UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Ciências - Campus Bauru

DEPARTAMENTO DE COMPUTAÇÃO

BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

MÉTODOS DE TESTE DE PENETRAÇÃO EM SISTEMAS WEB NA NUVEM

BAURU
2016

HUGO CICARELLI

MÉTODOS DE TESTE DE PENETRAÇÃO EM SISTEMAS WEB NA NUVEM

Trabalho de Conclusão de Curso do Curso de Ciência da Computação da Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Ciências, Campus Bauru.

Orientador: Prof. Dr. Kelton Augusto Pontara da Costa

Universidade Estadual Paulista "Júlio de Mesquita Filho"

Faculdade de Ciências

Ciência da Computação

BAURU

2016

Hugo Cicarelli
Métodos de Teste de Penetração em Sistemas Web na Nuvem/ Hugo Cicarelli. – Bauru, 2016-
22 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. Kelton Augusto Pontara da Costa

Trabalho de Conclusão de Curso – Universidade Estadual Paulista "Júlio de Mesquita Filho"
Faculdade de Ciências
Ciência da Computação, 2016.

1. PenTest 2. Cloud Computing 3. Security 4. Open Source I. Prof. Dr. Kelton Augusto Pontara da Costa. II. Universidade Estadual Paulista "Júlio de Mesquita Filho". III. Faculdade de Ciências. IV. Métodos de Teste de Penetração em Sistemas Web na Nuvem

Hugo Cicarelli

Métodos de Teste de Penetração em Sistemas Web na Nuvem

Trabalho de Conclusão de Curso do Curso de Ciência da Computação da Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Ciências, Campus Bauru.

Banca Examinadora

Prof. Dr. Kelton Augusto Pontara da Costa
Orientador

Prof. Dr. Simone das Graças Domingues Prado

Prof. Dr.

Bauru 2015

Espaço destinado à dedicátoria do texto.

Agradecimentos

Espaço destinado aos agradecimentos.

Espaço destinado à epígrafe.

Resumo

Espaço destinado à escrita do resumo.

Palavras-chave: Palavras-chave de seu resumo.

Abstract

Abstract area.

Keywords: Abstract keywords.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

Com o grande crescimento que se deu na tecnologia nos últimos anos, novas maneiras para melhorar o desempenho e armazenamento de recursos computacionais reduzido foram aprimoradas. Com a popularização da internet, foi possível manter computadores e sistemas computacionais conectados a qualquer momento, em qualquer lugar do mundo. Assim surgiram Sistemas em Nuvem (*Cloud Services*), capazes de serem alugados para alocar equipamentos de hardware e software, utilizados por empresas específicas, para que as mesmas não precisem se preocupar com gastos para melhorar seus recursos, podendo contratar serviços oferecidos na Nuvem, pagando por isto apenas o que for utilizado.

Como esses serviços se encarregam de manter a hospedagem de dados, além de manter o tráfico de usuários não congestionado, o cliente não se preocupa também com as ameaças que possa vir a ter. Nesse ponto, o sistema na nuvem terá que oferecer um sistema invunerável, para manter credibilidade.

Testes de Penetração, também conhecidos como *PenTest* ou Testes de Invasão, consistem em recolher informações sobre o alvo, identificar possíveis aberturas, tentativas de invasão e relatórios sobre o teste propriamente dito. O objetivo principal de um pentest é de determinar pontos fracos na segurança do sistema.

1.1 Problema

A cada dia que passa, novas tecnologias são criadas ou mesmo novos métodos são descobertos. Porém isso pode ser beneficiente para a sociedade como também para pessoas mal intencionadas. Tendo isso em vista, é necessário manter em dia conhecimento de todas as possíveis vulnerabilidades que um sistema possa a ter, para que não haja roubo de informações e dados sigilosos. Ao oferecer um serviço na nuvem, a empresa precisa garantir à seus clientes que não haverá invasão de terceiros, não havendo preocupação dos mesmos com os dados que eles disponibilizam para os serviços na nuvem.

2 Objetivos

2.1 Objetivos Gerais

Criação de uma ferramenta que automatize Testes de Penetração em Serviços na Nuvem.

2.2 Objetivos Específicos

a) Aprender metodologias de Teste de Penetração;

b) Aprender os vários tipos de Teste de Penetração;

c) Aprender sobre Computação na Nuvem;

3 Fundamentação Teórica

Práticas realizadas para determinar fraquezas na segurança de um Sistema Computacional, sendo este um Sistema Operacional, um Servidor, uma Rede de Computadores ou uma Aplicação, é chamado de Testes de Penetração, ou comumente conhecidos como *PenTests*.

A aplicação que gera este tipo de Teste, além de garantir que a segurança de um sistema esteja sempre atualizada, é de verificar a aptidão a qual a equipe de uma empresa possui ao se deparar com problemas de invasão externa.

Considera-se um ataque toda e qualquer invasão que um Sistema Computacional pode sofrer, sem aviso prévio. Este tipo ataque geralmente é realizado por alguém com um certo conhecimento técnico na área de programação e segurança. O responsável por tais atos de invasão é atribuído o nome de *Hacker*.

Hacker é um termo designado a pessoas cujo intuito é causa problemas como, por exemplo, inserindo vírus, roubando números de cartão de crédito. Porém, segundo Brunvand, há um equívoco nesta nominação, sendo chamados de *Crackers* os sujeitos que tentam se aproveitar de falhas em Sistemas.

De acordo com Raymond (1996), *Hacker* é definido como um programador engenhoso, um bom *hackeamento* é uma solução engenhosa para um problema de programação e *hackear* é o ato de solucionar este problema. Raymond ainda cita cinco possíveis características que qualificam um *hacker*:

a) Uma pessoa a qual aprecia aprender detalhes de uma linguagem de programação ou de um sistema;

b) Uma pessoa a qual aprecia programar ao invés de apenas teorizar;

c) Uma pessoa capaz de apreciar o *hackeamento* de outra pessoa;

d) Uma pessoa que aprende rapidamente uma linguagem de programação;

e) Uma pessoa que é perito em determinada linguagem de programação ou sistema computacional.

Portanto, um *PenTester*, pessoa que responsável por realizar tarefas de Testes de Penetração, pode ser considerado como *Hacker*.

Como Testes de Penetração tentam explorar fraquezas em algum Sistema Computacional, fornecendo relatórios sobre essas possíveis fraquezas com finalidade de solucioná-las, este pode ser incorporado como uma área de Segurança de Computadores.

3.1 Segurança

Desde sempre, o valor da informação foi essencial, e nos tempos atuais não é diferente. Com o aumento da tecnologia, existe uma grande preferência de manter informações virtualizadas, seja pela grande capacidade de armazenamento que os sistemas computacionais possuem, ou pelo fácil acesso que se dá devido à internet, por exemplo. Porém, manter informações centralizadas em um só lugar pode se tornar um problema, caso não mantenha a segurança de seus dispositivos atualizada.

Para proteger dados e informações tendo em mente as diversas arquiteturas de rede que existem, *Web Services*, aplicações, diferentes plataformas de servidores, está mais difícil do que nunca. Por os computadores e a internet de fato estar presente no nosso dia-a-dia nas últimas décadas, invasões não são mais realizadas por crianças curiosas se aventurando no mundo dos códigos.

Apesar de existirem métodos os quais previnem o roubo de dados ou invasão de sistemas, como é o caso de Anti-vírus, por exemplo, o melhor jeito de descobrir se um sistema está realmente seguro contra invasões é tentando invadir o mesmo, pois apenas assim será possível detectar problemas reais que *hackers* mal intesionados podem vir a causar.

Dessa forma, é possível ver Testes de Penetração como um ramo da Segurança de Computadores, tendo em vista de que eles são realizados visando melhor as atuais falhas que pode vir a se descobrir com o avanço de novos métodos.

3.2 Teste de Penetração

No início deste capítulo, explicamos superficialmente que Testes de Penetração, ou também chamados Testes de Invasão ou *PenTest*, são testes realizados de modo a simular um ataque mal intencionado à uma rede, aplicação ou sistema computacional. Os testes consistem em:

a) Recolher informações do alvo, antes do teste (reconhecimento);

b) Identificar possíveis pontos de entrada;

c) Tentativa de invasão, seja virtualmente ou pessoalmente;

d) Reportar as descobertas.

O objetivo de se realizar Testes de Invasão é determinar fraquezas na segurança justamente para reforçar a mesma nos sistemas testados, prevenindo assim que dados e informações sejam roubadas ou manipuladas por um *Cracker*. *Crackers*, como já foi dito, são *Hackers* que violam o Código de Ética dos *Hackers*, segundo Raymond. A linha que separa um *PenTester* de um *Cracker* é exatamente pelo fato de um *PenTester* ter sido contratado para realizar o ato de invadir o sistema, tendo uma permissão prévia concedida pelo dono do

sistema. Outro ponto que realizar testes de penetração podem contribuir, além de aumento da segurança, é testar a Política de Observação de uma empresa perante possíveis ataques, bem como testar o quão preparada está uma empresa para responder a possíveis ataques, e também verificar o quão ciente estão os funcionários quanto a brechas que podem resultar em uma invasão.

Testes de Invasão muitas vezes são confundidos com Avaliação de Vulnerabilidade. Porém isso é um erro comum, visto que o foco o qual se dá ao realizar um Teste de Penetração é na tentativa de ganhar um acesso ao sistema, a ponto de não existirem restrições a arquivos e dados sigilosos, enquanto que Avaliação de Vulnerabilidade tem ênfase em identificar pontos vulneráveis na segurança, não focando em tentar invadí-los.

Um *PenTester* tem como responsabilidade tentar invadir o sistema desejado de modo que irá usar os meios e métodos que um *Cracker* também usaria, para garantir que o sistema está seguro. Durante o processo de invasão, o *PenTester* estará fazendo um relatório detalhado, passando por todos os caminhos que ele tenha tomado, para que no final esteja especificado quais são as falhas do sistema, como foram descobertas e assim arrumá-las para que não haja potencial de invasão.

3.2.1 Por que realizar Testes de Penetração?

Precisa-se ter em mente de que uma falha corrigida ontem, pode resultar em uma falha imprevista hoje. Por conta disso, é importante manter constante as realizações de testes de penetração, garantindo assim um sistema seguro. Assim, é preciso estar sempre por dentro das novidades tecnológicas pois, atualizações podem ser facas de dois gumes: do mesmo modo que trazem novas medidas para prevenir quebras de segurança, podem também proporcionar novos meios para se invadir um sistema.

Northcutt et al. cita que o motivo principal para realização de Testes de Penetração é de encontrar vulnerabilidades através de ganho de acesso e resolver estas falhas. Porém, além desse motivo principal, também é citado que é uma boa prática ter o sistema verificado por olhos que não estavam inicialmente no projeto, podendo assim encontrar falhas não verificadas anteriormente. Outros motivos que são citados, podemos listar os seguintes:

a) Achar brechas antes que alguém mal intencionado ache: invasores podem estar explorando fraquezas a todo momento para tentar achar uma brecha. Como o autor cita, testes de penetração podem ser vistos como um Exame Médico Anual pois, não importa o quão saúdavel pareça, sempre é bom manter em dia os diagnósticos;

b) Reportar problemas achados ao gerente responsável: muitas vezes um problema pode ser apontado, e o teste de penetração auxilia em maneiras de resolver o problema;

c) Verificar configurações de segurança: realizar teste de invasão contribui para garantir

que o sistema esteja realmente seguro contra invasões, além de que, segundo o autor, uma opinião externa ao projeto garante que todos os pontos de vistas não possuem falhas;

d) Treinamento de segurança para a equipe: se um teste de penetração conseguir invadir com sucesso um sistema, isso pode indicar uma falta de treinamento por parte da equipe responsável pela segurança. Testes de penetração ajudam no treinamento da equipe, preparando para conseguirem identificar um ataque e impedí-lo antes que este seja bem sucedido;

e) Testar novas tecnologias: de acordo com o autor, a melhor maneira para se testar tecnologias novas, é quando elas ainda não foram lançadas. Testes de penetração podem ajudar a revelar falhas desconhecidas antes de um lançamento, para que o produto seja totalmente confiável.

3.2.2 Estágios de um Teste de Penetração

Weidman (2014) descreve os estágios que um Teste de Penetração percorre, que, de acordo com ela, totalizam em 7: Escopo, Reconhecimento, Modelo de Ameaça, Análise de Vulnerabilidade, Explorar Vulnerabilidades, Pós Exploração, Relatório.

A fase de Escopo é realizada antes mesmo de se começar o Teste. Consiste em um pré-engajamento, o qual envolve definir com o cliente os objetivos que o teste irá abordar. Nesta fase, o *PenTester* é encarregado de explicar ao cliente sobre como os testes ocorrerão, para que não haja falta de comunicação, o que pode resultar em uma intrusão além do esperado pelo lado do cliente. Este será o momento o qual se deve sentar com o cliente o que ele espera que um Teste de Penetração resulte, toda informação será crítica. Certas dúvidas terão que ser apresentadas, como o se terá que definir a maioria dos requisitos, quais portas de IP testar, quais ações serão permitidas pelo cliente, o trabalho será superficial, apenas verificando vulnerabilidades e brechas, ou poderá tentar derrubar o sistema, qual o horário que serão realizados os testes, entre outras perguntas técnicas. Por fim, é nesta fase que deverá ser providenciado um acordo, deixando claro que todas as informações obtidas serão mantidas confidencialmente, como também concedendo autorização para realizar os testes pois, caso contrário, poderá ser considerado um crime.

Após a fase de Escopo, ou Pré-engajamento, temos a fase de Reconhecimento. Durante essa fase, são analisadas informações sobre o alvo, bem como é feito uma análise de portas para se ter uma noção o tipo de sistema que se estará testando.

Modelo de Ameaça é a fase na qual se desenvolve como o ataque será realizado, a partir das informações reunidas na fase de Reconhecimento. Nesta fase será o momento no qual o *PenTester* pensa como um invasor e tentar explorar brechas que não seriam normalmente testadas, até conseguir algum acesso, caso estas existam.

Durante a fase de Análise de Vulnerabilidades, o *PenTester* fica responsável por descobrir vulnerabilidades que poderão vir a ser exploradas de modo que o teste seja bem sucedido. Nessa fase, será feita uma leitura das possíveis vulnerabilidades utilizando softwares que utilizam uma série de verificações. Porém não se pode confiar totalmente no software, sendo necessário também fazer uma análise manual, verificando a leitura dos resultados.

A quinta fase, a qual Weidman nomeou de Exploração de Vulnerabilidades, é onde o teste realmente ocorre. Nesta etapa, o *PenTester* irá se utilizar das brechas encontradas na etapa anterior e tentará explorar o máximo delas até que consiga realizar a invasão propriamente dita.

Na fase de de Pós Exploração, ocorre a análise dos dados coletados através da invasão, procurando por algum conteúdo com alto valor de informação, tentar conseguir acesso privilegiado ao sistema. De acordo com a autora, nesta parte será possível ver se as vulnerabilidades são realmente significativas, pois se somente for conseguido acesso a arquivos que não contém uma informação tão crítica, ainda será necessário resolvê-las, porém não são consideradas vulnerabilidades de alta prioridade.

A fase final será apresentado o relatório a respeito das descobertas encontradas. O relatório apresentado deve conter os pontos positivos a respeito do sistema do cliente, bem como deve estar bem detalhado a respeito de todos os passos tomados, como foi feita a invasão, para que seja possível reproduzir e, assim, resolver as vulnerabilidades encontradas. Um bom relatório pode ser dividido em Sumário Executivo e Relatório Técnico.

3.3 Computação na Nuvem

Computação na Nuvem é um termo designado para especificar um serviço de hospedagem de serviços utilizando a Internet, ou seja, ao invés de ser necessário montar um servidor com todos os requisitos necessários, se é alugado um espaço de um servidor e seu acesso é feito pela Internet, pagando somente por aquilo que se é usado.

Dentre os diversos benefícios que a Computação na Nuvem trás, podemos listar:

a) Os recursos oferecidos suprem a maioria das demandas de quase todos os ramos de empresas;

b) Elasticidade, ou seja, o poder de aumentar ou diminuir os recursos, conforme se é necessário;

c) Pagar somente pelos recursos que são utilizados.

3.3.1 Tipos de Serviços na Nuvem

Segundo Rouse, em '*A comprehensive look at the path to cloud migrations*', Serviços de Computação na Nuvem são divididos nos seguintes tipos:

a) Privado;

b) Público;

c) Hibrido.

Serviço na Nuvem do tipo Privado ocorre quando o servidor, o qual estão todos os arquivos e dados, se localiza internamente na própria empresa, mesmo não estando no ambiente de trabalho das equipes. Normalmente existe uma sala para conter os diversos *hardwares* e recursos que suprem a necessidade. Esse tipo é bastante usado por empresas visto que, por estarem localizados internamente, são ambientes de trabalho mais seguros, por oferecer controle total dos recursos e não compartilhar estes recursos ou informações com outras empresas.

O segundo tipo abordado pela autora, Serviço de Nuvem Público, é o tipo oferecido pelos grandes *Datacenters* como Google ou Amazon, por exemplo, e pode ser contratado por qualquer empresa. É a opção mais acessível pois os recursos computacionais são oferecidos através da Internet, e o seu custo é somente por recursos utilizados pela empresa. Uma grande vantagem da Nuvem Pública é que é possível escalonar os recursos conforme for necessário, ou seja, se for necessários mais recursos computacionais, a empresa terá que configurar os recursos de forma a suprir as necessidades, podendo diminuir posteriormente, pagando apenas o que foi utilizado. A desvantagem que faz com que muitas empresas ficarem em dúvidas se migram para esse tipo de Computação na Nuvem é o fator de que os recursos oferecidos estão localizados externamente aos da empresa contratante, o que levanta desconfiança quanto à segurança de dados.

O último tipo citado, Nuvem Híbrida, é uma associação dos tipos privado e público. Com a nuvem híbrida, é possível tratar com informações sensíveis na nuvem privada, o que elimina incertezas e desconfianças relacionadas ao sigilo de informação. Ao mesmo tempo que arquivos menos críticos, como backup, email e armazenamento de dados estáticos, podem ser hospedados utilizando nuvem pública, o que proporciona maior elasticidade e menos custo em relação à recursos internos.

3.3.2 Categorias de Serviços na Nuvem

Woodford, em seu artigo sobre introdução à Computação na Nuvem, cita os seguintes modelos de Serviços na Nuvem:

a) IaaS (*Infrastructure as a Service*): neste caso se tem acesso ao hardware de um sistema externo, como serviços de armazenamento ou servidores;

b) PaaS (*Platform as a Service*): se é utilizado tanto o software quanto o hardware fornecidos pelo serviço contratado;

c) SaaS (*Software as a Service*): significa que se utiliza o software do sistema oferecido.

4 Metodologia

4.1 Métodos e Etapas

Para o desenvolvimento do projeto foi realizado o levantamento bibliográfico de metodologias existentes para realizar Testes de Penetração, analisando seus diversos aspectos e quais nos auxiliariam melhor em nosso objetivo, bem como modos de como aplicá-las em Sistemas na Nuvem..

Com a base teórica definida a etapa seguinte foi aplicar uma estrutura modular que correspondesse ao modelo teórico, para que todas as etapas da extração e reconhecimento do *audio fingerprint* possam ser modificadas sem que alterem o funcionamento geral do processo. Essa estrutura adaptável foi aplicada com base no modelo teórico genérico de reconhecimento de áudio.

4.2 Materiais Utilizados

4.2.1 Ambiente de desenvolvimento

Para desenvolvimento do projeto foi utilizado o Sistema Operacional Kali Linux, uma distribuição Linux especializada em Testes de Intrusão e Auditoria de Segurança.

4.2.2 Github

O Github é ao mesmo tempo um servidor de armazenamento de código e uma rede social onde pode-se submeter modificações, fazer cópias e acompanhar modificações de códigos de outras pessoas. A rede foi essencial para o desenvolvimento deste projeto por armazenar vários sub-módulos e disponibilizar código-fonte para consulta.

Referências

BRUNVAND, E. *The Heroic Hacker: Legends of the Computer Age*. 1996. <https://www.cs.utah.edu/~elb/folklore/afs-paper/node9.html>. [Acessado em 22 de Maio de 2016]. Citado na página 14.

NORTHCUTT, S. et al. *Penetration Test: Assessing Your Overall Security Before Attackers Do*. <https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635>. [Acessado em 25 de Maio de 2016]. Citado na página 16.

RAYMOND, E. S. *The New Hacker's Dictionary*. [S.l.]: The MIT Press, 1996. ISBN 0262680920. Citado 2 vezes nas páginas 14 e 15.

ROUSE, M. *A comprehensive look at the path to cloud migrations*. <http://searchcloudcomputing.techtarget.com/definition/cloud-computing>. [Acessado em 28 de Maio de 2016]. Citado na página 19.

WEIDMAN, G. *Penetration Test: A Hands-On Introduction to Hacking*. [S.l.]: William Pollock, 2014. ISBN 1593275641. Citado 2 vezes nas páginas 17 e 18.

WOODFORD, C. *Cloud computing*. <http://www.explainthatstuff.com/cloud-computing-introduction.html>. [Acessado em 28 de Maio de 2016]. Citado na página 19.