UNIVERSIDADE SAGRADO CORAÇÃO

MAYARA GOMES ESGOTTI

SEGURANÇA EM SITES DE BANCOS UTILIZANDO A TÉCNICA PHISHING COM BACK TRACK

BAURU
2015

MAYARA GOMES ESGOTTI

SEGURANÇA EM SITES DE BANCOS UTILIZANDO A TÉCNICA PHISHING COM BACK TRACK

Trabalho de Conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais aplicadas como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2015

Esgotti, Mayara Gomes.

E753s

Segurança em sites de bancos utilizando a técnica Phishing com Back Track/ Mayara Gomes Esgotti.-- 2015.

45f. : il.

Orientador: Prof.Me. Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade do Sagrado Coração - Bauru - SP

1.Seguranças da Informação.2. Segurança Internet Banking.3. Ataques.4. PHISHING.5. BACKTRACK. I. Esgotti, Mayara Gomes. II. Título.

MAYARA GOMES ESGOTTI

SEGURANÇA EM SITES DE BANCO UTILIZANDO A TÉCNICA PHISHING COM BACK TRACK

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

Banca examinadora:

_____

Prof. Me. Henrique Pachioni Martins

Universidade Sagrado Coração

_____

Prof. Me. Patrick Pedreira Silva

Universidade Sagrado Coração

_____

Prof. Dr. Elvio Gilberto da Silva

Universidade Sagrado Coração

AGRADECIMENTOS

Gostaria de agradecer aos meus pais Angelica e Hugo que sonharam comigo, e fizeram o possível para que eu pudesse cursar uma faculdade, realizando assim meu sonho em me graduar em Ciência da Computação. Agradeço também aos meus irmãos Gabriel e Roberto, que assim como meus pais, me aguentaram estressada e ansiosa por causa de trabalhos e provas.

Registro minha gratidão ao professor Henrique Pachioni Martins que me ajudou muito, me incentivando, dando apoio, em que sua orientação foi muito importante para os resultados finais deste trabalho.

Aos meus amigos Atalita, Thiago, Rose e Renato que ao longo da faculdade me deram muita força e sempre foram compreensivos.

“Seu trabalho vai ocupar uma grande parte da sua vida, e a única maneira de estar verdadeiramente satisfeito é fazendo aquilo que você acredita ser um ótimo trabalho. E a única maneira de fazer um ótimo trabalho é fazendo o que você ama fazer. Se você ainda não encontrou, continue procurando.” (Steve Jobs)

RESUMO

A vida das pessoas anda cada vez mais corrida, cheias de compromisso, pensando nisso foi criada o internet banking para os clientes dos Bancos poderem realizar os seus serviços bancários em qualquer lugar e a qualquer hora do dia, com comodidade e facilidade, sem precisar enfrentar filas imensas. Conjuntamente com o Internet Banking surgiram novos conceitos e entre eles, a segurança desses serviços. Mas apesar desse serviço ter crescido muito nos últimos anos no Brasil, ainda existem aquelas pessoas que não fazem esses serviços por medo, ou até falta de conhecimento sobre o assunto. Exatamente sobre eles que este trabalho se refere. Explorando uma introdução sobre a segurança de Informação e de Internet Banking, enfocando assim os mecanismos que os e-bankings adquirem, as proteções de segurança como os Firewalls e os tipos de ataques. O principal objetivo deste trabalho é conscientizar as pessoas que, tomando alguns cuidados, é sim possível realizar serviços bancários online. Para provar para essas pessoas que fazer serviços bancários online são seguros, foram realizadas formas que demonstrará alguns métodos de se prevenir contra-ataques de hackers, onde foram enviados e-mail para possíveis vítimas, onde encaminharia para um site idêntico ao real, mas ao contrário é um link falso que com um pouco de atenção do usuário se dá para notar o risco de invadirem as contas. Os cuidados são apenas de quando clicar no link do e-mail que irá ser encaminhado ao site falso verificar cuidadosamente, os sites, principalmente onde é inserido o link que no caso de site falsificado ira aparecer outro endereço, não necessariamente o endereço de sites, pode também ser apenas números, indicando a máquina do atacante.

Palavras- chave: Seguranças da Informação, Segurança Internet Banking, Ataques, Firewall, PHISHING, BANCKTRACK.

ABSTRACT

Currently, people's lives are getting busier and busier, filled with appointments. Thinking of that, it was created the Internet Banking so that the clients of the banks could carry out their bank services wherever they are and whenever they want in a comfortable, easy and line-free way. Together with the Internet Banking, new concepts have come around such as the safety of these sorts of service. But in spite of the growth of that kind of service in the last few years in Brazil, there are still those people who do not make use of it due to fear or even lack of knowledge about this subject. It is exactly about those people that this research is about. Exploring an introduction about safety of information and the Internet Banking, then focusing on the mechanisms that e-banking acquire, the protections of safety, as the Firewalls and the kinds of attack. The major goal of this work is to bring people the knowledge that with little care and caution, it is surely possible to carry out bank services online. In order to prove them that those online bank services are really reliable, a couple of forms were made to prove some of the methods to prevent counter-attacks from hackers, where the e-mails were sent from if there is a victim, where it would lead to an identical website to the original ones, but unlike the original ones, they are a fake hyperlink. With little attention from the user, one can notice the risk of invading one's account. The care is only when clicking in an e-mail which might lead you to a fake website. Verifying carefully the websites, especially where the hyperlink is inserted in the fake website, if it is a fake website indeed, it will likely be taking you to another address, not necessarily the address of a website, but it could also be just numbers, indicating the attacker's machine.

Keywords: Security of information, Internet Banking Security, Attacks, Firewall, PHISHING, BACKTRACK

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

BI = Business Inteligence

CRM = Customer Relationship Management

DMZ = De- Militarized Zone

FTP = File TransferProtocol

HTTP = HyperText Transfer Protocol

ICMP = Internet Control Message Protocol

ID = Identity

LHF = Low Hanging Fruit

NAT = Network Address Translation

PAT = Port and Address Translation

TCP / IP = Transmission Control Protocol / Internet Protocol

TI = Tecnologia da Informação

TLS = Transport Layer Security

UDP = User Datagram Protocol

VPN = Virtual Private Network

SUMÁRIO

1 INTRODUÇÃO

Segundo Diniz (2000, apud VARGAS, 2006), a utilização da internet para ofertas de serviços bancários (banking) é a principal inovação tecnológica incorporada aos serviços bancários na última data. Associado à demanda dos clientes por maior conveniência e ao interesse dos bancos por economia, precisão e automação, o internet banking, que no início era considerado apenas mais um canal para a distribuição de serviços bancários, “passou a estar no centro das discussões sobre a evolução e o futuro dos bancos”.

De acordo com Santos (2001, apud CORREIA, 2008), a segurança é um desafio enfrentado pelas instituições que oferecem os serviços de e-banking, uma vez que ele é alvo frequente de fraudes. Na tentativa de superar esses problemas, as instituições bancárias brasileiras investem milhares de reais em tecnologia para a segurança.

Mais do que um canal com os clientes, a Internet já aderiu aos processos internos, no desenvolvimento de portais corporativos, e também é ferramenta essencial para a estruturação de metodologia de CRM e BI nos bancos, por permitir uma coleta de dados muito mais rica de clientes. A incorporação desta tecnologia no ambiente bancário ainda merece atenção especial, pois as tecnologias não evoluem somente sob o ímpeto de uma lógica interna, tecnológica ou científica se evoluem ou mudam porque são pressionadas na direção desde novo formato. (VARGAS, 2006).

Milhares de pessoas que utilizam a internet ainda têm muito receio em usar o banking, pois apesar de seguro, vemos muitos noticiários de golpes pela internet, então como cada vez esse serviço está tendo mais procura será realizado um trabalho de técnicas de invasão para mostrar se esses serviços são seguros.

Como nos dias atuais as pessoas estão cada dia mais apressados e sem tempo, algumas empresas e governos institucionais preferem o trabalho de banking pela comodidade e facilidade.

Um dos pontos mais importantes sobre segurança é saber o que devemos procurar proteger, portanto, quando se conectar a Internet, na maioria das vezes, estamos colocando em risco três elementos: a privacidade dos dados; a integridade dos dados; e a disponibilidade que expressa a capacidade de usar seus próprios dados. (ZWICKY et al., 2000).

1.1 OBJETIVOS

1.1.1 Objetivo geral

Demonstrar forma de se prevenir contra ataques de hackers sobre as técnicas phishing para as pessoas através de trabalhos bancários.

1.1.2 Objetivos específicos

- Identificar os tipos de ataques mais utilizados em fraudes de banco, e assim mostrar que o funcionamento dos sites e aplicativos bancários para trabalho on-line é seguro;
- Levantar os principais pontos de segurança dos sites web e principalmente bancários, para conscientizar as vitimas desses golpes;
- Mostrar como os fraudadores realizam seus golpes pela internet, podendo assim prevenir ataques.

1.2 JUSTIFICATIVA

Com base em pesquisas quantitativas realizada pela autora, onde foram entrevistadas em torno de umas cinqüenta pessoas, onde costumam utilizar os bancos para realizarem trabalhos de contas, e administrativos, para poder saber de suas seguranças ou não para trabalhos bancários em internet, comprovou-se que muitos usuários evitam o uso de atividades bancárias pelos sites e aplicativos, por medo de invasão e falta de conhecimento.

2 SEGURANÇA

2.1INFORMAÇÃO

Informações são consideradas o principal patrimônio de uma organização está também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se um ponto crucial para a sobrevivência das instituições que agregue valor ao negócio da administração em benefício da sociedade. (CONTAS DA UNIÃO, 2008).

A informação sempre foi muito importante e útil para as instituições, pois é algo que fazem as instituições ganharem tempo em suas jornadas diárias, a única coisa que mudou foi o modo que é armazenado essas informações, que antes eram em papéis e agora com a tecnologia são em computadores.

Na época em que as informações eram armazenadas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e com o uso de computadores de grande porte, a estrutura de segurança ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. (CONTAS DA UNIÃO, 2008).

Quando se fala em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade, e demais aspectos da segurança das informações dentro das necessidades do cliente. (LYRA, 2008).

Pode se dizer que a segurança nada mais é do que, a proteção e controle das informações, que trabalha junto com funções importantes, confiabilidade, integridade, disponibilidade, autenticação, legalidade, privacidade e auditoria. Onde estas informações são o que possibilita as redes privadas e/ou públicas de computadores a serem seguras.

Controle é tudo e qualquer mecanismo utilizado para diminuir as fraquezas (ou vulnerabilidade) de um ativo da informação, seja um equipamento, tecnologia, pessoa ou processo. Antes de ser consumida, a informação precisa de alguma organização, formatação, classificação ou análise para ser mais acessível e de fácil utilização. É preciso garantir que a informação depois de tratada continua íntegra,

bem como sua confidencialidade. (LYRA, 2008). A segurança é um processo de acompanhamento de informação antes e depois de sua implementação, para melhoria do equipamento e dos arquivos e, também, para a segurança dos próprios clientes.

Segundo Chakrabarti (2000 apud MARTINS, 2004), a internet, como algum outro produto, tende a ter falhas, e os pesquisadores começaram a pesquisar a importância de uma comunicação estar segura, e para superar a presença de usuários ou de hackers maliciosos. Para ser possível o acesso de pessoas em sites web, e principalmente bancários, de qualquer dispositivo são necessários que a internet utilizada tenha um bom software de segurança.

O treinamento de segurança, com relação à política da empresa criada para proteger o ativo de informações, precisa ser aplicado a todos que trabalham na empresa, e não apenas ao empregado que tem acesso eletrônico ou físico ao ativo de TI da empresa. (MITNICK, 2003).

Segundo Soares (1995 apud MITNICK, 2003), A autorização de uma política de segurança baseada em regras, normalmente apoia-se em informações sobre sensibilidade. Em um sistema seguro, os dados ou recursos devem ser marcados com rótulos de segurança que indicam seu nível de sensibilidade. Os processos atuando sob o controle de indivíduos devem adquirir os rótulos de segurança apropriados, que definem o nível de autorização do indivíduo que está controlando.

Segundo Soares (1995 apud MITNICK, 2003), As regras desse tipo de política utilizam os rótulos dos recursos e dos processos para determinar o tipo de acesso que pode ser efetuado. No caso de uma rede de computadores, os dispositivos que implementam os canais de comunicação também possuem rótulos de segurança. Nesse caso, as regras que definem a política de segurança também determinam quando é, ou não, permitido transmitir dados nesses canais, isto é, informações sensíveis só podem ser transmitidas em canais que oferecem o nível de segurança adequado.

2.2 INTERNET BANKING

Segundo SANTOS (2001 apud CORREIA, 2008), a segurança é um desafio enfrentado pelas instituições que oferecem o serviço de e-banking, uma vez que ele é alvo frequente de fraudes.

Segundo Albertin (2004 apud VARGAS 2006), os novos conceitos relativos aos negócios na era digital apresentam grandes ofertas de novas oportunidades de contribuição para as empresas de todos os portes e setores, que merecem ser conhecidos e explorados, por isso nos anos de 1995, a primeira oferta de serviços bancários como consultas, transferências, pagamentos entre outros serviços através da rede mundial, o que atualmente denomina-se Internet Banking, já eram observados.

Segundo Diniz (2000 apud VARGAS 2006), as atividades e serviços bancários oferecidos pela Internet podem ser classificados de diversas formas, o que destaca são as oportunidades que podem ser aproveitadas pelos bancos, composta por três categorias:

- Divulgação – Internet como veículo para divulgação de informação tanto de negócio quanto de publicidade;
- Transação – Internet como canal para operar transações bancárias, como em agências e caixas-eletrônicos;
- Relacionamento – Internet como ferramenta para aprimorar o relacionamento com os clientes.

Cada categoria apresenta níveis de interatividade diferentes: Básico, Intermediário e Avançado, no qual o nível básico, o banco explora a internet como mais um canal, já no nível intermediário algumas particularidades da internet são utilizadas, e no nível avançado, novas oportunidades de negócio proporcionadas pela internet são consideradas.

Grandes bancos continuarão a inovar na oferta de serviços visando ampliar a conveniência requerida pelos clientes, onde o mais importante é destacar a segurança das informações, preocupação inicial dos clientes e também dos primeiros bancos na Internet. (VARGAS, 2006).

Os sistemas de e-banking brasileiros utilizam vários mecanismos de segurança para proteger usuários de seus sistemas. Estes mecanismos de

segurança podem ser divididos em duas categorias: mecanismos contra-ataques remotos e mecanismos contra-ataques locais. Os mecanismos contra-ataques remotos visam a proteger usuários contra-ataques nos quais indivíduos, que agem de má fé possam capturar dados sensíveis sem que tenham penetrado no computador do usuário do sistema, estes mecanismos são altamente eficientes contra alguns tipos de ataques, como tentativas de sniffing[1].Já o mecanismo contra-ataques locais são mais eficientes contra os tipos de ataques de phishing. (CORREIA, 2008).

Para melhor navegação dos clientes dos bancos nos sites é preciso ter um bom programa de segurança, e este programa é dividido em vários tipos de mecanismos, dependendo do grau de necessidade do cliente.

2.2.1 Tipos de mecanismos

2.2.1.1Transport Layer Security

Segundo Recorla (2000 apud CORREIA, 2008), o TLS (Transport Layer Security) é um protocolo criptografado que provê comunicação na Internet para diversos serviços, inclusive o HTTP que é utilizado pelo e-banking. Este protocolo provê a autenticidade, privacidade e a integridade dos dados transmitidos entre duas aplicações que estejam se comunicando pela internet, também ajuda a prevenir que atacantes tenham acesso ou falsifiquem os dados transmitidos.

O protocolo TLS é bastante flexível, permitindo sua utilização com diferentes algoritmos de criptografia, tamanhos de chaves, tempo para renegociação das chaves, usando chaves de 1024 bits e o algoritmo RC4 para a criptografia dos dados em todos os serviços verificados. (CORREIA, 2008).

[1]Sniffing é o procedimento realizado por uma ferramenta conhecida como Sniffer, capaz de interceptar e registrar o tráfego de dados em rede de computadores.

2.2.1.2 Encerramento da sessão

Uma sessão é representada por informações que são mantidas nos servidores a respeito de cada conexão recebida por ele. Quando o cliente efetua a autenticação, são mantidas informações nos servidores que permitem que ele seja identificado como usuário autenticado e garantem acesso ao serviço, que é mantida de acordo com regras impostas pelo serviço. (CORREIA, 2008).

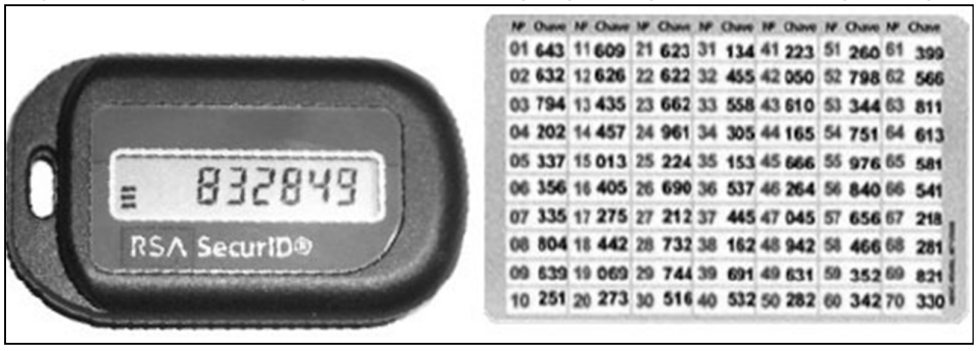
Segundo Stallings (2007 apud CORREIA, 2008), alguns e-bankings oferecem a flexibilidade de configuração do tempo de inatividade máximo, permitindo que o usuário configure a tolerância para até uma hora. Esta possibilidade de configurações da tolerância pode ser usada de maneira ingênua pelo usuário fazendo com que ele possa sofrer ataques, como roubo de cookie de sessão.

2.2.1.3 Chave temporal

Segundo Litterio (1995 apud CORREIA, 2008), a chave temporal é um mecanismo baseado no conceito do algoritmo criptografado one-time pad.

Chaves temporais são utilizadas para tentar contornar o risco do roubo de senhas. O seu conceito se baseia na utilização de chaves que são válidas por um curto período de tempo, também só pode ser utilizada no período de tempo entre a troca de chaves, que idealmente é pequeno. (CORREIA, 2008).

Figura 1 – Chave temporal eletrônica (esquerda) e em cartão (direita)



Fonte: Correia (2008).

A chave temporal foi encontrada em duas abordagens nos sistemas de e-banking (Figura 1). Uma abordagem implementa chaves temporais na forma de

token, que é um dispositivo eletrônico especializado na geração das chaves temporais, e garante a não repetição por um longo período. A outra abordagem implementa chaves temporais na forma de cartão com uma sequência de chaves, que serão solicitadas uma a cada tentativa de autenticação no serviço. (CORREIA, 2008).

2.2.1.4 Teclado virtual

Segundo Von Ahn (2004 apud CORREIA, 2008), o teclado virtual é o principal mecanismo de segurança utilizado para prevenir ataques locais gerados por softwares maliciosamente instalados nos computadores dos usuários, e se baseia no conceito de Completely Automated Public Turing test to tell Computers and Humans Apart. Um dos grandes desafios no projeto de mecanismos de segurança baseados em CAPTCHA é garantir elevado nível de segurança mantendo a usabilidade do sistema.

Figura 2 – Teclado virtual com representação direta (esquerda) e indireta (direita)

Fonte: Correia (2008)

Os princípios do CAPTCHA garantem que, embora seja fácil para humanos selecionar uma opção, seja muito difícil para um software, como um vírus instalado no computador do usuário, reconhecer esta seleção, e podem ser capturados como imagem que pode ser enviada para um sistema malicioso remoto junto com informações sobre a seleção do usuário impedindo a reconstrução dos dados

informados pelo usuário através das informações que o teclado virtual passa para o navegador submeter para o servidor. (CORREIA, 2008).

2.2.1.5 Identificação do computador

É um software que realiza coleta de dados com o objetivo de caracterizar de forma única o equipamento de onde deve ser permitindo o acesso ao serviço, as informações coletadas por esse tipo de software normalmente envolvem identificação de alguns dispositivos de hardware e o software. (CORREIA, 2008).

Pode se agregar bastante segurança ao acesso do serviço, porém são necessários cuidados para que outro computador não possa se passar por um equipamento autorizado, e também a coleta dessas informações no sistema requer comunicação com o sistema operacional. (CORREIA, 2008). Um problema maior é que a identificação do computador só atende às plataformas mais utilizadas, e se o tratamento dado a plataforma que não são atendidas a risco de um fraudador tome conta de dados secretos da vítima como: senha do cartão de crédito.

2.3 FIREWALLS

Firewall é um componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet ou entre outro conjunto de redes. (ZWICKY et al., 2000).

Segundo Bill Cheswick, da AT&T, uma rede protegida por um Firewall é como “uma casca crocante em torno de um miolo macio e fácil de mastigar”. (McCLURE et al., 2003, p. 48).

Para manter um nível absolutamente mínimo de segurança na Internet que seja eficaz, é preciso controlar a segurança nas fronteiras usando Firewalls que realizem todas as três funções básicas dos Firewalls, filtragem de pacotes, conversão de endereços da rede, e Proxy de serviço de alto nível. Os Firewalls também precisam ser dedicados principalmente ao desempenho das funções do Firewall, muitos serviços contêm faixa de login ou páginas de erro geradas automaticamente que identificam o produto Firewall que se está usando. (STREBE; PERKINS, 2002).

Isso pode ser perigoso se os hackers já tiverem descoberto algum ponto fraco nesse Firewall específico. É preciso também reforçar a ideia de um único ponto de controle no Firewall. Se tiver mais de um Firewall na empresa (talvez um Firewall conectando cada escritório remoto à Internet), deverá ter absoluta certeza de que todos eles estejam configurados da mesma maneira; “uma falha em qualquer um dos Firewalls poderá comprometer toda a rede, especialmente se estiverem sendo usados tunelamento seguro ou linhas privadas diretas para conectar os escritórios. (STREBE; PERKINS, 2002, p 110).

Ao conectar uma rede privada à internet, está na verdade, conectando a rede diretamente a todas as outras redes ligadas à internet diretamente. Não há nenhum ponto central inerente de controle de segurança. (STREBE; PERKINS, 2002).

Os Firewalls são usados para criar pontos de controle de segurança nas fronteiras das redes privadas, ao fornecer a função de roteamento entre a rede privada e a internet, os Firewalls inspecionam toda a comunicação passando entre as redes e/ou a transmitem ou a abandonam, dependendo de como cada comunicação segue as normas programadas. Se um Firewall estiver configurado adequadamente, e não contiver nenhum erro sério que possa ser explorado, a rede estará livre de riscos tanto quanto possíveis. (STREBE; PERKINS, 2002).

Os Firewalls mantêm uma conexão à internet mais segura possível, inspecionando e aprovando ou rejeitando cada tentativa de conexão feita entre a rede interna e as redes externas, como a internet. Firewalls poderosos protegem uma rede em todas as camadas de software – da camada de enlace dos dados até a camada de aplicação. (STREBE; PERKINS, 2002).

Os Firewalls se localizam nas fronteiras da rede – nas interconexões (gateways) que fornecem acesso a outras redes. Por essa razão, os Firewalls são considerados uma proteção das fronteiras, esta proteção é importante, pois sem ela, qualquer host da rede teria de realizar as funções de um Firewall sozinho, consumindo inutilmente recursos de computação, e aumentando o tempo necessário para conectar, autenticar e criptografar os dados nas redes locais de alta velocidade. (STREBE; PERKINS, 2002).

Por natureza, os Firewalls criam passagens estreitas entre a rede interna e externa para que todo o tráfego entre uma e outra tenha de passar através de um único ponto de controle. O servidor externo envia os dados de volta transmitindo-os

para a porta fornecida pelo cliente interno. Como o Firewalls inspecionam todo o tráfego trocado entre os dois hosts, ele sabe que a conexão foi iniciada pelo host interno conectado à sua interface interna, qual é o endereço IP do host, e qual é a porta na qual este espera receber o tráfego de retorno. (STREBE; PERKINS, 2002).

O Firewall lembra-se então de permitir que o host endereçado na mensagem de conexão retorne tráfego para o endereço IP do host interno somente na porta especificada, os hosts envolvidos na conexão fecham a conexão TCP, o Firewall remove a entrada de sua tabela de estados (sua memória de conexão) que permite ao host remoto retornar tráfego para o host interno (STREBE; PERKINS, 2002).

Os sistemas Firewalls são como um antivírus mais potente que protegem os dados importantes de contas da internet, como contas de uma rede para outra, para esse sistema ser utilizado com mais eficácia pode-se ter mais de um Firewall ligando em outros, mas todos tem que estar configurados normalmente. Pois com um mínimo de falha nessa segurança já é possível indivíduos indesejáveis entrar nessas contas e utilizá-las de forma irregular. Também é necessário ter em mente primeiro o que se pretende proteger como as conexões com as redes externas ou internas, pois a segurança envolvida depende muito da funcionalidade dos Firewalls.

Um Firewall serve para impedir que o perigo da internet se espalhe por sua rede interna, sendo assim serve a vários propósitos que são:

- Limita a entrada das pessoas a um ponto cuidadosamente controlado.
- Impede que os atacantes cheguem perto de suas outras defesas.
- Limita a saída das pessoas a um ponto cuidadosamente controlado.

Todo o tráfego que vem da internet ou que sai da sua rede interna passa através do Firewall, que é considerado como um separador, um limitador, um analisador que não se consegue proteger contra pessoas que já estão do lado de dentro, ele funciona melhor se acoplados a defesas internas. Também é um meio mais efetivo de conectar uma rede à internet e ainda assim proteger essa rede. (ZWICKY et al., 2000).

2.3.1 Tipos de firewalls

Dois tipos de Firewalls dominam o mercado hoje: proxies de aplicação e gateway de filtragem de pacotes (e alguma combinação híbrida deles). Embora os

proxies de aplicação sejam normalmente considerados mais seguros do que os gateways de filtragem de pacotes, sua natureza restritiva e suas limitações de desempenho têm restringido sua adoção principalmente ao tráfego interno da empresa, que sai, em vez do tráfego que entra no servidor Web ou DMZ (De-Militarized Zone, rede de perímetro) da empresa. Por outro lado, os gateways de filtragem de pacotes, ou os gateways de filtragem de pacotes com estados, mais sofisticados, podem ser encontrados em muitas organizações maiores, com requisitos de alto desempenho para entrada e saída. (McCLURE et al., 2003).

Os Firewalls têm protegido inúmeras redes contra olhares curiosos e vândalos maliciosos. Vulnerabilidades de segurança são descobertas a cada ano com praticamente qualquer firewall no mercado. Pior ainda, a maioria dos firewalls normalmente é mal configurada, mal mantida e mal monitorada, transformando-os em batentes de porta eletrônicos, mantendo a porta bem aberta. (McCLURE et al., 2003).

Um Firewall bem projetado, configurado e mantido é quase impenetrável. A maior parte dos atacantes habilidosos sabe disso. Eles simplesmente contornarão o firewall explorando relacionamentos de confiança e vulnerabilidades de segurança do elo mais fraco, ou então a evitarão inteiramente, o atacante se esforça ao máximo para contornar o firewall forte, ou então a evitarão inteiramente, atacando-o através de uma conta discada, resultando em: a maior parte dos atacantes se esforçar ao máximo para contornar um firewall bem protegido. (McCLURE et al., 2003).

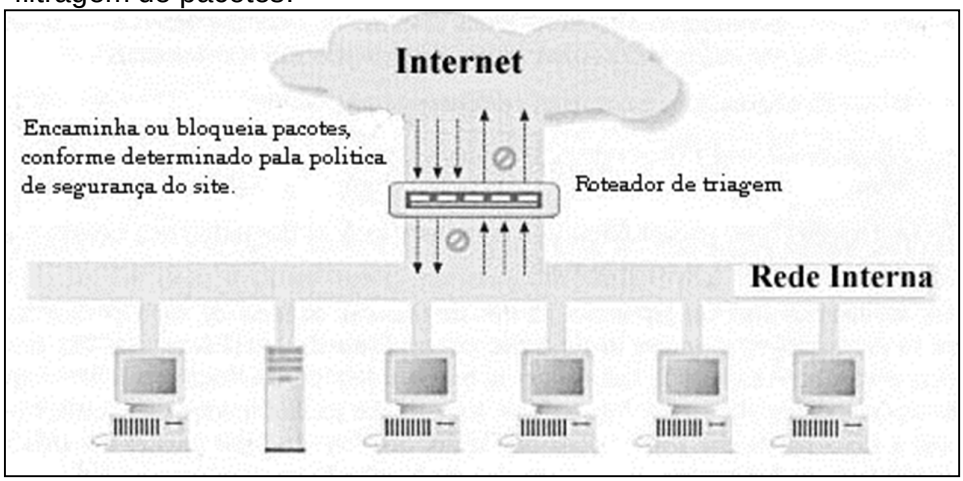
Administradores de firewall sabem da importância de conhecer seu inimigo. Saber os primeiros passos que um atacante realizará para evitar seus firewalls, e o que deixará na dianteira para detectar e reagir a um ataque. (McCLURE et al., 2003).

2.3.1.1Filtragem de pacote

Os sistemas de filtragem de pacotes fazem o roteamento (encaminhamento) de pacotes entre hosts internos e externos. Eles permitem ou bloqueiam certos tipos de pacotes de um modo que reflete a própria política de segurança de um site como

mostra a Figura 3, o tipo de roteador usado em um firewall de filtragem de pacotes é conhecido como roteador de triagem.

Figura 3 – O uso de um roteador de triagem para executar a filtragem de pacotes.



Fonte: Zwicky et al. (2000)

As principais informações do roteador para filtragem de pacotes são:

- Endereço IP de origem.
- Endereço IP de destino.
- Protocolo (indica se o pacote é um pacote TCP,UDP ou ICMP)
- Porta TCP ou UDP de origem.
- Porta TCP ou UDP de destino.
- Tipo de mensagem ICMP.
- Tamanho do pacote.

O roteador também pode inspecionar além dos cabeçalhos de pacotes, examinando dados presentes mais adiante no pacote, permitindo filtrar pacotes com base em informações mais detalhadas (como o nome da página da web que alguém esta solicitando) e verificar quais pacotes parecem estar formatados da maneira esperada para sua porta de destino, e que ajuda a captar vários ataques de negação de serviço baseado em pacotes defeituosos, também conhece detalhes sobre o pacote que não estão refletidos no próprio pacote, como:

- A interface à qual chega o pacote.
- A interface para onde o pacote vai. (ZWICKY et al., 2000).

A filtragem de pacote nada mais é do que um roteador que faz uma triagem das informações mais importantes das que não são importantes, depois dessa enxugada de informações é transmitido para outro host, ou seja, tem-se a origem e o destino do pacote.

2.3.1.2 Serviços de Proxy

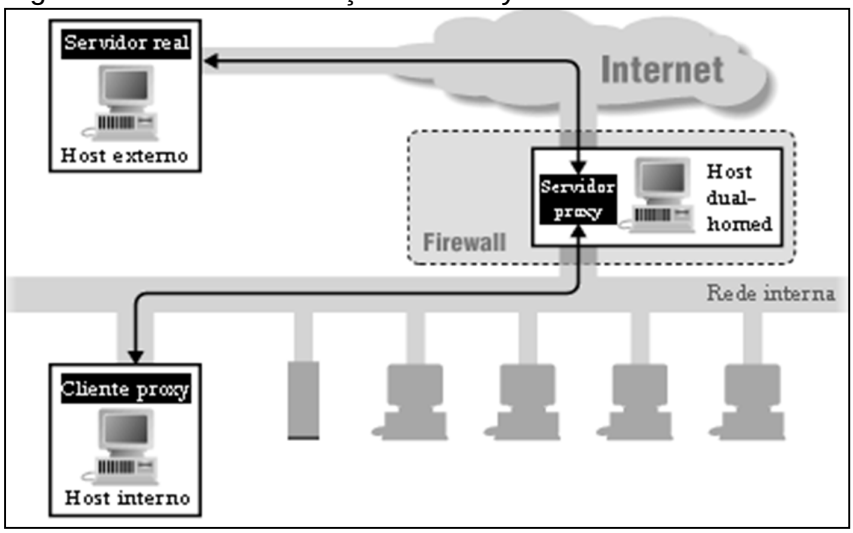
Os serviços de Proxy são programas, aplicativos ou servidores especializados que tomam as solicitações de usuários de serviços da Internet (como FTP e Telnet) e os encaminham aos serviços reais. Os proxies fornecem conexões substitutas e atuam como gateways para os serviços, também são executados para fins de segurança que funcionam em um host de firewall: seja um host dual-homed com uma interface na rede interna, e uma na rede externa, ou algum outro host de bastião que tenha acesso à internet, e que seja acessível a partir das máquinas internas, e também os proxies são projetadas principalmente visando à eficiência da rede em vez da segurança. Os proxies de cachê podem reduzir significativamente a carga em conexões de rede. (ZWICKY et al., 2000).

Existem servidores Proxy que oferecem tanto segurança quanto cache. Os serviços de Proxy estão situados, de forma mais ou menos transparente, entre um usuário do lado de dentro (na rede interna) e um serviço no local de fora (na Internet), existem sistemas que fornecem um híbrido entre filtragem de pacotes e uso de proxies, onde um dispositivo de rede intercepta a conexão e atua como um Proxy ou redireciona a conexão para um Proxy.

Como mostra a Figura 4 um serviço de Proxy exige dois componentes: um servidor Proxy e um cliente Proxy.O servidor Proxy funciona no host dual-homed, já um cliente Proxy é uma versão especial de um programa cliente normal que se comunica com o servidor Proxy, em vez de se comunicar com servidor real na internet. (ZWICKY et al., 2000).

O servidor Proxy pode controlar o que os usuários fazem, porque é capaz de tomar decisões sobre os pedidos que processa. Dependendo da política de segurança de seu site, os pedidos podem ser concedidos ou recusados. (ZWICKY et al., 2000).

Figura 4 – O uso de serviços de Proxy com um host dual-homed



Fonte: Zwicky et al. (2000)

2.3.1.3 Conversão de endereço de rede

A conversão (ou tradução) de endereço de rede (NAT) permite que uma rede utilize internamente um conjunto de endereços de rede, e use um conjunto diferente ao lidar com redes externas. Sozinha, a conversão de endereços de rede não oferece nenhuma segurança, mas ajuda a ocultar o layout da rede interna e a força as conexões a passarem por um ponto de estrangulamento (porque conexão para endereços não convertidos não funcionarão, e o ponto de estrangulamento faz a conversão). Com a filtragem de pacote, a conversão de endereços de rede funciona fazendo-se um roteador executar trabalho extra, o roteador não apenas encaminha pacotes, mas também os modifica. Os sistemas de conversão de endereço de rede também podem modificar os números de porta de origem e destino (isso se chama conversão de porta de endereço ou PAT-Port and AddressTranslation). (ZWICKY et al., 2000).

Os sistemas de conversão de endereços de rede podem usar diferentes esquemas para fazer a conversão entre endereços internos e externos:

- Alocar um único endereço de host externo para cada endereço interno e sempre aplicar a mesma conversão.
- Alocar dinamicamente um endereço de host externo toda vez que um host interno inicia uma conexão, sem modificar números de portas.

- Criar um mapeamento fixo de endereços internos para endereços visíveis externamente.
- Alocar dinamicamente um endereço de host externo e um par de portas, toda vez que um host interno inicia uma conexão. (ZWICKY et al., 2000).

2.3.1.4 Redes privadas virtuais

Uma rede privada virtual (VPN – Virtual Private Network) é um modo de empregar criptografia e proteção de integridade, de forma que possa usar uma rede pública (por exemplo, a Internet) como se ela fosse uma rede privada. A criação de uma conexão privativa de alta velocidade e longa distância entre dois sites é muito mais dispendiosa que conectar os mesmos, dois sites, a uma rede pública de alta velocidade, mas também é muito mais segura. (ZWICKY et al., 2000).

Uma rede privada virtual é uma tentativa de combinar as vantagens de uma rede pública (ela é econômica e está amplamente disponível), com algumas das vantagens de uma rede privada (ela é segura). Fundamentalmente, todas as redes privadas virtuais que funcionam sobre a Internet empregam o mesmo princípio: o tráfego seja criptografado, tem sua integridade protegida e é encapsulada em novos pacotes, que são enviados através da Internet para algo que desfaz o encapsulamento, verifica a integridade e decodifica o tráfego (ZWICKY et al., 2000).

2.4 ATAQUES

Muitos ataques são complicados e envolvem diversas etapas e planejamento elaborado, além de combinar o conhecimento da manipulação e tecnologia. (MITNICK, 2003).

Muitos atacantes agem de uma forma tão fácil, mas que ninguém imagina ser usada, esta forma, eles apenas pedem informações de certa empresa. Por exemplo: O atacante liga para o número particular de uma empresa a escolha e se passa por técnico de TI da própria empresa, pedindo informações como quais instalações eles precisam usar, e a pessoa acreditando na versão do atacante passa todas as informações.

Segundo Mitnick (2003, p. 26), isso acontece porque “É da natureza humana confiar em nossos colegas de trabalho, particularmente quando a solicitação passa no teste como razoável, então os atacantes se usam desses conhecimentos para explorar suas vítimas e atingir seus objetivos”. Por estarem passando confiança para as pessoas, os atacantes são considerados como habilidosos e astuciosos, pois incluem perguntas chaves no meio de outras perguntas, e sem a percepção do ocorrido é realizado o ataque simples e direto.

Os trapaceiros de informações experientes não têm escrúpulos em ligar para o governo federal, estadual ou municipal para saber os procedimentos da aplicação das leis. Com tais informações em mãos, o engenheiro social pode contornar as verificações de segurança da sua empresa. Em um cenário da engenharia social, os ativos da empresa não são os únicos que correm riscos. Às vezes as vítimas são os clientes de uma empresa, também o trabalho no serviço ao cliente tem a sua parcela de frustração e a de erros inocentes, sendo que alguns deles podem ter consequências infelizes para os clientes de uma empresa. (MITNICK, 2003).

2.4.1 Invasão de rede

O processo inteiro de invasão pode ser automatizado com ferramentas de invasão tradicionais, chamadas discadores de guerra ou discadores demônio. Basicamente, estes são ferramentas que discam programaticamente para grandes bancos de números de telefone, registram conexão de dados válida (chamadas portadoras, ou carriers), tentam identificar o sistema na outra ponta da linha telefônica e opcionalmente tentam realizar um logon, adivinhando nomes de usuários e senhas comuns. Os hackers maliciosos normalmente começarão com o nome de uma empresa e colherão uma lista de intervalos em potencial do máximo de fontes que puderem. (McCLURE et al., 2003).

Quando os resultados de saída de qualquer um dos discadores de guerra estiverem disponíveis, o próximo passo é categorizar os resultados no que chamamos de domínio, a experiência com uma grande variedade de servidores de acesso discado e os sistemas operacionais são insubstituíveis. A forma em que você escolhe quais sistemas irá penetrar ainda mais depende de diversos fatores, como o

tempo que você deseja gastar, quanto esforço e largura de banda de computação estão a sua disposição, e quais são as suas habilidades de adivinhação de scripting.

Ligar de volta para os modems que foram descobertos, com um software de comunicação simples, é o primeiro passo importante para colocar os resultados em domínio para fins de teste. Ao discar de volta para uma conexão, é importante tentar entender as características da conexão com fatores importantes que caracterizam uma conexão de modem e, portanto, ajudarão nos seus esforços de scripting que são:

- Se a conexão possui um limite de tempo ou de tentativas.
- Se o fato de ultrapassar esses limites deixa a conexão inutilizável (isso ocasionalmente acontece).
- Se a conexão é permitida apenas em certos horários.
- Se você pode presumir corretamente o nível de autenticação (ou seja, apenas ID de usuário ou apenas ID de usuário e senha).
- Se a conexão possui um método de identificação exclusivo, que parece ser do tipo desafio-resposta, como no SecurID.
- Se você pode identificar o número máximo de caracteres para as respostas aos campos de ID de usuário ou senha.
- Se você pode determinar algo sobre a composição alfanumérica ou de caracteres especiais dos campos de ID de usuário e senha
- Se qualquer informação adicional poderia ser colhida da digitação de outros tipos de caracteres de interrupção no teclado, como CTRL-C, CTRL-Z e assim por diante.
- Se os banners do sistema estão presentes ou se mudaram desde as primeiras tentativas de descobertas e quais os tipos de informações apresentados nesses banners. Isso pode ser útil para tentativas de adivinhação ou para manobras de engenharia social.

Quando tiver essas informações, normalmente poderá colocar as conexões no que chamaremos simplesmente de domínio de penetração de discagem de guerra, onde existem quatro domínios a considerar ao tentar penetrar ainda mais nos sistemas descobertos, além das técnicas de adivinhações simples no teclado, a área que deve ser eliminada primeiro, que é chamada de LHF (LowHangingFruit –

fruta pendurada em galho baixo), que são senhas e que são descobertas com facilidade ou usadas comumente para sistemas identificáveis (a experiência conta muito nesse caso), ou seja, produz mais resultados.

Os outros domínios de força bruta são baseados principalmente no número de mecanismos de autenticação e no número de tentativas permitidas para tentar o acesso a esses mecanismos com tentativas ilimitadas que são:

- Primeiro – Única autenticação: sistemas com somente um tipo de senha ou ID, e o modem não desconecta depois de determinado número de tentativas malsucedidas;
- Segundo – Única autenticação: Sistema com somente um tipo de senha ou ID, e o modem desconecta depois de determinado números de tentativas malsucedidas;
- Terceiro – Autenticação dupla: Sistemas nos quais existem dois tipos de mecanismos de autenticação, como ID e senha, e o modem não desconecta depois de determinado número de tentativas malsucedidas;
- Quarta – Autenticação dupla: Sistemas nos quais existem dois tipos de mecanismo de autenticação, como ID e senha, e o modem desconecta depois de determinado número de tentativas malsucedidas. (McCLURE, 2003).

Em geral, quanto mais fundo você for na lista de domínios, mas tempo será preciso para penetrar em um sistema. Ao se mover pelos domínios, o processo de scripting torna-se mais sensível, devido ao número de ações que precisam ser realizadas. (McCLURE, 2003).

2.4.2 Phishing

Segundo Filho (2014, p. 5):

> A palavra phishing, uma corruptela do verbo inglês fishing (pescar, em português), é utilizada para designar alguns tipos de condutas fraudulentas que são cometidas na rede. São muito comuns as mensagens eletrônicas (e-mails) onde são feitas propaganda de pechinchas comerciais, são solicitados renovações de cadastro, são feitos convites para visualização de sites, são ofertas gratuitamente soluções técnicas para vírus, entre outras [...] assim as pessoas mal informadas e desatentas acabam clicando para verificar o conteúdo do site onde se pede informações pessoais, e é onde muitas pessoas caem.

Phishing é um tipo de ameaça da Internet, que é aplicada através de comunicação em programas de instant messaging, telefone e como uma mensagem de e-mail, onde nessa mensagem está pedindo para clicar em um link que encaminhará a pessoa automaticamente para um anexo que será baixado e ao baixar automaticamente vem um vírus junto, ou também por uns sites falsos muito parecidos graficamente com os sites verdadeiros e que pedem informações pessoais como exemplo: confirmar a senha do cartão de crédito de um determinado banco. E assim que a pessoa digita o número a pessoa maliciosa que enviou o e-mail está pronto para pegar esses dados e aplicar o golpe imediatamente.

A categoria delituosa em questão consiste exatamente nisso: em “pescar” ou “fisgar” qualquer pessoa desavisada, não acostumada com esse tipo de fraude. O phishing, portanto, é uma modalidade de spam, em que a mensagem, além de indesejada, é também fraudulenta. Assim, o phisherman pode ter como alvo os dados de um usuário, e respectivos números da conta e senhas bancárias, para serem utilizados em sites de Internet banking, ou pode coletar dados de cartão de crédito e senhas utilizadas em sites de comércio eletrônico ou de leilão e de sistemas de pagamento online. (FILHO, 2014).

2.5 SOFTWARES LIVRES

2.5.1 Backtrack

O BACTRACK é uma ferramenta voltada para testes de penetração, muito utilizada por auditores, analista de segurança de redes e sistemas e hackers éticos (GIAVAROTO; SANTOS, 2013).

2.5.1.1 Metodologia de Teste de Penetração (PenetrationTesting)

Definido como Penetration testing, trata-se de um método para testar e descobrir vulnerabilidades em uma rede ou sistemas operacionais, onde se insere um método de avaliação de segurança, aplicando simulações de ataques como se fosse um estranho mal-intencionado no intuito de invadir um sistema. Tais Pentest possibilitam verificar a real estrutura do sistema, que é vasculhado em todas as

áreas inerentes à estrutura de segurança. São de suma importância os testes aplicados, pois através deles poderemos verificar falhas em hardware e software utilizados e criar mecanismos de defesas ou ajustes adequados. Com o intuito de proteção, os testes de penetração são de extrema importância para uma empresa ou organização, o importante é funcionar e ter o retorno esperado. Desta forma, inúmeros problemas de segurança são implantados em sistemas com o intuito de roubar informações, práticas de crimes e outros adjacentes. (GIAVAROTO; SANTOS, 2013).

A meta do pentest é puramente aplicar as melhores técnicas de segurança, a fim de proteger o maior patrimônio que existe a informação. (GIAVAROTO; SANTOS, 2013).

Um profissional da área de segurança envolvido com pentest precisa apenas pensar como um Blackhat, Cracker ou Hacker, e possuir os mesmos costumes (mecanismos) de raciocínio relacionado a descobrir as vulnerabilidades do sistema-alvo. (GIAVOROTO; SANTOS, 2013)

Todas as informações levantadas durante o processo do pentest resultarão em relatórios técnicos pormenorizados, incluindo soluções pertinentes ao sistema legado (hardware e software) avaliado, Pentest, no entanto, caracteriza-se como uma completa auditoria de segurança, pela qual explora de forma abrangente todos os aspectos que envolvem a segurança de um sistema, e uma sequência de processos é aplicada constituindo várias fases do processo de investigação, ou seja, um levantamento maciço de informações contribuirá com um resultado positivo em cima do alvo. (GIAVOROTO; SANTOS, 2013)

Considerando que todas as informações adquiridas pelo pentest serão aplicadas em benefício do sistema investigado e analisado (GIAVAROTO; SANTOS, 2013).

3 METODOLOGIA

O trabalho é composto pelos termos e conceitos relacionados com a segurança da internet, para assim ser demonstrado aos usuários de bancos um mínimo de conhecimento sobre as ferramentas de ataques pela internet, mais utilizadas pelos hackers nos dias atuais, juntamente com um estudo de caso completo e detalhado sobre o funcionamento de aplicativos móveis e sites de bancos públicos e privados, para logo depois desse entendimento, ser feita uma pesquisa de campo para entender o quanto de usuários utilizam o internet banking e os motivos pelo qual os que não o utilizam, também para testar os conhecimentos das pessoas sobre as técnicas PHISHING.

Foi instalado o software máquina virtual, que serve para instalar vários softwares em um mesmo computador, onde dentro dele foi instalada a ferramenta BACKTRACK, que é utilizada para teste de penetração, foi utilizado para os estudos sobre ataque com a técnica PHISHING que é mais utilizados nas invasões de bancos. Demonstrando alguns cuidados para não serem vitimas de hackers maliciosos, e também mostrar como utilizar a internet banking sem ser vítima.

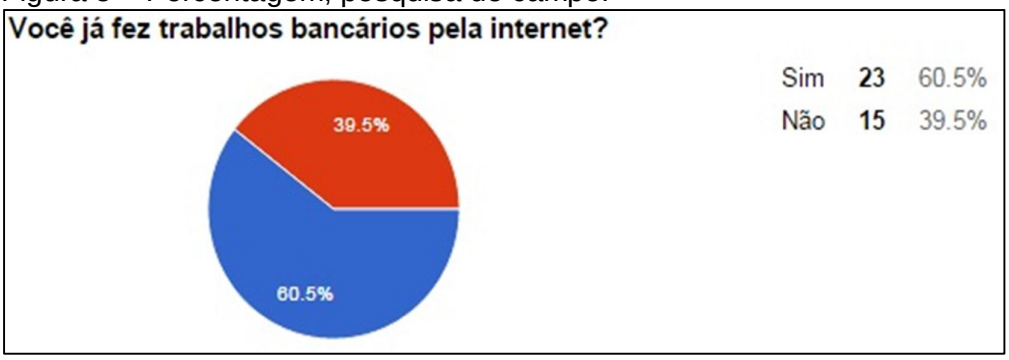
Os resultados esperados são: demonstrar como os hackers fazem seus ataques para também poder expôr informações sobre segurança e informações de Internet Banking, e que todos possam ter acesso sem medo nem receio de nada, expondo assim, de forma pratica e fácil, os modos de segurança.

3.1 APLICAÇÕES DA METODOLOGIA

Figura 5 e 6 mostra resultado de uma pesquisa de campo, onde foi realizado em faculdades da cidade de Bauru, e online pelas redes sociais, onde tiveram trinta e oito pessoas questionadas entre as faixas etárias de dezoito a quarenta anos de idade, onde são estudantes universitários e profissionais em geral, que em algum momento já realizaram algum tipo de trabalhos bancários.

Suas respostas foram que vinte e seis pessoas já realizaram trabalhos bancários e quinze pessoas não. São menos pessoas que não realizaram, mas a maioria das respostas foi por insegurança, por isso foi realizado essa técnica, para poder ter, mais adeptos aos trabalhos bancários.

Figura 5 – Porcentagem, pesquisa de campo.



Fonte: Elaborada pela autora

Figura 6 – Pesquisa de Campo – Respostas, sobre realizarem trabalhos bancários online.

Se não. Por qual motivo?	
Medo de Invadirem a conta	Não foi necessário até o momento.
Insegurança	Pois não confio na internet por mais que o computador esteja seguro
Medo de invasão de conta	Não Precisei
Pois não confio muito	tempo e comodidade. utilizo o celular para banco.
medo	insegurança de passar dados
Falta de Segurança	
Não confiar	

Fonte: Elaborada pela autora

Logo depois, foi realizado passo a passo de como os hackers conseguem realizar esse trabalho de invasão, isso foi feito para demonstrar às pessoas que não tem confiança, verificar que não é preciso tanta insegurança, pois tendo bastante atenção não têm problema de invadirem as contas.

Já conectado no BACK TRACK será verificado passo a passo de como é clonado um site.

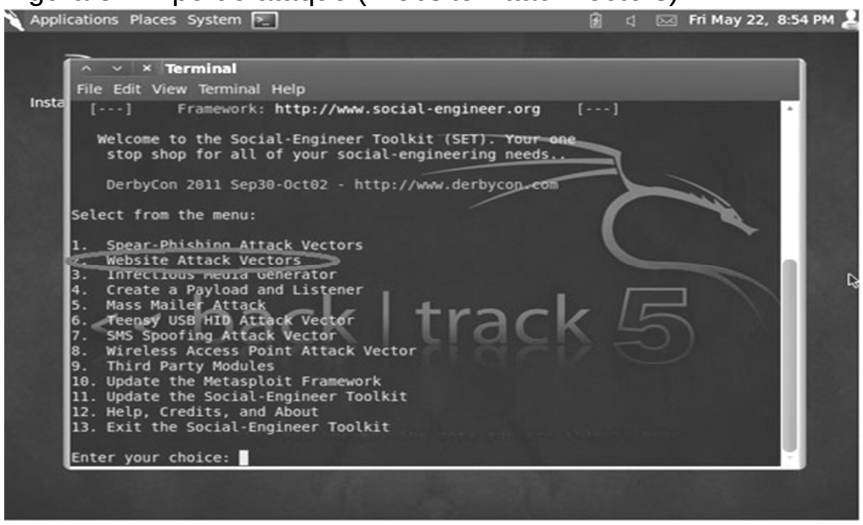
1. Entrar no Set do Social Engineering Toolkit, onde é realizado testes de invasão.

Figura 7 – Testes de invasão (Social Enginering Toolkit).

Fonte: Elaborada pela autora

2. Depois de entrar no Social será escolhido o tipo de ataque que queremos, no caso será ataque por sites.

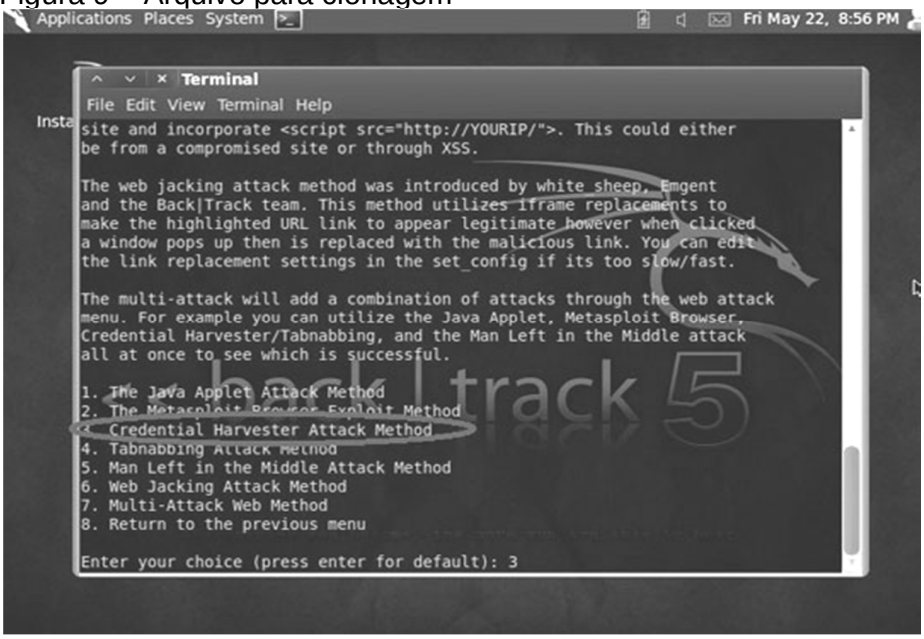
Figura 8 – Tipo de ataque (Website AttackVectors)



Fonte: Elaborada pela autora

3. Logo depois, é escolhido o tipo de arquivo para a clonagem do site.

Figura 9 – Arquivo para clonagem



Fonte: Elaborada pela autora

4. O próximo passo é o tipo de ataque dentro do website, que no caso é Site Cloner, o endereço do site a ser clonado.

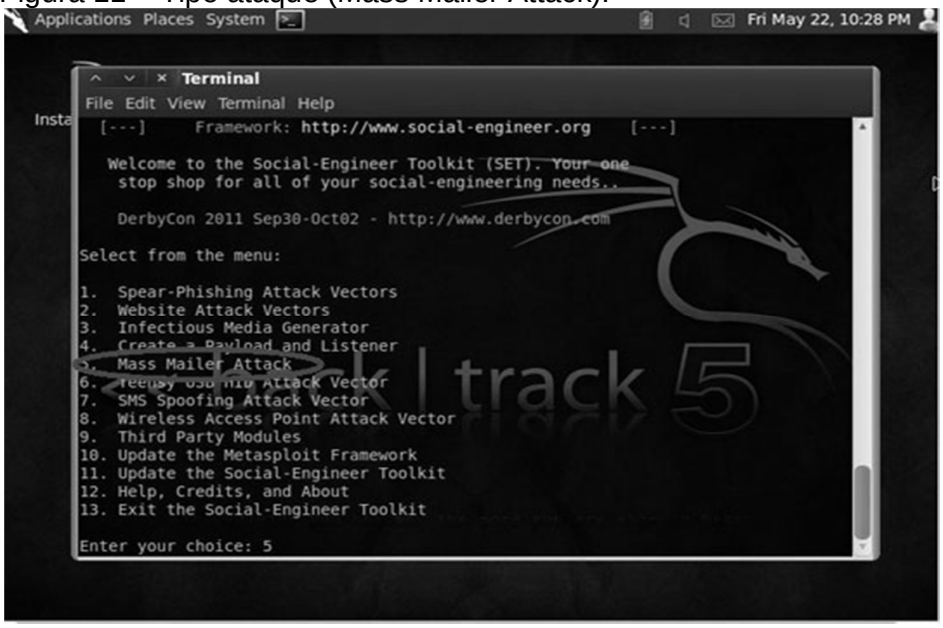
Figura 10 – Tipo ataque dentro do website (Site Cloner), e endereço do site

Fonte: Elaborada pela autora

Logo depois de realizada a clonagem do site desejado, foi criado um e-mail com o link do site falso, para mostrar para vítima um link como se fosse do site verdadeiro.É possível verificar passo a passo:

1. Depois de clonar o site, deve-se voltar para o Social Engineering Toolkit e escolher o tipo de ataque que deve ser enviado por um e-mail para vítima, que será o Mass Mailer Attack.

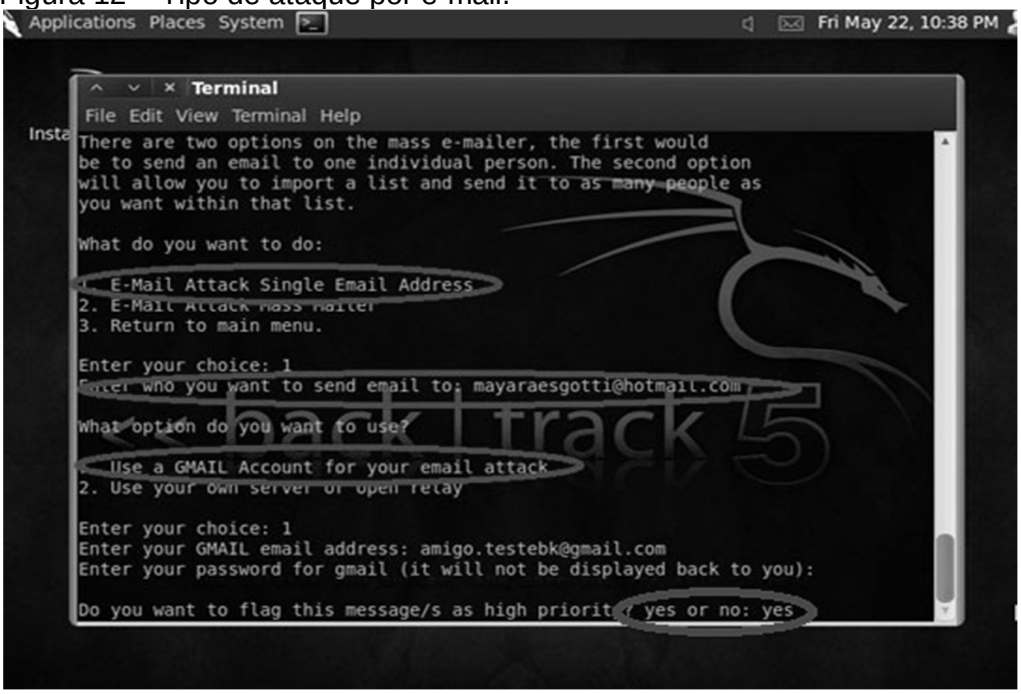
Figura 11 – Tipo ataque (Mass Mailer Attack).



Fonte: Elaborada pela autora

2. Logo em seguida foi informado o tipo de ataque por e-mail, ou seja, informar se deseja mandar “E-mail Attack Single” (para uma pessoa só) ou “E-mail Attack Mass Mailer” (para várias pessoas), no caso de e-mail simples, foi informado o e-mail a ser enviada, a mensagem, o tipo de servidor, ou seja, e-mail do atacante que nesse caso é o Gmail, e o e-mail do atacante e se a mensagem é de alguma prioridade.

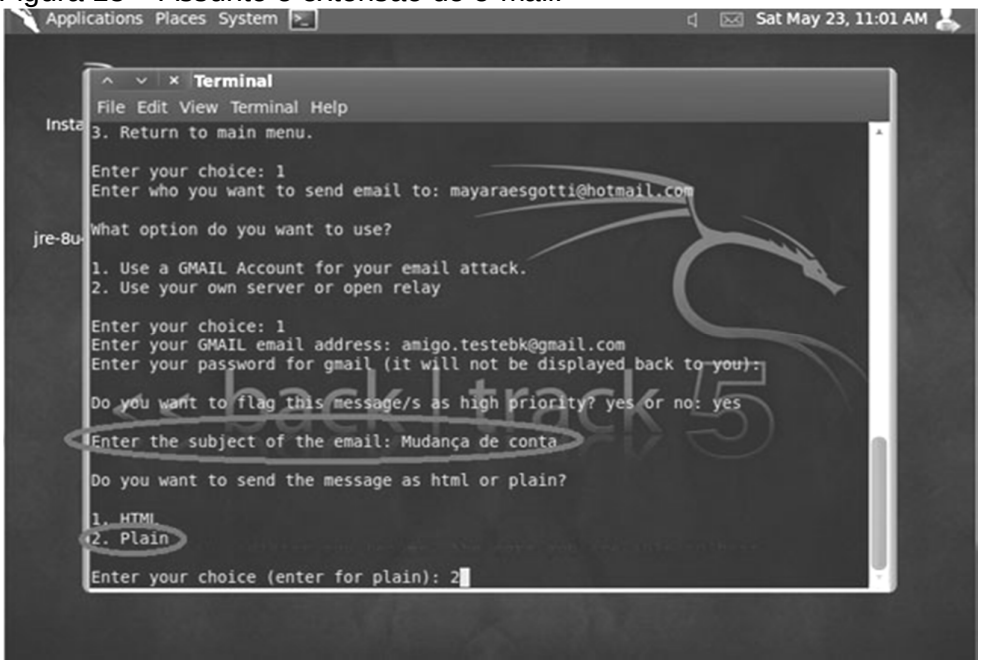
Figura 12 – Tipo de ataque por e-mail.



Fonte: Elaborada pela autora

3. Próximo passo é o assunto e o tipo de extensão que será elaborado o e-mail

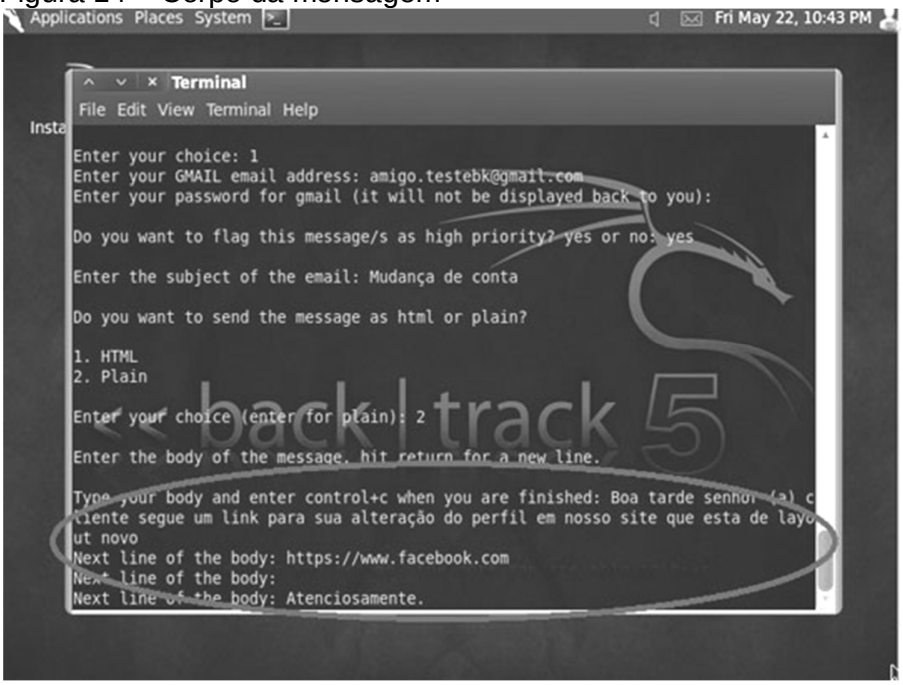
Figura 13 – Assunto e extensão de e-mail.



Fonte: Elaborada pela autora

4. E, por fim, foi criado o corpo da mensagem e, logo depois, clicado ctrl+c para ser enviada a mensagem.

Figura 14 – Corpo da mensagem



Fonte: Elaborada pela autora

Em seguida o e-mail será enviado para a vítima do suposto ataque do hacker de invasão de bancos com um link que o direcionará para um site falso, onde serão encaminhadas as informações que a vítima digitar no suposto site de volta ao atacante.

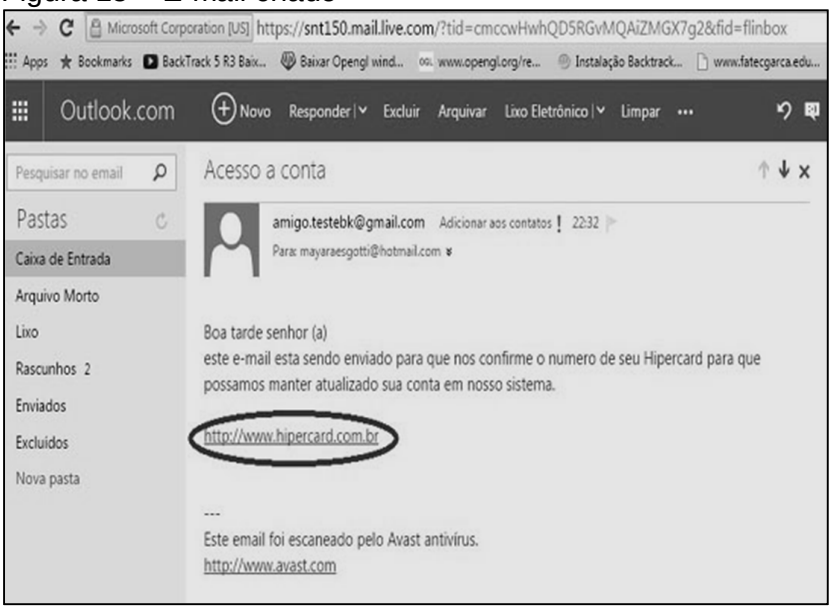
4 RESULTADOS

Com a elaboração deste trabalho foi possível chegar a resultados, em que demonstra as pessoas que sempre tiveram insegurança em realizar trabalhos bancários online e que se prevenindo e tomando alguns cuidados simples é possível, sim, navegar com segurança e sem transtornos depois.

Com uma pesquisa de campo foi comprovado que ainda existe aquelas pessoas que não realizam trabalhos bancários online, e maioria das respostas sobre o assunto foram por insegurança, de terem suas contas invadidas.Então foi possível demonstrar que tem como navegar com segurança.

Então, logo em seguida, é enviado um e-mail à vítima, onde tem um link que aparentemente é do site que deseja navegar.

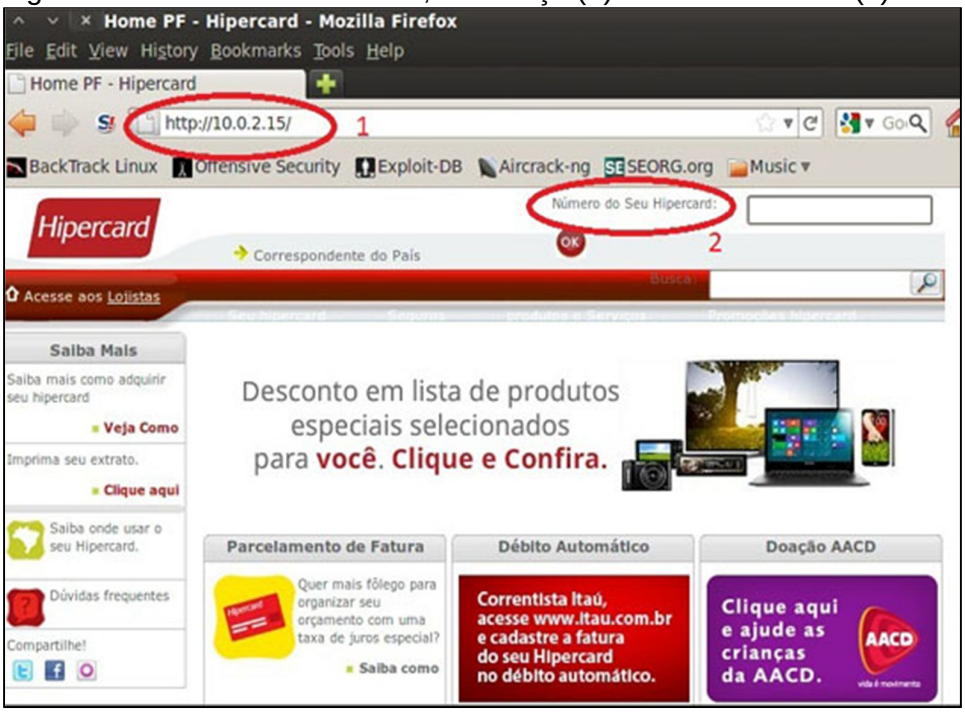
Figura 15 – E-mail criado



Fonte: Elaborada pela autora

Assim que a vítima clica no link que parecia apenas uma navegação ao site desejado, a vítima é automaticamente encaminhado ao site falso. Por isso deve-se tomar cuidado. A Figura 16 mostra que a parte mais importante de se notar quando é aberto um link de um site pelo e-mail, é quando o site abrir e verificar se o endereço está igual do site que navegar com frequência, se caso tiver um nome diferente o ideal é fechar imediatamente.

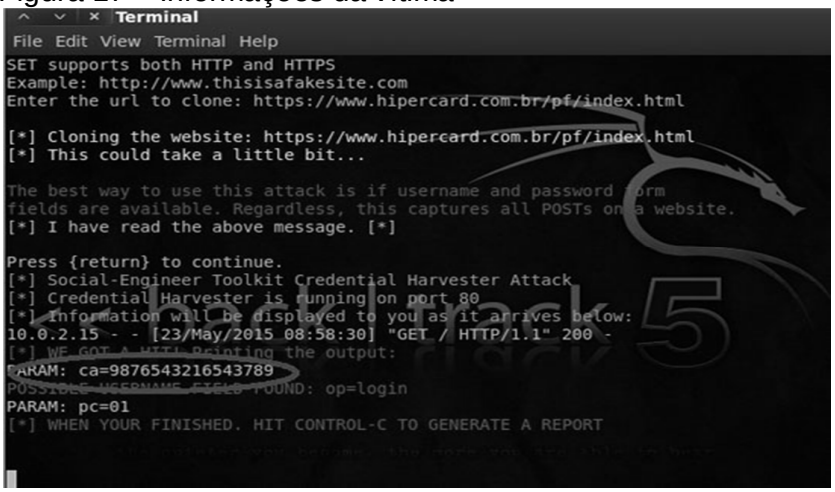
Figura 16 – Tela Site falsificado, Endereço (1) e Numero cartão (2)



Fonte: Elaborada pela autora

E se a vítima não percebe de que se trata de um site falsificado e insere o número de conta ou até o número de cartão será encaminhado ao atacante uma lista com toda a informação da vítima em relação aquele site, como mostra a Figura 17.

Figura 17 – Informações da vítima



Fonte: Elaborada pela autora

5 CONCLUSÃO

Foram feitos uns cem testes sobre a técnica de Phishing tipo de conduta fraudulenta, muito utilizada por hacker em invasão de banco, sendo esses testes sobre clonagem de sites bancários e envio com link do site falso por e-mail das possíveis vitimas que podem ser qualquer pessoa que realize trabalhos bancários online, onde foi possível perceber que são mínimos os sites que ainda permitem serem clonados e que seja possível pegar as informações, a maioria permite que sejam clonados, mas na hora que a vítima digita as informações no site falso, as informações não são informadas de volta para o atacante, onde são os sites que já têm a segurança, e são na maioria.

Também foi demonstrado que mesmo se o site bancário tiver a segurança necessária, mas a pessoa não tiver o software instalado no computador onde se está acessando o site, mesmo assim está correndo risco, então foi mostrado que a melhor forma de estar seguro será sempre que clicar em algum link mandado por e-mail é visualizar o endereço do site que costuma acessar, se não estiver esse endereço pode não ser o mesmo site, e se tiver dúvidas da idoneidade do mesmo não passe as informações pessoais.

Os trabalhos futuros são de continuar os testes de Phishing para todos os sites bancários, para poder assim demonstrar quais são seguros ou não, depois de verificado, os que não forem seguros, conscientizar as pessoas da melhor forma de se navegar naquele mesmo site. Logo depois verificar os outros tipos de ataques existentes no sistema operacional do BackTrack, para sempre poder orientar as pessoas de como se prevenir para não caírem nesses golpes, ou seja, trabalhando sempre com prevenção.

REFERÊNCIAS

CONTAS DA UNIÃO. T; **Secretaria de Fiscalização de Tecnologia da Informação**. 3 ed. Brasília: TCU, 2008.

CORREIA, M. A.; **Segurança em Internet Banking,** 2008. Disponível em: https://ins3rt.s3.amazonaws.com/media/papers/Sbseg2008_BancoDoBrasil.pdf, Acesso em 17 de Abril de 2014.

FILHO Reinaldo, D.; **A Responsabilidade dos Bancos pelos Prejuízos Resultantes do Phishing.** Disponível em: <HTTP://dialnet.unirioja.es/servlet/articulo?codigo=2857931>. Acesso em: 15 de Fev.de 2014.

GIAVOROTO, S. C. R; SANTOS, G. R; **Backtrack Linux:** Auditoria e Teste de invasão em redes de computadores. Rio de Janeiro: Editora Ciência Moderna Ltda, 2013.

LYRA, R. M.; **Segurança e auditoria em sistemas de informação.** Rio de Janeiro: Ciência Moderna, 2008.

MARTINS, P. H.; **Estudo exploratório sobre arquitetura de firewalls e os elementos associados nas implementações dos mesmos em redes de computadores de pequenas e médias empresas da região de Bauru.** Monografia (Especialização em Sistema de Informação para Internet). 61p. Bauru. Universidade do Sagrado Coração, 2004.

MITINICK, K. D. et al. **A arte de enganar:** Ataques de Hackers: Controlando o Fator humano na Segurança da Informação. 4 ed. São Paulo: Pearson Makron Books 2003.

McCLURE, S.; et al. **Hacker Expostos:** Segredos e Soluções para a segurança de Redes. Rio de Janeiro: Campus, 2003.

STREBE, M.; PERKINS, C.; **Firewalls,** Makron Books: São Paulo, 2002.

VARGAS, G; **10 Anos de Internet Banking:** Desvendando o processo de incorporação de tecnologia em um banco brasileiro através de uma abordagem sociotécnica, 2006. Disponível em: <http://gvpesquisa.fgv.br/sites/gvpesquisa.fgv.br/files/publicacoes/10%20Anos%20de%20Internet%20Banking.pdf>, Acesso em 03 de Maio de 2014.

ZWICKY, E. D. et al. **Construindo Firewalls Para a Internet.**2 ed. Rio de Janeiro: Campus 2000.

ANEXO - INSTALAÇÃO DO BACKTRACK

A instalação do BACKTRACK é relativamente fácil, poderá instalá-lo diretamente em sua máquina, em uma máquina virtual, rodar diretamente de um CD ou até mesmo em um dispositivo pen drive.

1. Após inserir o CD de instalação ou o dispositivo, a tela de subida do sistema será exibida, selecione o modo Default Boot TextMode.

Figura 18 – Tela Inicial BACKTRACK

Fonte: Giavoroto (2013)

2. Próximo passo será entrar em modo gráfico, digite startx para poder entrar em modo gráfico.

Figura 19 – Carregamento de ambiente gráfico

Fonte: Giavoroto (2013)

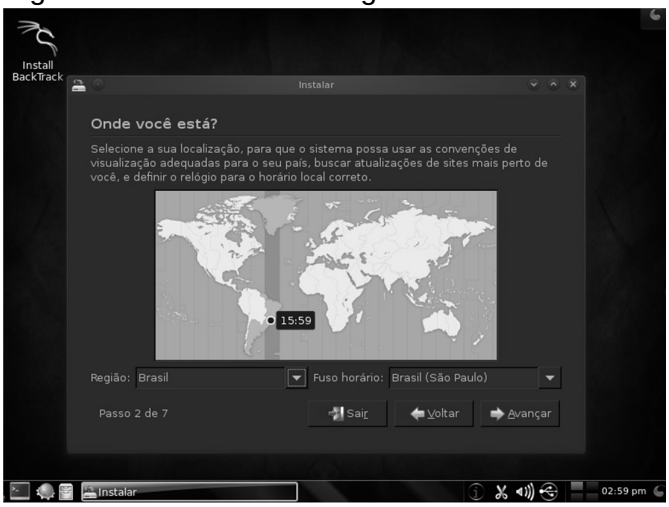
3. Já no modo gráfico do BACKTRACK, dê um clique duplo no ícone Install BACKTRACK existente na área de trabalho, a janela de seleção de idioma surgirá, selecione o idioma desejado e clique em avançar.

Figura 20 – Seleção de Idiomas

Fonte: Elaborada pela autora

4. Será exibida a tela para seleção da região e horário, ajuste conforme sua região e fuso horário.

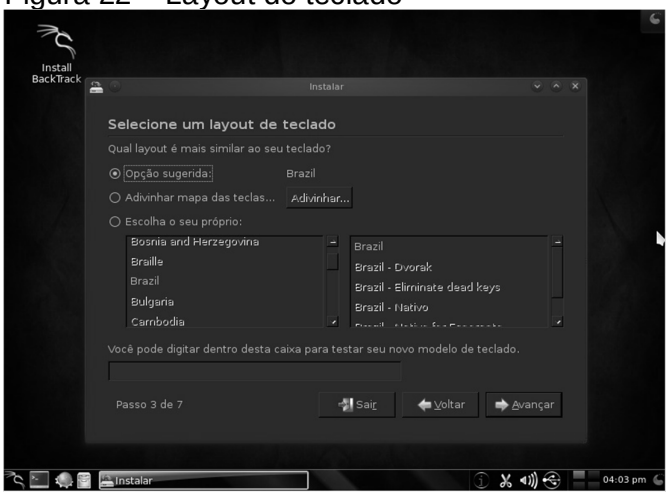
Figura 21 – Escolha da Região e fuso horário



Fonte: Elaborada pela autora

5. Em seguida, a tela de configuração do teclado será mostrada, basta selecionar o layout que parece com seu teclado.

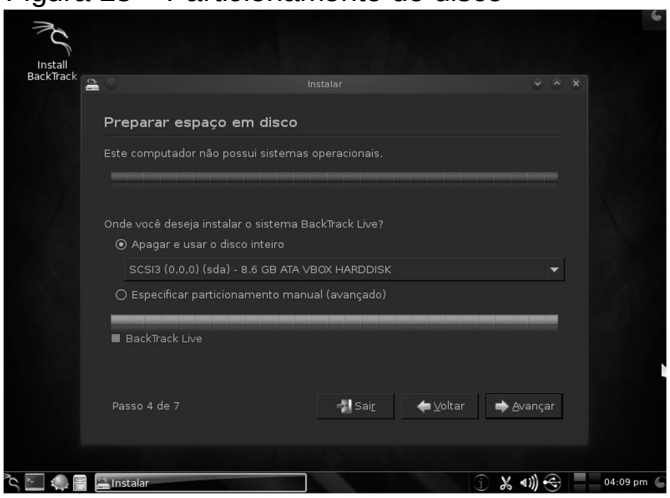
Figura 22 – Layout do teclado



Fonte: Elaborada pela autora

6. Será exibida uma janela de particionamento, selecione apagar e usar disco.

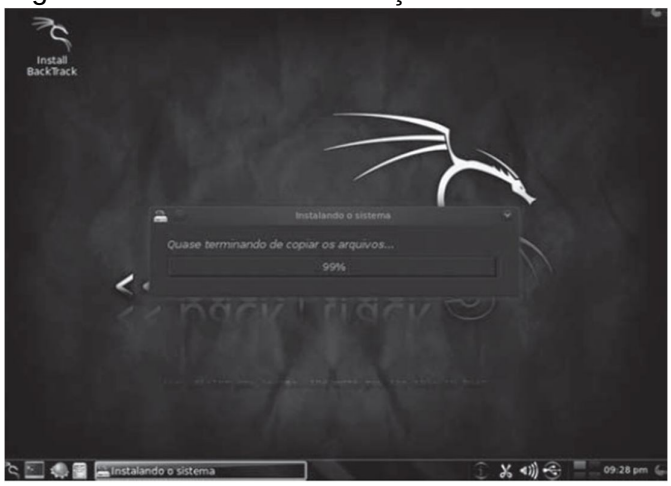
Figura 23 – Particionamento do disco



Fonte: Elaborada pela autora

7. Por fim, será exibida a janela sobre o status da instalação.

Figura 24 – Status de Instalação



Fonte: Elaborada pela autora.