Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GABRIEL AUGUSTO NARCISO BARREIROS

PESQUISA SOBRE OS TIPOS DE ATAQUES ÀS VULNERABILIDADES COM KALI LINUX

Assis/SP
2017

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GABRIEL AUGUSTO NARCISO BARREIROS

PESQUISA SOBRE OS TIPOS DE ATAQUES ÀS VULNERABILIDADES COM KALI LINUX

Projeto de pesquisa apresentado ao curso de Análise e Desenvolvimento de Sistemas do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito à obtenção do Certificado de Conclusão.

Orientando(a): Gabriel Augusto Narciso Barreiros
Orientador(a): Prof. Douglas Sanches da Cunha

Assis/SP
2017

PESQUISA SOBRE OS TIPOS DE ATAQUES ÀS VULNERABILIDADES COM KALI LINUX

GABRIEL AUGUSTO NARCISO BARREIROS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Prof. Douglas Sanches da Cunha

Examinador: _____
Prof. Fábio Eder Cardoso

Assis/SP
2017

DEDICATÓRIA

Dedico este trabalho a todos, a toda minha família, principalmente as pessoas que passaram por minha vida e me ensinaram com experiência de vida a ter força para eu estar aqui, e aos meus pais que me ajudaram muito, dando muito carinho, educação e serem exemplos de pessoa para eu poder ser quem sou hoje e realizar essa pesquisa. Dedico também a todos meus amigos que me ajudaram em trabalho, diversão e apoio sempre que precisei para realizar esse sonho.

AGRADECIMENTOS

Agradeço primeiramente a todas dificuldades, altos e baixos que passei por me ensinar a ser uma pessoa melhor a cada dia e ter forças para batalhar todos os dias.

Aos meus pais por acreditar em mim, me ajudar sempre quando precisava me distrair um pouco para melhorar a autoestima.

Aos meus amigos pelo apoio, incetivo, paciência e compreensão durante todos esses anos.

E por fim sou grato por todas as pessoas que me ajudaram direta ou indiretamente na execução deste trabalho.

“A minha sorte foi passar madrugadas estudando...”

Leandro Karnal

RESUMO

Com o passar do tempo e a evolução da informática, a Internet tornou-se não apenas útil, mas obrigatória à vida das pessoas. Com o rápido avanço da tecnologias, a segurança da informação não conseguiu acompanhar este avanço, tornando-se de certa forma ineficaz, dando espaço para que hackers sem ética, conseguisse acessar com facilidade os dados e furtar os mesmos de pessoas comuns e empresas. Com a mesma base de conhecimento dos *hackers*, pessoas bem intencionadas utilizam essas mesmas técnicas para garantir a segurança dos dados através de testes de vulnerabilidade, assim essas pessoas começaram a ser chamadas de *hackers* éticos.

Palavras-chave: Segurança da informação; Internet; Hackers; Teste de vulnerabilidade; Kali Linux.

ABSTRACT

Over time and the evolution of technology, the Internet has become not only helpful for the people, but also, essential for and individual's lives. With the progression of technology, the security of people's information was unable to keep pace with the same advancement, making it ineffective, which gave unethical hackers the ability to easily access data and steal data from individuals and businesses. With the same knowledge base as hackers, well-intentioned people utilize the same techniques and strategies to ensure data security through vulnerability testing, leading these people to start being called ethical hackers.

Keywords: Security Information; Internet; Hackers; Vulnerability Testing; Kali Linux.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

Com o passar do tempo e a evolução da informática, a Internet tornou-se não apenas útil, mas relevante à vida das pessoas. Foi popularizada tão rapidamente que exigiu um rápido aprendizado a respeito de seu uso básico, deixando para trás os cuidados com a segurança da informação. Neste capítulo será falado sobre o objetivos do trabalho, justificativas e motivações sobre no que foi inspriado para o desenvolvimento dessa pesquisa, e por fim, a estrutura para o desenvolvimento do projeto O gráfico abaixo representado pela Figura 1 mostra essa evolução do uso da mobilidade no ano de 2015.

Figura 1: Comportamento dos usuários de internet em todo o mundo (WE ARE SOCIAL)

Portanto, deixando de garantir as três características básicas da segurança da informação que são a confidencialidade, integridade e disponibilidade. A confidencialidade é a garantia do resguardo das informações em confiança para que pessoas não autorizadas tenham acesso às mesmas, a integridade é garantir que a informação chegará ao seu destino sem sofrer nenhum tipo de dano ou modificação e a disponibilidade é a garantia de acesso à 13informação onde quer que o usuário esteja, se a informação estiver disponível para o acesso (TANENBAUM, 2003).

As três características básicas são fundamentais para uma rede sem fio ou para uma rede de computadores cabeada, possibilitando assim um acesso seguro ao usuário, mas hoje existem diversas ferramentas de invasão a rede, essas invasões têm como objetivo adquirir dados importantes para uso indevido, ou para chantagear o proprietário dos dados furtados. Essas ferramentas também são muito utilizadas para encontrar a vulnerabilidade na rede para que não haja a possibilidade de invasão para roubo de informações (Mendes, Douglas Rocha).

1.1 OBJETIVO

Este trabalho tem como objetivo detectar vulnerabilidade em uma rede de dados e comunicação, ou seja, vulnerabilidade de uma rede onde há diversos computadores integrados na mesma, descrever as falhas detectadas para que seja possível mostrando a importância de investir na segurança dos dados a partir das análises realizadas sobre os relatórios gerados a partir da utilização das ferramentas disponíveis na distribuição *Kali.*

Com base dos fatos apresentados por PEREIRA (2015) é importante implementar, melhorar a segurança para garantir a integridade dos dados que são transmitidos através da rede de 14 computadores, pois invasor ou vírus instalados e propagando pela rede podem ocasionar uma séria vulnerabilidade na rede e ter dados roubados, perdidos ou criptografados.

1.2 JUSTIFICATIVAS

Visando o grande número de dispositivos e equipamentos com acesso à Internet e a falta de segurança principalmente em ambientes corporativos, o número de ataques de invasores e até mesmo de vírus implantados em uma máquina que se propaga através da rede possibilitando a invasão ou perda de dados (ERICSSON, 2015; PEREIRA, 2015).

Linux GNU/Linux baseada no Debian. O Kali Linux é um projeto *open source* que é mantida e financiada pela ofensiva de Segurança, um fornecedor de treinamento de segurança da informação de classe mundial e serviços de teste de penetração, ou seja, tem como finalidade voltada principalmente em auditoria e segurança de rede computadores (KALI LINUX, 2013).

Atualmente as empresas utilizando a tecnologia *Cloud Computing* que é a migração dos dados para a nuvem, ou seja, seus dados podem estar em qualquer lugar do mundo, assim trazendo maior disponibilidade dos dados, podem ser acessados de qualquer lugar do mundo. Porém a maior dúvida de empresas é a questão manter a segurança de informações confidenciais fora do domínio dos empresários, com isso é possível afirmar que a *Cloud Computing* é segura, pois os provedores deste tipo de serviço seguem normas internacionais de segurança, tal como a *International Organization for Standardization* (ISO), *Secure Socket Layer* (SSL), criptografias avançadas, entre outros métodos de segurança (RITTINGHOUSE, 2010).

Ainda segundo Rittinghouse (2010), com a aplicação da *Cloud Computing*, o meio corporativo tem apenas de filtrar as informações que são feitas *upload* para a nuvem para garantir a integridade dos dados que estão sendo transmitidos.

A partir dos testes de falha de segurança, é possível ajuda a manter a integridade de dados de equipamentos em rede, tais testes podem detectar vulnerabilidades de sérios riscos para o ambiente corporativo ou doméstico e assim aplicando as técnicas e promover possíveis soluções para blindar uma rede de computadores e de dispositivos móveis.

1.3 MOTIVAÇÃO

O desenvolvimento deste projeto de pesquisa consiste no fato de que o teste de falhas de segurança é um tema ainda pouco abordado e pode contribuir com a qualidade e segurança de dados. O teste de falha de segurança é realizado para manter a integridade de dados presentes em uma rede, tais testes podem detectar as vulnerabilidades críticas que podem causa sérios riscos para o ambiente corporativo ou doméstico.

Outra motivação é a chance de atuar no mercado de trabalho que necessita de profissionais com conhecimento na linha do tema desta pesquisa, uma vez que a área de segurança de dados e teste de falhas de segurança necessita de profissionais capacitados.

1.4 ESTRUTURA DO TRABALHO

O presente trabalho está dividido em seis capítulos. O Capítulo 1, apresenta a Introdução, os objetivos, justificativas e motivações para o desenvolvimento da pesquisa. O Capítulo 2 aborda aspectos gerais sobre segurança da Informação, apresenta o conceito de segurança digital, os métodos e técnicas de segurança digital, as vulnerabilidades e falhas de segurança, os três tipos de invasores, quais as motivações e consequência de uma invasão e o histórico de incidentes de segurança da informação. O Capítulo 3 será apresentado o conceito geral de rede de computadores, será tratado os diferentes tipos de técnicas de invasão, os mecanismos de criptografia e os desafios e oportunidades em redes de computadores. O Capítulo 4 será tratado a proposta do trabalho que consiste em realizar testes de vulnerabilidade para detectar possível brechas para ocorrer uma invasão e ocasionar na perda de informação, este destes serão aplicados com o intuito de demostrar a importância de se investir na segurança dos dados e mostrar como se prevenir contra os mesmos. O Capítulo 5 informado todos os processos realizados no decorrer da pesquisas, os métodos e técnicas utilizadas e a demonstração do ambiente construído e os métodos para de proteção contra os ataques. O Capítulo 6 será tratado a conclusão do trabalho, onde será descrito as considerações finais, a conclusão final e os trabalhos futuros que serão realizados.

2. ASPECTOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

O termo segurança é usado com o significado de minimizar a vulnerabilidade de bens e recursos. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém (ISO 89F).

Neste capítulo será abordado os métodos, técnicas, ferramentas e vários tipos de fundamentos usado tanto por profissionais hackers ético como por hackers não éticos, com o objetivo de mostrar como funciona a ação de um criminoso digital.

2.1 FUNDAMENTOS DE SEGURANÇA DIGITAL

A segurança da informação bem como a segurança das redes de computadores têm se tornado um tema bastante comum ao longo dos anos que decorreram após o surgimento da Internet. Porém, mesmo com a evolução da tecnologia e a disponibilidade de um acervo infinito de informações sobre o tema, empresas de pequeno e médio porte ainda têm grandes dificuldades na implantação de políticas e ferramentas eficazes na segurança da informação. Isto ocorre por que grande parte das ferramentas disponíveis no mercado exigem um nível de conhecimento técnico alto, ou uma grande disponibilidade para gerenciar tais tecnologias.

A segurança é a necessidade de proteger os dados contra acessos e manipulações, sendo intencionais ou não das informações confidenciais por pessoas não autorizadas ou a utilização de um computador ou dispositivos não autorizados.

2.2 MÉTODOS E TÉCNICAS DE SEGURANÇA DIGITAL

A segurança em rede de computadores é o resguardo dos dados mantidos na rede, ou seja, na segurança das informações que estão sendo armazenadas em um determinado local (ZOTTO, 2012).

Aplicar técnicas e métodos de segurança é um fator primordial para qualquer segmento que utilize esta tecnologia. Portanto, deixando de garantir as três características básicas da segurança da informação que são a confidencialidade, integridade e disponibilidade. Segundo KUROSE (2006) e ZOTTO (2012), para que possa estabelecer uma conexão de segura, é necessário ter as seguintes propriedades, a confidencialidade é a garantia do resguardo das informações em confiança para que pessoas não autorizadas tenham acesso às mesmas, a integridade é garantir que a informação chegará ao seu destino sem sofrer nenhum tipo de dano ou modificação por acidente ou por má intenção de segundo 17 durante a transmissão, e a disponibilidade é a garantia de acesso à informação onde quer que o usuário esteja, se a informação estiver disponível para o acesso. A disponibilidade, um dos maiores fatores que levaram ao uso de políticas de segurança de rede, que surgiu principalmente após o advindo a Internet, foi devido aos ataques *Denial Of Service* (DoS). A disponibilidade contém três características principais: A pontualidade, o sistema está disponível a todo o momento, a continuidade, os usuários

continuam trabalhando mesmo que o sinal estiver fraco ou tenha ficado inativo. E a robustez não permitir que todos os funcionários trabalhem nos sistemas de informação.

2.3 VULNERABILIDADES E FALHAS DE SEGURANÇA: MOTIVAÇÃO E CONSEQUÊNCIAS

Antes de tratar das motivações de um invasor de sistemas e as consequências posteriores ao ato de invadir, devem ser apresentados os termos mais utilizados para definir os diferentes tipos de invasores, quais sejam, o *Hacker,* o *Cracker*, o *Lammer* (QUEIROZ, 2007).

No mundo da segurança computacional, existem alguns termos utilizados pelos especialistas para se referir aos *hacker*s.

Segundo GIAVAROTO (2015), autor do livro Kali Linux – Introdução ao *Penetration Testing* (2015-, p. 5):

Black Hat ou *cracker* é um especialista que usa suas habilidades de forma maliciosa e para o mal; alguns exemplos são invasões não autorizadas, furto de informações, negações de serviço etc.

Gray Hat é um termo que foi criado para qualificar um tipo de *hacker* que, na maioria das vezes atua dentro da lei, porém alguns de seus atos podem ser qualificados como estando às margens da lei.

O *White Hat* ou *hacker* ético é um profissional com conhecimento na área de segurança computacional que utiliza suas habilidades para o bem, como por exemplo, o teste de penetração. Apesar de o *hacker* ético utilizar as mesmas 18 ferramentas do *black hat*, ele as utiliza de forma ética e somente mediante autorização.

2.3.1 HACKER, CRACKER, LAMMERS

O *hacker* é a pessoa que descobre a falha de segurança no sistema, informa a falha e desenvolve a correção para a falha encontrada para que a mesma não seja identificada por pessoas má intencionadas que possam realizar possíveis ataques àquele sistema (HIMANEN, 2001; RAYMOND, 2002).

O indivíduo que explora a deficiência na segurança de um sistema computacional ou produto sem qualquer intenção perversa, com o intuito de chamar a atenção dos desenvolvedores, é chamado de *cracker* é a pessoa que utiliza do conhecimento de segurança da informação para realizar invasão em sistemas, quebrar senhas, roubar informações, ou seja, é um vândalo virtual (MORIMOTO, 2005; CINTO, 2015).

Já o L*ammer* é um termo utilizado para as pessoas que não possuem nenhum ou pouco conhecimento sobre *hack* e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques. Conhecido atualmente também por "*Script Kiddie*" que utilizam *exploits*, *trojan*, entre outros. O *Lammer* foi um termo depreciativo utilizado com maior frequência no final da década de 80 e na década de 90, atribuído àqueles que realizam ataques da área de segurança da informação, mas não possuem conhecimento necessário para desenvolver suas próprias ferramentas para realizar ataques (CANALTECH, 2016c). Segundo Canaltech.

Ao contrário de *hackers*, os ataques de *lammers* quase sempre são amadores, justamente pelo baixo conhecimento que possuem sobre programação e tecnologia. Alguns desses são apenas curiosos aventureiros da Internet e do mundo virtual, procurando por diversão, ou novas maneiras de se satisfazerem na Internet (KALI LINUX, 2015).

2.3.2 MOTIVAÇÕES E CONSEQUÊNCIAS

O *hacker* precisa se sentir desafiado, instigado a prosseguir com a ação. Muitas vezes essas pessoas agem somente por agir, para perceberem que algo é possível e que eles conseguem fazer. *Hackers* gostam de resolver problemas e, quanto mais complexos esses 19 problemas, melhor. Alguns não realizam invasões apenas por serem desafiados, mas também realizam essas ações, por curiosidade de descobrir como funciona o sistema, por diversão, dinheiro, fama ou pelo fato de alguém ou alguma empresa ir contra seus ideais (ARRUDA, 2011).

Sobre todos os atos de invasores há consequências por mais simples que sejam as mesmas, podendo ser uma perda de produtividade de um serviço até a mais complexa a privação de reputação e consequente a perda de mercado. É interessante notar que os prejuízos dependem do valor da informação que está em jogo, porém devem ser considerados tanto os valores tangíveis quanto os valores intangíveis.

Dessa forma, as consequências da invasão bem-sucedida à uma empresa pode variadas, mas são sempre negativas. De acordo com (HORTON; MUGGE, 2003), algumas delas são: Monitoramento não autorizado, descoberta e vazamento de informações confidenciais, modificação não autorizada de servidores e da base de dados da organização, negação ou corrupção de serviços e fraude ou perdas financeiras (QUEIROZ, 2007).

2.4 HISTÓRICO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Segundo ARRUDA (2012), a evolução da segurança da informação é realizada simultânea ao dos sistemas computacionais, infelizmente isso não ocorre, as evoluções dos sistemas computacionais são muito mais rápidas, todos os dias novos sistemas são desenvolvidos e a maioria não é realizada os testes para identificar erros de segurança. Atualmente são raros os sistemas que não tenham falhas graves de segurança.

Em Abril de 2011, um grupo de *hacker*s assumiu a autoria do ataque a *Playstation Network*, o serviço da Sony que possibilita jogadores do mundo todo jogarem juntos *on-line*, e cerca de 77 milhões de usuário ficam sem acesso ao serviço, pois o ataque levou a toda a rede ficar *off-line* e a empresa teve prejuízo de US$ 24 bilhões. Segundo os *hacker*s a motivação para este ataque foi o processo que a Sony moveu contra o George Hotz, um rapaz que é responsável pelo desbloqueio do console Playstation 3 (ARRUDA, 2012).

Em Março de 2011, a RSA, uma empresa especializa em segurança e criptografia teve de gastar cerca de US$ 66 milhões e tempo para corrigir uma falha de segurança que com a falha um *hacker* invadiu os servidores da RSA e obteve mais de 40 milhões de chaves de autenticação usadas para acessar redes corporativas e governamentais (ARRUDA, 2012).

Em janeiro de 2016, o grupo de *hacker*s brasileiro "*ASOR Hack Team*", invadiu o banco de dados do Conselho Administrativo de Defesa Econômica (CADE) e publicou na *web* 20 diversos dados juntamente com os *logins* e senhas de usuários do sistema. Segundo o grupo a ação foi uma resposta ao veto da presidente Dilma Rousseff à auditoria da dívida pública (MÜLLER, 2016).

O fato está ocorrendo há uma semana e impedindo que os profissionais do hospital *Hollywood Presbyterian Medical Center* em Los Angeles, acessem dados essenciais como

arquivos de pacientes e resultados de exames grave. O *hacker* está exigindo que o hospital pague 9 mil *bitcoins* para remover um *ransomware* que está bloqueando os computadores do hospital (ROSTON, 2016). *Bitcoins* é uma moeda virtual que equivale ao dinheiro real, está mesma moeda é utilizada para transações online, é a forma ideal de pagamento, pois é rápido e seguro. É uma tecnologia inovadora (MERCADO BITCOIN.NET, 2016).

3. REDES DE COMPUTADORES

Redes de computadores são estruturas lógicas e físicas que permite que dois ou mais computadores troquem informações entre si. Possibilitam o compartilhamento de recursos tais como unidades de disco rígido, *scanners* e impressoras. Neste capítulo será abordado alguns conceito de redes e também os tipos de ataques mais conhecidos e utilizados por hackers, com objetivos de mostrar os desafios e oportunidades existentes na área da segurança digital.

Uma rede de computadores é definida de acordo com sua abrangência geográfica, topologia, meio físico e protocolo. Algumas das classificações por abrangência geográfica são PAN, LAN, MAN, WAN e SAN.

PAN, As redes do tipo PAN, ou Redes de Área Pessoal, são usadas para que dispositivos se comuniquem dentro de uma distância bastante limitada. Um exemplo disso são as redes Bluetooth e UWB, como pode ver na imagem logo abaixo.

Figura 2: Rede PAN (PINTO,2010).

LAN, As chamadas Local Area Networks, ou Redes Locais, interligam computadores presentes dentro de um mesmo espaço físico. Isso pode acontecer dentro de uma

empresa, de uma escola ou dentro da sua própria casa, sendo possível a troca de informações e recursos entre os dispositivos participantes.

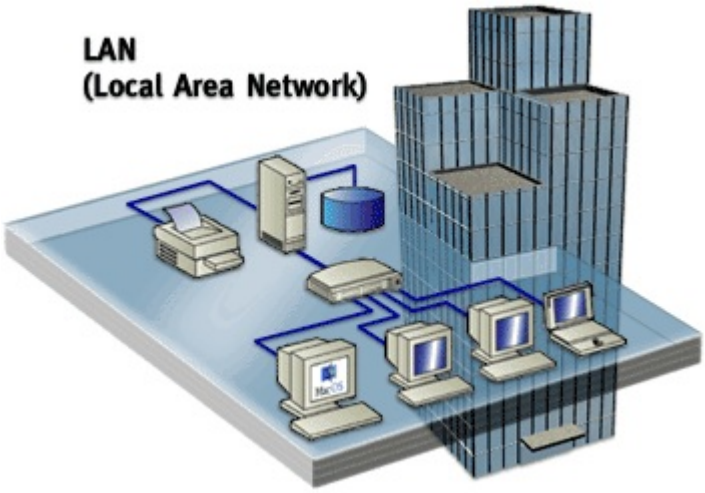

Figura 3: Rede LAN (Éder Giovani, 2013).

MAN, Imaginemos, por exemplo, que uma empresa possui dois escritórios em uma mesma cidade e deseja que os computadores permaneçam interligados. Para isso existe a Metropolitan Area Network, ou Rede Metropolitana, que conecta diversas Redes Locais dentro de algumas dezenas de quilômetros, a figura 4 ilustra isso logo abaixo.

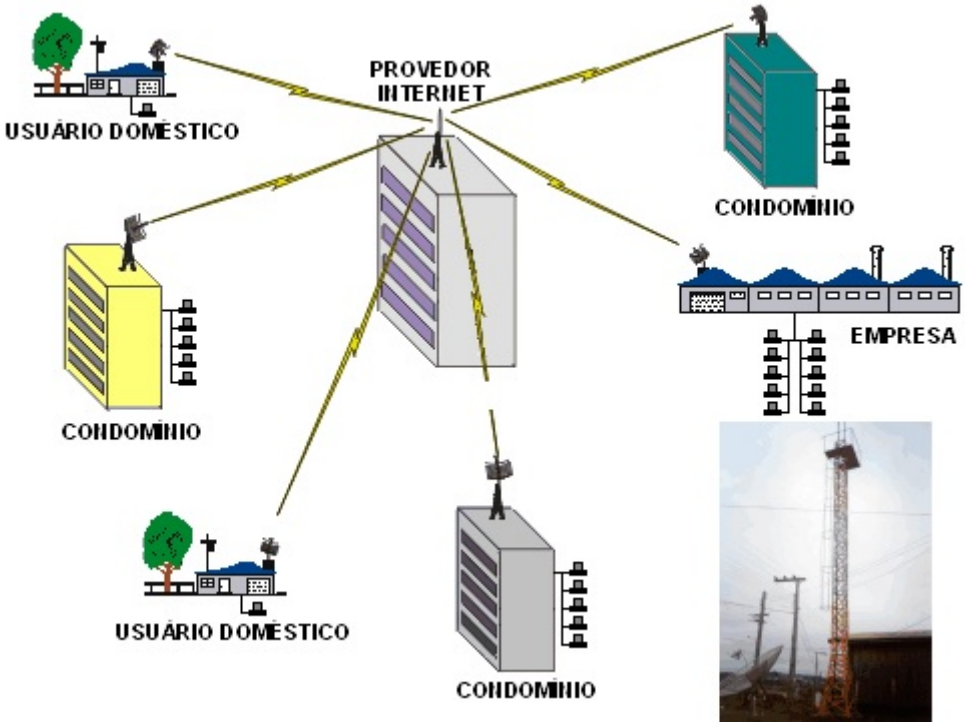

Figura 4: Rede MAN (Éder Giovani, 2013).

Na figura 4 podemos ver um rede WAN, A Wide Area Network, ou Rede de Longa Distância, vai um pouco além da MAN e consegue abranger uma área maior, como um país ou até mesmo um continente.

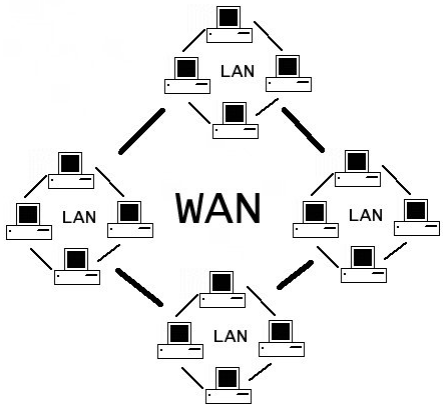

Figura 5: Rede WAN (Papel Digital, 2015).

SAN, As SANs, ou Redes de Área de Armazenamento, são utilizadas para fazer a comunicação de um servidor e outros computadores, ficando restritas a isso.

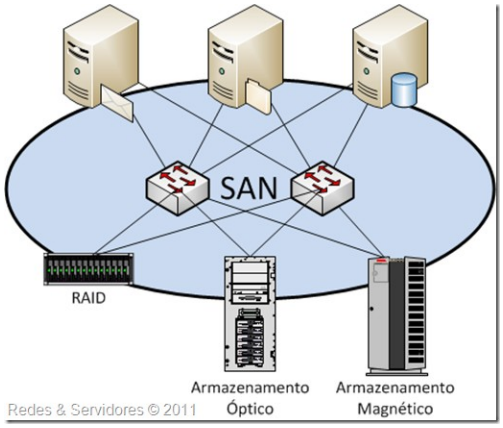

Figura 6: Rede SAN (Rui Natário, 2011).

As topologias de redes são a forma em que os computadores e dispositivos estão interligados, tais redes em anel, barramento, estrela, malha, ponto-a-ponto e árvore.

A Figura 7 representa a topologia de anel todos os computadores são conectados através de um circuito fechado, em série e o último computador conectado a sequência se conectará novamente ao primeiro computador da sequência.

Há algumas vulnerabilidades na topologia de anel, a falha de um nó pode provocar a falha da rede e também há dificuldade de localização das falhas, reconfigurar a rede. Softwares de alto nível se encarregam de reconhecer nós defeituosos e removê-lo da rede e assim reconfigurando novamente automaticamente. Entretanto, pode ocorrer eventualidade no estabelecimento de protocolo de acesso à rede dado que cada nó que terá de assegurar a continuidade do sistema e só após a certificação da rede o mesmo estará disponível para enviar informação (PINHEIRO, 2016).

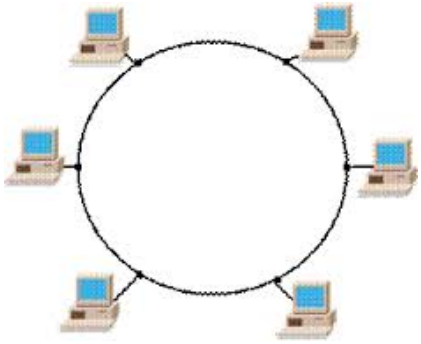

Figura 7: Representação da topologia de anel (PINHEIRO, 2006).

A Figura 8 representa a topologia de barramento, os computadores são interligados por um cabo comum ou link de comunicação. A desvantagem da topologia de barramento é enquanto uma máquina transmite um sinal toda à rede fica ocupada, se outra máquina tentar transmitir um sinal ocorrerá uma colisão e será preciso reiniciar a transmissão, ou seja, quanto mais máquinas estiverem conectadas pior será o desempenho da rede. A vantagem é a fácil instalação e a possibilidade de expansão sem afetar a rede, ou seja, possível expandir com a rede ativa. A vulnerabilidade deste barramento é a dificuldade de mudar ou mover nós é uma desvantagem e praticamente não oferece tolerância a falhas. Há grande dificuldade de diagnosticar falhas ou erros e defeitos no barramento interromperá. Entretanto, em uma rede adequadamente projetada e construída, tais defeitos não são comuns. Uma falha em uma única estação de trabalho geralmente não afeta a rede toda (PINHEIRO, 2016).

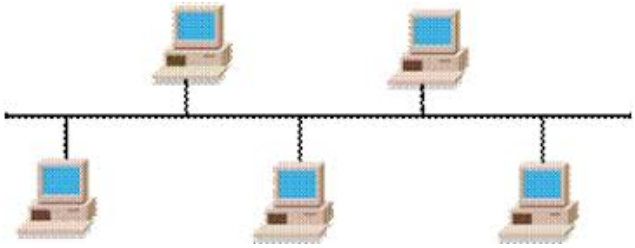

Figura 8: Representação da topologia de barramento (PINHEIRO, 2006).

A Figura 9 representa a topologia de estrela, é a mais utilizada com cabos de par trançado e um concentrador que pode ser *hubs* ou um *switchs*. As máquinas são conectadas todas ao um *hub* ou *switch* e o mesmo é encarregado de transmitir todos os dados para todas as máquinas. A vantagem desta topologia é a facilidade em encontrar falha, em realizar modificações e a simplicidade no protocolo de comunicação. A desvantagem é que depende de um *hub* ou *switch*, o custo da rede é mais elevado e a distância é limitada a 100 metros sem um amplificador (PINHEIRO, 2016).

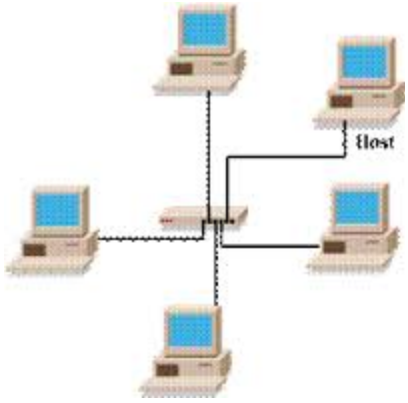

Figura 9: Representação da tologia de estrela (PINHEIRO, 2006).

A Figura 10 representa a topologia de malha, é muito utilizada por ser fácil de configurar e instalar os dispositivos na rede. Todas as máquinas estão interligadas, ou seja, todos os nós estão atados a todos os outros nós, assim o tempo de transmissão de dados é reduzido pelo fato de haver diversos caminhos até o destino (CARNEVAL et al., 2010).

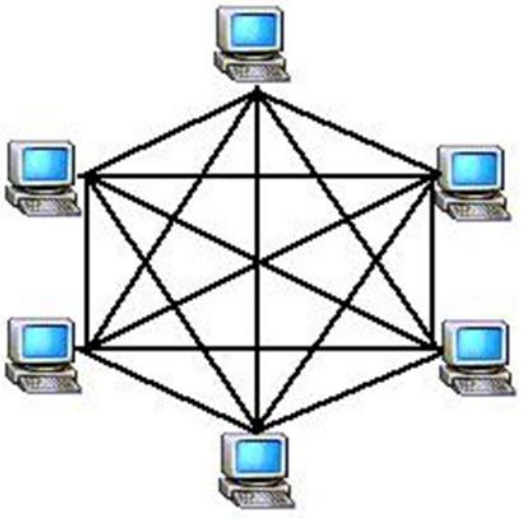

Figura 10: Representação da topologia de malha (VINICIUS, 2012).

A Figura 11 representa a topologia de ponto-a-ponto, a estrutura da rede é configurada de forma que não há necessidade de ter um computador central para receber todos os dados, todas as máquinas são interligadas podendo funcionar tanto como cliente quanto como servidor, assim compartilhando arquivos e serviços (GOMES, 1999).

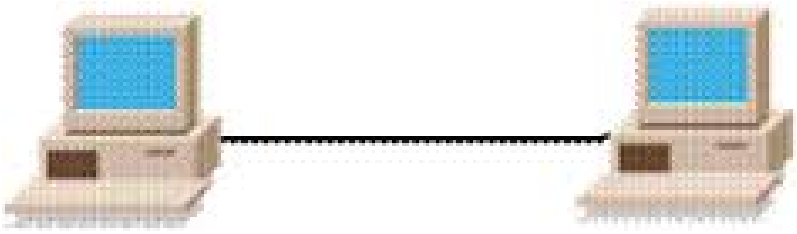

Figura 11: Representação da topologia ponto-a-ponto (PINHEIRO, 2006).

Segundo PINHEIRO (2016), na topologia em árvore é essencialmente uma série de barras interconectadas. Geralmente existe uma barra centrais onde outros ramos menores se conectam. Esta ligação é realizada através de derivadores e as conexões das estações realizadas do mesmo modo que no sistema de barra padrão. Cuidados adicionais devem ser tomados nas redes em árvore, pois cada ramificação significa que o sinal deverá se propagar por dois caminhos diferentes. A menos que estes caminhos estejam perfeitamente casados, os sinais terão velocidades de propagação diferentes e refletirão os sinais de diferente maneira. Em geral, redes em árvore, representada pela Figura 12, trabalha com taxas de transmissão menores do que as redes em barramento comum por estes motivos.

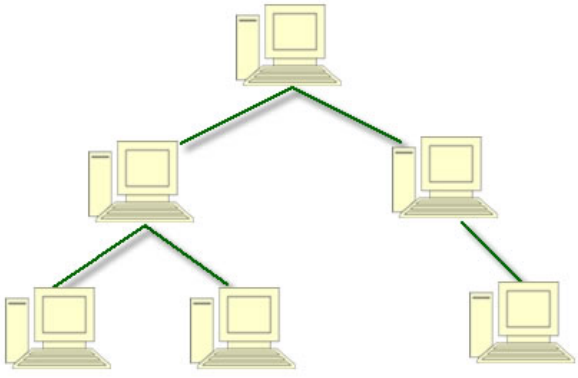

Figura 12: Representação da topologia de árvore (MARTINEZ, 2016).

3.1 VULNERABILIDADES E FALHAS DE SEGURANÇA

Vulnerabilidade é uma deficiência de segurança, são falhas de segurança causadas por erros humanos, erros de programação, má configuração de algum *software* ou de rede. Caso o invasor consiga explorar essa vulnerabilidade pode ocasionar no roubo de dados, ataques como spoofing, implantação de vírus e *malwares*.

Segundo GUIMARÃES et al. (2016), a segurança deve ser entendida como parte fundamental da cultura interna da empresa, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética da empresa. As ameaças à vulnerabilidade nos sistemas computacionais vêm crescendo em uma velocidade proporcional e muitas 33 vezes superior ao avanço tecnológico, dessa forma, faz-se necessário implementar uma política de segurança.

Segundo Kevin David Mitnick, “Segurança não é um produto que se pode comprar de prateleira, mas que consiste de políticas, pessoas, processos e tecnologia.” (REDE SEGURA, 2016).

3.2 TÉCNICAS DE INVASÃO

Segundo Kevin David Mitnick, "Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: O hacker convencerá alguém a entrar no escritório e ligar aquele computador. Tudo é uma questão de tempo, paciência, personalidade e persistência." (PENSADOR, 2016).

Nesta sessão será definido algumas técnicas de invasão mais utilizada para roubo de dados, implantação de vírus, elevarem o trafego de informações em um site para derruba-lo, implementação de *malwares*, entre outros. Tais técnicas como, *spoofing* DNS, IP e ARP, *sniffers, exploits*, ataques DoS e DDoS, *war driving* e *war chalking* e técnicas para quebras senha.

3.2.1 SPOOFING, DNS SPOOFING, SPOOFING IP, SPOOFING ARP

Um ataque de *spoofing* é quando uma pessoa personaliza um dispositivo ou uma rede com finalidade de atacar uma rede, roubar dados, distribuir vírus para ter controle de acesso aos *hosts*, assim podendo realizar os diferentes tipos de ataque de *spoofing*, o *Internet Protocol* (IP), *Domain Name System* (DNS), e *Address Resolution Protocol* (ARP) (DUPAUL, 2016).

O *spoofing* por IP é um dos métodos de ataque mais utilizados. Neste ataque, o invasor envia pacotes IP a partir de um falso endereço de origem, a fim de se disfarçar. Ataques de negação de serviço, muitas vezes usar *spoofing* IP sobrecarregar as redes e dispositivos com pacotes que parecem ser de endereços IP de origem legítima (DUPAUL, 2016).

ARP é um protocolo que resolve os endereços IP para *Media Access Control* (MAC), ou seja, ele identifica o IP para transmissão de dados. Em um ataque *spoofing* ARP, o invasor envia mensagens ARP falsificadas através de uma rede de área local, a fim de vincular o endereço MAC do invasor com o endereço IP de um membro legítimo da rede. Os invasores costumam usar ARP *spoofing* para roubar informações, modificar dados em trânsito ou parar o tráfego em uma *Local Area Network* (LAN). Ataques de *spoofing* ARP também podem ser usados para facilitar outros tipos de ataques, tais como, sequestro de sessão e de negação de ataque *Man-in-The-Middle* (MITM), ou seja, instalam armadilhas entre o usuário e sites relevantes. ARP *spoofing* só funciona em redes locais que utilizam o *Address Resolution Protocol* (REAL PROTECT, 2015; DUPAUL, 2016).

O *Domain Name System* (DNS) é um sistema que associa nomes de domínios com endereços IP. Em um ataque *spoofing* servidor DNS, um invasor modifica o servidor DNS, a fim de redirecionar um nome de domínio específico para um endereço diferente. Em muitos casos, o novo endereço será para um servidor que esteja sendo controlada pelo

invasor e contém pastas infectados com *malwares*. Ataques de *spoofing* do servidor DNS são muito utilizados para espalhar *worms* e vírus (PC, 2016).

3.2.2 SNIFFERS

Sniffers são *softwares* utilizados para capturar pacotes que estão transmitidos em um segmento de rede, são de grande utilidade para o sistema de *Instrusion Detection Systems* (IDS), sistemas que identificam invasores na rede (TACIO, 2011).
O Sniffer é uma ferramenta de apoio para realização de análises de tráfego de informações e também é a ferramenta de ataques para furto de informações de dentro de um segmento de rede. Essa ferramenta funciona da seguinte forma, ela vê os pacotes que estão sendo transmitidos, captura os e analisa o conteúdo daquele pacote (ZANCANELLA, 2006).

Essa ferramenta tem maior facilidade em capturar pacotes em redes baseadas em *hubs*, o *hub* é um dispositivo que tem como finalidade de interligar computadores em uma rede, trabalhando de forma simples, recebendo os dados e transmitindo para as demais máquinas da rede (ALECRIM, 2004).

Segundo ZANCANELLA (2006), quando uma máquina é ligada no *Hub* e alguma informação é enviada para outra máquina primeira os dados vão passar por todas as portas do hub e consequentemente vão passar por todas as máquinas até encontrar a máquina de destino. Se alguma máquina estiver com um *Sniffer* instalado tudo o que for transmitido através da camada de rede será capturado pelo mesmo e exibidos para o usuário do *Sniffer*, os dados que são capturados são organizados por tipos de protocolos, *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP), *File Transfer Protocol* (FTP), *Internet Control Message Protocol* (ICMP), entre outros tipos.

Hoje existem diversos tipos de *Sniffers*, alguns são simples e com poucos recursos e outros há recursos avançados e são complexos e de difícil utilização, com possibilidade de geração de relatórios das análises da rede, o mais utilizado hoje é o *Wireshark.*

3.2.3 EXPLOITS

O *exploit* é um pedaço de *software*, dados ou uma sequência de comandos, este método tem como finalidade para descobrir vulnerabilidade e também para ganhar domínio sobre um sistema de computador, ou seja, tornar um defeito ou falha como vantagem (CANALTECH, 2016a).

Segundo CANALTECH (2016a), para fins maléficos, um exploit pode dar a um cracker o controle de um sistema de computador, permitindo a execução de determinados processos por meio de acesso não autorizado a sistemas, ou ainda realizar um ataque de negação de serviço. Os invasores têm como fins utilizar essas máquinas como *zumbie*, ou seja, usa-las para realizar ataques em grande escala seja para derrubar um servidor ou serviço, ou o invasor quer somente roubar informações da máquina que está sendo acessada.

3.2.4 ATAQUES DoS e DDoS

Os ataques *Denial of Service* (DoS) tem como objetivo derrubar, negar algum serviço que esteja sendo executado, porém não é feito com o objetivo de invasão, mas sim para torna-lo indisponível para usuário. Como por exemplo, tornar um servidor *web* indisponível enviando um enorme volume de requisições para uma página de um único endereço, caso o servidor não haja nenhuma regra de *Firewall* ou na aplicação para conter esse tipo de ataque, irá ocorrer um saturamento do serviço e o mesmo ficará indisponível (MORIMOTO, 2010).

Os ataques *Distributed denial of service* (DDoS) tem como objetivo o mesmo do DoS porém os ataques são lançados através de diversos *hosts,* ou seja, de diferentes lugares do mundo de forma simultânea. Os *hosts* controlados são chamados de *zumbie*, são as máquinas quais os *hackers* invadiram e implementaram *exploit*. Nesse caso de ataques DDoS é muito difícil conter pelo fato de serem endereços diferentes das requisições, nesta situação a empresa responsável por realizar os bloqueios é a empresa que administra os links de acesso (MORIMOTO, 2010).

3.2.5 QUEBRA DE SENHAS

Aplicar técnicas e métodos de segurança é um fator primordial para qualquer segmento que utilize esta tecnologia. Alguns procedimentos básicos, como inserção de senhas

complexas, evitam que qualquer pessoa, má intencionada, tente obter vantagens, ilicitamente, no uso das redes sem fio.

Para realizar a quebra de senhas *wireless* é utilizado o Sistema Kali Linux, que é uma distribuição GNU/Linux baseada no sistema operacional Debian, é um projeto *open source* que é mantido e financiado pela ofensiva de Segurança, um fornecedor de treinamento de segurança da informação de classe mundial e serviços de teste de penetração, ou seja, tem como finalidade voltada principalmente em auditoria e segurança de rede computadores (KALI LINUX, 2013).

Ainda segundo o site oficial do Kali Linux, existem diversas ferramentas disponíveis para realização de ataques, defesa e análise de dados, tais como NMAP (utilizado para realizar escaneamento de portas abertas), Wireshark (utilizado para capturar pacotes que estão trafegando pela rede), Aircrack-ng (software para realização de testes de segurança em rede sem fio), entre outras.

3.2.6 VÍRUS E MALWARES

Vírus é um *software* que infecta o sistema, se replicando e tentando se espalhar rapidamente para outros computadores, via e-mail, redes sociais, rede, dispositivos 39 plugados no computador como *pen drive*, discos rígidos externos, entre outros. Estes vírus têm como objetivo prejudicar o desempenho do computador podem causar danos ao sistema do computador, tais danos como, formatar o disco rígido, apagar arquivos do sistema ou arquivos do usuário e utilizar a memória do computador para torna-lo lento (STI, 2016).

Malwares é um termo utilizado para todos os *softwares* que se instalam nos computadores comandados para se infiltrar na máquina causar danos mais graves, como roubar informações e senhas divulgar serviços, entre outros (STI, 2016).

3.2.7 WARDRIVING E WARCHALKING

O termo *wardriving* foi escolhido por Peter Shipley para batizar a atividade de dirigir um automóvel à procura de redes sem fio abertas, passíveis de invasão. Para realização desta técnica é necessário um automóvel, um computador portátil, uma placa *wireless* USB para a captura dos pacotes de comunicação e uma antena com grande potencial

para poder identificar as redes existentes. O objetivo desta técnica é de mapear as redes sem fios sem segurança para uso e/ou também para identificar as redes sem fios e realizar ataques para obter informações de pessoas ou de uma empresa (DELAET; SCHAUWERS, 2004; WARDRIVING, 2013; PEIXOTO, 2016).

O *war chalking* é a prática de escrever símbolos indicando a existência de redes *wireless* e informando sobre suas configurações. As marcas usualmente feitas em giz em calçadas indicam a posição de redes sem fio, facilitando a localização para uso de conexões alheias pelos simpatizantes da ideia. Os praticantes desta técnica utilizam alguns símbolos e escritas para identificação das redes, o Open Node significa que a rede é vulnerável, *Closed Node* serve para uma rede fechada, e a letra W dentro do círculo informa que a rede wireless utiliza o padrão de segurança *Wireless Equivalent Privacy* (WEP), com presença de criptografia (DELAET, 2004; WARDRIVING, 2013; PEIXOTO, 2016). Em cima de cada símbolo, tem se o *Service Set Identifier* (SSID), que funciona como uma senha para o *login* na rede, obtidos através de *softwares* próprios conhecidos como *sniffers*. Esta prática se encontra em crescimento em vários lugares do mundo, particularmente na Inglaterra, onde ocorreu eventualidade em que estudantes utilizaram este meio para se reunirem e usaram a rede *wireless* de um escritório localizado no térreo de um edifício (DELAET, 2004; WARDRIVING, 2013; PEIXOTO, 2016).

3.2.8 IMPLICAÇÕES LEGAIS

Todos os praticantes da técnica *wardrivers* e *warchalkers* consideram se como uma organização e alegam ser totalmente legal o uso de ondas disponíveis no ar para realizar conexão com a Internet, mesmo que estas não sendo dos mesmos, ou seja, sendo de pessoas desconhecidas. O argumento utilizado como defesa dos praticantes é a garantia de liberdade de utilização de ondas de rádio presentes no espaço aéreo. Nos Estados Unidos, o órgão responsável pelas comunicações, o *Federal Communications Commission* (FCC) reservou as estações usadas por redes *wireless* para uso público, e esta falta de regulamentação é utilizada como princípio de legitimidade para a utilização de redes alheias que apresentam algum tipo de abertura na estrutura. Desde que não causem dano, os wardrivers e warchalkers acreditam atuar dentro da legalidade e moralidade (PEIXOTO, 2016).

Segundo PEIXOTO (2016), a utilização indevida de recursos de comunicação alheios configura ilícito penal no Brasil. Alguns dispositivos em nosso ordenamento jurídico já descrevem a tipicidade de atos advindos do *warchalking*, como o art. 155, § 3º do Código Penal, que define o chamado furto de sinal, o art. 151, que dispõe sobre violação de correspondência, principalmente em seus incisos II e IV e os artigos 186 e 927 do Novo Código Civil, que genericamente indicam a necessidade de ressarcimento em casos de danos a terceiros. Porém, é destacado a previsão específica do enquadramento das consequências do *wardriving* e *warchalking* no Projeto de Lei nº 84, de 1999, aprovado em Plenário da Câmara recentemente, que dá nova redação ao Código Penal Brasileiro.

A lei prevê o “acesso indevido”, a consequência de práticas de *wardriving* e *warchalking*, com a efetivação da ação de invadir uma rede *wireless*, apenando com detenção e multa o invasor de redes e sistemas informatizados.

3.2.9 PHISHING

Phishing é um método de fraude eletrônica, caracteriza-se por tentativas de adquirir informações restritas e de extrema importância, tais como senhas e números de cartão de crédito. Essas informações são adquiridas de forma qual uma pessoa se passar confiável ou se passa pela empresa enviando uma comunicação eletrônica oficial via e-mail principalmente e utilizando *web*sites maliciosos (BINDNER,2014; CANALTECH, 2016b; NORTON, 2016).

A Figura 13 é uma representação real de um e-mail encaminhado para um possível vítima do método *phishing*.

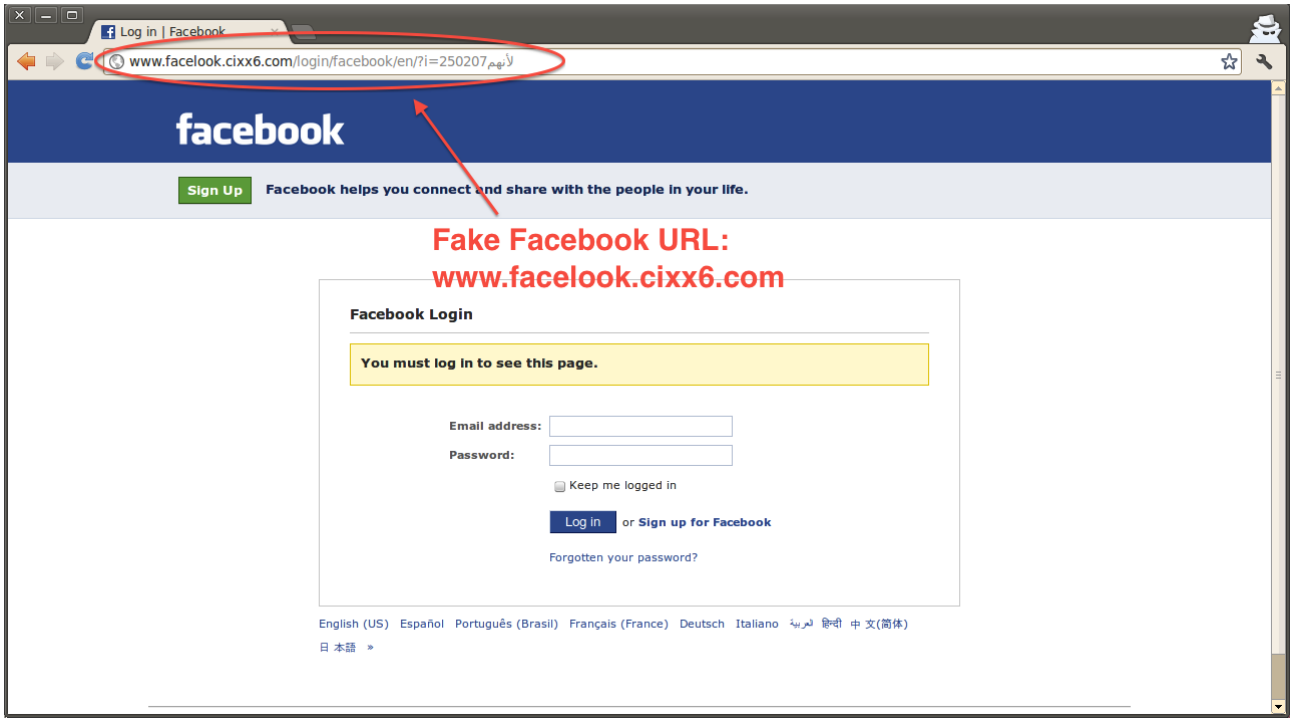

Figura 13: Representação de um Site Phishing

3.4 DESAFIOS E OPORTUNIDADES EM REDES DE COMPUTADORES

Na área de rede de computadores as oportunidades são grandes, pois a quantidade de pessoas capacitadas para as oportunidades são poucas (LEITE, 2015), segundo NASCIMENTO (2013).

*A falta de mão de obra qualificada para atender o mercado preocupa. Estudo realizado pela da consultoria IDC, encomendado pela Cisco na América Latina, aponta que a demanda por profissionais de tecnologia da informação e comunicação (TIC) no Brasil excederá a oferta em 32% para o ano de 2015, chegando a uma lacuna de 117.200 trabalhadores especializados em redes e conectividade (*Priscila Nascimento, 2013*).*

A maioria das pessoas formadas na área de computação seguem a área de desenvolvimento de software, hardware e banco de dados, poucos seguem na área de redes por falta de contato e prática.

4 KALI LINUX: TESTE DE INTRUSÃO E AUDITORIA DE SEGURANÇA

O objetivo desse capítulo é falar sobre o sistema utilizado na pesquisa, Kali Linux, e a metodologia utilizada por um hackers ao realizar um pentest, teste de vulnerabilidade ou até mesmo uma invasão real. A metodologia exige algumas etapas indispensaveis para que um ataque, feito por profissional ou criminoso, seja bem-sucedido. As etapas são, reconhecimento, scanning, exploração de vulnerabilidades, preservação de acesso e geração de relatórios, no qual será abordado mais a frente.

O Kali Linux é a mais nova distribuição de segurança Linux disponibilizada pela *Offensive* Security, utilizando como base a distribuição Debian 7.0, o Kali Linux compõem mais de trezentas ferramentas de segurança e de testes de invasão classificadas em grupo. O Kali Linux é a continuação da linhagem do BackTrack, que é um sistema com os mesmos objetivos do Kali Linux (KALI LINUX, 2013; BINDNER, 2014).

4.1 TESTE DE VULNERABILIDADE

Teste de vulnerabilidade é um método legal realizado por profissionais autorizadas com a finalidade de descobrir fraquezas presentes na rede que está sendo aplicado os testes (TERZI, 2015).

Segundo LUCHI (2013) e TERZI (2015), existem diferentes tipos de técnicas de penetração, tais como, *Blind* ou *Black Box* onde o auditor não conhece o alvo dos testes mas o alvo 47 sabe quais testes são executados; o *Double Blind, Gray box, Double Gray Box, Reversal ou White Box e o Tandem.*

Double Blind esta técnica é bem parecida com a anterior porém nenhum dos lados tem conhecimento, ou seja, o auditor não conhece o alvo e nem o alvo conhece os testes que serão realizados. O *Gray Box* nesta prática o auditor conhece parcialmente o alvo, como se fosse um funcionário insatisfeito com a empresa e o mesmo quer realizar um ataque. O *Double Gray Box* funciona da mesma maneira que o anterior porém o alvo tem conhecimento dos ataques que serão realizados. O *Reversal* ou *White Box*, o auditor tem total conhecimento infraestrutura, usuários e sistemas do alvo. E o *Tandem* funciona da

mesma maneira que o anterior, porém o alvo tem total conhecimento sobre o ataque que ocorrerá (LUCHI, 2013; TERZI, 2015).

*Na realiza*ção de teste de penetração, ou teste de intrusão existem cinco etapas a serem seguindas, a ultima etapa pode ser alterada, depende do tipo de *hacker*. As tais cinco etapas que serão tratadas são, o reconhecimento, scanning, exploração de falhas, preservação de acesso e geração de relatório.

4.1.1 RECONHECIMENTO

Nessa fase o auditor terá de aprender tudo sobre a rede e a empresa que serão aplicado os teste. Nessa fase o auditor não realiza nenhum tipo de penetração no sistema de defesa do alvo, somente identifica e documenta as informações do alvo (BINDNER, 2014).

4.1.2 SCANNING

Nessa fase o auditor irá utilizar as informações coletadas na etapa anterior para coletar novas informações, utilizando uma ferramenta de *scanning* assim possibilitando obter mais informações sobre a infraestrutura do sistema e sobre a rede do alvo (BINDNER, 2014).

4.1.3 EXPLORAÇÃO DE FALHAS

Após a utilização das ferramentas de *scanning* é possível detectar falhas, a partir da descoberta de falhas nessa etapa o *hacker ético* explora a falha no sistema para entrar no sistema e sair com as informações que deseja sem ser notado e sem deixar rastros para que posteriormente seja identificado uma invasão (BINDNER, 2014).

4.1.4 PRESERVAÇÃO DE ACESSO

Após a identificação da vulnerabilidade e a invasão ter sido realizada o auditor deixa anotado todos os passos realizado e o mesmo deixa portas abertas de forma que o alvo não desconfie para que se haja a necessidade de haver um futuro acesso o mesmo não precise explorar novamente a rede (BINDNER, 2014).

4.1.5 GERAÇÃO DE RELATÓRIOS

Após a realização de todas as etapas anteriores, o auditor irá documentar diversos relatórios de cada etapa realizada. Depois da criação dos relatórios estes são enviados a uma equipe que solucionará o problema para não haver outra ocorrências (BINDNER, 2014).

4.2 PRINCIPAIS FUNCIONALIDADES E RECURSOS

Em cada fase do teste de penetração, é necessário o uso de ferramentas específicas do Kali Linux e algumas técnicas. A seguir será apresentado a ferramenta NMAP que será utiliizada no trabalho como ferramenta principal e outros que também podem ser utilizadas.

Nmap, é uma ferramenta livre e *open source* para a descoberta de rede e auditoria de segurança, é utilizado para descobrir serviços ou servidores em uma rede, identificar *host* conectados à rede, scanner de portas TCP e UDP abertas, detecção de sistema operacional determinando o sistema e as características de *hardware* do *host*, detecta versão de serviços e aplicações na rede, entre outras funcionalidades (KALI TOOLS, 2014c).

Nmap utiliza pacotes IP brutos de novas maneiras para determinar o que está disponível na rede, que serviços estão oferecendo, o que os sistemas operacionais eles estão executando, que tipo de filtros de pacotes e 50 firewalls estão em uso, e dezenas de outras características. Ele foi projetado para digitalizar rapidamente grandes redes, mas funciona bem contra redes individuais(NMAP.ORG).

Nmap foi nomeado "Segurança Produto do Ano" pelo Linux Jornal, Info Mundial, LinuxQuestions.Org e Codetalker Digest. Foi ainda apresentado em doze filmes, incluindo The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum (LINUX JOURNAL).

Nikto2 é uma ferramenta para realizar varreduras de vulnerabilidade, ou seja, realiza buscar por falhas de segurança na rede, informa descoberta de host e além dele detectar a vulnerabilidade o mesmo explora e gerando resultados. A ferramenta não vem acoplada com o Kali Linux ela é instalada de forma gratuita (CIRT, 2017).

Metasploit é uma ferramenta desenvolvida por H.D. Moore, ela possui diversos *exploits*, *payloads* para realização de testes de vulnerabilidade de sistemas, plataformas, servidores, entre outros (ARAGÃO, 2011).

Existem inúmeras ferramentas para realizar testes de falhas de segurança, cada uma tem sua funcionalidade mas podem ser utilizadas em diferentes ambiente de testes, porém existem as que são especificas para um determinado ambiente. As ferramentas apresentadas nesse capítulo podem ser utilizadas em qualquer ambiente de teste.

5. DESENVOLVIMENTO DO PROJETO

Neste capítulo será utilizado um site considerado livre para hackear (Safe To Hack), Testphp Vulnweb foi o site escolhido, desenvolvido pela empresa Acunetix. Nesse capítulo será apresentado alguns tipos de analíses, as analíses mais comuns que são realizadas por invasores. Assim como formas de defesa com intuito de previnir o maxímo possível de invasão a uma empresa ou computador doméstico.

Para realização dos processos de detecção de falhas de segurança foram utilizadas diversas ferramentas, para realizar o reconhecimento irá ser utilizado o Nmap. E para a defesa será abordado sobre alguns software como firewall e outras medidas a ser tomadas para uma maior segurança na rede.

5.1 ETAPAS DE ATAQUES

Nesse capítulo será tratado o processo foi dividido em três etapas, para iniciar a análise do ambiente primeiramente foi realizado a etapa de reconhecimento do ambiente que será atacado, ou seja, coletado as informacões necessárias para realizar o ataque. A segunda e ultima etapa é a análise dos resultados coletados para demonstração das possíveis formas de penetrar no sistemas através das falhas.

5.1.1 RECONHECIMENTO

Nessa etapa foi utilizado o NMAP, que é um software de escanemento de ambientes, que tem como objetivo detectar portas abertas, versões de sistemas, entre outros, que facilitam a entrada do atacante.

A ferramenta NMAP permite que utilizemos tanto o link personalizado (exemplo: www.google.com.br), como também o IP. É recomendo que se utilize o IP pois traz mais precisão e qualidade para a varredura. A figura 14 ilustra uma forma facíl e rapida de descobrir o IP de um site utilizando o comando **ping.**

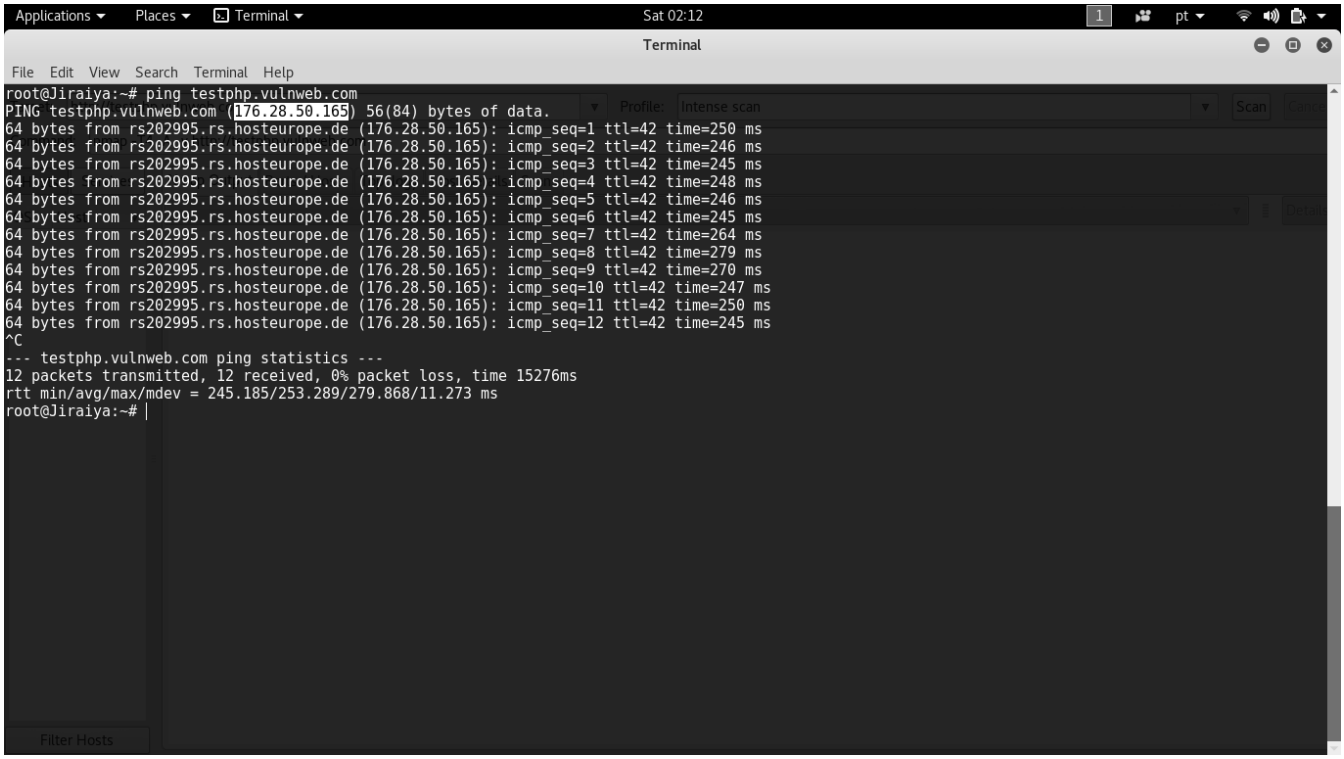

Figura 14: Descobrindo o IP.

A Figura 15 ilustra o inicio de uma varredura, foi utilizado o seguinte comando **nmap -T4 -A -V ENDEREÇO_IP**. Esse comando irá listar todas as portas descobertas, qual é o tipo de serviço correspondente a mesma, topologia e rota pelo qual o sistemas passa e muitas outras informações sobre o sistema.

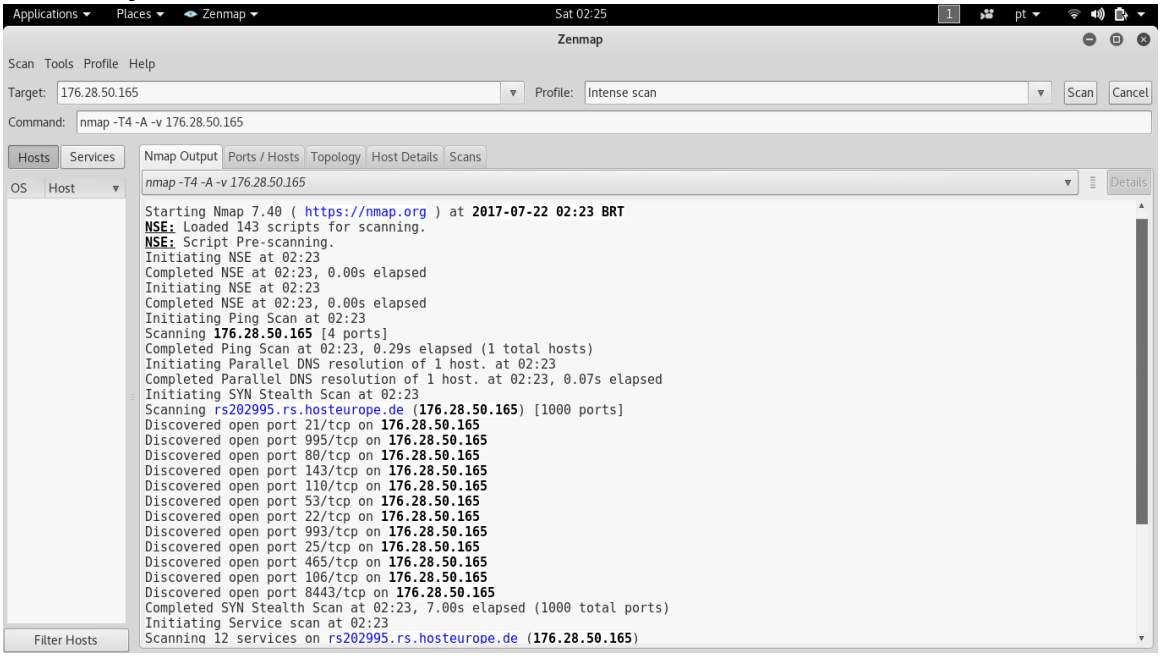

Figura 15: Inciando varredura com NMAP.

Todo sistema que esteja sendo utilizado existem portas pelo qual recebem e enviam pacote de dados, as imagem 16 mostrará as portas scaneadas assim como algumas informações sobre elas como a porta, estado, serviço, versão.

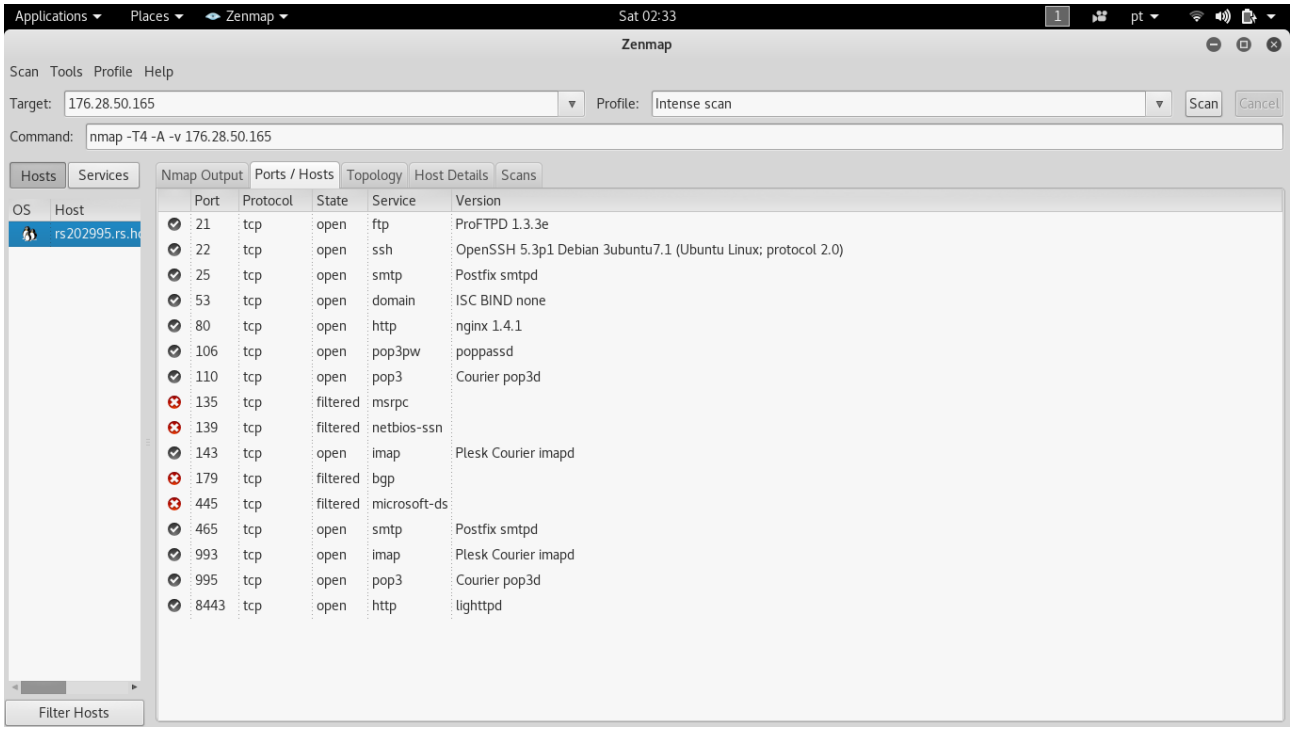

Figura 16: Informações sobre todas as portas scaneadas.

Outras informações que o NMAP pode trazer é a versão do sistema do alvo, o estado, o último boot, nome do domínio. Todos essas importantes informações serão ilustradas na imagens 17.

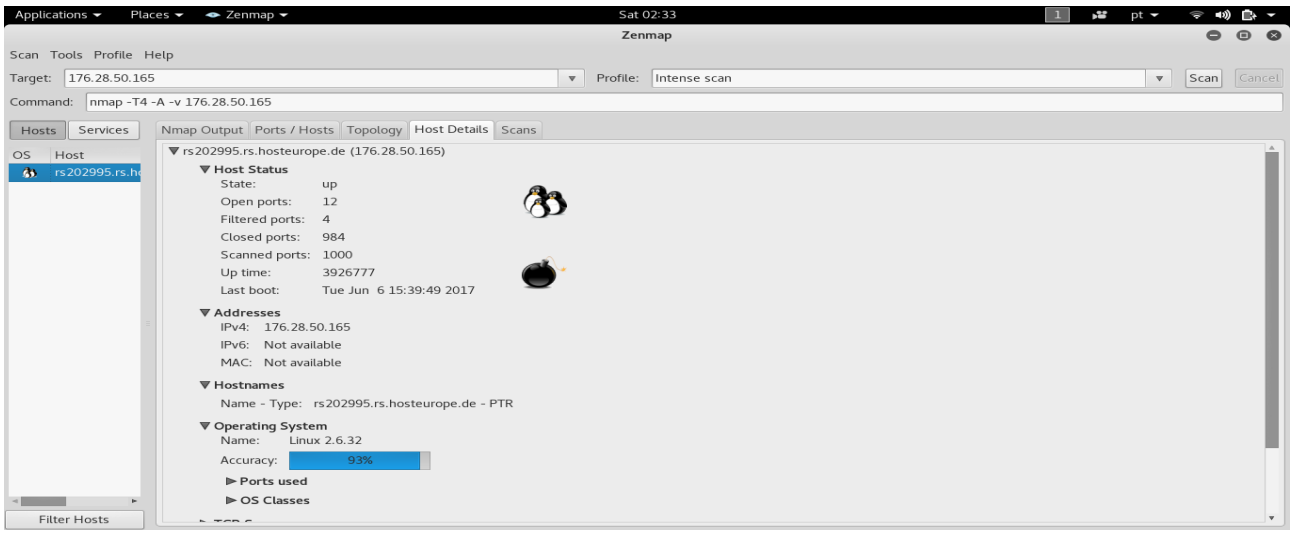

Figura 17: Detalhes do Alvo.

Umas das informações mais importantes para um ataque é saber a rota utilizada pelo roteador, o nmap conseguer nos trazer a topologia e a rota feita do computador invasor até o computador alvo. A figura 18 ilustra de forma clara e objetiva o caminho completo.

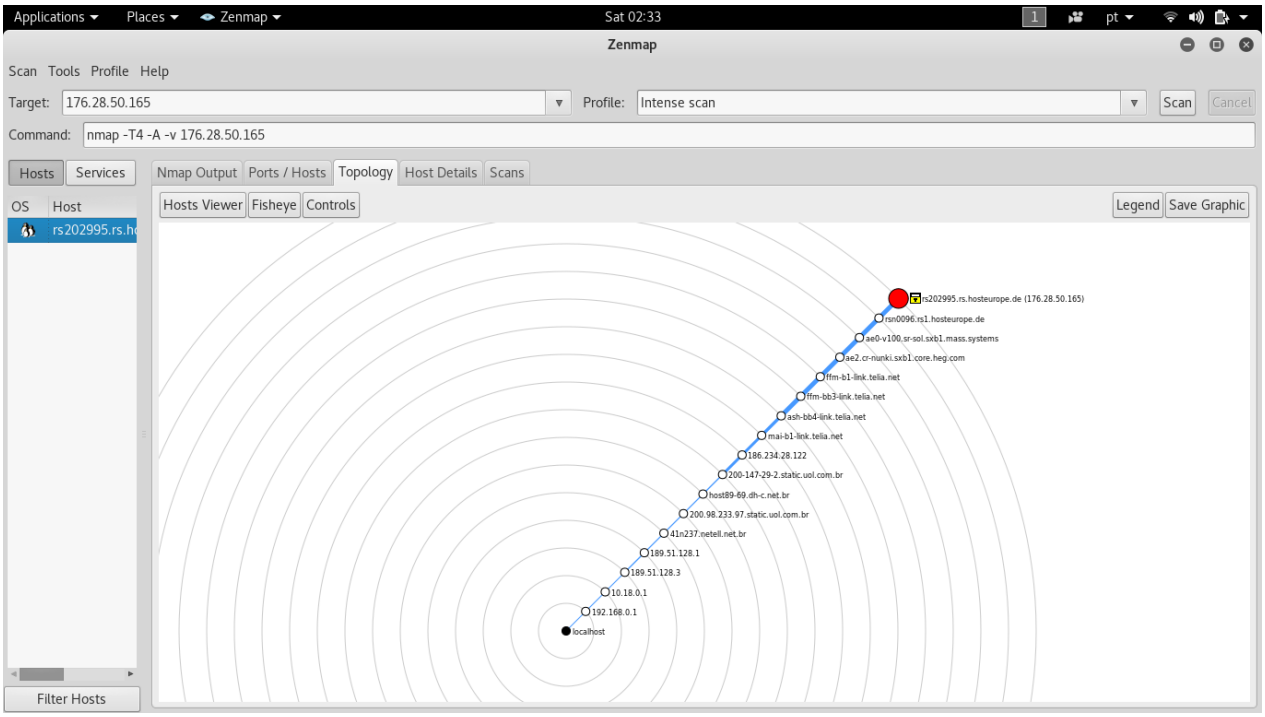

Figura 18: Topologia e Traceroute.

5.1.2 ANÁLISE DOS RESULTADOS

A partir da coleta das informações realizada e apresentada na sessão anterior (5.1.1) realizou-se a análise das mesmas para saber um possível tipo de ataque, os tipos das portas que foram descobertas, isso irá ajudar em qual ataque pode ser realizado e qual ferramenta será utilizada por um invasor.

Na Figura 16 pode-se observar as portas que foram descobertas, sendo as, 21(*File Transfer Protocol* (FTP)), 22 (*Secure Shell* (SSH)), 53(domain), 80(http), 106(pop3pw), 110 (pop3), 143 (imap) e 465 (smtp), 993(imap), 995(pop3), 8443(http), nas Figuras 15, 17 e 18 são apresentadas mais informações, além das portas que foram descobertas, com os parâmetros utilizados juntamente ao comando foi possível adquirir mais informações tais como, a versão do serviço do samba (serviço de compartilhamento de arquivos)

instalado, versão do sistema operacional instalado, versão do SSH e FTP, serviço *web* Apache, entre outras informações.

Em cada uma dessas informações podem haver falhas na seguranças, nas portas, versões desatualizadas de sistemas, no próximo tópico iremos abordar as possíveis falhas no sistemas com auxílio da ferramenta *Nikto*.

5.2 POSSÍVEIS FALHAS E FORMA DE INVASÃO AO SISTEMA

Umas das portas abertar é a 80 que em 99% das vezes é um porta utilizada pelo HTTP/HTTPS (protocolo de transferência de HiperTexto), usada para transferir páginas WWW. Caso o sistema estiver com o firewall desativo ou até mesmo mal configurado, seria facíl aplicar um *exploit* (usando a ferramenta metasploit) feito para tomar o sistema e ter acesso ao shell.
Segundo o NMAP existe 93% de chance de o site estar alocado em um servidor com Linux, e pela alta porcentagem de segurança de um sistema assim podemos dizer que existe uma segurança boa quanto ao firewall, de qualquer forma poderiamos usar um exploit com script feito para burlar essa barreira.

Por outro lado a porta 21 (File Transfer protocol - Protocolo de transferência de arquivo) aberta, uma porta usando para transferência de arquivos e dependendo do site pode ser um facilidade imensa a invasão por essa porta, pois a maioria dos sites usando uma senha padrão de FTP (admin:admin, anonymous:anonymous). De qualquer forma caso a senha e login seja modificada poderiamos usar ferramentas de Brute Force (quebra de senha por tentativa), como a Hydra, Jhon The Ripper, assim quebrando a senha e modificando os arquivos do site.

A figura 19 ilustra a utilização da porta FTP para realizar o logon em um site.

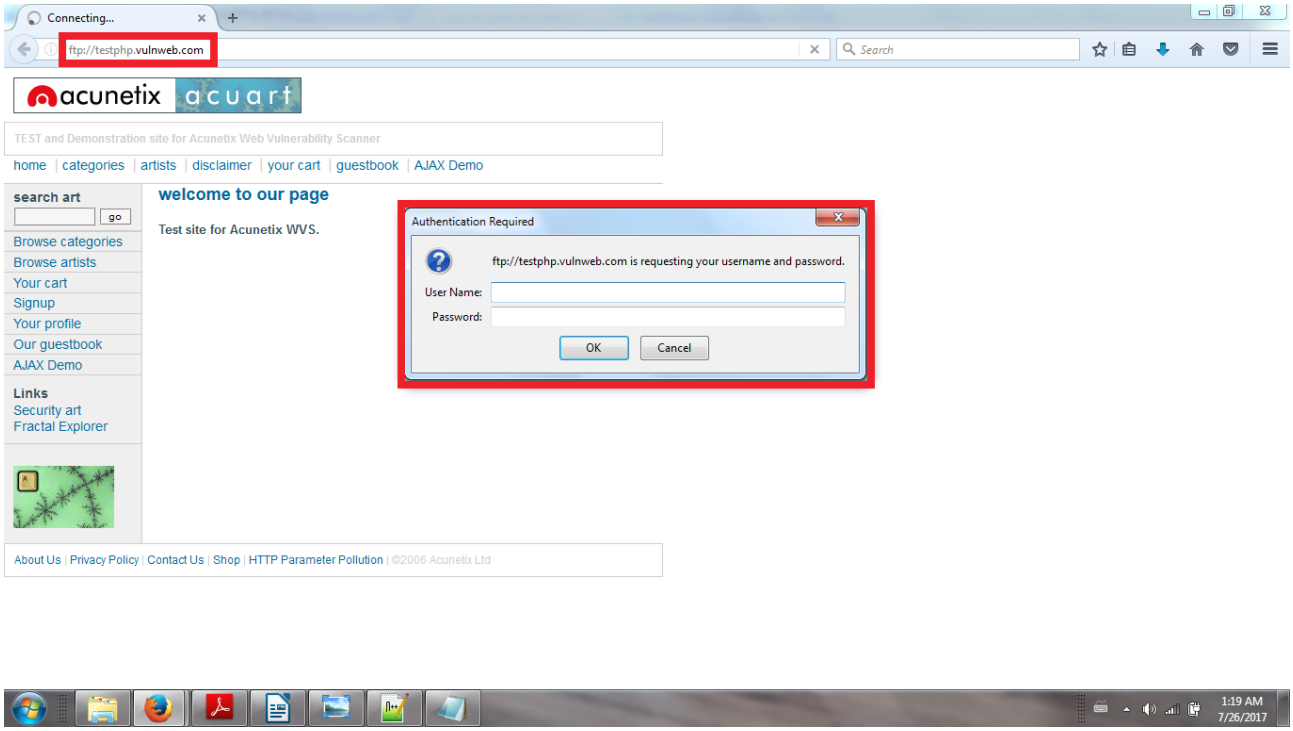

Figura 19: Ilustração de login pela porta 21 (FTP).

5.2.1 ANALISANDO FALHAS COM NIKTO

Nikto é um web server scanner de codigo aberto (Open Source) patrocinado pelo *Netsparker* que executa testes abrangentes contra servidores web em vários aspectos, incluind mais de 6700 arquivos/programas perigosos, checa versões desatualizadas de mais de 1250 servidores, e problemas especificos de mais de 270 servidores. Também análise por falhas nas confugurações do sistema em busca de vulnerabilidades em arquivos, opções de server HTTP, e tentará identificar servidores e softwares instalados.

Na imagens 20 poderemos ver o scaneamento feito com Nikito e todas as falhas/informações coletadas para que se possa realizar um ataque ao sistema alvo.

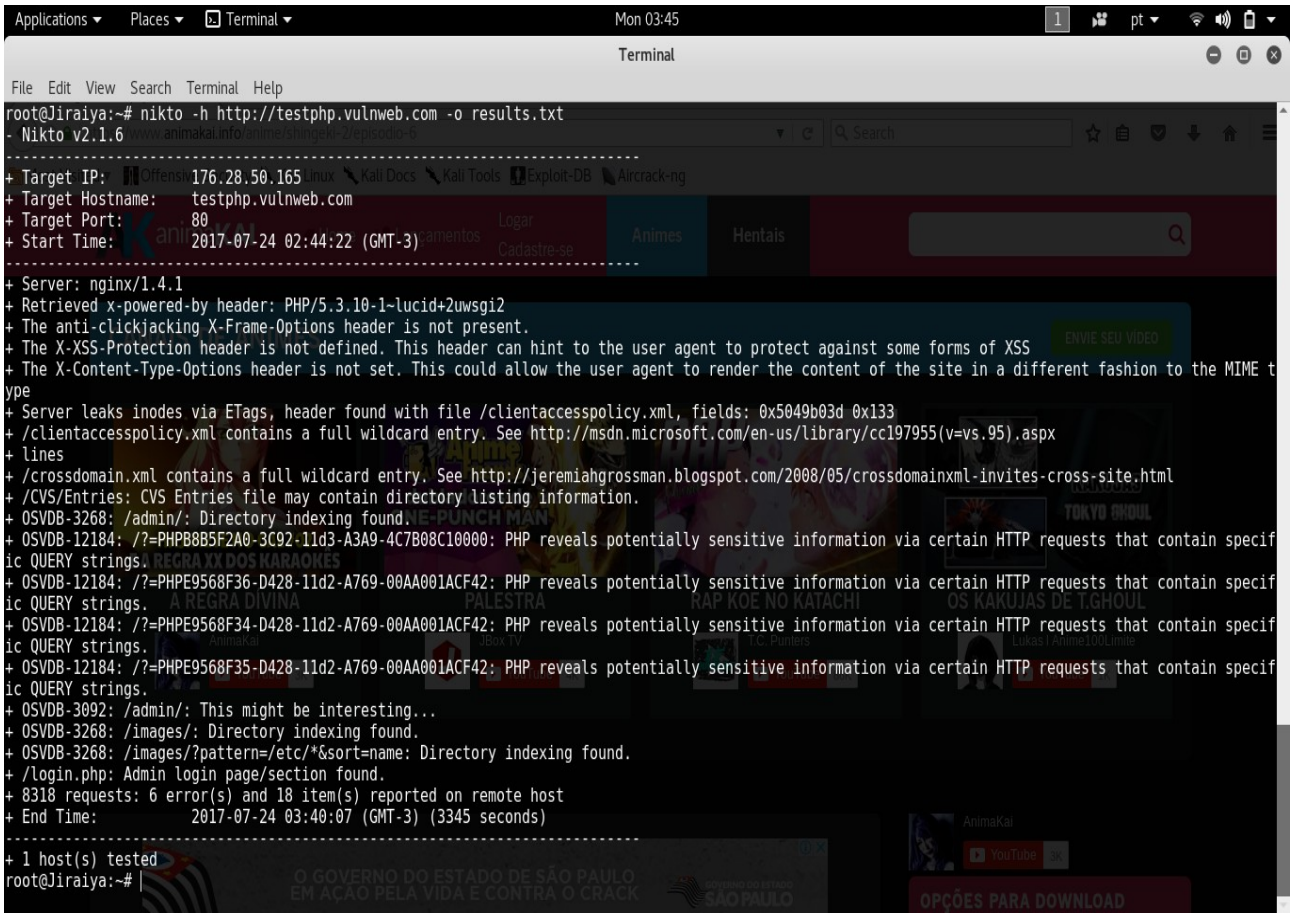

Figura 20: Ilustração do escaneamento com Nikto.

Na imagem 20 pode-se ver logo de início algumas informações como a versão do PHP, com base nisso basta pesquisar algumas falhas baseadas nessa versão usada pelo site.

O PHP existem algumas falhas que em versões mais recentes foram corrigidas, mas, nesse caso sabemos que quando utilizado em modo CGI existem uma possibilidade de chamar parâmetros diretamente pela URL, exemplo: http://localhost/index.php?-s, o servidor executaria o PHP com o parâmetro -s, que exibe o código fonte do arquivo, e não o HTML gerado por ele. Só isso seria um problema suficiente (afinal, é comum inserir dados como senhas do banco de dados no código fonte), mas o time de hackers que descobriu a falha também percebeu que ela permite inserir código malicioso no arquivo e executá-lo(Paulo Graveheart).

Outra falha nessa versão no PHP apareceu após tentarem atualizar a segurança com ataques DoS, os desenvolvedores limitaram o número de parâmetros de entrada para mil. Devido aos erros de implementação, os hackers podem intencionalmente exceder esse

limite e injetar e executar código. O bug é considerado crítico já que o código pode ser injetado remotamente através da web(Allison, 2012).

Clickjacking é um tipo de ataque no qual o invasor modificar um botão de uma pagina através da injeção de um código direcionando para algum tipo de armadilha ou outra pagina maliciosa, pode-se ver na imagem 20 que este site é vulneravel a este tipo de ataque. Utilizando essa falha na segurança pode se roubar dados, colocar virús na na vitima que cair nessa armadilha e outros tipos de perigos (Owasp). A imagem 21 representa um ataque Clickjacking.

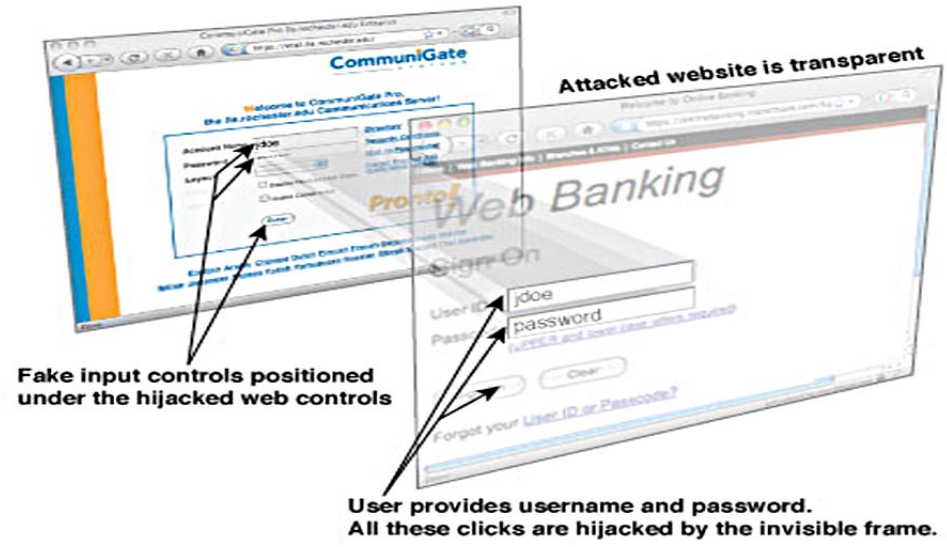

Figura 21: Representação de um ataque Clickjacking.

Outras vulnerabilidades estão presentes nesse site com uma versão desatualizada só Silverlight 4 que é utilizado para a comunicação entre domínios. Esse tipo de aplicação necessita de proteção contra vários tipos de vulnerabilidades na segurança que podem ser usadas para explorar aplicativos na Web como Cross-site scipting (XSS), ele manipula domínios através de códigos javascript que executa comandos não autorizados.

Nikto também nos traz outras informações sobre vulnerabilidades e como previni-las, na imagem 21 podemos ver algumas linhas indicando exploit que podem ser usando e um diretório específico, por exemplo: OSVDB-3092: /logs/: This might be interesting…

Isso é considerado um vulnerabilidade que pode ser atacada com o exploit econtrado no fórum OSVDB artigo 3093, e pode ser corrigido modificando algumas configurações no apache. Ele está dizendo que encontrou algumas possíveis vulnerabilidades e o site está rodando PHP-Nuke e Vbulletin, se você quer rodar esta aplicação, tenha certeza que está tudo totalmente atualizado.

5.2.2 FORMAS DE CORRIGIR VULNERABILIDADES

Para corrigir as vulnerabilidades encontradas pelo Nikto pode variar de acordo com os resultados, neste caso existe algumas modificações a ser feitas, como:

- Modificar as opções do apache;
- Instalar um modulo de segurança (Alta recomendação);
- Verificar se o PHP e aplicações web estão restritas pelo usuario MySQL
- Fazer verificações com outros aplicativos como Nessus e OpenVAS.

5.3 DEFESA

O recurso de segurança mais utilizado para garantir a integridade dos dados que trafegam pela rede tanto em ambiente corporativo como o doméstico é o *firewall*. Em geral, ambientes corporativos utilizam-se de um servidor *firewall*, tendo como exemplo um servidor exclusivamente dedicado para este *firewall* o qual conterá todas as regras de gerenciamento e segurança da rede.

Segundo ALECRIM (2013), *firewall* é uma solução de segurança baseada em *hardware* ou *software* que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede é possível determinar quais operações de transmissão ou/e recepção de dados podem ser executadas. O *firewall* sempre se encontrará entre a rede interna e a rede externa (*Internet*), a Figura 22 ilustra a funcionalidade do *firewall* em uma rede.

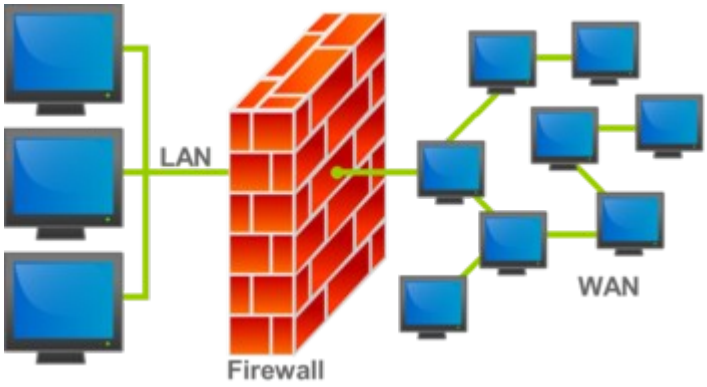

Figura 22: Ilustração do funcionamento de firewall.

Na maioria das empresas é utilizado um servidor com sistema operacional de distribuição Linux, normalmente é utilizado a distribuição Debian, pelo fato de não ter muitos pacotes, *softwares*, serviços executando, ou seja, os serviços que serão utilizados devem ser instalados ou compilados. Após a instalação do servidor *firewall,* são aplicadas regras de *iptables* para defender o sistema de ataques.

Iptables foi concebido por Rusty Russel, é um sistema de controle de filtros para protocolos de rede, são divididas em três tipos, a *Filter*, NAT (*Network Address Translation*) e *Mangle* (NETO, 2004).

A tabela *Filter* é a padrão, onde são aplicadas as regras de filtro de pacotes da rede, é dividida em três conjuntos, INPUT utilizada para analisar tudo o que chega para o *firewall*, FORWARD é utilizada para redirecionar todas as solicitações para servidores ou *interface* de rede e OUTPUT analisa os pacotes que estão sendo gerados para sair do *firewall* (NETO, 2004).

A tabela NAT (*Network Address Translation*) é utilizada para alterar características de origem ou destino de um pacote, ou seja, utilizando ela pode encaminhar um pacote para outro destino. Dentro a mesma as regras são divididas em três conjuntos PREROUTING utilizado para analisar os pacotes que estão entrando pela *interface* de rede, POSTROUTING utilizado para analisar os pacotes que estão saindo pela *interface* de rede e OUTPUT utilizado para analisar os pacotes que estão sendo gerados pela própria máquina (NETO, 2004).

E por fim a tabela *Mangle* é utilizada para especificar ações para o tratamento do tráfego dos pacotes que atravessam as tabelas, ou seja, é utilizada para marcar os pacotes. Sendo dividida em dois conjuntos, PREROUTING modifica os pacotes dando um tratamento 65 especial antes que os mesmos sejam roteados e OUTPUT altera os pacotes gerados localmente antes que os mesmos sejam roteados (NETO, 2004).

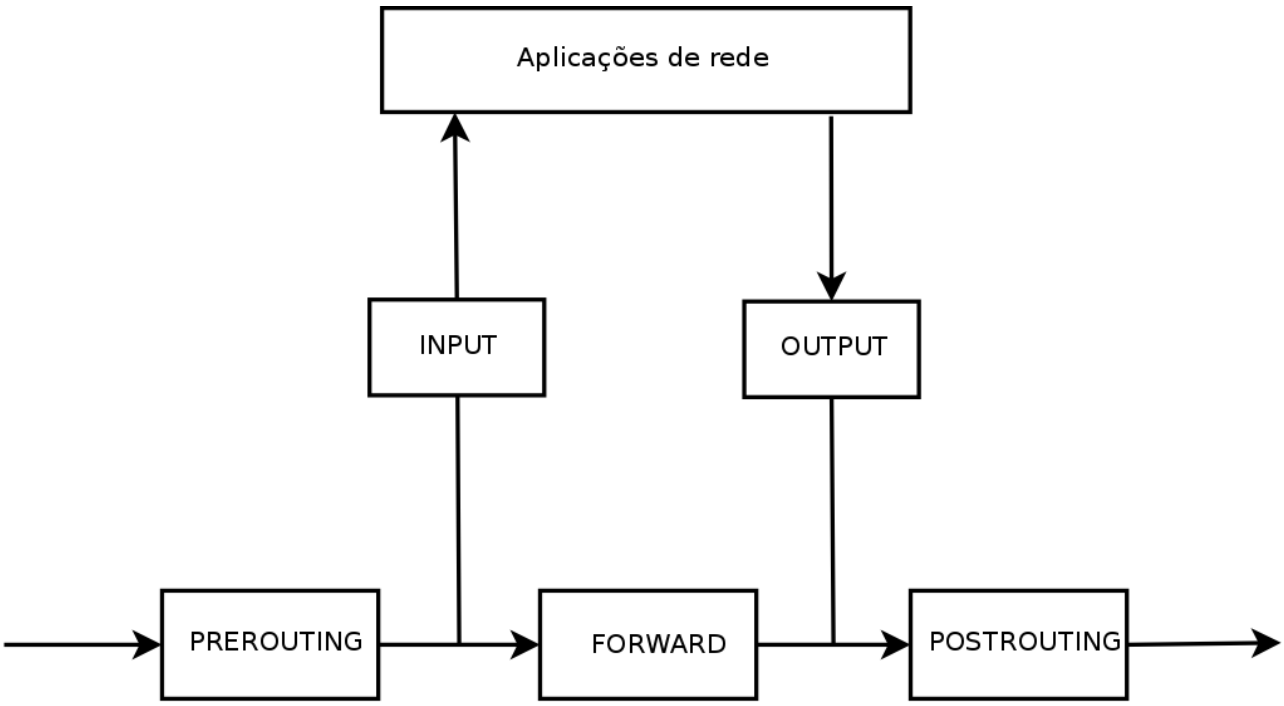

Figura 23: Ilustração do funcionamento das tabelas.

Firewalls de software são programas que podem ser instalados no seu computador, baixá-los diretamente de um site ou carregá-los a partir de um CD ou DVD. Os firewalls de software são por vezes incluídas como parte de um pacote de segurança na internet. Norton Internet Security e Kaspersky Internet Security, por exemplo, ambos vêm com um firewall. O pfSense é um software livre, licenciado sob BSD license, baseado no sistema operacional FreeBSD e adaptado para assumir o papel de um *firewall* e/ou roteador de redes.[1] Ele possui recursos que muitas vezes, só encontrada em firewalls comerciais caros.

Firewalls de hardware são mais caros do que os de software e são comumente usado em redes acessadas por vários computadores. O site TI Evalue observa que eles "têm a vantagem de ser separado do seu computador, se o seu computador pegar um vírus que

poderia desativar o firewall . " Os firewalls de software são adequados para a maioria dos usuários domésticos , e algum software de firewall pode incluir um bom nível de proteção contra vírus e spyware.

5.3.1 DEFESA DE ENGENHARIA SOCIAL

Engenharia social é termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações

A palestra do ex-hacker e especialista em segurança Kevin Mitnick, considerado ídolo pelos aficcionados por tecnologia, foi o ponto alto do segundo dia da Campus Party. Mitnick chegou a ser preso por suas atividades e hoje é consultor de segurança digital para empresas.Segundo ele, os hackers de hoje enganam as pessoas para conseguir informações pessoais e seus ataques são um misto de engenharia social e conhecimento de software. A engenharia social, método para convencer pessoas a revelar suas informações pesooais e vitais, é a forma mais simples para conseguir dados e lesar os incautos. Como ainda não inventaram remédio contra ingenuidade (ou burrice, nas palavras de Mitnick), o método continua eficaz.Segue um pequeno resumo sobre o que NÃO fazer para estar menos vulnerável a ataques de hackers:

- Confiar em qualquer pesquisa que peça dados pessoais (pode fornecer informações que facilitem o roubo de identidade e dados para revelar senhas, como, por exemplo, o nome do animal de estimação);
- Fornecer senhas por meios eletrônicos (telefone, e-mail, etc);
- Digitar senhas em computadores públicos;
- Publicar informações pessoais em redes de relacionamento;
- Acreditar em tudo que chega pelo e-mail;
- Ligar para números de telefone informados por fontes que não sejam oficiais (centrais telefônicas de bancos, por exemplo - há centrais falsas que capturam as senhas digitadas);
- Confiar em redes sem fios abertas;

- Abrir arquivos de Office ou PDF de fontes desconhecidas;
- Deixar a função *autorun* do Windows habilitada (uma mídia removível - pendrive, CD, DVD... - consegue infiltrar arquivos contaminados no computador);
- Confiar demais nas pessoas - hackers exploram a boa vontade dos outros para conseguir dados;
- Pensar que esse tipo de roubo de informações só acontece com os outros;
- Conceder o "benefício da dúvida" (confiança inicial) às pessoas;
- Ser descuidado com o próprio lixo físico, deixando disponíveis nome, números de documentos, endereços, etc.

Mitnick também enfatizou que deve-se prestar atenção em quem pede suas informações. Enquanto não souber exatamente quem quer seus dados, negue tudo.

"Mesmo quando o usuário classifica a informação como restrita nas redes sociais, o mundo pode ver. Até um amigo seu pode passar informações para um criminoso sem saber".

6. CONCLUSÃO

Com base em no capítulo 1 pode-se ver a alta necessidade da segurança da informação através das estatisticas realizadas por site como Linux Journal e We Are Social, que liga diretamente com o objetivo do trabalho para informar pessoas desse perigo. Já no capítulo 2 mostramos os aspectos gerais sobre a segurança da informação, alguns fundamentos, técnicas, métodos, além de algumas vulnerabilidades. Assim possibilitando ligar com os fundamentos de redes de computadores no capitulo 3, todos os aspectos de segurança digital. No capítulo 4 tem como objetivo mostar as etapas usadas por profissionais da segurança ao realizar um pentest ou análise de vulnerabilidades, no qual foi usado no trabalho. E por último o capítulo 5 apresenta-se o desenvolvimento do trabalho, técnicas, metodologias, ferramentas, resultados e outras informações sobre a pesquisa.

A partir do conhecimento adquirido durante o desenvolvimento dessa pesquisa é possível afirmar que a maior preocupação hoje de empresas e pessoas comuns é a segurança das informações que as mesmas armazenam, disponibilizam e adquirem. Apesar de que a maioria das empresas de porte médio/pequeno já consideram os riscos e os prejuízos que uma invasão pode causar, muitas delas ainda não investem na segurança das informações.

No desenvolvimento do projeto, foram encontradas dificuldades em encontrar matérias em uma linguagem mais comum, pois a maioria do conteúdo é descrito em russo e inglês. Além disso, modelar e simular um ambiente real para apresentar os fatores que facilitam a invasão.

Por fim, com o desenvolvimento desse projeto e com todos os acontecimentos divulgados na *Internet*, em um futuro próximo o investimento na segurança de informações e na capacitação de pessoas na área será muito maior por conta dos fatores apresentados no decorrer do projeto.

Com todo conhecimento adquirido ao longo dessa pesquisa, outras pesquisas específicas podem ser desenvolvidas na area da segurança digital, tais como, análise de crimes ciberneticos com computação forense, explorar a engenharia social mais profundamente com intuito de expor como funcionar *A Arte de Enganar* utilizada por

hackers não éticos, e até mesmo analisar novos sistemas de segurança com design mais familiar e amigá para ajudar usúrios mais leigos.

Conclui-se, por tanto, que o projeto apresentou o quanto é importante investir em segurança das informações tanto empresariais quanto pessoais, que hoje o número de invasões em empresas principalmente vem crescendo a cada dia e mostra o quanto as empresas estão despreparadas em questões de segurança de dados.

REFERÊNCIAS

AEON. **Segurança da informação: entenda os riscos e consequências de perder seus dados**. Disponível em <http://www.aeon.com.br/seguranca-da-informacao-entenda-os-riscos-e-consequencias-de-perder-seus-dados>. Acesso em 08/07/2017.

ALECRIM, Emerson. Info Wester, 2013 **O que é firewall?.** Disponível em <http://www.infowester.com/firewall.php>. Acesso em 09/07/2017.

ARAGÃO, Francisco. **Metasploit – Sabe o que é?.** Pplware no coments, 2011. Disponível em <http://pplware.sapo.pt/internet/metasploit-sabe-o-que-e/>. Acesso em 09/07/2017.

AZEVEDO, Caio de Avelar. **Cabos**. 2011. Disponível em <http://basicoderedes1.blogspot.com.br/2011/08/cabos.html>. Acesso em 08/07/2017.

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

CANALTECH. **O que é Exploit?.** Canaltech, 2016a. Disponível em <http://canaltech.com.br/o-que-e/o-que-e/O-que-e-exploit/>. Acesso em 09/07/2017.

CANALTECH. **O que é Phishing Scam?.** Canaltech, 2016b. Disponível em <http://canaltech.com.br/o-que-e/*hacker*/O-que-e-Phishing-Scam/>. Acesso em 09/07/2017.

GALLO, Michael A.; HANCOCK, W. M. **Comunicação entre Computadores e Tecnologias de Rede.** São Paulo, 2003.

GIAVAROTO, Sílvio César Roxo; SANTOS, Gerson Raimundo dos. **Kali Linux – Introdução ao Penetration Testing**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2015.

KALI TOOLS. **Nmap Package Description.** 2014c. Disponível em <http://tools.kali.org/information-gathering/nmap>. Acesso em 10/07/2017.

MARTINEZ, Marina. **Topologias de Redes.** InfoEscola. Disponível em <http://www.infoescola.com/informatica/topologias-de-redes/>. Acesso em 10/07/2017.

MORIMOTO, Carlos E. **Cracker.** 2005. Disponível em <http://www.hardware.com.br/termos/cracker>. Acesso em 10/07/2017.

NASCIMENTO, Priscila. **Profissionais de redes de computadores têm campo promissor.** Virando Bixo, 2013. Disponível em <http://www.virandobixo.com.br/noticias/NOT,0,0,852688,Profissionais+de+redes+de+computadores+tem+campo+aquecido.aspx>. Acesso em 11/07/2017.

NORTON. **Phishing**. Disponível em < http://canaltech.com.br/o-que-e/*hacker*/O-que-e-Phishing-Scam/>. Acesso em 12/07/2017.

PINHEIRO, José Maurício Santos. **Topologias Redes de Comunicação.** Projeto de Redes, 2006 Disponível <http://www.projetoderedes.com.br/artigos/artigo_topologias_de_rede.php>. Acesso em 113/07/2017.

PINHEIRO, José Maurício S. **Topologias de Redes.** Centro Universitário Geraldo Di Biase. Disponível em <https://www.projetoderedes.com.br/aulas/ugb_redes_I/ugb_redes_I_material_de_apoio_0-4.pdf>. Acesso em 14/07/2017.

PINTO, Pedro. **LAN, MAN, WAN PAN, SAN ... Sabe a diferença.** PPLWare no comments, 2010. Disponível em <http://pplware.sapo.pt/tutoriais/networking/lan-man-wan-pan-san-%E2%80%A6-sabe-a-diferenca/>. Acesso em 15/07/2017.

PEIXOTO, Rodney de Castro**. Tecnologias wireless demandam cuidados extras – a prática do wardriving e warchalking**. Disponível em <http://www.ambito-80 juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=4266>. Acesso em 16/07/2017.

PENSADOR. **Kevin David Mitnick**. Disponível em <http://pensador.uol.com.br/autor/kevin_david_mitnick/>. Acesso em 17/07/2017.

PEREIRA, Jonathas Bitencourt; SOUZA, Marta Alves de; COSTA, Helder Rodrigues Da. **Segurança da informação em ambientes corporativos**. Disponível em <http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a29.pdf>. Acesso em 18/07/2017.

RITTINGHOUSE, John W.; RANSOME, James F. **Cloud Computing Implementation, Management, and Security.** CRC Press, 2010.

SCHLEMER, Elgio. **Estrutura do IPTables 2: a tabela nat.** Viva o Linux, 2007. Disponível em <http://www.vivaolinux.com.br/imagens/artigo/comunidade/figuraGanchos.png>. Acesso em 19/07/2017.

SOARES, L. F. G.; LEMES, G.; COLCHER, S. **Redes de Computadores; das LANs, MANs e WANs: às Redes ATM**. 2º Ed., Rio de Janeiro, Ed. Campus, 1995.

RIOS, Leonardo. **2017 Digital Yearbook**. Fullpack, 2017. Disponível em <http://fullpack.net/blog2/2017-digital-yearbook-analise-brasil/>. Acesso em 20/07/2017.

RASMUSSEN, Bruna. **Conheça os Principais Tipos de Redes.** Canaltech, 2017. Disponível em <https://corporate.canaltech.com.br/o-que-e/infra/lan-wlan-man-wan-pan-conheca-os-principais-tipos-de-redes/>. Acesso em 21/07/2017

CUNHA, G, B, Éder. **Redes de Computadores.** Fabri.ms, 2013. Disponível em <http://fabrica.ms.senac.br/2013/07/redes-de-computadores-parte-v/>. Acesso em 22/07/2017.

SULLO, Chris; LODGE, David. **Nikto2.** Cirt, 2017. Disponível em <https://cirt.net/Nikto2>. Acesso em 22/07/2017.

GRAVEHEART, Paulo. **Falha de Segurança no PHP.** Tecnoblog, 2012. Disponível em <https://tecnoblog.net/100565/falha-seguranca-php/>. Acesso em 23/07/2017.

MICROSOFT. **Making a Service Available Across Domain Boundaries.** Microsoft, 2015. Disponível em <https://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx>. Accesso em 24/07/2017.

Allison. **Vulnerabilidade Crítica de Segurança no PHP.** SWX Softwares, 2012. Disponível em <http://swx.com.br/2012/02/vulnerabilidade-critica-de-seguranca-no-php-esta-sendo-corrigida-atualizacao/>. Acecsso em 25/07/2017.

OWASP. **Clickjacking.** OWASP, 2017. Disponível em <https://www.owasp.org/index.php/Clickjacking>. Acesso em 26/07/2017.

GROSSMAN, Jeremiah. **Crossmain.xml Invites Cross-site Mayhem.** Blog Jeremiah, 2008. Disponível em <http://blog.jeremiahgrossman.com/2008/05/crossdomainxml-invites-cross-site.html>. Acesso em 27/07/2017.

Julio. **Nikto Probe Warning Messages.** Servedeafult, 2010. Disponível em <https://serverfault.com/questions/126954/nikto-probe-warning-messages>. Acesso em 28/07/2017.

COMPUTADOR, Pt. **A Difrença Entre Um Firewall e Firewall Software.** Disponível em <http://ptcomputador.com/Software/antivirus-software/101169.html>. Acesso em 28/07/2017.

TERRA, Dúvidas. **O Que é Engenharia Social.** Disponívem em <https://duvidas.terra.com.br/duvidas/558/o-que-e-engenharia-social-e-que-exemplos-podem-ser-citados-sobre-este-metodo-de-ataque>. Acesso em 30/07/2017.