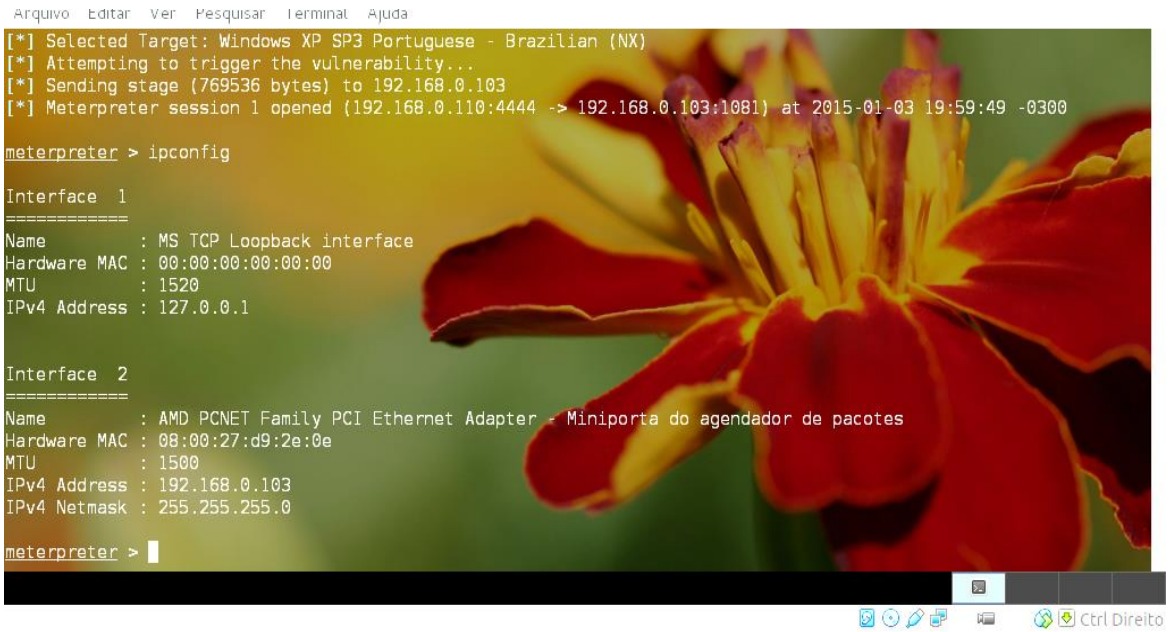

Figura 5. Máquina Windows XP invadida

Fonte (Print screen gerado pela autora)

Durante os comandos inseridos no console do *metasploit,* o sistema não retornou ao usuário nenhuma mensagem ou chamou a atenção para algo que talvez estivesse dando ou não correto. Só se foi possível comprovar que a invasão foi bem sucedida após o último comando *#exploit* em que foi observado que o *Kali Linux* invadiu o *Windows* XP, entrou em modo *meterpreter (figura 5).*

Diante dos objetivos propostos para este trabalho, bem como o experimento aqui realizado para atender a esses objetivos, traçam-se no próximo capítulo os resultados encontrados.

CAPÍTULO V – Resultados

Diante do que foi proposto por este trabalho e perante o experimento realizado no capítulo anterior, pode-se agora ressaltar alguns fatores que contribuem para utilização da distribuição *Kali Linux* por empresas de pequeno e médio porte que desejam manter seus ativos seguros de invasões por indivíduos mal intencionados.

É importante ressaltar que o que diferencia uma empresa de pequeno porte para uma de grande porte destaca-se segundo Filion (1996) é que sua posição no comércio ou indústria da qual faz parte não seja dominante; o número de empregados não seja superior a 500; e que seja possuída e operada independentemente. Além do nível de segurança que precisa existir sobre seus ativos.

Portanto, destacam-se alguns fatores que favorecem o uso da distribuição *Kali Linux* por microempresas, dentre elas está o fator de ser totalmente grátis. Qualquer empresa que deseje adquire-la não terá custo algum em sua aquisição.

Quem está de posse da distribuição tem em suas mãos *Kali Linux* mais de 300 ferramentas de teste de intrusão e auditoria, podendo efetuar um simples escaneamento a invasões complexas a sistemas operacionais. No teste realizado, foi feito um escaneamento utilizando o NMAP, um teste de intrusão simples que mostrou vulnerabilidades possíveis de ataques aos sistemas, tais como o MS06-025, MS07-029, CONFICKER e o MS08-067 já citados e este último explorado, o que já permitiria a empresa tomar as decisões possíveis para resolver o problema de vulnerabilidade em seu sistema.

Kali Linux possui muitas outras opções de ferramentas que proporcionam uma invasão mais complexa em sistemas. O próprio *Metasploit*, utilizado para este trabalho, oferece recursos mais complexos de intrusão que devem ser utilizados segundo a necessidade de cada empresa. Para este teste foi suficiente explorar ferramentas menos complexas, uma vez que o teste aqui realizado tinha como objetivo demonstrar o funcionamento da distribuição em testes de intrusão e auditoria. Para a utilização das demais ferramentas disponíveis no sistema é preciso um conhecimento maior em relação a sua funcionalidade, além de ter uma noção básica do sistema operacional Linux para se dar os primeiros passos. Isto é possível através de cursos sobre o *Kali Linux*.

Levando-se em consideração que seria necessário a realização de testes de intrusão com funções mais complexas da distribuição, a equipe de TI da empresa deverá ser preparada para utilizar as ferramentas de forma a ter sucesso em suas operações. As capacitações devem ser dadas aos funcionários.

Como já citado um ponto a favor do *Kali Linux* é pelo fato de ser gratuito, o que faz com que a capacitação não seja um gasto elevado levando-se em consideração que a licença do software é isenta. A distribuição oferece recursos suficientes para que empresas de pequeno e médio porte encontrem as vulnerabilidades que seus sistemas podem apresentar. Isto foi demonstrado no teste realizado, levando em consideração que os endereços IP's estavam em uma mesma faixa. Além disso, pode ser utilizado tanto com interface gráfica como em forma textual.

CAPÍTULO VI – Conclusões

A principal função dos testes de intrusão é verificar o quão vulnerável se encontra o sistema, a fim de proporcionar ao responsável uma visão ampla e preventiva de como resolver os problemas e riscos de intrusão em seu sistema. Toda organização trata suas informações como o bem ativo mais preciso que existe, pois, nesses dados estão o sucesso ou o fracasso de sua empresa.

Diante disso, torna-se importante manter toda a rede computacional ou tecnológica por onde percorrem essas informações livres de riscos de invasões, assim, a distribuição *Kali Linux* vem auxiliar pequenas e médias empresas a conseguirem atingir esse objetivo.

6.1 Limitações da Pesquisa

Um dos fatores que limitaram essa pesquisa consistiu na dificuldade de material (estações de trabalho) para realizar os testes, outro fator é que o Kali Linux é uma distribuição “nova”, ou seja, está há pouco tempo no mercado e por isso ainda não foi devidamente testada pela comunidade acadêmica, dificultando assim o embasamento teórico para essa pesquisa.

6.2 Trabalhos Futuros

Como já descrito, o experimento realizado neste trabalho foi feito a partir de duas máquinas interligadas entre si com mesma faixa de endereços IP, ou seja, estavam numa mesma rede. A partir disso, sugere-se a realização de testes de intrusão utilizando Armitage, que é a versão do mestasploit com interface gráfica, a partir de máquinas que fazem parte de redes diferentes, a fim de verificar a veracidade da distribuição Kali Linux também em redes diferentes.

Mesmo diante das limitações encontradas no decorrer do experimento e perante os fatos relatados e mostrados neste trabalho, pode-se perceber que *Kali Linux* é uma excelente alternativa para quem deseja manter seu sistema seguro de invasões com baixo custo, pois, mesmo sem existir muitos embasamentos teóricos

para fundamentá-lo, é a distribuição mais completa que pode ajudar profissionais com o mínimo de conhecimento em Linux a realizar do mais simples aos mais complexos testes de intrusão.

REFERÊNCIA

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002 - **Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação.** ABNT, 2005.

BackTrack – PenetrationTestingDistribution. Disponível em: <http://www.backtrack-linux.org/> Acesso em 03 nov. 2014

BORGES, Cristiano Goulart; HELENA, Eduardo André de S.. **Estudo Comparativo de Metodologias de Pentests.** Universidade Luterana do Brasil.Rio Grande do Sul, 2011.

BROAD, James; BINDNER, Andrew. **Hacking com *Kali Linux*: Técnicas práticas para testes de invasão.** 1.ed. São Paulo: Novatec, 2014.

CAINE. Disponível em: <http://www.caine-live.net/>. Acesso em 12/04/2015.

CIPOLI, Pedro. **O que é Engenharia Social?.**Disponível em: <http://corporate.canaltech.com.br/o-que-e/seguranca/O-que-e-Engenharia-Social/>. Acesso em 19 jan. 2014.

COLEMAN, Gabriella. **The Anthropology of Hackers.** Set. 2010. Disponível em: <http://www.theatlantic.com/technology/archive/2010/09/the-anthropology-of-hackers/63308/>. Acesso em 13 abril 2015.

COSTA, Ana Clara. **Novos sites do governo federal são invadidos por hackers.** *Exame.com*, São Paulo, ago. 2011. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/sites-do-governo-federal-voltam-a-sair-do-ar>. Acesso em 23 set. 2014.

DOMINGUES apud CASTELLS, Manuel. **A Sociedade em Rede.** São Paulo: Paz e Terra, 2001.

E-EFENSE. **Helix3 Enterpraise.** Disponível em: <http://www.e-fense.com/h3-enterprise.php>. Acesso em 12 abril 2015.

Eleven Paths. **FOCA**. Disponível em: <https://www.elevenpaths.com/labstools/foca/index.html>. Acesso em 9 abril 2015.

FALCÃO, Joaquim. LEMOS, Ronaldo. **Estudo Sobre Software Livre.**

FILION, Louis Jaques. **Free Trade: The Need for a DefinitionofSmall Business.** Apud. PINHEIRO, Maurício. Gestão e Desempenho das Empresas de Pequeno Porte: Uma Abordagem Conceitual e Empírica. São Paulo: 1996. Tese de Doutorado, FEA/USP, p. 21-22.

GENERAL SECURITY. **Automated Vulnerability Testing with winAUTOPWN.** Infosec Institute, 2011. Disponível em: <http://resources.infosecinstitute.com/vulnerability-testing-winautopwn/>. Acesso em: 12 abril 2015.

GIAVAROTO, Sílvio César Roxo. SANTOS, Gerson Raimundo dos. **Backtrack Linux – Auditoria e Testes de Invasão em Redes de Computadores.** Rio de Janeiro: Editora Ciência Moderna LTDA., 2013.

GONCALVES, M. *ProtectingYour Web Site with Firewalls.* Prentice-Hall, Inc., 1997. 290p.

HAISCHT, DANIEL S. **Criptografia de e-mails com Anubis: Proteção Egípcia.** SysAdmin, 2006. Disponível em: <https://www.linuxnewmedia.com.br/images/uploads/pdf_aberto/LM21_anubis.pdf>. Acesso em: 12 abril 2015.

IWATA, ROBERTO R. **Software Livre x Software Proprietário e suas implicações econômicas e políticas.** 2009. 41f. Monografia (Ciências Econômicas). Universidade Federal de Santa Catarina, Santa Catarina. 2009.

***KALI LINUX*.** Disponível em: <http://docs.kali.org/category/introduction>. Acesso em 23 set. 2014.

KAUARK, Fabiana da Silva. MANHÃES, Fernanda Castro. MEDEIROS, Carlos Henrique. **Metodologia da Pesquisa: Um guia prático.** Itabuna: Via Litterarum Editora, 2010.

KIOSKEIA. **Introdução à segurança informática.** Disponível em: <http://pt.kioskea.net/contents/623-introducao-a-seguranca-informatica>. Acesso em 13 abril 2015.

KIOSKERA. **Introdução aos ataques.** Disponível em: <http://pt.kioskea.net/contents/16-introducao-aos-ataques>. Acesso em 13 abril 2015.

METASPLOIT. Disponível em: <http://www.metasploit.com/>. Acesso em 12 abril 2015.

MORAES, Paulo. **Mente Anti-Hacker: Proteja-se.**Rio de Janeiro: Brasport, 2011.

NAKAMURA, E.T.; GEUS, P.L. **Segurança de redes em ambientes corporativos.**2.ed. São Paulo: Futura, 2003.

NAMP.ORG. **Namp.** Disponível em: <http://nmap.org/download.html>. Acesso em 12 abril 2015

O que é GNU?.GNUOperating System. Disponível em: <http://www.gnu.org/>. Acesso em 27 out. 2014.

Sharpe, Richard. **Guia do Usuário do Wireshark.**2014. Disponível em: <https://www.wireshark.org/docs/wsug_html/> Acesso em 9 abril 2015.

SOARES, Rafael. **Auditoria Teste de Invasão(Pentest) – Planejamento, Preparação e Execução.** Blog SegInfo. Disponível em:

<http://www.seginfo.com.br/auditoria-teste-de-invasaopentest-planejamento-preparacao-e-execucao/>. Acesso em 10 nov. 2014.

TESTE DE INVASÃO. Disponível em: <http://www.testedeinvasao.com.br/oque/>. Acesso em 11 nov. 2014.

TSHARK. Disponível em: <https://www.wireshark.org/docs/man-pages/tshark.html>. Acesso em 11 abril 2015.

UMRAO, Sachin; KAUR, Mandeep; GUPTA , G. K. **VULNERABILITY ASSESSMENT AND PENETRATION TESTING.** In: InternationalJournalof Computer & Communication Technology. Índia, 2012.

VENERSSON, Susanne. **PenetrationTesting in a Web ApplicationEnvironment**. Projeto de Graduação. LinnaeusUniversity, 2010. 74f. Disponível em: < http://lnu.diva- portal.org/smash/get/diva2:356502/FULLTEXT01 />. Acesso em 23 set. 2014.

WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras.** Tradução: Fábio Freitas da Silva. Rio de Janeiro: Campus, 2000.