UNIVERSIDADE FEEVALE

JULIANO VIEIRA DA ROCHA

IDENTIFICAÇÃO DE IMPLICAÇÕES PARA TESTES DE PENETRAÇÃO EM SERVIDORES VIRTUAIS

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo
2016

JULIANO VIEIRA DA ROCHA

IDENTIFICAÇÃO DE IMPLICAÇÕES PARA TESTES DE PENETRAÇÃO EM SERVIDORES VIRTUAIS

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

Orientador: Prof. Me. Daniel Dalalana Bertoglio

Novo Hamburgo
2016

RESUMO

Ambientes virtuais não são tecnologias modernas, eles foram criados pela IBM ainda nos anos 60, desenvolvidos para auxiliar na divisão de seus *mainframes* em diversos ambientes, cada um com seu próprio Sistema Operacional e recursos independentes, para diversos usuários concomitantes. No fim dos anos 90, esta técnica passou a ser estudada novamente, desta vez, com a finalidade de desenvolver novas características aos ambientes modernos. Essa nova onda de virtualização iniciou-se também em razão da disseminação exponencial da internet pela população em geral, com isso, houve o aumento de sistemas e redes privadas vulneráveis a web. Com isso, a segurança passou a ser identificada como sendo uma das áreas mais importantes para estes estudos e desenvolvimento de novas tecnologias, sendo ela própria, parte importante de todas as outras áreas de sistemas de informação, incluindo a virtualização. Sendo assim, este trabalho é uma pesquisa na área de segurança que visa identificar dados relevantes para a melhor execução de *Pentest* em ambientes virtuais. Com estes dados um analista de segurança ou auditor, poderão preparar e executar testes da melhor forma para gerar relatórios com os melhores dados possíveis.

Palavras-chave: virtualização, *mainframes, Pentest*, segurança, sistemas de informação.

SUMÁRIO

5

MOTIVAÇÃO

No formato moderno, uma máquina virtual (*Virtual Machine –VM*) em geral, é definida como um software que simula um computador real. Também pode ser definida como sendo uma cópia isolada e eficiente de uma máquina física. Ela é criada por um monitor de máquinas virtuais *(Virtual Machine Monitor),* oferecendo diversos ambientes completos similares a uma máquina real. Desta forma cada máquina trabalha de forma independente, cada uma com seus próprios recursos de hardware e suas próprias aplicações. (MAZIERO; LAUREANO, 2008)

A virtualização tornou-se de grande importância econômica e comercial para os maiores negócios da informática da atualidade. A modernização destas técnicas possibilitou o surgimento de um dos maiores conceitos que revolucionaram o mundo dos negócios digitais, a *Cloud Computing*. A virtualização de ambientes também se mostrou de grande importância para a redução dos custos, a flexibilidade e otimização de recursos computacionais para as corporações. Mostrou-se ainda eficiente na diminuição do impacto com os futuros descartes destas máquinas que podem ser descontinuadas ou ficar sem suporte adequado. (CARISSIMI, 2010)

As primeiras técnicas e experimentos na utilização de máquinas virtuais datam da década de 60, época em que foram criados pela IBM *(International Business Machines),* com intuito de particionar e compartilhar o uso de seus grandes e caros hardwares, os *mainframes*. Esta técnica proporcionou a IBM dividir logicamente essas poderosas máquinas, criando assim diversos ambientes individuais e completos para cada usuário. Cada divisão possuía seu próprio sistema operacional, independente dos ambientes dos demais usuários, possibilitando assim a execução de múltiplas tarefas e diversos aplicativos simultaneamente. (DALPIAZ, 2010)

Essa realidade foi sendo alterada a partir dos anos de 1980 e 1990, com o surgimento e popularização dos computadores pessoais. Nesta época, disponibilizar um computador completo para cada usuário ao invés de manter sistemas maiores e mais complexos, tornou-se mais barato e simples para as empresas, tornando, a partir de então, a tecnologia de *mainframes* obsoleta. (DEXHEIMER, 2012)

No entanto, a partir dos anos 2000, iniciou-se novamente uma crescente onda de interesse em técnicas de virtualização, porém não mais utilizada apenas para dividir ambientes físicos e possibilitar paralelismo dos recursos. A partir desta época, os objetivos buscados com a virtualização passaram a ser o baixo custo de infraestrutura, adaptabilidade, balanceamento de carga e suporte a aplicações legadas. Mas, além destas características descritas, após a

crescente popularização da internet, a segurança foi identificada como um dos principais pontos a serem alcançados. (MATTOS, 2012)

A segurança da informação tem representado uma boa parte dos investimentos de empresas em tecnologia da informação, aumentando a cada ano. Alguns indícios para esta preocupação são números como os identificados pela CERT.br(Centro de Estudos, resposta e Tratamento de Incidentes de Segurança no Brasil), onde no ano de 2015 foi identificado um aumento de 128% nas notificações de ataques a servidores Web em relação a 2014, totalizando 65.647 notificações. (CERT, 2016)

Essa preocupação com segurança da informação por parte das empresas vem aumentando na mesma proporção que a utilização de ambientes virtuais, por isso, assumir que estas informações possam estar de alguma forma expostas à internet, exige investimentos cada vez maiores por parte das empresas e do governo, para implantação de processos e mecanismos que auxiliem na mitigação e redução a níveis aceitáveis das ameaças virtuais. (CARDOSO; MENEZES; ROCHA, 2015)

No contexto da virtualização em razão deste crescimento da preocupação com a segurança das informações, segundo o site Computer World (2007), diversos CIOS ficam receosos ao cogitar a implementação de ambientes virtuais em suas empresas, “Estou esperando para implementar a virtualização de servidores por que estou ouvindo discussões sobre falhas de segurança no *hypervisor*”, disse Craig Bush, administrador de redes da *Exactech*, nos Estados Unidos. “Um servidor com brechas não derruba a nossa rede inteira, mas se é possível que isso aconteça ao derrubar o *hypervisor*, prefiro esperar até que as questões de segurança estejam mais resolvidas antes de adotar virtualização”.

Para garantir que os dados e informações de uma organização estejam em segurança e para identificar a existências de possíveis vulnerabilidades, são necessárias ações e investimentos em processos, infraestrutura de hardwares e softwares de sistemas de monitoramento e prevenção. Junto a isso, é necessário também que as empresas executem testes periódicos e estruturados de segurança para avaliação da rede. Para tanto, um processo de auditoria torna-se imprescindível na gestão da segurança da informação, apenas por meio deste processo é possível manter conformidade com as políticas de gestão do negócio e segurança assinado pelos responsáveis na gestão da empresa. (CARDOSO; MENEZES; ROCHA, 2015).

A identificação de falhas de seguranças e apontamento de vulnerabilidades em sistemas de informação não é uma tarefa simples, mas é de suma importância para garantir a proteção do ambiente de ataques reais. É necessário implantar sistemas de monitoramento de toda a infra-

estrura de TI (Tecnologia da informação) da empresa. Ações proativas e não apenas reativas, são de grande importância para identificação de vulnerabilidades. (DOMINGUES, 2012).

Uma das ações que podem ser efetuadas, dentre os vários processos de auditorias existentes, são os testes de penetração (*Pentest*), que são as tentativas controladas de invasão de um sistema ou rede privada, com o objetivo de identificar suas possíveis vulnerabilidades. Ele é executado da mesma forma que um ataque real. Desta forma é possível gerar relatórios com listas de vulnerabilidades, para mitigar e tratar as falhas, antes que estas possam ser exploradas por indivíduos mal intencionados. (BERTOGLIO; ZORZO, 2015).

Conforme dito por Bertoglio (2015), para a realização de um *Pentest* bem-sucedido, são necessários seguir alguns passos antes da intrusão, para desta forma obter uma visão geral do ambiente a ser testado, alguns destes passos descritos são: o escaneamento e identificação dos sistemas, identificação e descoberta de serviços, identificação e exploração de falhas e vulnerabilidades.

Pensando na segurança especificamente de ambientes virtualizados, é nesta etapa anterior ao teste de invasão, que este trabalho será iniciado, visando buscar formas de identificação de ambientes de máquinas virtuais, para que o teste possa ser efetuado de forma customizada. Explorando as vulnerabilidades específicas destes ambientes, sejam elas de SO, de *Hypervisor* ou de redes, deste tipo de máquinas, por isso, é importante que sejam identificadas todas estas possíveis vulnerabilidades antes mesmo da execução da intrusão. Desta forma, serão levantadas neste trabalho quais podem ser estas possíveis implicações que os ambientes virtualizados podem oferecer às análises, para um teste de penetração (*Pentest*).

Assim, este trabalho é norteado pela seguinte questão de pesquisa: “quais as implicações do uso de virtualização de servidores para avaliação de segurança utilizando testes de penetração?”. Partindo dessa premissa, o objetivo deste trabalho é identificar todas as variáveis que existem na utilização de *Pentest* em ambientes virtualizados.

OBJETIVOS

Objetivo Gerais

Apresentar um estudo teórico e prático sobre as implicações técnicas para execução de *Pentest* em servidores virtualizados.

Objetivos Específicos

- Apresentar um embasamento teórico sobre testes de intrusão em ambientes de virtualizados;
- Explorar suas características principais, processo de execução, e impactos gerados;
- Descrever os tipos de técnicas de *Pentest*, melhores práticas, procedimentos de análise e geração de relatório;
- Realizar o experimento de *Pentest* em ambientes virtuais distintos;
- Identificar a ocorrência de dados relevantes que possam resultar em comprovação ou não da questão abordada.

METODOLOGIA

O presente trabalho tem como característica de metodologia de desenvolvimento, um caráter explicativo-experimental. Uma pesquisa explicativa é quando o pesquisador busca explicar as razões, os motivos e as causas das coisas, por meio de documentação, registro, análise, classificação e interpretação de fenômenos observados (PRODANOV, 2013, p.53). Ao utilizar esta metodologia, o pesquisador visa identificar os fatores que determinam ou contribuem para a ocorrência do fenômeno a ser analisado. Conforme dito por GIL (2002, p.42) "Este é o tipo de pesquisa que mais aprofunda o conhecimento da realidade porque explica a razão, o porquê das coisas. Por isso mesmo, é o tipo mais complexo e delicado, já que o risco de cometer erros aumenta consideravelmente".

A pesquisa será composta por duas etapas: pesquisa bibliográfica e pesquisa prática experimental. A pesquisa bibliográfica é desenvolvida com base em materiais já publicados, incluindo livros, revistas, publicações em periódicos e artigos científicos, monografias, teses, dissertações, internet. (PRODANOV, 2013, p.54). Nesta etapa, será aprofundado o estudo do tema proposto, a pesquisa por busca de problemas semelhantes apontados e documentados por outros pesquisadores. Bem como pesquisar por possíveis soluções para o problema, não apenas em relação à virtualização, mas também a segurança destes ambientes e técnicas de *Pentest*.

A pesquisa experimental será a parte prática do trabalho, onde envolverá a utilização de ferramentas de virtualização para à criação de máquinas virtuais e simulação de máquinas físicas reais, realizadas em ambientes segregados, onde serão efetuados testes de invasão. Estes ambientes serão atacadas propositalmente por estas ferramentas de *Pentest* para, a partir disso, realizar um levantamento de dados para a análise posterior. A partir desta avaliação, será efetuada uma investigação para a detecção, ou não, de vulnerabilidades especificas em razão dos testes em ambientes virtualizados, e suas possíveis soluções e ações para sanar os mesmos. Ou ainda se os mesmos dados ocorrem em um ambiente físico.

Desenho de Pesquisa

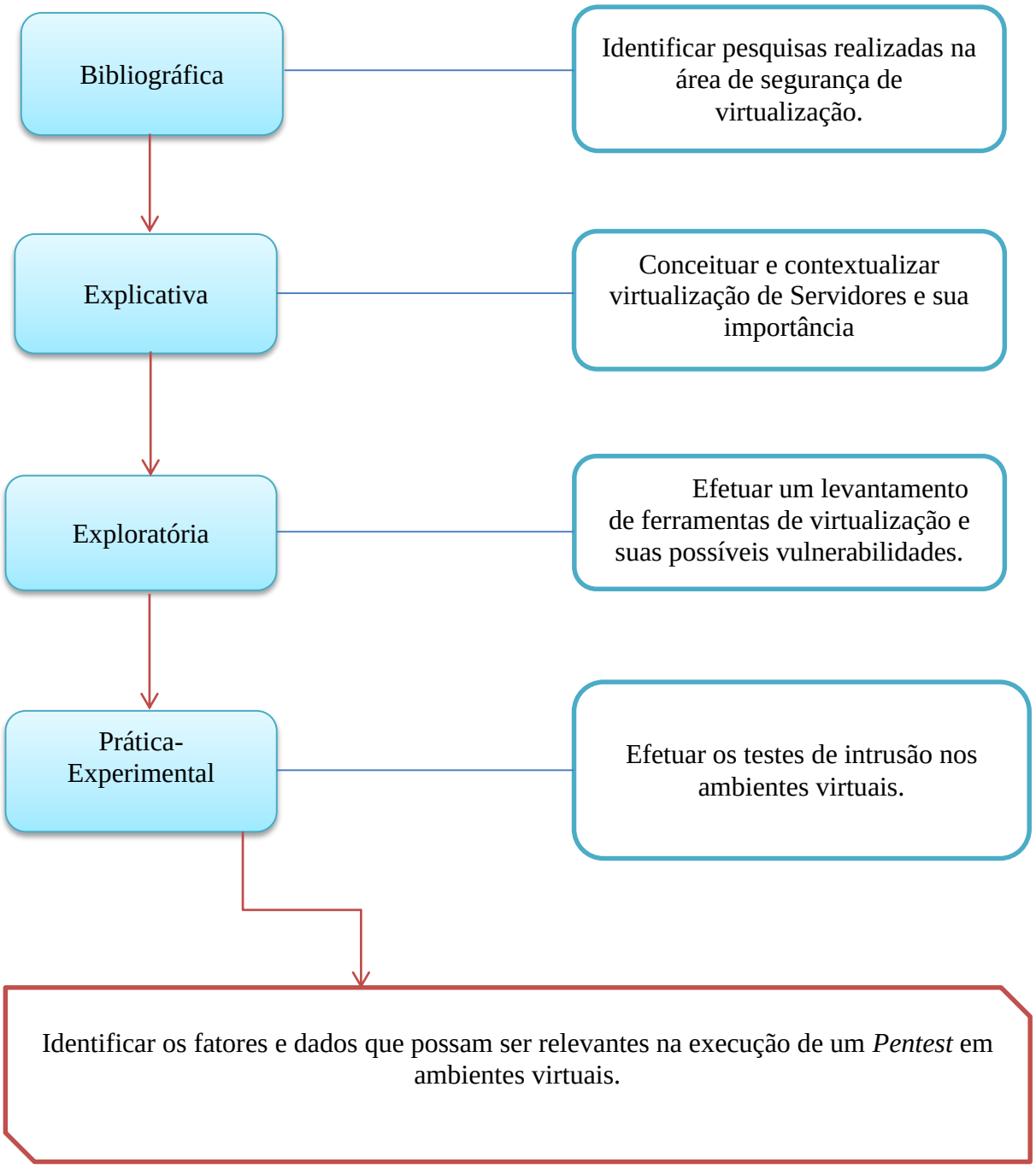

Figura 1: modelo de pesquisa

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses			
	Ago	Set	Out	Nov
Estudo sobre o Conceito de Virtualização e contexto para segurança				
Revisão e entrega do anteprojeto				
Estudo de técnicas de Pentest e Emuladores				
Redação do TCC I				
Revisão e entrega do TCC I				
Desenvolver e entregar o Trabalho de Conclusão I				

Trabalho de Conclusão II

Etapa	Meses			
	Mar	Abr	Mai	Jun
Identificar ferramentas para os testes				
Realizar testes de invasão dos ambientes				
Efetuar análise dos dados levantados				
Redação do TCC II				
Revisão e entrega do TCC II				

BIBLIOGRAFIA

Amaral, F. E. (2009), "**O que é Virtualização**", Disponível em: http://www.tecmundo.com.br/web/1624-o-que-e-virtualizacao-.htm>. Acessado em: 20/08/2016.

BERTOGLIO, Daniel Dalalana; ZORZO, Avelino Francisco. **"Uma mapeamento sistemático sobre testes de penetração"**. Relatório técnico nº 084 – Programa de Pós-Graduação em Ciências da Computação, Pontíficia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015.

CHEN, Peter M.; NOBLE, Brian D.; "**When Virtual Is Better Than Real**", Proceedings of the Workshop on Hot Topics in Operating Systems – HotOS . Department of Electrical Engineering and Computer Science University of Michigan, 2001.

CARISSIMI, Alexandre."**Virtualização: da teoria a soluções**", 26º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2013. São Paulo

CASTELLS, Manuel. "**A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade"**. Rio de Janeiro, RJ: Jorge Zahar, 2003. 243 p.

Cert.br, Incidentes Reportados ao CERT.br -- janeiro a dezembro de 2015 , Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/analise.html> Acesso em: 30/08/2016.

Computer World.**"Virtualização é o calcanhar-de-aquiles"**. Novembro de 2007. Disponível em : < http://computerworld.com.br/seguranca/2007/11/29/idgnoticia.2007-11-28.9921851123>. Acessado em: 25/08/2016.

CREASY, R. J. **" The Origin of the VM/370 Time-sharing System"** . IBM J. Res. Develop., [S.l.], v.25, n.5, p. 483-490, Sept. 1981. Disponível em:<http://www.research.ibm.com/journal/rd/255/ibmrd2505M.pdf>. Acesso em: jun.2008.

DUARTE, Otto **; Virtualização - VMWare e Xen**; Disponível em: http://www.gta.ufrj.br/grad/09_1/versaofinal/virtualizacao/conceito%20de%20virtualizacao.html

DEXHEIMER, Daniel; "**Análise de desempenho de ambientes virtualizados: um estudo teórico e pratico**". Trabalho de conclusão de curso. Universidade Feevale. 2012.

DALPIAZ, Rodrigo Luiz; "**Dispositivos Virtuais de Rede: Um Estudo Comparativo de desempenho entre Vmxnet E Vmxnet3**". Trabalho de conclusão de curso. Universidade Feevale. 2011.

DOMINGUES; Davi Eduardo. **"Testes de invasão em ambiente corporativo".** Universidade Católica de Brasília. 2012.

FONTES, Edison. "**Segurança da Informação: o usuário faz a diferença"**. 1ª edição. São Paulo: Saraiva, 2006

GIL, Antonio Carlos. "**Como elaborar projetos de pesquisa".** 5. ed. São Paulo: Atlas, 2010. 184p.

JONES, M.Tim (2007), "**Emulação do Sistema com o QEMU: A máquina dentro da máquina**", http://www.ibm.com/developerworks/br/library/l-qemu/. Acessado em: 16/08/2016.

MATTOS, Diogo Menezes Ferrazani. "**Virtualização: VMWare e Xen**". Universidade Federal do Rio de Janeiro. 2012. Disponível em: http://www.gta.ufrj.br/grad/08_1/virtual/artigo.pdf. Acessado em: 25/08/2016.

MAZIERO, Carlos Alberto; LAUREANO, Marcos Aurelio Pchek. **Virtualização: Conceitos e Aplicações em Segurança**. Centro Universitário Franciscano (UNIFAE). Dec. 8, 2010, [online]https://www.researchgate.net/profile/Carlos_Maziero/publication/237681120_Virtualizao_Conceitos_e_Aplicaes_em_Segurana/links/0a85e539b24b4524e7000000.pdf.Acessado em:13/08/2016.

MENEZES; Pablo Marques, CARDOSO; Lanay M., ROCHA; Fabio Gomes. **"Segurança em redes de computadores uma visão sobre o processo de pentest"**. Publicado na revista Interfaces Científicas, 2015. Disponível em :< https://www.researchgate.net/publication/281425985_Seguranca_em_redes_de_computadores_uma_visao_sobre_o_processo_de_Pentest >. Acessado em 15/08/2016.

PARKATUS, Eliésio; D'UFECH, Saulo Muzzolon; ORLVSKI, Regiane."**Virtualização – Conceitos e Aplicações".** Faculdade de Guaraicá – Guarapuava – PR.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. "**Metodologia do Trabalho Cientifíco: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico**", 2º Edição. Novo Hamburgo: Feevale, 2013.

VMWARE Virtual Networking Concepts. Vmware. Disponível em:<http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf.> Acessado em: 16/08/2016.

WHITAKER, Andrew; NEWMAN, Daniel P. "**Penetration testing and networkdefense"**. Cisco Press, 2005. Disponível em: < http://dl2.cbtnet.ir/books/wp-content/uploads/2015/08/Cisco.Press_.Penetration.Testing.and_.Network.Defense.Oct_.2005.pdf >. Acessado em: 16/08/2016.