UNIVERSIDADE DO SAGRADO CORAÇÃO

FELIPE ROBERTO FONSECA PEREIRA

ANÁLISE DE VULNERABILIDADE EM SISTEMAS COMPUTACIONAIS UTILIZANDO FERRAMENTAS DE DISTRIBUIÇÃO LIVRE

BAURU
2015

FELIPE ROBERTO FONSECA PEREIRA

ANÁLISE DE VULNERABILIDADE EM SISTEMAS COMPUTACIONAIS UTILIZANDO FERRAMENTAS DE DISTRIBUIÇÃO LIVRE

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. Dr. Elvio Gilberto da Silva.

BAURU
2015

Pereira, Felipe Roberto Fonseca

P4364a

Análise de vulnerabilidade em sistemas computacionais utilizando ferramentas de distribuição livre / Felipe Roberto Fonseca Pereira. -- 2015.

60f. : il.

Orientador: Prof. Dr. Elvio Gilberto da Silva.

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

1. Análise de vulnerabilidade. 2. Sistemas computacionais. 3. Ferramentas. 4. Linux. 5. Pentest. I. Silva, Elvio Gilberto da. II. Título.

FELIPE ROBERTO FONSECA PEREIRA

ANÁLISE DE VULNERABILIDADE EM SISTEMAS COMPUTACIONAIS UTILIZANDO FERRAMENTAS DE DISTRIBUIÇÃO LIVRE

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Dr. Elvio Gilberto da Silva.

Banca examinadora:

_____

Prof. Dr. Elvio Gilberto da Silva
Universidade do Sagrado Coração

_____

Prof. Me. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____

Prof. Esp. Alex Setolin Beirigo
Universidade do Sagrado Coração

Bauru,8 de Dezembro de 2015.

RESUMO

A redução dos preços dos computadores e a facilidade de conexão à internet tem causado grande aumento na popularidade dos dispositivos computacionais. O aumento da conectividade faz com que a segurança da informação seja um assunto cada vez mais reincidente no atual cenário computacional. Novas tecnologias são desenvolvidas a cada momento, da mesma forma, falhas são descobertas, exploradas e corrigidas enquanto estas tecnologias estão em uso. A evolução contínua da segurança e de novas tecnologias traduz-se, na prática, em uma impossibilidade de possuir ou desenvolver um sistema 100% seguro. Como alternativa a essa impossibilidade deve-se buscar vulnerabilidades, estudá-las e explorá-las, limitando-as ou corrigindo-as. Avaliações preventivas nos sistemas computacionais podem revelar falhas potenciais a serem consideradas e corrigidas antes que um usuário mal intencionado possa explorá-las. O objetivo principal do presente trabalho foi demonstrar as vulnerabilidades de acesso privilegiado em sistemas computacionais utilizando técnicas de invasão com o sistema operacional Linux e ferramentas de livre distribuição. O estudo foi desenvolvido em duas fases distintas: uma fase de investigação dos aspectos teóricos, e uma etapa prática de aplicação das técnicas de invasão, com o intuito de obter acesso a um sistema computacional. Dentre os diversos ataques pesquisados, o “Brute Force” foi o que se mostrou mais efetivo quando utilizado em conjunto com uma wordlist. Como exemplo deste processo pode-se citar um teste realizado com o servidor de e-mails - Gmail, o qual após 100 tentativas de senhas bloqueou o usuário por cerca de 3 minutos, além de que, para testar estas 100 senhas pode-se levar um tempo considerável, entretanto, se a senha estiver em uma posição bem alta na wordlist, o processo pode levar de semanas a anos, tornando-se assim ineficiente. Espera-se com esse trabalho contribuir para melhoria da segurança dos sistemas computacionais.

Palavras-chave: Análise de vulnerabilidade. Sistemas computacionais. Ferramentas. Linux.

ABSTRACT

The reduction in the prices of computers and internet connection facility has caused huge increase in the popularity of computing devices. Increased connectivity means that information security is an issue increasingly recurrent in the current computing scenario. New technologies are developed every time, in the same way, faults are discovered, explored and corrected while these technologies in use. The continuous evolution of security and new technologies is reflected in practice in an inability to have or develop a 100% secure system. As an alternative to this inability must be sought vulnerabilities, study them and exploit them, limiting them or correcting them. Preventive evaluation in computer systems can reveal potential failures to be considered and corrected before a malicious user can exploit them. The main objective of this study was to demonstrate the privileged access vulnerabilities in computer systems using hacking techniques to the Linux operating system and free distribution tools. The study was conducted in two phases: a phase of investigation of the theoretical aspects and practical stage of implementation of hacking techniques, in order to gain access to a computer system. Among the several researched attacks, "Brute Force" was what was more effective when used in conjunction with a wordlist. As an example of this process can cite a test conducted with the e-mail server Gmail, which after 100 attempts passwords locked the user for about three minutes, and that to test these 100 passwords can be taken considerable time, however, if the password is in a very high position in the wordlist, the process can take anywhere from weeks to years, thus making it ineffective. It is hoped that this work contribute to improving the security of computer systems.

Keywords: vulnerability analysis. Computer systems. Tools. Linux.

LISTA DE ILUSTAÇÕES

SUMARIO

1 INTRODUÇÃO

Atualmente o uso de tecnologias e sistemas computacionais estão presente no dia a dia de toda população, e são diversos os meios de acesso a informação e formas de comunicação, muitas utilizam-se de sistemas computacionais para fazer a troca de dados por meios de e-mails, redes sociais e mensagens. Para isto tem a necessidade de sistemas que possuem formas de autenticação pessoal.

Através de logins e senhas os usuários confirmam sua identidade e ganham acesso ao sistema. Devido a esta popularização ao acesso de sistemas computacionais, muitas pessoas mal intencionadas podem aproveitar-se de algumas vulnerabilidades e ganhar acesso privilegiado de forma indevida, obtendo informações confidenciais.

O aumento da conectividade, ao mesmo tempo em que é positivo pelo avanço tecnológico, faz com que a segurança da informação seja um assunto cada vez mais reincidente no atual cenário computacional. Entre os anos de 2010 e 2012, os aumentos sofridos e reportados por empresas e instituições brasileiras passam de 200%. (ESTATÍSTICAS CERT.BR, 2012). As empresas estão sendo cada vez mais vítimas de muitos ataques, vindos dos mais variados locais, ocasionando danos incalculáveis.

Essa evolução de ataques virtuais denota a carência por um modelo eficaz de segurança que assegure a integridade dos recursos, tanto em nível de usuários domésticos como organizacionais. Devido a isso, muitas vezes justifica-se a contratação externa de uma empresa de auditoria para avaliar a segurança de um sistema computacional, simulando um ataque de uma fonte maliciosa, isso dependendo do escopo e do tamanho da empresa, evitando assim perdas financeiras.

Novas tecnologias são desenvolvidas a cada momento e incorporadas aos sistemas de comunicação em um processo contínuo. Da mesma forma, falhas são descobertas, exploradas e corrigidas enquanto estas tecnologias estão em uso. Isso gera um constante conflito entre a geração de novas funcionalidades e a segurança relacionada ao seu uso. (NAKAMURA; GEUS, 2007).

A evolução contínua da segurança e de novas tecnologias traduz-se, na prática, em uma impossibilidade de possuir ou desenvolver um sistema 100% seguro.

Como alternativa a essa impossibilidade deve-se buscar vulnerabilidades, estudá-las e explorá-las, limitando-as ou corrigindo-as. (FARMER; VENEMA, 1993). Avaliações preventivas nos recursos de sistemas computacionais podem revelar falhas potenciais a serem consideradas e corrigidas antes que um usuário mal intencionado possa explorá-las.

Com base neste contexto, o objetivo deste trabalho é Demonstrar as vulnerabilidades de acesso privilegiado em sistemas computacionais utilizando técnicas de invasão com o sistema operacional Linux, colaborando assim, com a disseminação do conhecimento na área de segurança de informação.

2 OBJETIVOS

A seguir serão explorados os objetivos do trabalho.

2.1 OBJETIVO GERAL

Demonstrar as vulnerabilidades de acesso privilegiado em sistemas computacionais utilizando técnicas de invasão com o sistema operacional Linux, colaborando assim, com a disseminação do conhecimento na área de segurança de informação.

2.2 OBJETIVOS ESPECÍFICOS

a) Estudar tipos de testes de invasão, tipos de ataques, ferramentas de ataques e soluções gratuitas;
b) Conceituar ambientes de invasão e termos específicos da área, afim de demonstrar e exemplificar técnicas utilizadas para invasões;
c) Pesquisar sobre vulnerabilidades em sistemas computacionais
d) Apresentar técnicas de invasão utilizando o sistema operacional Kali Linux e backtrack;
e) Demonstrar diversas ferramentas contidas nos sistemas operacionais Backtrack e Kali de forma pratica e didática.
f) Apresentar análises de tempo, efetividade, etc, com base nas ferramentas que serão utilizadas para os testes, afim de descobrir qual o melhor método de realizar um ataque bruteforce.
g) Pesquisar formas de proteção e criação de logins seguros contra ataques;
h) Redigir relatório comparativo, afim de apresentar aos interessados as vulnerabilidades detectadas;
i) Elaborar orientações de proteção contra ataques e invasões.

3 REVISÃO DA LITERATURA

3.1 INFORMAÇÃO

Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. (SILVA FILHO, 2004).

Informação é tudo aquilo que pode gerar conhecimento, que será utilizado por alguém ou alguma estrutura posteriormente, sendo necessário seu armazenamento para futura consulta. (SILVA FILHO, 2004).

Para Oliveira (2000), a informação é um recurso vital para a empresa e integra, quando devidamente estruturada, os diversos subsistemas e, portanto, as funções das várias unidades organizacionais da empresa.

3.1.1 Segurança da informação

Segundo Associação Brasileira De Normas Técnicas (ABNT, 2005) pode-se entender como segurança de informação vários aspectos, consideramos a informação como um ativo, algo que tenha valor, ou seja, o nome e informações de funcionários, documentos de analises e testes feitos pela empresa, projetos ou a parte financeira da empresa. Todas estas informações devem ser armazenadas e mantidas por sistemas seguros, e o conteúdo destes dados são chamados de ativos e como todo ativo, deve ser protegido pelos responsáveis de segurança.

Em conformidade com a ABNT (2005), Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

De acordo com a norma americana Instituto Nacional de Padrões de tecnologia (NIST) define segurança da computação como:

> A proteção conferida a um sistema de informação automatizado, a fim de atingir os objetivos da preservação da integridade,

> disponibilidade e confiabilidade dos recursos de um sistema de informação (incluindo hardware, software, firmware e telecomunicações). (NIST, 2008).

Complementando esta informação encontra-se na norma ABNT NBR ISO/IEC 27001 (2013) que um sistema de gestão de segurança deve preservar a confidencialidade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos, e fornecer confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

Segurança da informação refere-se a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repudio e confiabilidade, podem também estar envolvidas com a segurança da informação.

Disponibilidade é a obrigação de manter o serviço ou acesso sempre ativo, a informação não pode em nenhuma circunstância estar retida, ela existe para ser armazena e acessada quando necessário, temos que levar em conta que caso a disponibilidade seja interrompida por algum advento causará ônus a parte contratante, podendo até certo ponto ser imensurável. A disponibilidade de informação de uma empresa pode ser calculada levando em conta o prejuízo causado por algum advento. (TANENBAUM, 2003).

Confidencialidade é a propriedade de que a informação não esteja disponível ou revelada a indivíduos ou entidades que não são autorizados, é o dever que inclui a preservação das informações privadas.

Em um sistema computacional deve haver controles para garantir que a informação seja disponibilizada apenas para aqueles que possuem autorização prévia, a informação deve ser confidencial e manter-se confidencial. Toda informação deve ter medidas para acesso, e este acesso deve ser controlado e preservado, caso seja violado os danos são dos mais variados, caso uma mensagem seja vista por algum fora do limite de acesso pode causar prejuízo e constrangimento aos envolvidos. (MARTINS, 2004).

Integridade assegura que as informações e programas são alterados apenas de um modo especifico e autorizado, garante que o sistema execute de uma forma prevista, livre de manipulações não autorizadas e manter as configurações estabelecidas pelo criador até o fim de seu ciclo (criação,

manutenção e descarte). A perda da integridade tornar a informação sem valor, ou com seu objetivo subvertido. (SILVA FILHO, 2004).

Chamamos de Confidentiality, Integrity, and Availability (CIA) uma conhecida e respeitada política de desenvolvimento, usada para identificar áreas com problemas e soluções necessárias para a segurança da informação, ela ajuda os interessados a refletirem sobre os importantes aspectos da segurança de TI.

Segundo Vallabhaneni (2002) são conceitos importantes a serem considerados no estudo da segurança da informação:

a) Entidade: usuário, processo ou dispositivo que irá acessar uma determinada informação ou serviço;

b) Atributos: características únicas pertencentes a entidade que permite distingui-la das demais entidades;

c) Identificação: processo de reconhecimento da entidade através de seus atributos;

d) Autenticação: processo de validação da identidade da entidade;

e) Autorização: processo de prover ou retirar privilégios de uma entidade;

f) Contabilização (accountability): processo para realizar o log das ações realizadas por uma entidade;

g) Controle (assurance): garante que os princípios básicos de segurança (tríade CIA) e de contabilização estejam assegurados

h) Não –repúdio: assegura para uma entidade a negação de uma ação realizada.

i) Auditoria (audit): revisão por uma entidade independente sobre os controles e a conformidade dos requisitos de segurança.

A necessidade de uma rede segura e eficaz transcende o limite da produtividade, quando por um lado a eficiência do negócio através de novos métodos e produtos garantem uma grande vantagem competitiva, a falta de segurança pode colocar tudo em risco e por ventura, gerando grandes prejuízos, até exaurir toda finança da empresa.

3.1.2 VIGILÂNCIAS

Segundo Krutz e Vines (2001) deve-se designar um responsável pela classificação da informação. Recomenda-se que esta tarefa seja desempenhada pelo proprietário da informação ou sistema. Todas as informações geradas devem receber uma classificação. Periodicamente, o proprietário da informação deverá revisar a classificação fornecida, pois a criticidade da informação pode ser alterada ao longo do tempo.

Por exemplo, o desenvolvimento e o lançamento de um novo produto, somente deve ser classificada como informação confidencial e tratada como tal até o lançamento do produto, pois após esse evento, ela deixa de ser uma informação confidencial, e passa a ser pública.

Todos os membros da organização devem entender a importância da segurança para a mesma, atuando todos como guardiões da rede. Já o aspecto técnico compreende um processo regular e consistente, que inclui o monitoramento dos sistemas e da rede.

É necessária a definição de como responder a alarmes e alertas, como e quando checar a implementação e as mudanças nos dispositivos de segurança e como ser vigilante com relação às senhas de usuários. (NAKAMURA; GEUS, 2007).

3.1.3 SEGURANÇA DA INFORMAÇÃO EM AMBIENTE CORPORATIVO

O moderno mundo globalizado propicia as empresas um ambiente feroz e agressivo, as quais necessitam se reinventar a cada dia, lançar novos produtos, conquistar novos clientes e superar diariamente seus concorrentes. Manter uma imagem boa de sua empresa é essencial.

As consequências das falhas em um sistema computacional pode resultar na interrupção do serviço, causando ônus aos colaboradores e clientes, e além destas falhas que afira diretamente a rotina dos envolvidos há outras formas de detrimentos ainda superiores a serem estudados, como a de extravio de informações consideradas sigilosas, como estratégias de negócio, táticas a serem abordadas, pesquisas de mercado realizada pela empresa, informações

de clientes ou colaboradores balanços financeiros e etc. (NAKAMURA; GEUS, 2007).

Os dispositivos como cabos, servidores, switches, roteadores e computadores possuem um valor financeiro mensuráveis, porém, as informações e registros contidos em periféricos de armazenamento são de importância fundamental à continuidade da empresa, e muito mais valiosa de que qualquer equipamento tangível, objetivo de segurança de rede não é na rede em si, mais nos dados que nela trafegam. (NESTLER, 2011).

Qualquer destas características que estão livres para serem comprometidas são consideradas vulnerabilidades. Um risco é qualquer possibilidade de dano a informação, existe nos estágios de armazenamento, transmissão e processamento, sendo assim, a informação pode estar vulnerável de diferentes formas em qualquer um destes estados. (NESTLER, 2011).

Uma falha, uma comunicação com informações falsas ou um roubo ou fraude de informações pode trazer graves consequências para a organização, como a perda de mercado, de negócios e, consequentemente, perdas financeiras. Desse modo, a proteção, não só das informações e de seu capital intelectual, mas também de todos os recursos envolvidos na infraestrutura de rede, deve ser tratada com a devida importância. (NAKAMURA; GEUS, 2007).

Desta maneira é necessário investir em infraestrutura e processos de continuidade, pois caso haja uma invasão, os danos são cataclísmico, se algum atacante divulgue informações confidenciais de seus clientes, denigrira sua imagem, causando prejuízos imensuráveis. De acordo com Muller (2014), e segundo os analistas consultados pelo The Hollywood Reporter, a Sony Pictures terá um prejuízo de cerca de US$ 200 milhões em decorrência dos ataques hacker que comprometeram toda a rede da empresa. O uso eficiente de tecnologias para evolução da empresa deve ser encarado como uma ferramenta crucial para o desenvolvimento e permanência da empresa no mercado.

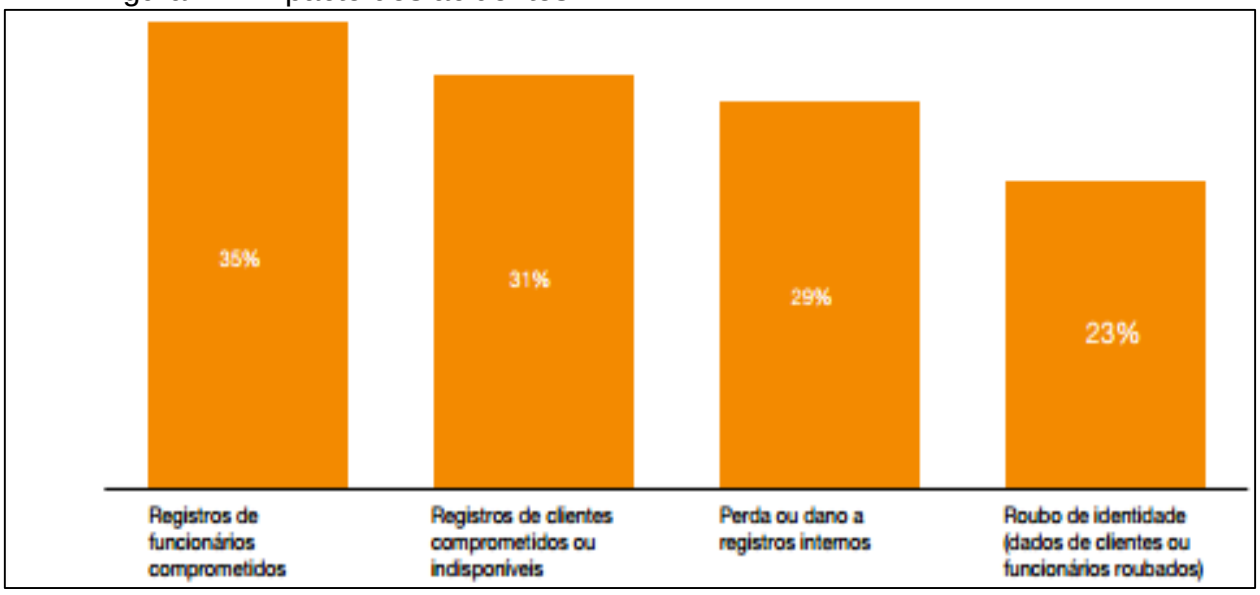
O uso da tecnologia possui um sentido muito amplo, e deve-se tirar proveito das inovações tanto para a criação e desenvolvimento de produtos quanto para o estabelecimento de novos canais de relacionamento com os clientes. (NAKAMURA; GEUS, 2007). Com o advento da tecnologia surgiram novos desafios quanto a segurança da informação, toda corporação está vulnerável a ataques provenientes desta conectividade moderna.

Os ataques aos sistemas apresentam objetivos diferentes e o seu sucesso depende do grau de segurança dos alvos e da consequente capacidade do hacker em atacá-los. Conforme ABNT (2005), infelizmente ainda alguns sistemas não foram projetados para serem seguros, a maneira de protege-los ainda é limitada, e em alguns casos carecem de profissionais capazes de assegura-las, as técnicas de segurança devem ser apoiadas por uma eficiente gestão e procedimentos técnicos apropriados.

Uma segurança plena requer o engajamento de todos os colaboradores envolvidos e políticas rigorosas para manter a rede segura, em alguns casos é necessário contratar uma consultoria externa para assegurar toda confiabilidade da rede.

Os problemas a serem resolvidos nos ambientes cooperativos refletem fielmente a situação de muitas organizações atuais que buscam a vantagem competitiva por meio da necessária utilização da tecnologia. O ambiente cooperativo é complexo, e a segurança necessária a ser implementada é igualmente complexa, envolvendo aspectos de negócios, humanos, tecnológicos, processuais e jurídicos. (NAKAMURA; GEUS, 2007).

Figura 1 – Impacto dos acidentes.



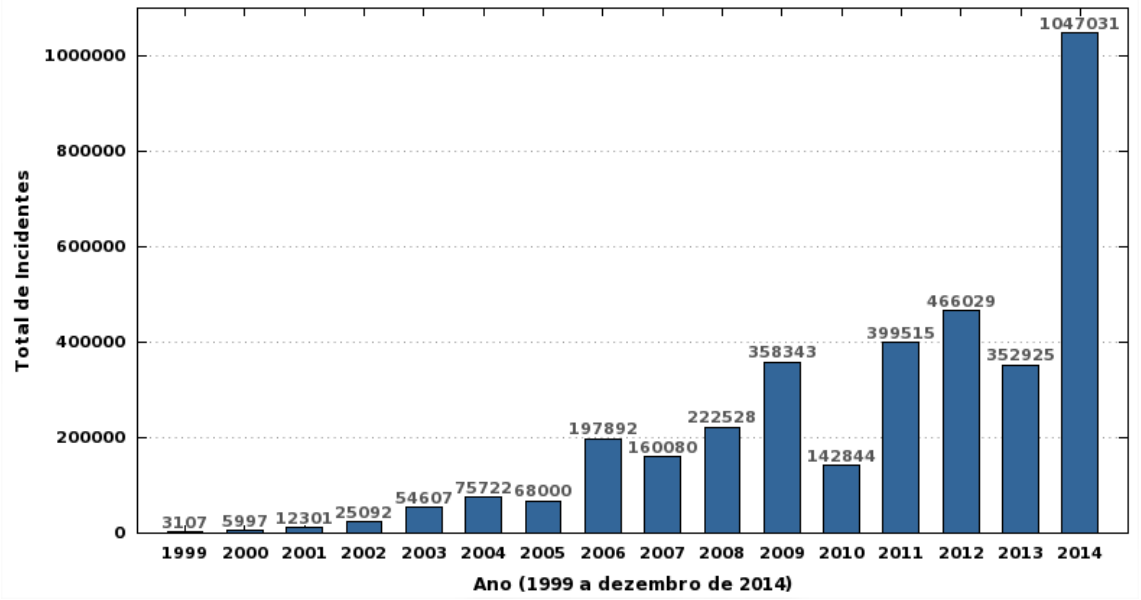
Fonte: Alves (2015).

Segundo dados apresentados na Figura 1, 29% do impacto se refere a perda de informações sigilosas pela empresa, e a maior parte dos dados ferem diretamente funcionários, que são expostos dados de maneira indevida.

“Cerca de 60% de todas ameaças (de softwares malignos) dos últimos 20 anos surgiram nos últimos 12 meses” segundo Weafer (2014 apud ALVES, 2015), Vice-Presidente de segurança da informação da Sysmantec (empresa provedora de serviços relacionado a segurança da informação e programas maliciosos). A cada dia surgem novas formas de ameaças, forcejando burlar a segurança afim de causar os mais dissímis danos.

A Figura 2 ilustra que o número de incidentes envolvendo segurança da informação em empresas mais que duplicou de 2013 a 2014 mostrando a necessidade no investimento e estudo desta área afim de combater de maneira contundente os invasores.

Figura 2 - Total de incidentes reportados



Fonte: Estatísticas CERT.BR (2014).

3.2 TESTE DE INVASÃO

Segundo Muniz e Lakhani (2013), auditoria é uma avaliação técnica feita em um sistema ou aplicativo, estas avaliações são realizadas por especialistas capazes de identificar vulnerabilidades em sistemas, aplicações e processos. Ainda segundo o autor, o teste de invasão vai além de apenas uma avaliação, pois identificando as vulnerabilidades, realiza-se testes para aferir se um atacante pode ou não utilizar-se destas vulnerabilidades para invadir ou ferir a integralidade do sistema. Como por exemplo, o auditor em um teste de invasão,

utilizando-se de inúmeras ferramentas, tenta atacar estas vulnerabilidades da mesma maneira que um atacante mal intencionado para verificar quais são realmente passiveis de exploração, reduzindo assim a lista de falhas a serem corrigidas.

Um bom teste de invasão não é aquele que abrange a rede inteira, e sim o que possui um objetivo especifico em um sistema ou rede especifica, qualidade é sempre melhor que quantidade. Teste de invasão serve para mensurar a efetividade da segurança existente, refere-se ao termo em inglês “penetration test” ou “pentest”. (MUNIZ; LAKHANI, 2013).

Teste de invasão(pentest) é a metodologia, processos, e procedimentos usados por aqueles que realizam testes, com aprovação do administrador da rede, seguindo guias de tentativas especificas para burlar determinada rede ou sistema, este tipo de teste é associado em acessar as configurações e controles técnicos, administrativos e operacionais do sistema. Estes testes não devem ser de conhecimento da equipe de rede, apenas os mais altos cargos podem ter ciência da realização, para garantir a confiabilidade do teste. (BROAD; BINDNER,2014).

Teste de invasão é uma análise profunda sobre a real segurança que uma organização possui, somente desta forma é possível saber quais são os riscos, qualifica-los e tomar atitudes para conte-los, priorizando os mesmos com base em critérios adotados pelos administradores e interessados.

Após ciência dos riscos e vulnerabilidade aferida no sistema, é necessário transmitir estas informações através de relatórios elaborados pelos contratados do teste de invasão, com base no conhecimento obtido neste relatório, é possível que os interessados responsáveis pela segurança da informação tomem as providências, dando prioridade naquelas onde mais apresentam risco ao objetivo de negócio da organização. (BROAD; BINDNER, 2014).

Novas ameaças surgem todo dia, juntamente a isso, falhas e erros em sistemas que garantem a segurança são descobertos logo após seu lançamento, convém ao administrador de rede ou responsável pela segurança da informação atualizar-se sempre que possível, e que o teste de vulnerabilidade e análise de riscos sejam feitos periodicamente para contemplar qualquer mudança ou descoberta de novos meios de invasão afim de sempre está atualizado garantindo assim a máxima segurança. (MUNIZ; LAKHANI, 2013).

Após a identificação e catalogação das vulnerabilidades, e equipe responsável por criar e manter a segurança em meios computacionais adotara novos meios de proteção minimizando os riscos, porém é inaplicável a garantia de total segurança, e para isto deve-se adotar normas e padrões universais para reduzir as falhas a um nível aceitável. Há controles já conhecidos como normas ABNT/IEC, ISO, CERT dentre outras, ou então a criação de um conjunto de controles que visam suprir todas as necessidades de uma empresa, com aspectos específicos e voltado para necessidade de cada organização. (NAKAMURA; GEUS, 2007).

O teste de invasão(pentest) deve seguir rigorosos ciclos e diretrizes, e uma vasta pesquisa sobre o alvo. O ataque deve ser estruturado, calculado e quando possível, antes de iniciar, é interessante, em um ambiente controlado como um laboratório, testar e verificar todos as técnicas que serão realizadas no alvo, afim de prevenir-se sobre possíveis adversidades que possam ocorrer na realização do pentest. (WILHELM, 2010).

É importante também, levantar o maior número de informações da vítima, e após a invasão no alvo, é necessário realizar novamente o ciclo de obtenção de informação, pois quanto maior o número de informações que possui, maiores será a probabilidade de sucesso na invasão.

3.3 WHITE HAT E BLACK HAT

Muitas vezes é comum aparecer em meios jornalísticos o uso da palavra hacker empregada de forma equivocada, então serão vistas adiante definições dos termos utilizados, diferenciando cada tipo de profissional.

Sabe-se que um “hacker ético” utiliza-se das mesmas ferramentas e técnicas que um “hacker malicioso”. É necessário ter as mesmas autorizações que um intruso pode ter, ou seja, ele não terá nenhuma facilidade ou acesso privilegiado aos sistemas da empresa, precisa estar na mesma posição que qualquer pessoa de fora estaria, ele não pode ter senhas, acesso a máquina ou servidores, ele precisa chegar o mais próximo ao que uma pessoa maliciosa possa estar. (BALOCH,2015).

Engebretson (2013) destaca que a grande diferença entre os hackers éticos e um hacker malicioso baseia-se em três grandes pontos chaves:

autorização, motivação e intenção. Autorização não trata-se apenas de receber senhas de acesso, mais da autorização do administrador da rede ou da pessoa que a mantem confia a um “hacker ético”.

O Hacker ético usara de todas as formas de invasão para obter acesso a rede, e após exaustivos testes, apresentara um relatório ao contratante demonstrando qual é a sua vulnerabilidade. Vários são motivos para invadir uma rede, pode-se querer apresentar aos interessados que sua rede e sistema não estão seguros e qual é a melhor maneira de proteger-se, ou então a intenção pode ser para invadir o sistema e roubar dados e informações, ou então destruir todo o sistema para benefício próprio ou de terceiros. (ENGEBRETSON, 2013).

Schineier (2001) cita diversos responsáveis por estes ataques, mas destaca-se os seguintes grupos:

Hackers: possui várias definições, em geral possuem grandes conhecimento em tecnologia e formas de invadir sistemas. São sempre especialistas, possuindo ou não formação acadêmica conseguem encontrar falhas e obter autorização de maneira furtiva, podendo ser um administrador de redes ou até mesmo um adolescente buscando conhecimento mais aprofundados em técnicas de invasão.

Criminosos solitários (Black hat): criminosos comuns que se especializam em tecnologia para aplicar golpes afim de obter rendimento financeiro.

Insiders maliciosos: são funcionários ou prestadores de serviços que por motivos como descontentamento com a empresa ou repudio a algum funcionário aproveitam-se de sua posição e prejudicam a empresa voluntariamente.

Insiders inocentes: aqueles funcionários com pouco conhecimento em informática, que involuntariamente cria o ensejo para uma usuário malicioso aproveitar-se.

Segundo Baloch (2015), “White hat hacker” é o tipo de hacker referenciado como um profissional que garante a segurança da informação, ou que pesquisa sobre técnicas de segurança. São empregados ou prestadores de serviços contratados por empresas, autorizados a atacar afim de encontrar vulnerabilidades que um atacante poderia estar disponível a explorar.

“Black hat hacker”, também conhecido como “cracker”, este tipo de hacker é referenciado como uma pessoa mal intencionado, ou “bad guy” que utiliza-se de seu conhecimento para propósitos negativos. Também referenciado na mídia

como “hackers”. “Gray hat hacker” é o hacker que fica entre o White e Black hat, ele pode trabalhar como um profissional da segurança, e ficar responsável em descobrir as vulnerabilidades da mesma forma que um White hat, e pode deixar alguma vulnerabilidade para acesso futuro afim de obter informação confidencial e oferecer aos concorrentes.

Ainda segundo o autor citado anteriormente, existem ele outros 3 tipos de hackers, como o hacker de elite, também referenciado como “1337”, que é alguém que possui um profundo conhecimento de como criar softwares que consiga invadir um sistema, e também modificar códigos de alguém afim de criar erros e falhas no sistema.

Hackativista é definido como um grupo de hackers trabalhando juntos por uma causa ou proposta. Buscam causas políticas, liberdade de expressão, direitos humanos e etc. (BALOCH,2015).

E por fim o hacker ético, que é aquele que foi contratado e permitido que ataque o sistema para identificar vulnerabilidades, que um atacante mal intencionado poderia tirar vantagem. (BALOCH,2015).

3.4 METODOLOGIA DE UM TESTE DE INVASÃO

Todo o processo de teste de invasão (pentest) pode ser divido em uma série de passos até atingir o objetivo, quando colocado todos os passos alinhados forma uma compreensiva metodologia para atingir o sucesso no pentest. Quando um “Black hat” está invadindo o sistema, ele não utiliza nenhuma metodologia ou alguma sequência de processos categorizado, pois o objetivo é apenas invadir, porem para um “White hat” contratado, deve a cada passo catalogar as vulnerabilidades afim de no final ter uma visão geral e aprofundada de todas as vulnerabilidades encontrada no sistema. Não podemos esquecer que a necessidade de renovação processual facilita a criação do levantamento das variáveis envolvidas. (BALOCH, 2015).

Penetration test engagement standard (PTES) foi desenvolvido em 2011 com sua última edição em 2014, resultante de anos de experiência dos profissionais de segurança mais bem sucedidos no mundo.

Segundo Engebretson (2013), o uso de uma metodologia permite segmentar todo o processo de pentes em diversas etapas. Compreender e

seguir uma metodologia é um importante passo para o domínio básico de testes de invasão(hacking). Dependendo do autor pesquisado, este processo normalmente pode conter quatro ou cinco passos ou fases. Embora todos os nomes ou números possam variar entre metodologias, o importante é que este processo possibilitar a visualização de todos os passos do teste de penetração.

Teste de invasão (pentest) é uma subclasse do hacking ético, compreende uma serie de métodos e processos que testa e ao mesmo tempo protege a segurança da informação em uma organização. O teste prova-se útil em encontrar vulnerabilidades em um determinado sistema computacional, e verifica se um atacante pode se aproveitar destas vulnerabilidades para obter acesso não autorizado a um registro. (BALOCH, 2015).

Baloch (2015) define ainda que há alguns passos são imprescindíveis antes do início do teste de invasão, primeiramente é necessária uma permissão para atacar. Há de ter um acordo formalizado em contrato, assinado por ambas as partes (organização contratante e profissional que garante o pentest), neste contrato deve haver especificações do ataque, permissão e todos os requisitos legais para garantir a legalidade do processo. Após isto, deve-se definir o engajamento e qual parte da organização deve ser testada, pode haver a necessidade de que apenas parte da organização seja testada.

O White hat deve ter ciência que não pode ultrapassar os limites concedidos pela organização. Deve ter formalizado em contrato, a duração do projeto, contendo a data de início e fim, a metodologia usada pelo pentest, os objetivos a serem atingidos, objetivo este que deve ser diluído, para pequenos objetivos, e no final a junção de todos mostra qual foi o real sucesso do teste de invasão. (BALOCH, 2015).

Outro ponto importante a ser discutido com o contratante são as técnicas permitidas, pois caso seja lançado um ataque comprometa algum serviço essencial a empresa, causara prejuízos, então ataques que ferem diretamente as continuidades dos processos organizacionais devem ser discutidas e esclarecidas para ambas as partes.

3.4.1 METODOLOGIAS DE PENTEST CONHECIDAS

Como visto anteriormente, a escolha de uma metodologia é importante para obter resultados em um teste de invasão, existem diversos metodologias, e cada auditor pode adapta-las de acordo com suas necessidades. A seguir serão apresentadas as mais conhecidas

3.4.2 OSSTMM

É um manual gratuito que basicamente inclui quase todos os passos em um teste de invasão. Esta metodologia consiste em um estudo aprofundado no que sua segurança possui e do que ela precisa.Com a aplicação da metodologia OSSTMM, é levantado um profundo conhecimento da conectividade das aplicações, incluindo pessoas, processos organizacionais, sistemas e qualquer relação que as aplicações possuem. (HERZOG, 2014).

3.4.3 NIST

O NIST é mais simples, com técnicas aplicadas no dia a dia da organização, ele possui 4 passos, consistindo em escancear, descobrir, atacar e reportar. O teste começa com o planejamento, definindo objetivos, alvos e limites, seguido pela busca, ou conhecimento da rede, esta etapa é muito importante pois nela que serão descobertos possíveis vulnerabilidades, erros ou falhas.

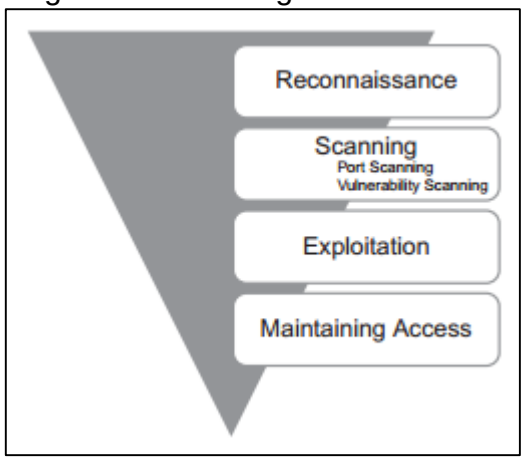
Após verificar brechas e meios para invadir o sistema, começa o ataque, que é considerado peça fundamental no teste de invasão, aqui serão encontrados os riscos, e quais informações estão vulneráveis, e por fim é o relatório, onde o auditor relata quais vulnerabilidades o sistema possui e como pode defender-se.(NIST.GOV, 2008).

3.4.4 METODOLOGIA DE PENTEST ZEH

Estudando sobre metodologias como NIST ou OSSTMM, percebe-se que elas compartilham passos comuns, por mais que uma possa ser mais detalhada que a outra, há diversas similaridades, o ZEH é o nome dado a fusão destas metodologias de teste de invasão, modelado com 4 passos que são: 1) reconhecimento; 2) varredura; 3) exploração e 4) mantendo acesso, auditores de segurança normalmente seguem estas sequências de processos.

Neste trabalho são abordados os principais aspectos que devem ocorrer em um pentest, que são reconhecimento, varredura, exploração e manter o acesso, para ajudar na visualização de cada processo, um triangulo mostrando cada etapa. A figura 3 ilustra a metodologia de pentest ZEH

Figura 3 Metodologia ZEH.



Fonte: Engebretson (2011).

Este processo de 4 etapas é conhecido como ZEH (zero entry hacking), a primeira etapa conhecida como “reconhecimento”, alguns profissionais responsáveis pelo pentest costumam não fazê-la, e pular diretamente para parte de varredura, porem isso deixará com reduzido número de alvos, pois não saberá todos os Ips que estão disponíveis na rede, reduzindo assim sua chance de sucesso. (ENGEBRETSON, 2011).

3.5 RECONHECIMENTO

Nesta etapa são feitas pesquisas sobre a organização, servem para entender todo o ambiente coorporativo relativo ao alvo, incluindo pesquisa sobre empregados, parceiros comerciais bem como empresas contratadas para prestar algum tipo de serviço a organização, diretores e etc, pois normalmente o auditor deve começar apenas obtendo o nome da organização, e através de suas técnicas e métodos se aprofunda sobre todos os aspectos da empresa, até conseguir o acesso. (ENGEBRETSON, 2011).

O auditor não irá atacar a empresa, apenas encontrar suas vulnerabilidades, ela pode estar em clientes ou fornecedores, consiste em encontrar pontos de risco.

Segundo Engebretson (2013, tradução nossa), o primeiro passo em qualquer trabalho é a pesquisa. Quanto mais preparado você estiver, maior é sua chance de sucesso. Os criados do Backtrack encontraram uma frase do Abraham Lincoln que disse, “Se eu tenho seis horas para cortar uma arvore, gastaria as primeiras quatro horas afiando meu machado”.

Como foi visto no exemplo acima, a preparação é um dos pontos cruciais de qualquer trabalho. Seja para descobrir uma senha, ou saber qual endereço de IP posso atacar, é sempre aconselhável que o auditor saiba tudo o que estiver disponível sobre a empresa, pois isso fara grande diferença em fases futuras no teste de invasão(pentest).

3.5.1 ENGENHARIA SOCIAL

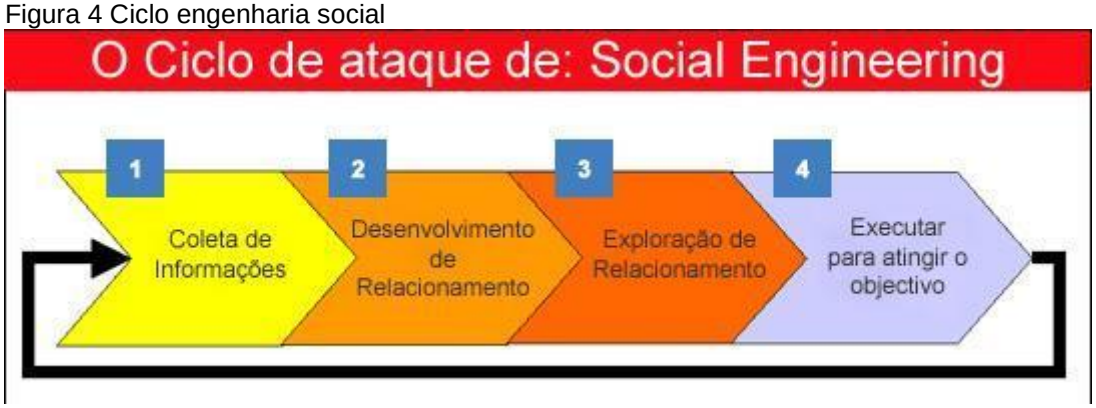
Um das mais simples e efetivas formas de reconhecimento é a engenharia social.

> A Engenharia social é o processo de explorar a fraqueza do “humano” que é inerente em qualquer organização. Quando utilizado a engenharia social, o principal objetivo do atacante é conseguir fazer com que o empregado divulgue algumas informações que supostamente seria confidencial. (ENGEBRESTSON, 2011, p. 38, tradução nossa)

A engenharia social no teste de invasão diz para o atacante testar a segurança da organização atacando os envolvidos da empresa. É nela onde você poderá fazer com que os empregados caiam em armadilhas e façam coisas que eles não pretendiam fazer. (BALOCH, 2015).

A Figura 4 representa o ciclo a ser realizado na etapa da engenharia social.

Figura 4 Ciclo engenharia social



Fonte: Reprodução/Google(2015)

3.5.2 VARREDURA(SCANNING)

Varredura em redes, ou scan, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados. (Cartilha.cert.br, 2015).

Nesta etapa o auditor utilizando-se das informações obtida no reconhecimento, através de acessos públicos como ips de sites, ou de acesso remoto, verifica e lista todas as vulnerabilidades que poderá utilizar-se futuramente para obtenção de acesso na rede, nesta etapa são listados Ips e portas abertas(vulneráveis) que futuramente o atacante utilizara para acessar a rede interna da organização. (ENGEBRETSON, 2011).

No mundo globalizado, onde todo dia as informações devem estar acessíveis de qualquer lugar e plataforma, as informações precisam estar disponíveis de diversas formas e para diversas plataforma como celulares, notebook, tabletes e etc, com esta vasta disponibilidade vem o ônus do risco,

onde por meio de varreduras e scan na rede, um atacante pode descobrir algumas destas formas de obter acesso privilegiado as informações confidenciais da empresa. (ENGEBRETSON, 2011)

Nesta etapa serão listados os Ips, endereços lógicos de um dispositivo eletrônico com comunicação interligado a outros dispositivos, descobrir um Ip pode ser comparado a encontrar o endereço de uma casa a qual deseja visitar, ele é considerado o alvo, pois serão nele que os ataques são direcionados, além de encontrar o ips(endereço) temos também que nele procurarmos por entradas, que são chamadas portas, são pelas portas que o acesso é obtido. A porta é a entrada de um sistema, sabendo o ips e a porta alvo, podemos iniciar a exploração. (ENGEBRETSON, 2011)

3.5.3 EXPLORAÇÃO

Exploração é o processo de obter controle de um sistema. Na etapa anterior(scan) obtivemos informações sobre algumas vulnerabilidades da rede, lá foram encontradas Ips e portas, e nesta etapa vamos obter acesso a rede através destas entradas.

Procurar e verificar quais vulnerabilidades em etapas anteriores são realmente possíveis de serem exploradas, e qual o possível ganho de informações privilegiadas pode-se ter acesso. O sucesso desta etapa depende muito das etapas anteriores no levantamento de informações.

> Nesta fase, o sistema é violado, devido à descoberta de vulnerabilidade, a invasão é consolidada e, através dela, podemos explorar as camadas internas do sistema, a fim de descobrir outros meios, pelos quais possa potencializar nosso ataque. Podemos verificar as estruturas de diretórios, políticas de senhas, enfim, várias alternativas podem ser aplicadas extraindo o máximo de informações. O reconhecimento do sistema pode ser ampliado conforme a necessidade específica relacionada aos posteriores pentest que serão aplicados. Uma análise geral do sistema ou mapeamento geral e detalhado será caracterizado pela personalidade de cada indivíduo invasor. (GIAVAROTO; SANTOS, 2013).

Exploração significa dentre outras, entrar em um sistema com privilégios de um usuário com total acesso no alvo. Usuários e senhas devem ser testados para de maneira que até que não seja obtido o acesso através do login, não pare as tentativas, isto pode ser feito manualmente, porem levaria muito tempo até atingir o objetivo, então este processo é realizado de maneira automatizada, utilizando de softwares que consistem em testar todas as possíveis formas de acesso. Caso este acesso seja obtido, o auditor pode entrar no sistema com privilégios de administrador e conseguir o que deseja, como informações, controles remotos e etc.

3.6 SISTEMAS OPERACIONAIS PARA TESTE DE INVASÃO

Sem um software o computar é apenas um conjunto de peças interligadas sem nenhum uso, porem com um software é possível o armazenamento, processamento o acesso a informações e dados.

Pode-se dividir os softwares em dois grupos: Programas de sistema, que realizam a informação referentes ao computador, e os aplicativos, que realizam as ações e necessidades do usuário. O programa de sistema mais simples é o sistema operacional, cuja tarefa é controlar os recursos do computador.

3.6.1 LINUX

Para realizar qualquer tarefa é necessário o uso de ferramentas, e o Linux é o sistema operacional que mais fornece suporte para ferramentas de teste de invasão, pois tanto nos sistemas MAC OS e Windows, por mais que ela esteja disponível, é no Linux onde elas estão praticamente nativas, pois ele é uma distribuição livre onde qualquer programador pode alterar seu código fonte para criar modificações desejadas.

O Linux possui diversas distribuições, e as ferramentas que serão apresentadas funcionam em qualquer um, porem para este trabalho utilizaremos o backtrack 5 e Kali Linux.

Será apresentado a seguir o uso de algumas distribuições Linux:

- *Redhat Linux*—Usado para propósitos de administração
- *Debian Linux*—Feito para ser usado apenas em código aberto

- *Ubuntu Linux*—Geralmente usado para tarefas diárias e uso pessoal.
- *Mac OS X*—Usado em todos os sistemas da apple.
- *Solaris*—Usado para fins comerciais.
- *Backtrack Linux e Kali*—Usado para teste de invasão(pentest).

3.6.2 BACKTRACK

O Backtrack é uma distribuição do Linux, evoluiu a partir do Slackware, criado em maio de 2006 pela empresa Offensive Security, que foca em testes de invasão em redes corporativas e treinamentos. Lançou o Backtrack, como um projeto focado em testes de invasão.

Segundo o site backtrack-linux.org (2015) “A evolução do Backtrack levou anos de desenvolvimento, e ajudas incontáveis da comunidade de segurança. “Backtrack originalmente começou com as mais recentes versões das “Live Linux “distribuições chamadas WHOPPIX, IWHAX e Auditor.

O Backtrack foi inicialmente desenvolvido para ser um “live CD” e empregado em auditorias, foi desenvolvido para não deixar nenhum registro em logs do sistema. Com milhões de downloads, tornou-se o mais adotado teste de invasão à rede existente, e amplamente utilizado pela comunidade de segurança da informação por todo o mundo.

Segundo Ramachandran (2011), Backtrack é uma plataforma de Pentest (Teste de invasão) e auditoria de segurança com avançadas ferramentas para identificar, detectar e explorar qualquer vulnerabilidade descoberta no ambiente de rede. A figura 5 ilustra a tela principal do Backtrack 5

Figura 5 Backtrack 5 ferramentas de ataque

Fonte: Google imagens (2015).

A Figura 6 mostra o histórico de versões disponibilizadas

Figura 6 Versões do Backtrack

Data	Release
26/05/2006	Backtrack v1
06/03/2007	Backtrack v2
19/06/2008	BackTrack v3
09/01/2010	BackTrack v4
08/05/2010	BackTrack 4 R1
22/11/2010	BackTrack 4 R2
10/05/2011	BackTrack 5 release (Linux kernel 2.6.38)
18/08/2012	BackTrack 5 R1 release (Linux kernel 2.6.39.5)
01/03/2012	BackTrack 5 R2 release (Linux kernel 3.2.6)
13/08/2012	BackTrack 5 R3 release

Fonte: (Backtrack-linux.org, 2015).
Nota: Adaptado pelo autor.

3.6.3 KALI LINUX

Após 7 anos da primeira versão do Backtrack, os desenvolvedores estavam pensando na versão 6, colocaram assim todas as metas que ansiavam atingir, e após uma profunda analise, perceberam que precisaria de uma reestruturação, e queria ficaria melhor desenvolver outro sistema utilizando-se de novas tecnologias e processos. (AHARONI, 2012).

Esta reestruturação levou a uma outra grande escolha, mudar a plataforma base. E apesar da vasta mudança na estrutura do sistema, o uso dele continua quase o mesmo para o usuário, apenas com pequenas modificações no padrão de hierarquia de arquivos do sistema. Segundo os desenvolvedores, a decisão de mudança do nome foi necessária pois todas estas significantes mudanças, manter o nome Backtrack acrescentando apenas mais uma versão

(6) não faria justiça aos esforços desta reestruturação, a equipe de desenvolvimento queria enviar uma mensagem aos usuários mostrando que grandes alterações foram feitas. (AHARONI,2012).

Kali Linux é um projeto de código aberto (qualquer um pode obter e modificar o código fonte) fundado e mantido pela “Offensive Security”, uma provedora a nível mundial de treinamento e testes de invasão com foco em segurança da informação. (AHARONI,2012).

Assim como o Backtrack, o Kali Linux é carregado a partir de um live CD. Lançado em 13 de março de 2013, contém mais de 600 ferramentas para testes de invasão, sua disponibilização é gratuita e de código aberto. (AHARONI,2012).

3.6.4 DIFERENÇA ENTRE KALI E BACKTRACK

Com esta reestruturação, o Kali diferenciou-se de seu predecessor Backtrack, após revisarem todas as ferramentas contidas no Backtrack, foi eliminado um grande número que já não funcionava mais ou era igual a outras contidas no sistema. Como o Kali é uma ferramenta apenas para o propósito de testes de invasão, apenas um usuário com acesso total é definido como modelo, ele também bloqueia por padrão serviços de redes adicionais como bluetooth para que apenas que o usuário habilita fiquem disponíveis. (AHARONI,2012).

3.7 ATAQUES

Nesta etapa serão apresentados diversos ataques que são feitos em um teste de invasão.

3.7.1 TCP

Antes de falar sobre os ataques, que é o foco deste trabalho, é necessário entender um pouco sobre o protocolo TCP. Segundo Souza (2003), “TCP (Transmission Control Protocol) foi projetado especificamente para oferecer um fluxo de bytes fim a fim confiável em uma inter-rede não confiável”. É o protocolo que permite a trafego de dados e informações em redes de computadores, é usado para manter a comunicação entre um cliente e servidor, ou seja, de um usuário e serviço.

3.7.2 FTP

É usado para enviar e receber arquivos, é pelo protocolo FTP que conseguimos fazer nossos downloads de vídeos, musicas, livros e textos. Ele usa a porta 21, e é com estas informações que irei utilizar para atacar um serviço. (SOUZA, 2003).

3.7.3 SMTP

Utilizado para correios eletrônicos, funciona na porta 21, um pentester poderá entrar no SMTP diversas mensagens enviadas dos funcionários da empresa. (SOUZA, 2003).

3.7.4 HTTP

É usado para navegação na internet, digitando a URL de um site poderá acessa-lo, o protocolo usado neste processo é o HTTP, ele funciona na porta 80. (SOUZA, 2003).

3.8 Atacando serviços de acesso remoto.

Neste trabalho será focado a obtenção de acesso a sistemas computacionais usando softwares como Hydra, Medusa e John the Ripper(JTR), que detalharemos cada um deles nos próximos tópicos.

3.8.1 Ataque de força bruta e quebra de senhas

Um ataque de força bruta sobre senhas criptografadas com algum algoritmo significa, dentro de um limite pré-estabelecido, gerar todas as senhas possíveis, criptografar cada uma e comparar com a senha criptografada original, até que alguma das senhas geradas e criptografadas seja igual à senha criptografada original. (STALLINGS, 2010).

Durante este tipo de ataque, o atacante está tentando contornar os mecanismos de segurança ao ter conhecimento mínimo sobre eles. Ele tenta adivinhar a senha por meio de incansáveis tentativas de acesso. Possuiu alguns métodos, como de ataques de dicionário, que consiste na criação de uma lista de palavras contendo todas as possíveis combinações de senhas, este número pode chegar a milhões, e requer grande poder computacional para ser bem sucedido, é uma forma de ataque onerosa que não garante nenhum sucesso, porém é o meio mais simples de se invadir um sistema computacional.

Ataque de força bruta (com determinadas classes de personagens, por exemplo: alfa numérico, caracteres especiais) que o atacante está tentando alcançar sua meta. Considerando-se um método estabelecido, o número de tentativas, a eficiência do sistema, o qual realiza o ataque e eficácia estimada do sistema que é atacada, o atacante for capaz de calcular o tempo que o ataque deverá durar. Ataques de força bruta, por outro lado, que inclui todas as classes de personagens, não dá nenhuma certeza de sucesso. “Um ataque de dicionário se utiliza de listas de palavras que às vezes contêm dicionários inteiros e que podem ser altamente especializados.” (STEIN, 2007)

Segundo Baloch (2015, tradução nossa), um ataque tradicional de força bruta, é verificado todas as possíveis combinações da senha correta. Este processo pode levar até anos dependendo do tamanho da senha da vítima, porem torna-se útil quando usado para senhas pequenas.

Existem também os ataques híbridos, onde é combinado o tradicional ataque de força bruta com o ataque de quebra de senhas (ataques de dicionário). A ideia central dele é aplicar um ataque de força bruta em uma lista de dicionário. Este método também pode ser chamado de “Online password Cracker”. Baloch nos dá um exemplo que será visto a seguir:

No exemplo a ser destacado Baloch (2015, tradução nossa) diz que “Uma universidade implantou uma política de senhas onde a senha é o primeiro nome seguido pela data de nascimento. Se o primeiro nome é Felipe e nasceu em 3 de fevereiro de 1993 a senha seria felipe321993”. Neste caso nem o tradicional ataque de força bruta ou o ataque de dicionário seriam efetivos, porem o hibrido seria.

Este processo faz que o software usado para atacar envie um usuário e senha para o alvo, se ambos estão incorretos, retorna um erro no log com falha.

Então o software irá enviar o próximo usuário e senha presente na lista. Este processo continua até que seja encontrado os usuários e senha do sistema.

Engebretson, (2013, p 86) alerta que deve-se tomar cuidado pois em alguns sistemas de acesso remoto o sistema emprega que as tentativas que resultam em erro têm um limite. E atingido este limite o seu ips e usuários podem ser bloqueados.

3.8.2 SOFTWARES PARA ATAQUE

Serão listados e apresentados alguns softwares que serão utilizados para ataques.

3.8.3 HYDRA

Presente no Backtrack e Kali, um dos mais antigos quebradores de senha desenvolvido pelo “The hackers Choice(THC)”, uma comunidade de estudos hackers.

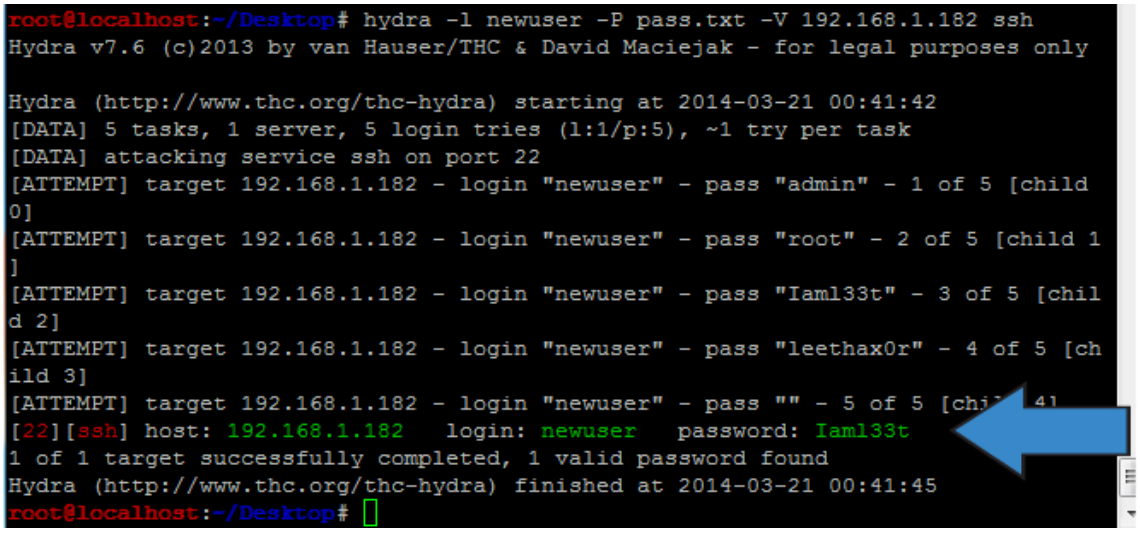
Segundo Muniz, J e Lakhani (2013), o Hydra é ideal para ataque a e-mails, pois pode definir o IP do alvo e o protocolo POP3 e SMTP como administrador.

Já vem com uma lista de usuários e senha pré definida, mais podemos altera-la conforme necessidade, ou então carregar novas lista de palavras(wordlist) a nossa escolha. Há vários sites dedicados a criar estas wordlists.

Ele abrange diversos protocolos entre eles:TELNET, FTP, Firebird, HTTP-GET, HTTP-HEAD, HTTPS-GET, HTTP-HEAD, HTTP-PROXY, HTTP-PROXYNTLM, HTTP-FORM-GET, HTTP-FORM-POST, HTTPS-FORM-GET, HTTPS-FORMPOSTLDAP2, LADP3, SMB, SMBNT, MS-SQL, MYSQL, POSTGRES, POP3 NTLM, IMAP, IMAP-NTLM, NCP, NNTP, PCNFS, ICQ, SAP/R3, Cisco auth, Cisco enable, SMTP-AUTH, SMTP-AUTH NTLM, SSH2, SNMP, CVS, Cisco AAA, REXEC, SOCKS5, VNC, POP3 e VMware-Auth

A Figura 7 mostra o sucesso na recuperação de uma senha.

Figura 7 Hydra



Fonte: Google imagens (2015).

3.8.4 MEDUSA

Medusa é uma outra alternativa para quebrar senhas, é um software que usa o ataque de força bruta juntamente com as listas de palavras(wordlists), porem mais rápida e estável do que a Hydra pois ela possui mais suporte ao uso do Thread do processador.

3.8.5 JOHN THE RIPPER

Outro cracker de senha, ela é bem rápida e útil, já vem nativo nos sistemas operacionais Backtrack e Kali, pode ser usado tanto para ataques de dicionário quanto para quebrar senha, também já vem com uma wordlist pré definida.

4 TRABALHOS CORRELATOS.

A cada dia surgem novas ameaças, bem como formas de ataca, juntamente a isto surgem estudos sobre estas formas de ataque propondo meios que procuram abranger as mais diversificadas vulnerabilidades. Profissionais de segurança precisam constantemente se atualizar afim de estar apto a implementar os mais modernos mecanismos de defesa conhecidos.

Perante estas necessidades o meio acadêmico está sempre realizando pesquisas e estudos sobre o assunto, e ultimamente tem crescido a quantidade de estudantes propostos a realizar este tipo de pesquisa.

No decorrer desta pesquisa foi possível ter contato com os mais diversos trabalhos relacionados com segurança da informação, dentro deste contexto existe o trabalho do aluno da USC que foi de grande valia nesta pesquisa.

Dentro deste contexto pode-se citar o trabalho de conclusão de curso intitulado “Análise das principais vulnerabilidades presentes em aplicações web e implementações de segurança utilizando a linguagem interpretada livre php”, de autoria do William Dias Silva de Castro Souza, que aborda testes práticos com as ferramentas do Backtrack afim de realizar um teste de invasão em sites PHP.

Dessa forma, este trabalho tem como intuito analisar algumas ferramentas de pentest a fim de coletar resultados relevantes sobre sua eficiência e qualidade durante o processo, e também colaborar com futuros trabalhos e pesquisas sobre o assunto abordado.

5 METODOLOGIA

O propósito das pesquisas exploratórias é proporcionar ao investigador maior familiaridade com o problema, objetivando torná-lo mais explícito ou construir hipótese. Uma pesquisa de cunho exploratório tende a ser bastante flexível, pois leva em consideração os mais variados aspectos relativos ao problema estudado. De modo geral, pesquisas realizadas com propósitos acadêmicos, pelo menos inicialmente, assumem esse caráter exploratório, pois neste momento é pouco provável que o pesquisador tenha uma definição clara do que irá investigar. (GIL, 2010).

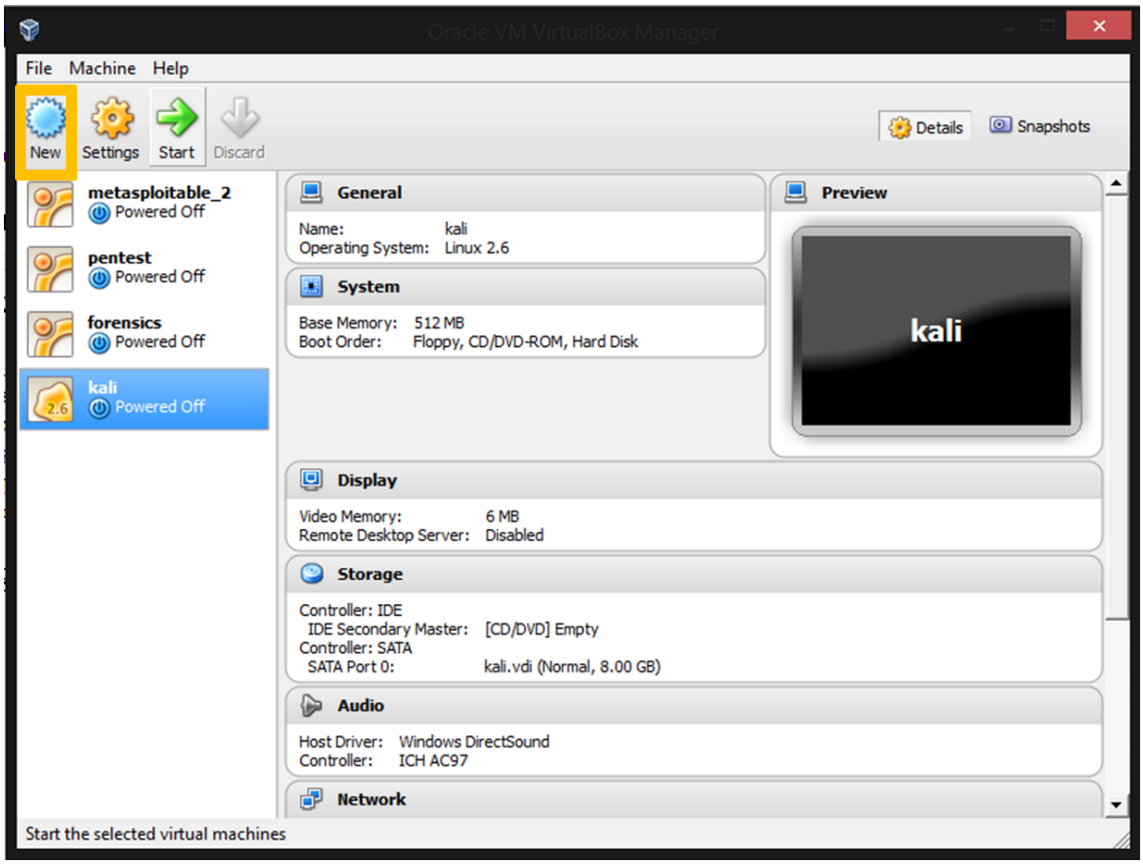
De acordo com Lakatos e Marconi (1992, p. 43), “a finalidade da pesquisa bibliográfica é colocar o pesquisador em contato com tudo aquilo que já foi escrito sobre determinado assunto. A pesquisa bibliográfica não é mera repetição do que já foi dito ou escrito sobre determinado assunto, mais “oferece meios para definir, resolver, não somente problemas já conhecidos, como também explorar novas áreas, onde os problemas ainda não se cristalizam suficientemente” (MANZO, 1971 citado por LAKATOS; MARCONI, 1992, p. 43).

Este trabalho foi desenvolvido em duas fases distintas: uma fase de investigação dos aspectos teóricos e uma etapa prática de aplicação das técnicas de invasão em sistemas computacionais. Além de apresentar e demonstrar diversas técnicas de instrução, afim de obter acesso a um sistema computacional

Com o conhecimento obtido através da leitura de livro científicos, foram apresentadas técnicas afim de realizar um ataque BRUTE FORCE, para isto foi criada uma máquina virtual com o sistema operacional Kali Linux.

Na Figura 8 é mostrada a tela inicial do VirtualBox, ferramenta de distribuição gratuita que foi utilizada para criação da maquina virtual.

Figura 8 Máquina Virtual VirtualBox



Fonte: Elaborada pelo autor.

Foi realizado download gratuito do Kali Linux (disponível em https://www.kali.org/downloads/).

Na Figura 9 é mostrada a tela inicial do Kali, demonstrando as ferramentas para ataque a senhas.

Figura 9 Kali Linux- Ferramentas de ataque a senhas

Fonte: Elaborado pelo autor.

Após realizado estes passos foi iniciado o teste de invasão, utilizando a metodologia ZEH de pentest. A metodologia ZEH (Zero Entry Hacking) é um modelo simples de quatro etapas (ENGEBRETSON, 2011), destinada a orientar o processo de planejamento, preparação e execução de todas as ações associadas ao teste de penetração. A cada nova etapa, o processo entra sucessivamente em um novo nível de detalhe, até que seja identificado o objeto de estudo do teste, conduzindo de forma clara as ações do responsável pela atividade.

O foco foi em ataques a senha, e para demonstrar diversas formas de ataques foram criados serviços que requerem senhas para efetuar o login, e em um ambiente controlado foi realizado ataques a estes serviços. As senhas tiveram um nível de complexidade leve, caso contrário poderá levar dias para ser descoberta. Foi realizado um ataque de dicionário utilizando wordlist junto com ataque força bruta, tentado descobrir a senha com combinações de até 4

caracteres, tornando-se assim um ataque híbrido, onde foi utilizando uma wordlist com um ataque de força bruta.

Após realizado todos os testes foi criado um relatório mostrando analises e estatísticas sobre o ataque, como tempo de duração e qual método foi mais eficaz.

E através das estatísticas aferidas, foram gerados relatórios mostrando quais as principais vulnerabilidades em senhas, e também qual é a melhor forma de se criar uma senha, e os fatores que deve-se atentar do ponto de vista de segurança.

6 Resultados

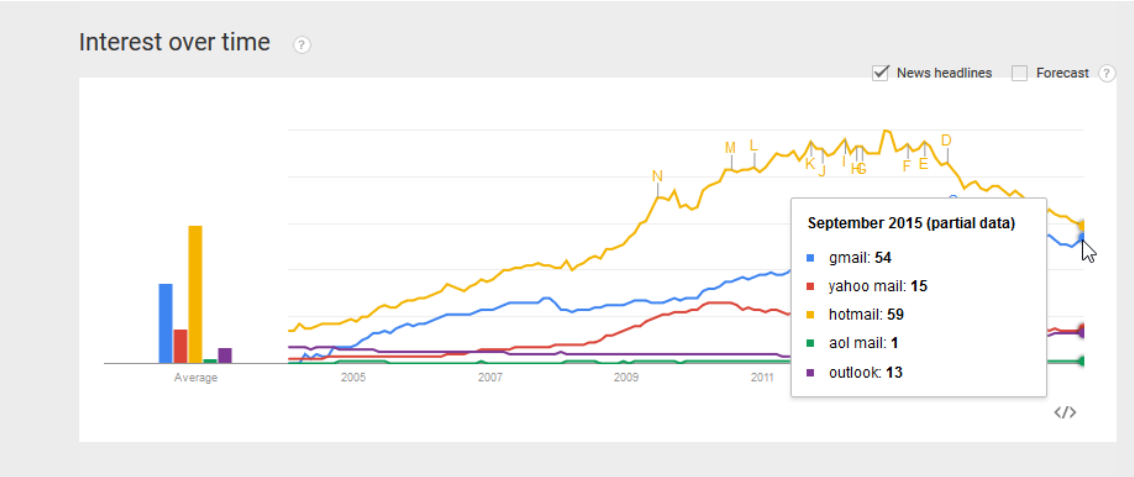
Para demonstrar a efetividade e tempo necessário para realizar um ataque de força bruta utilizando dicionário de palavras, é preciso ter algum serviço ou conta para teste, diversos serviços hoje são atacados por meio do bruteforce, tais como SSH, FTP ou qualquer outro que necessite de login e senha, porem grande parte dos usuários possuem conta de e-mail e poucos desconhecem o quão são vulneráveis caso utilizem uma senha curta demais, no gráfico alustrado na Figura 10 fornecido pelo Google(2015) que os termos mais procurados no Google foi sobre ataques aos serviços de e-mail.

Figura 10 Popularidade dos tipos de ataque

Fonte:Google Trends(2015)

Neste trabalho foram abordadas tentativas de quebra de senha em um e-mail criado para este fim, onde o primeiro passo foi saber em qual servidor seriam realizados os ataques, segundo dados do Google Trends(2015), o Hotmail é o serviço de e-mail mais procurado, porem projeções indicam que em pouco tempo o Gmail será o serviço de e-mail mais utilizado. Na Figura 15 é mostrada a popularidade dos servidores de e-mails, e constatado o mais popular.

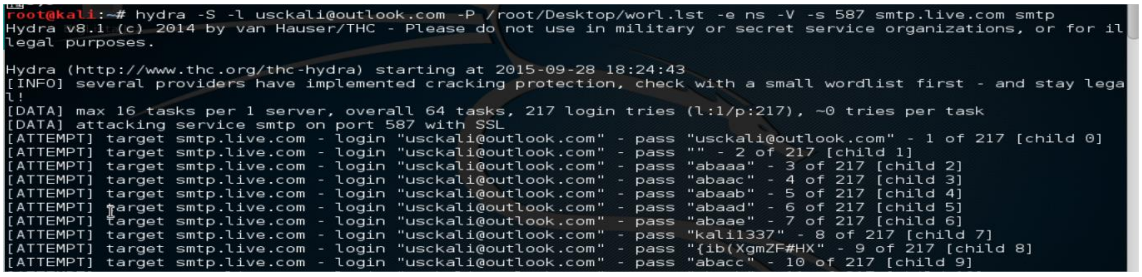
Figura 11 - Popularidade dos serviços de Email



Fonte: Elaborado pelo autor.

Para este trabalho foi escolhido o Gmail, pois além de estar na lista dos mais populares, ele possibilita este tipo de ataque, após testes no Outlook foi aferido que este ataque tornou-se ineficiente pois gera erros, e mesmo passando pela senha correta ele não sinaliza mostrando sucesso conforme visto na Figura 12:

Figura 12 Ataque ao Gmail



Fonte: Elaborado pelo autor.

Foi criado então um e-mail no Gmail, segundo mais popular, com o endereço usckali@gmail.com, com a senha kali1337, a senha contém uma complexidade media, e preenche os requisitos mínimos exigidos pelo Google, que precisa ter no mínimo 8 caracteres e também letras e números. Porém é importante ressaltar que em ataques de dicionário, o tamanho da senha é até certo ponto irrelevante.

Após criado o e-mail usckali@gmail.com deu-se início aos os ataques de dicionário utilizando primeiramente o Hydra, depois o Medusa e por fim o Ncrack, softwares estes mais conhecidas da área de bruteforce.

Foram avaliados 3 softwares procurando os seguintes parâmetros:

ATAQUE A EMAIL
Efetividade (se encontrou a senha certa)
COM A SENHA NA POSIÇÃO 10
COM A SENHA NA POSIÇÃO 500
COM A SENHA NA POSIÇÃO 50000

Duração do processo:(tempo até encontrar a senha correta)
COM A SENHA NA POSIÇÃO 10
COM A SENHA NA POSIÇÃO 500
COM A SENHA NA POSIÇÃO 50000

FTP

COM A SENHA NA POSIÇÃO 10
COM A SENHA NA POSIÇÃO 500
COM A SENHA NA POSIÇÃO 50000

Duração do processo:(tempo até encontrar a senha correta)
COM A SENHA NA POSIÇÃO 10
COM A SENHA NA POSIÇÃO 500
COM A SENHA NA POSIÇÃO 50000

6.1 Hydra

Iniciando pelo Hydra foi utilizado o código ilustrado na Figura 13:

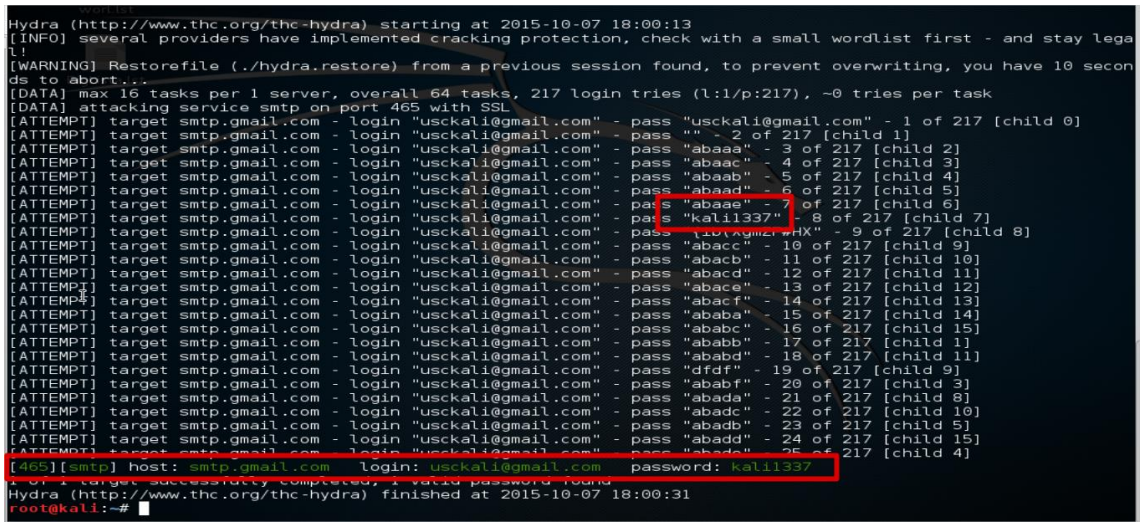
Figura 13 Ataque ao Gmail

Fonte: Elaborado pelo autor.

No primeiro bloco de comandos informa-se qual é o endereço a ser atacado, depois onde está localizada a wordlist (no caso em

root/Desktop/worl.lst), e por fim dizemos qual é o endereço do servidor do e-mail e serviço que será atacado, que no caso foi o SMTP, então o Hydra começou a verificar todas as palavras contidas na lista, e quando a combinação de senha e e-mail deu sucesso ele retornou com a mensagem mostrada na Figura 14 com o seguinte resultado:

Figura 14 Ataque utilizando o Hydra



Fonte: Elaborado pelo autor.

Como a senha estava na posição 8 da wordlist, demorou apenas 13 segundos para encontrar a senha correta, porem rodando o mesmo comando novamente demorou apenas 8 segundos, então conclui-se que este tempo variar, dependo do uso da internet e velocidade do servidor vítima.

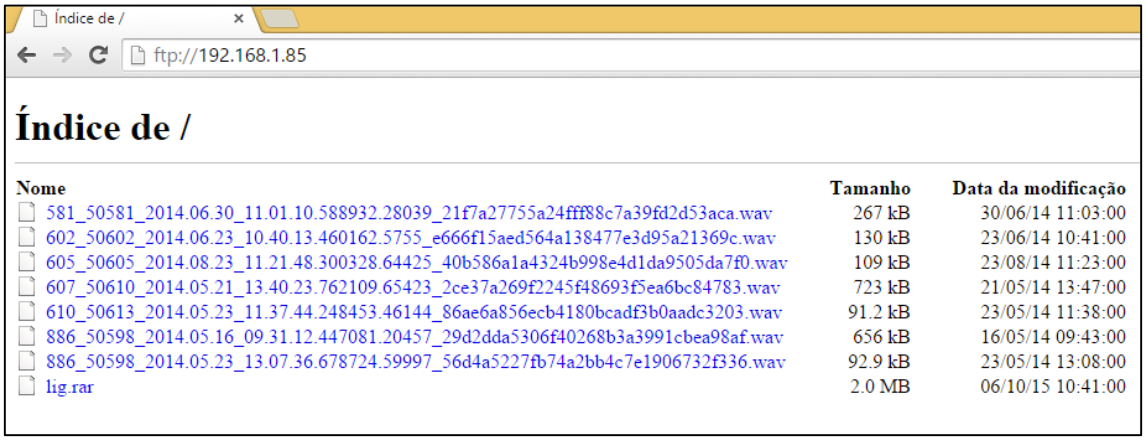
Foi colocado para aferir sua efetividade com a senha na posição 500 da lista, porém, o software não reconheceu a senha correta, na primeira tentativa mostrou que a senha era uma outra, diferente da correta, e em outra foi mostrado que nenhuma senha compatível foi encontrada.

Para minimizarmos problemas com o servidor do Google, pois ele possui mecanismos que barram um ip após tentativas erradas, pois foi visto que na primeira vez que foi executado o comando deu certo, depois executei novamente e deu erro. Foi criado então um serviço FTP de uma máquina Windows, pois

neste ambiente é possível ter o total controle de todas as variáveis como bloqueio de IP e restrições.

Em uma máquina portando o Windows 8.1 foi habilitado o serviço FTP executando na porta 21 com o ip local da máquina que é 192.168.1.85 conforme vemos na Figura 15:

Figura 15 - Serviço de FTP



Fonte: Elaborado pelo autor.

O para efetuar o login é necessário um usuário e senha (usuário teste, senha kali1337). Com o serviço criado a ativo foi novamente utilizado o Kali e retornado os ataques Utilizando o Hydra.

Colando a senha na posição 10000 o ataque iniciou-se as 12:03:36 e finalizando as 12:03:48 durando apenas 12 segundos para verificar 10 mil senhas, em outro teste demorou cerca de 2 minutos para verificar 100mil senhas. O ataque foi efetivo, pois retornou com o usuário e senha corretos, sem erros ou falhas de mostrar uma senha validando quando na verdade deveria ser outra.

O Hydra mostra-se eficiente quando ataca serviços de SSH ou FTP, para e-mails smtp ou pop3 ele consegue encontrar a senha certa porem apresentou falhas, pois na primeira vez que executei com a senha na posição 10 da lista ele encontrou, porem depois de executar procurando mais de 500 senhas

apresentou erros, hora ele não encontrava a senha e hora apontava uma senha invalida como a correta.

Na Figura 16 e 17 ilustram os resultados obtidos com o Hydra, mostrando-se ineficiente para ataque ao Gmail, e eficiente ao ataque ao serviço FTP.

Figura 16 - Comparativo de resultados - Hydra

Hydra		
Ataque ao Gmail		
Posição da senha	Classificação	Tempo
10	Efetivo	5-15 segundos
500	Não Efetivo	Não Avaliado
50000	Não Efetivo	Não Avaliado

Fonte: Elaborado pelo autor.

Figura 17 Resultados do Hydra FTP

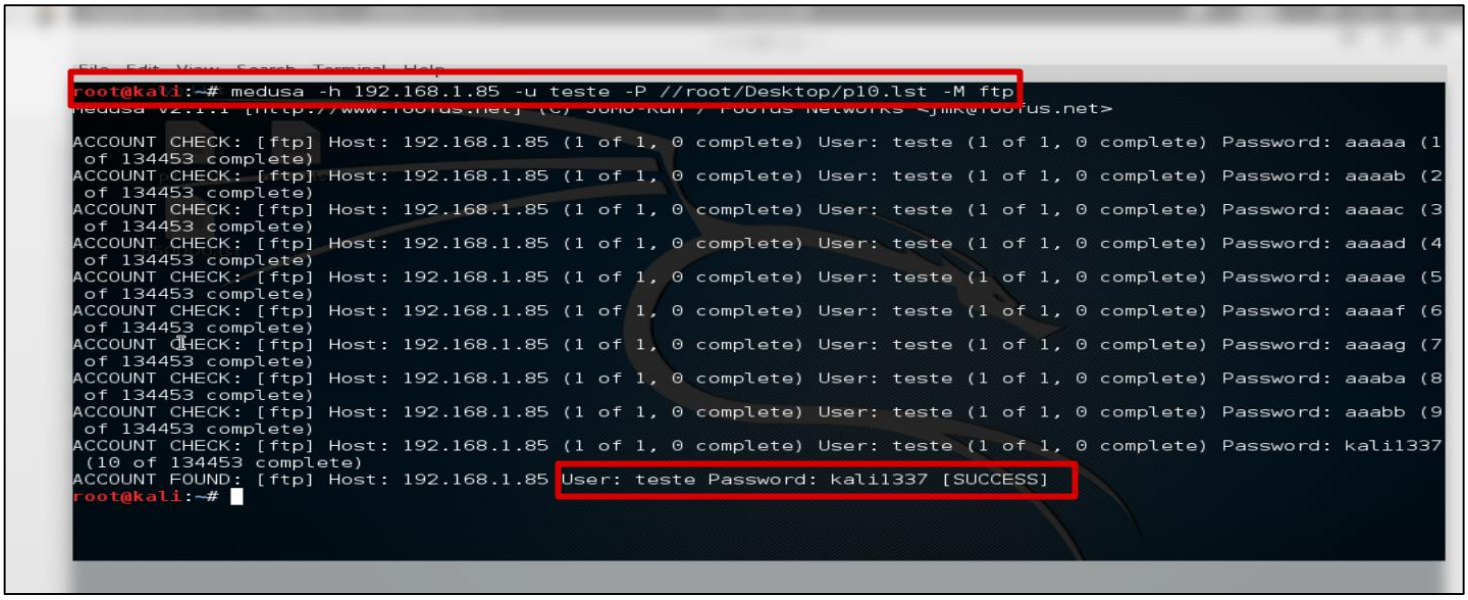
Hydra		
Ataque ao FTP		
Posição da senha	Classificação	Tempo
10	Efetivo	Instantâneo
500	Efetivo	2 - 5 segundos
50000	Efetivo	Cerca de 1 minuto

Fonte: Elaborado pelo autor.

6.2 Medusa

No medusa foram testados os mesmos parâmetros que já citados anteriormente, começando pelo FTP, com a senha na posição 10, foi efetivo e buscou instantaneamente conforme vemos na Figura 18:

Figura 18 Utilização do Medusa



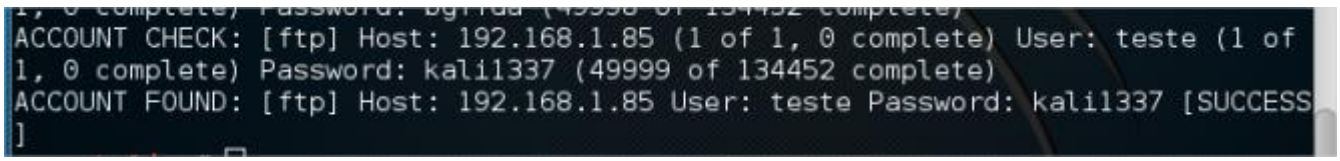
Com a senha na posição 500 também foi efetivo e demorou cerca de 5 segundos:

Figura 19 Sucesso do Medusa

Fonte: Elaborado pelo Autor

Com a senha na posição 50.000 também foi efetivo, porem o ataque durou 00:06:35, demorando um pouco mais do que o Hydra, conforme ilustrado na Figura 20.

Figura 20 Utilização do Medusa



Fonte: Elaborada pelo autor.

Com o gmail, com 10 tentativas ele mostrou-se eficiente, encontrando em 10 segundo a senha na posição 10.A Figura 21 ilustra o sucesso da tentativa.

Figura 21 Utilização do Medusa

Fonte: Elaborado pelo autor.

Com a senha na posição 500 a medusa mostrou erro, dizendo que foi efetuada muitas tentativas, e pede para tentar novamente depois, pelo aferido, após 2 minutos ele permite mais 100 tentativas e então apresenta o mesmo erro.Com 50.000 linhas não foi necessário fazer teste pois não passou dos 100.

Na Figura 22 é apresentado um comparativo de efetividade do software medusa.

Figura 22 - Comparativo Medusa

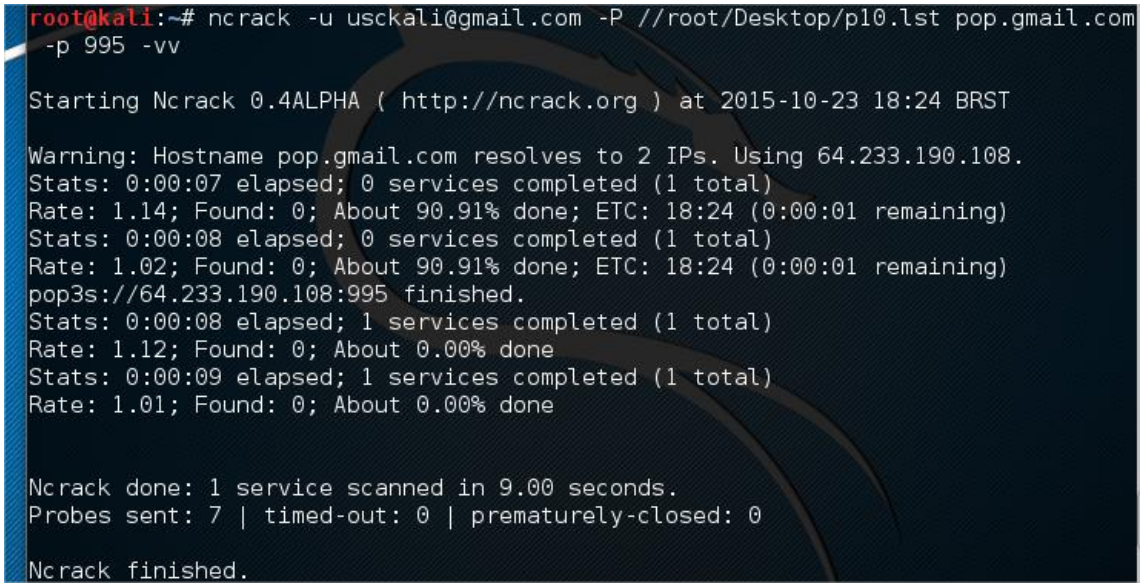
Medusa		
Ataque ao Gmail		
Posição da senha	**Classificação**	**Tempo**
10	Efetivo	5-15 segundos
500	Não Efetivo	Não Avaliado
50000	Não Efetivo	Não Avaliado
Medusa		
Ataque ao FTP		
Posição da senha	**Classificação**	**Tempo**
10	Efetivo	Instantâneo
500	Efetivo	3 a 5 segundos
50000	Efetivo	Cerca de 6 minutos

Fonte: Elaborado pelo autor.

6.3 Ncrack

O Ncrack segue a mesmas linhas do Hydra e Medusa, realizando teste de bruteforce, começando com o servidor de e-mail com a senha na 10 posição temos o seguinte resultado abaixo, mostrando que não foi possível realizar o ataque bem sucedido, pois o Gmail ainda não barrou o software. Na Figura 23 é ilustrado o sucesso com a senha na posição 10 da lista.

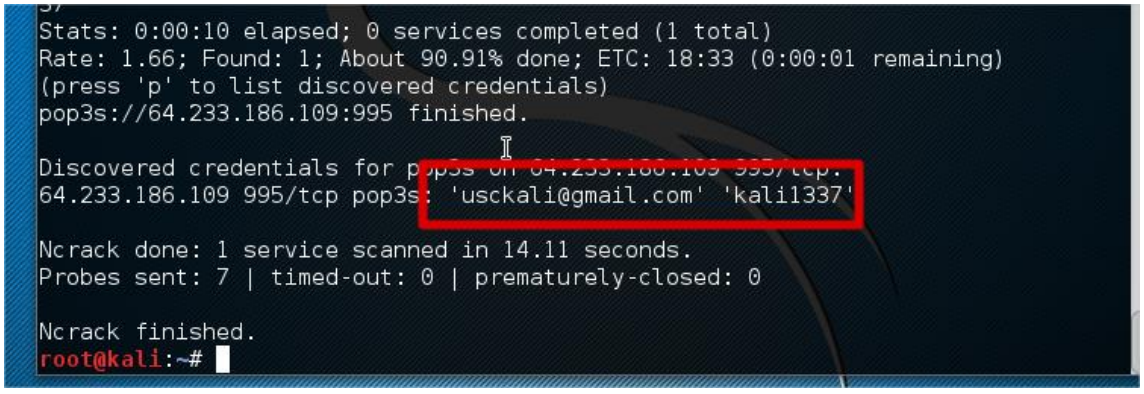
Figura 23 - Utilização do Ncrack



Fonte: Elaborado pelo autor.

Porem após breve pesquisa, foi aferido que a conta POP no gmail, não vem por padrão ativa, sendo necessária ativar via configuração, e após ativa, foi obtido sucesso conforme visto na Figura 24:

Figura 24 - Sucesso do Ncrack



Fonte: Elaborado pelo autor.

Foi necessário realizar o ataque de maneira no Ncrack, pois o mesmo não suporte SMTP, apenas POP.

Na Figura 25 mostra o ataque com a senha na posição 500:

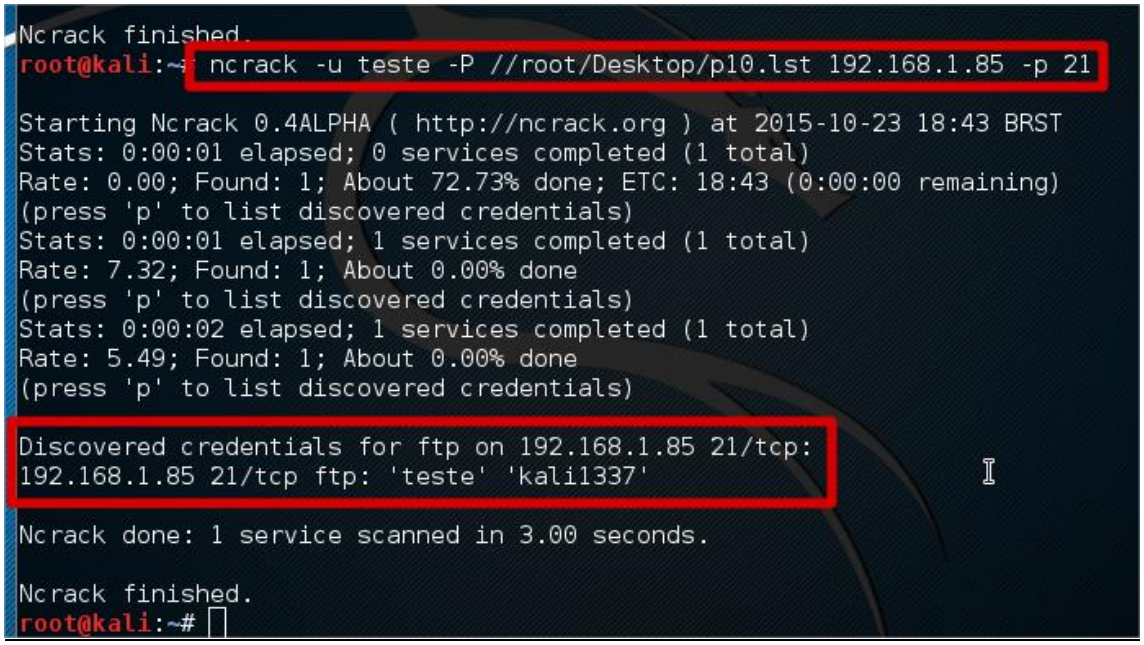
Figura 25 Ncrack

Fonte: Elaborado pelo autor.

Porém não foi obtido sucesso, e após 18 segundos mostrou que não foi possível encontrar a senha correta. E mesmo após várias tentativas não foi obtivo nenhum resultado, seguindo esta mesma linha, com a senha na posição 50000 também não foi possível descobrir, o Ncrack para ataque brute force no email também mostrou ineficiente, pois o servidor de destino possui mecanismos de defesas conta este tipo de ataque.

Iniciando o ataque brute force para ftp lançamos o comando para descobrir a senha do serviço FTP na posição 10 e foi obtido o resultado ilustrado na Figura 26:

Figura 26 Utilização do Ncrack



Fonte: Elaborado pelo autor.

Com a senha na posição 500 também foi obtivo sucesso mostrando assim o seguinte resultado:

Figura 27 Sucesso Ncrack

Fonte: Elaborado pelo autor.

E por fim, com a senha na posição 50000 também foi obtido sucesso, porem o processo todo levou 1 hora e 30 minutos para ser feito. Na Figura 28 é ilustrado os resultados obtido com o Ncrack.

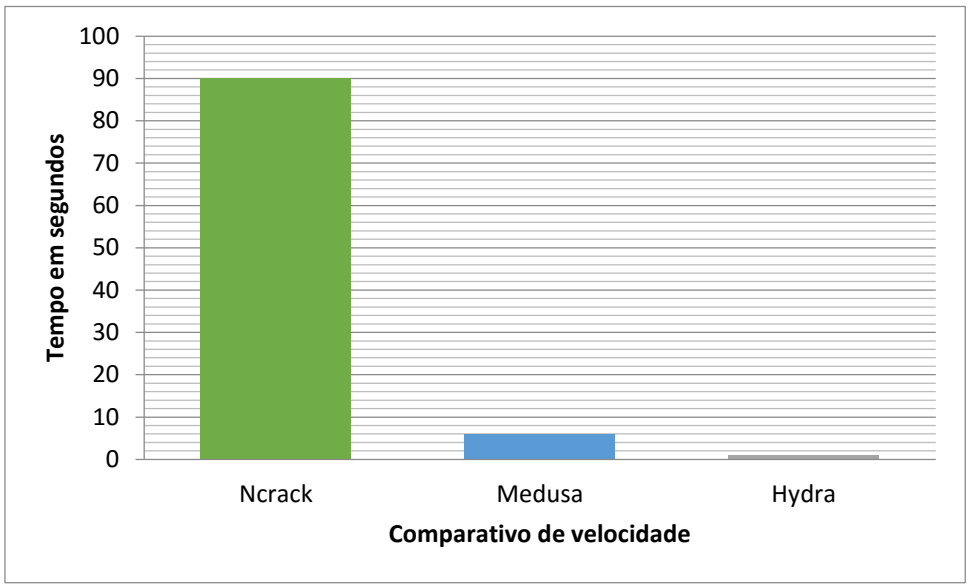
Figura 28 Comparativo do Ncrack

Ncrack		
Ataque ao Gmail		
Posição da senha	**Classificação**	**Tempo**
10	Efetivo	14 segundos
500	Não Efetivo	Não Avaliado
50000	Não Efetivo	Não Avaliado
Ncrack		
Ataque ao FTP		
Posição da senha	**Classificação**	**Tempo**
10	Efetivo	3 segundos
500	Efetivo	54 segundos
50000	Efetivo	1 hora e 30 minutos

Fonte: Elaborado pelo autor.

Na Figura 29 segue em comparativo do tempo levado (em segundos) pelos 3 softwares aferidos, para descobrir a senha no Gmail na posição 10 da wordlist.

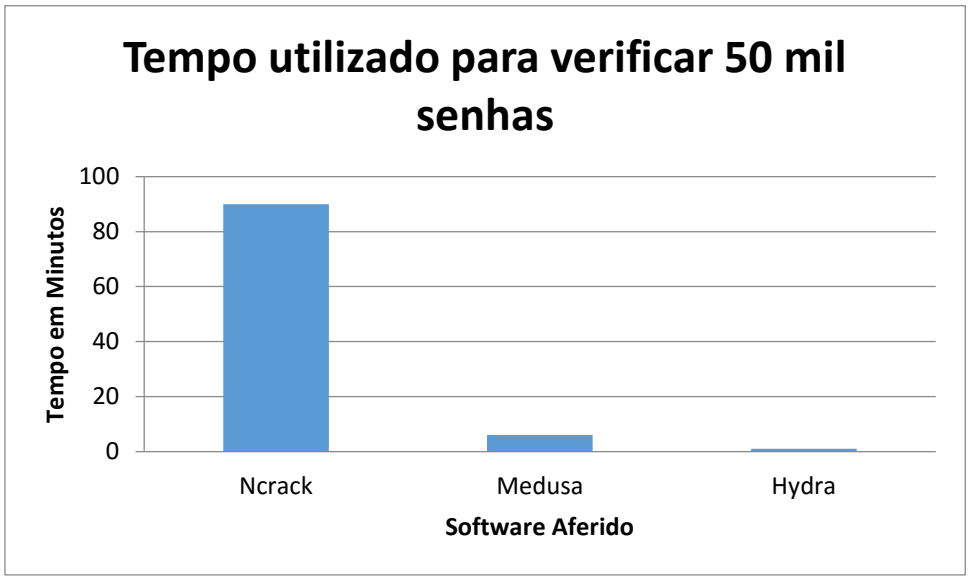
Figura 29 - Comparativo de Efetividade



Fonte: Elaborado pelo autor.

Na Figura 30 tem-se o tempo levado para verificar 50mil senhas no serviço FTP

Figura 30 Comparativo de Efetividade



Fonte: Elaborado pelo autor.

7 Considerações finais.

O ataque bruteforce utilizando wordlist é efetivo, porem há diversos meio de se proteger de um ataque desta natureza, pois como pode ser observado no Gmail, após cerca de 100 tentativas de senhas, ele bloqueia o usuário por cerca de 3 minutos, e para tentar estas 100 senhas pode levar um tempo, então se a senha estiver em uma posição bem alta na lista, o processo poderia levar de semanas a anos, tornando-se assim ineficiente.

No ataque bruteforce com wordlist, o login e senhas são buscados através de uma base padrão, caso sua senha algo simples, como apenas um nome, ou então seu nome e algum numero obtido através de suas informações pessoas, ela pode estar vulnerável, pois, o atacante sabendo destas informações pode mescla-la e descobrir assim sua senha, então para que a senha seja a mais segura possível é aconselhável que não utilize informações pessoas, e se possível números aleatórios, e como ele compara combinações, quanto maior sua senha for, maior será o tempo que levara para descobrir, pois é utilizado de combinações para descobrir.

Foi aferido e comparado o funcionamento de 3 softwares que possuem a mesma funcionalidade, e em relação a ataque ao Gmail, todos foram ineficientes, pois para verificar mais de 100 senhas eles foram interrompidos pelas políticas de segurança do Google, até 100 senhas o Medusa e Hydra obtiveram desempenho semelhantes, levando cerca de 15 segundos para verificar as possibilidades, porem após 100 tentativas foram bloqueados, tornando-se assim ineficientes.

Em relação ao ataque no serviço criado, todos os softwares obtiveram sucesso, porem vale ressaltar que não foi criado nenhuma politica de segurança, tornando assim o serviço vulnerável a ataques. É bem comum que serviços FTP possuem por padrão politicas de segurança que assim como o Gmail, torne inviável um ataque bruteforce. Na comparação dos softwares o Hydra foi o que mais obteve êxito, porém, conseguiu verificar 50 mil senhas em menos de 1 minuto, então neste teste o Hydra foi o mais eficiente.

É o resultado esperado pois o Hydra sendo o mais popular, é espero que seja também o mais eficiente, e neste trabalho estas expectativas foram comprovadas.

REFERÊNCIAS

AHAROMI, M. **The Birth of Kali linux**. Kali, 2012. Disponível em: <https://www.kali.org/news/birth-of-kali/>. Acesso em: 26 mar. 2015.

AHAROMI,**Should i use kali linux**. Kali, 2012. Disponível em: <http://docs.kali.org/introduction/should-i-use-kali-linux>. Acesso em: 26 mar. 2015.

ALI, S.; HERIYANTO, T. **BackTrack 4**. Birmingham, UK: Packt, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS . NBR ISO/IEC: Tecnologia da informação — **Técnicas de segurança** — Código de prática para a gestão da segurança da informação. Rio de Janeiro: 2005

Back|Track Linux **Penetration Testing Distribution**. Offensive-security, c2015. Disponível em: <https://www.offensive-security.com/community-projects/backtrack-linux/>. Acesso em: 6 mar. 2015.

BACKTRACK Linux - **Penetration Testing Distribution. Backtrack-linux**, c2014. Disponível em: <http://backtrack-linux.org>. Acesso em: 12 abr. 2015.

Baloch, R. **Ethical hacking and penetration testing guide**. Waltham: Elsevier, 2015.

BROAD, J.; BINDNER, A. **Hacking with Kali**. Waltham, MA: Elsevier Science, 2014.

DALZIEL, H. **Kali Linux review and a brief history of the BackTrack pentesting distro**. Concise-courses, 2013. Disponível em: <http://www.concise-courses.com/security/kali-linux-review-and-history/>. Acesso em: 6 mar. 2015.

D'ANDREA, E. P.; ALVES, F. Título. **Pwc**, 2015. Disponível em: <http://www.pwc.com.br>. Acesso em: 27 abr. 2015.

ENGEBRETSON, P. **The basics of hacking and penetration testing**. Amsterdam: Elsevier, 2013.

ESTATÍSTICAS dos **Incidentes Reportados ao CERT.br**. Cert, 2014. Disponível em: <http://www.cert.br/stats/>. Acesso em: 11 abr. 2015.

ESTATÍSTICAS mantidas pelo **CERT.br**. Cert, 2012. Disponível em: <http://www.cert.br/stats/>. Acesso em: 11 abr. 2015.

FARMER, D.; VENEMA, W. **Improving the security of your site by braking int it**. Rockland, MA, 1993.

GIAVAROTO, S. C. R.; SANTOS, G. R. dos. **Backtrack Linux - Auditoria e Teste de Invasão em Redes de Computadores**. Rio de Janeiro: Ciência Moderna, 2013.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 5. ed. São Paulo: Atlas, 2010.

Herzog, P. ISECOM - **Open Source Security Testing Methodology Manual** (OSSTMM). Disponível em: <http://www.isecom.org/research/osstmm.html>. Acesso em: 5 jun. 2015.

KRUTZ, R.; VINES, R.; **The CISSP Prep Guide: Mastering the Ten Domains of Computer Security**. Local: Wiley Press, 2001.

MARTINS, A., SAUKAS E., ZANARDO, J. SCAI: **Sistema de Controle de Acesso para os Requisitos da Saúde**. In: CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE, 9. 2004, Ribeirão Preto. Anais... Ribeirão Preto, 2004. Disponível em: <http://www.sbis.org.br/cbis9/arquivos/960.pdf>. Acesso em: 12 abr. 2015.

MULLER, L. **Ataque hacker rendeu US$ 200 milhões em prejuízo para a Sony Pictures**. Tecmundo, 2014. Disponível em: <http://www.tecmundo.com.br/ataque-hacker/69727-ataque-hacker-rendeu-us-200-milhoes-prejuizo-sony-pictures.htm>. Acesso em: 27 abr. 2015. (TecMundo, 2014)

MUNIZ, J.; LAKHANI, A**. Web Penetration Testing with Kali Linux**. Birmingham: Packt Publishing, 2013.

MUNIZ, J.; LAKHANI, A. Web Penetration Testing with Kali Linux. Birmingham: Packt, 2013.

NAKAMURA, E.; GEUS, P. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

NESTLER, V. et al. **Principles of Computer Security**: CompTIA Security+TM and Beyond Lab Manual. 2. ed. New York: The McGraw-Hill, 2011.

OLIVEIRA, J. F. de. **Sistemas de informação: um enfoque gerencial inserido no contexto empresarial e tecnológico**. São Paulo: Érica, 2000.

RAMACHANDRAN, V. **BackTrack 5 wireless penetration testing**. Birmingham, UK: Packt, 2011.

SCHNEIER, B. **The futility of Digital Copy Prevention Crypto-Gram**.New York.Addison Wesley, 2001.

SILVA FILHO, A. M. da. **Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações**. Revista Espaço Acadêmico, Maringá, v. 42, 2004.

STALLINGS, W. **Cryptography and Network Security**. 5th. ed. [Sl.]: Prentice-Hall, 2010.

Stein, M. **Security Systems**. New York: William Morrow, 2007.

TANENBAUM, A.; Souza, V. **Redes de computadores**. Rio de Janeiro: Elsevier, 2003.

VALLABHANENI, S.; **CISSP Textbook**. Local: SRV Professional Publications, 2002..

VAUGHAN, E. **Risk Management**. New Baskerville: John Wiley & Sons. 1997.

WILHELM, T. **Professional penetration testing**. Rockland, MA: Syngress, 2010.