**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 PARA SISTEMAS WEB NA NUVEM

BAURU
2016

HUGO CICARELLI

# MÉTODOS DE TESTE DE PENETRAÇÃO PARA 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 para Sistemas Web na Nuvem/ Hugo Cicarelli. – Bauru, 2016-
16 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 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 para Sistemas Web na Nuvem

Hugo Cicarelli

# Métodos de Teste de Penetração para 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, surgiram novas maneiras para sanar quesitos de gastos e desempenho quanto às necessidades básicas. Os sistemas em nuvem (*Cloud Services*) surgiram de modo a terceirizar o hardware utilizado, sendo que o cliente paga apenas o que paga, deixando para este apenas se preocupar com o produto que será comercializado.

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

Justamente como a tecnologia está crescendo, novas ameaças aparecem diariamente. Ao oferecer um serviço que irá dispor de todos os dados de seus clientes, eles tem que possuir uma garantia de que não perderão seus dados.

Por esse motivo, é necessário manter em dia as possíveis vulnerabilidades, mantendo uma maior segurança para ambos os lados.

# 2 Objetivos

## 2.1 Objetivos Gerais

Estudar metodologias de Teste de Penetração em *Cloud Services*, analisando a possibilidade de criar uma ferramenta que automatize esta tarefa.

## 2.2 Objetivos Específicos

a) Aprender metodologias de Teste de Penetração;

b) Estudar sobre *Cloud Service*;

c) Tentar prever qual será o futuro da *Cloud Computing*;

# 3 Fundamentação Teórica

Testes de Penetração, ou *PenTests*, são práticas realizadas para determinar fraquezas na segurança de algum sistema, este podendo ser um Sistema de Computador, uma Rede de Computadores ou uma Aplicação Web, por exemplo. Além de determinar fraquezas, pode ser usado em empresas para verificar o quão apto estão seus funcionários para terem consciência das fraquezas e como irão responder diante de um ataque.

Considera-se um ataque toda e qualquer invasão que um Sistema Computacional pode sofrer, sem aviso prévio. Este ataque geralmente é realizado por alguém com um certo conhecimento técnico na área de programação e segurança. Esta pessoa é comumente chamada de *Hacker*.

Um *Hacker* geralmente é considerado uma pessoa cujo intuito é causa problemas como, por exemplo, inserindo vírus, roubando números de cartão de crédito. Porém, segundo Brunvand, o nome para pessoas que buscam se aproveitar de falhas em sistemas para ganho pessoal é dado de *Crackers*.

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.

# Referências

BRUNVAND, E. *The Heroic Hacker: Legends of the Computer Age*. 1996. <https://www.cs.utah.edu/~elb/folklore/afs-paper/node9.html>. [Online; accessed 19-July-2008]. Citado na página 14.

RAYMOND, E. S. *The New Hacker's Dictionary*. [S.l.]: The MIT Press, 1996. ISBN 0262680920. Citado na página 14.