Um Estudo Sobre a Análise de Vulnerabilidades em Sistemas Computacionais – das Ferramentas ao Uso.

Wilson Jacobsen, Mariana Pompeo Freitas, Gustavo Rotondo, Daniela Almeida, Alex Camargo, Érico Amaral
Engenharia de Computação, Universidade Federal do Pampa (Unipampa)
Caixa Postal 96400-000 – Bagé – RS – Brazil
{willl.jacobsen, maripompeof, danilinalmeida}@gmail.com,
gustavo_.rotondo@hotmail.com, alexcamargoweb@gmail.com,
erico.amaral@unipampa.edu.br

Abstract. *This paper presents extracts from a research that addresses the importance of information security and analyzing vulnerabilities in computer systems. The aim is to describe ways to reduce risks related threats and protect the area of information technology organizations. The observation of the results suggests that an effective solution, which provides an adequate level of protection can be achieved with preventive actions for analysis and correction of system vulnerabilities. To achieve the objectives of this study were proposed and implemented experiments with different tools in order to identify such vulnerabilities.*

Keywords*: Information security, Vulnerabilities.*

Resumo. *Este artigo apresenta o extrato de uma pesquisa que aborda a importância da segurança da informação e da análise de vulnerabilidades em sistemas computacionais. O intuito é descrever formas de diminuir riscos e proteger organizações de ameaças relacionadas a área de tecnologia da informação. A observação dos resultados permite afirmar que uma solução efetiva, que forneça um nível adequado de proteção, pode ser alcançada com ações preventivas de análise e correção das vulnerabilidades do sistema. Para atingir os objetivos deste estudo foram propostos e implementados experimentos, com diferentes ferramentas, a fim de identificar tais vulnerabilidades.*

Palavras-chave*: Segurança da informação, Vulnerabilidades.*

1. Introdução

A evolução dos sistemas computacionais e das Tecnologias de Informação, aliadas ao crescimento do uso de sistemas de armazenamento de dados, aumentam exponencialmente a dependência dos usuários e organizações de uma estrutura

confiável e segura. A ocorrência de incidentes de segurança da informação, como a perda, roubo ou exposição indevida de dados são fatores de grande relevância neste tipo de situação, as quais implicam, inevitavelmente, em relevantes prejuízos segundo Oost (2010). A ocorrência do incidente exige a restauração dos serviços e a tentativa de manutenção da integridade dos dados, com isso a organização enfrentará um cenário onde, dificilmente, conseguirá reverter ou diminuir os prejuízos, posto que tais procedimentos podem comprometer recursos críticos. Uma alternativa para a redução deste tipo de transtorno está inserida em ações proativas com o investimento na análise e correção das vulnerabilidades dos sistemas. Beal (2005) define a vulnerabilidade como uma fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque. Em um sistema existem diversas vulnerabilidades que podem ser exploradas por um cracker, cabe ao responsável da área de segurança garantir que as vulnerabilidades existentes não sejam um risco para a empresa, para isso devemos conhecer as vulnerabilidades e maneiras de calcular os riscos. Existem várias maneiras de se descobrir uma vulnerabilidade, a mais prática e barata é usar analisadores de vulnerabilidades disponíveis no mercado, tanto pagos quanto gratuitos, cabe a empresa escolher qual solução se adequa a seus objetivos e necessidades. Esta pesquisa almeja apresentar a importância da identificação e análise de vulnerabilidades, como procedimento preventivo a incidentes de segurança, com base em um estudo teórico e prático sobre os principais analisadores disponíveis no mercado, com foco na utilização em organizações de pequeno ou médio porte com pouco investimento em segurança de informação que adotam em suas estações de trabalho e servidores o sistema operacional Windows. A estrutura abordada neste artigo é composta de 7 seções organizadas da seguinte forma: na seção 2 será apresentado a metodologia; na seção 3 temos os referenciais teóricos que serviram de base para esse documento; os trabalhos correlatos são expostos na seção 4; na seção 5 é apresentada a implementação, onde são descritos todos os experimentos e as ferramentas utilizadas nesse estudo; na seção 6 temos os resultados e discussões; por fim na seção 7 têm-se a conclusão.

2. Metodologia

Este estudo vislumbra, a partir de uma relevante pesquisa bibliográfica sobre o tema vulnerabilidade e também um levantamento técnico de mercado sobre ferramentas para análise deste tipo de falha, apresentar elementos que permitam a um administrador de ambientes computacionais reduzir o risco agregado a seus equipamentos, processos e infraestrutura. O infográfico representado na Figura 3 apresenta as etapas adotadas para a pesquisa.

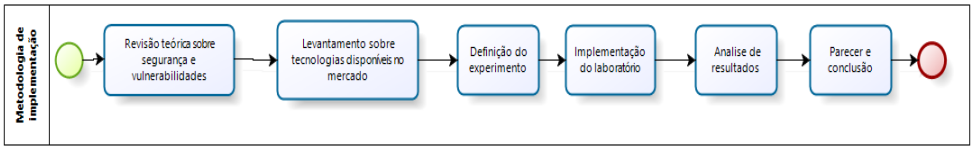

Figura 3. Etapas adotadas na pesquisa.

Para alcançar o objetivo delineado será realizado um conjunto de experimentos com os scanners de vulnerabilidades Nessus e OpenVas, a fim de solucionar as dúvidas sobre qual software apresenta melhor desempenho em diferentes aspectos. Em um laboratório de pesquisa será implementado um cenário contendo um conjunto de computadores

conectados em uma rede local, a partir daí será feita a análise dos computadores com as ferramentas e a comparação dos resultados obtidos. Foi feita uma comparação entre o Nessus e o OpenVas de forma qualitativa, levando-se em conta as seguintes características: Facilidade de instalação; Disponibilidade para sistemas operacionais; Custo da instalação; Facilidade de operação do sistema; Facilidade de identificar o problema e as possíveis soluções pelo relatório obtido na análise e; Analisar a importância da vulnerabilidade destacada pelo scanner.

3. Referencial Teórico

Para embasar a proposta deste artigo fez-se necessário um levantamento teórico de aspectos relevantes ao tema, os quais são apresentados nesta seção, iniciando pelo levantamento sobre conceitos básicos de segurança, vulnerabilidades e trabalhos correlatos.

2.1. Aspectos de Segurança em Computadores

Segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio. (NBR ISO/IEC 27002:2005). Os princípios básicos da segurança podem ser resumidos em Confidencialidade, Integridade e Disponibilidade (CID), os quais orientam, de forma básica, que somente alterações e adições autorizadas pelo proprietário da informação devem ser realizadas, os acessos aos dados devem ser exclusivos as pessoas autorizadas e tais informações devem estar disponíveis sempre que necessário. Para Alencar *et. al.* (2013) as ações para prover um nível adequado de segurança da informação não são realizadas em âmbito comum, por usuários de sistemas computacionais. Estes indivíduos devem estar atentos a técnicas utilizadas para o roubo de informação, como engenharia social, as quais visam a obtenção de dados por meio de métodos de persuasão. Neste contexto é importante garantir que a informação possua um nível adequado de segurança e, que não existam vulnerabilidades sobre as mesmas.

2.2. Vulnerabilidades em Sistemas Computacionais

Para Willie e David (2013) a vulnerabilidade é uma lacuna, um erro ou fraqueza na forma como um sistema é projetado, usado e protegido. Quando uma vulnerabilidade é explorada, pode resultar em acesso não autorizado, escalação de privilégios, negação de serviço ao ativo, entre outros. A NBR ISO/IEC 27002:2005 define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Segundo a empresa Sourcefire (2013), analisando produtos lançados nos últimos 25 anos, o sistema operacional Windows XP lidera o ranking de vulnerabilidades e reclamações. Para resolver falhas de segurança ou melhorar o desempenho, os sistemas operacionais lançam atualizações, porém podem não resolver todos os problemas, e muitas vezes deixar outras falhas, portanto uma análise das vulnerabilidades de um sistema computacional não é uma tarefa fácil. Segundo SCGS (2013), em 2013 o Windows era o sistema operacional mais usado nos computadores.

2.3. Soluções para análise de vulnerabilidades

A análise de vulnerabilidades não é um ataque feito sobre um sistema, mas sim verificações de portas para conhecer aplicações, suas atualizações e correção de erros, identificando assim suas falhas geradas por atualizações ou pela falta delas. Segundo Willie e David (2013), há muitas soluções para a análise de vulnerabilidade, os principais são o Nessus e o OpenVAS que são usados para fazer a varredura em busca de vulnerabilidades, o OpenVAS (Sistema de Avaliação de Vulnerabilidade Aberto), é um excelente programa utilizado na avaliação de vulnerabilidades, sendo este uma ramificação do projeto Nessus. Uma característica importante do OpenVAS é o fato de ser gratuito, além de ser parte do conjunto de aplicações instaladas na distribuição Kali Linux[1]. Para a análise de vulnerabilidades, com estes softwares, é preciso a instalação e configuração de servidor OpenVas e de um cliente, que pode ser qualquer computador, que possua acesso via navegador a este servidor. Com este sistema em funcionamento é possível analisar todos os sistemas conectados em rede. Para Muniz e Lakhani (2013), a análise só será útil desde que o profissional de segurança tenha conhecimento de como realizar o cálculo dos riscos de cada problema encontrado, bem como fornecer o custo esperado para reduzir esses riscos. Cabe a ele decidir se o risco associado à vulnerabilidade encontrada justifica o gasto necessário para reduzi-la a um nível aceitável. Para tal decisão utiliza-se um modelo de cálculo que estima o impacto e a probabilidade da vulnerabilidade a ser explorada, e então calculam-se e analisam-se os riscos. Por riscos, a norma ISO/IEC Guide 73:2002,12 define como: "A combinação da probabilidade de um evento e suas consequências".

4. Trabalhos Correlatos

Adicionalmente ao referencial teórico apresentado na seção 2, esta seção apresenta dois trabalhos correlatos relacionados ao tema de pesquisa descrito neste artigo. O estudo publicado "*Nessus/OpenVASComparison Test*" em 2009 pelo *Laboratory for Systems andSignals* (LSS) apresenta os resultados obtidos por meio de testes realizados em seu ambiente de rede. Neste experimento a análise de vulnerabilidades foi realizada por dois scanners, onde os níveis de vulnerabilidades de 15 diferentes servidores foram avaliados em pleno ambiente de produção, este artigo apresenta uma proposta parecida, mas usou-se as ferramentas versão 2013 e um ambiente de teste menor, com apenas utilizando apenas computadores com o sistema operacional Windows. A pesquisa intitulada "*Audit System at CESNET-CERTS*", por Vachek (2009), relata técnicas de auditoria em sistemas baseadas em servidores Linux e ferramentas de análise de vulnerabilidade a fim de apresentar um modelo efetivo de auditoria.

---

[1]Kali Linux é uma avançada distribuição Linux especializada em Testes de Intrusão e Auditoria de Segurança. Construído a partir do Backtrack, depois de rever as ferramentas que continham nesse. O Kali adere aos padrões de desenvolvimento do Debian. (http://www.kalilinux.com.br).

5. Implementação

Para a realização dos experimentos deste estudo implementou-se, em um laboratório de redes, uma infraestrutura com quatro computadores conectados fisicamente por meio de um switch gerenciável. Dois dos sistemas desta rede foram analisados pelo OpenVAS e o Nessus, em tempo de produção, conforme está ilustrado na Figura 4:

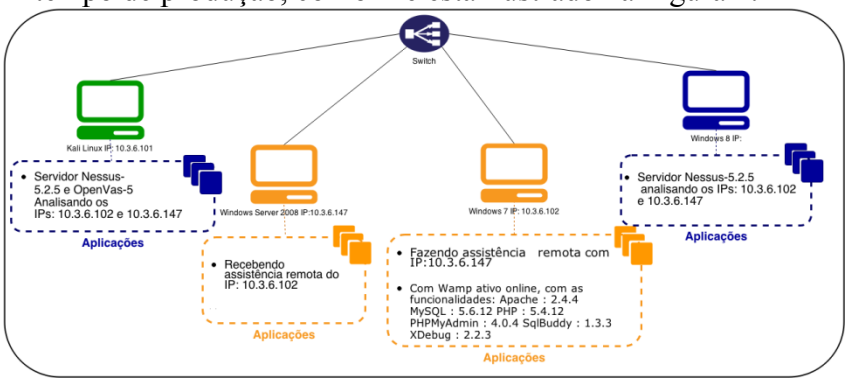

Figura 4. Estrutura da rede identificando as aplicações executadas em cada computador.

O intuito do experimento está na identificação das vulnerabilidades inerentes aos sistemas e que podem ser identificadas pelas aplicações de monitoramento. Para que os testes fossem o mais próximo possível da realidade, foram simuladas diferentes situações, como um sistema real em produção, a fim de obter uma precisão válida dos resultados. Algumas das tarefas realizadas, durante o monitoramento foram: assistência remota, conexão e permissões a compartilhamentos e serviços web e acesso a um servidor WAMP (Windows, Apache, MySQL, PHP). A plataforma de testes estava baseada no Sistema Operacional Windows, tendo como variantes as versões: Windows 7, Windows 2008 e Windows XP. A adoção do Windows se justifica pela sua utilização em grande escala em ambientes de pequenas e médias empresas.

6. Resultados e Discussões

Os resultados das comparações dos testes estão representados na Tabela 1, a justificativa para cada resultado pode ser observado na tabela Tabela 2, nesta se encontram as características avaliadas nos programas.

Tabela 1. Itens avaliados e suas respectivas notas de acordo com os programas.

Cód.	Itens Avaliados	Avaliação Nessus	Avaliação OpenVas	Justificativas Nessus	Jutificativa OpenVas
A	Facilidade de instalação	++	+ -	Nessus: Seu download é rápido e pode ser feito no site oficial do programa, sua instalação também é rápida, há a necessidade de um cadastro online, o que atrasa a instalação, possui uma interface gráfica intuitiva, por fim os tutoriais para instalação podem ser encontrados no site do software.	OpenVas: Download também pode ser feito no site oficial, sua instalação é complexa, pois é preciso configurar em linhas de comando, apesar disso houve facilidade para se encontrar tutoriais contendo scripts que facilitam o processo de instalação.
B	Disponibilidade para sistemas operacionais	++	+ -	Cliente/Servidor rodam em todas as plataformas: Linux, Windows e Mac OS X	O Servidor só tem suporte para Linux, mas o cliente OpenVas pode ser acessado pelo browser em todos os sistemas operacionais.
C	Custo da instalação,	- -	++	O Nessus é um software pago, custa em torno de $1500,00 por ano, mas conta com uma versão gratuita com algumas limitações como por exemplo o uso em apenas algumas redes locais.	É um software livre com a licença sob a licença GPL.
D	Facilidade de operação do sistema,	++	+ -	Fácil operação, já tem uma seleção de testes prontos com conjuntos de pluguins selecionados para diferentes tipos de cenários	Apresenta interface gráfica, sua configuração é mais complexa, porém o usuário tem mais liberdade para escolher o modelo de varredura, e modificar todos os pluguins.
E	Facilidade de identificar o problema e as possíveis solução pelo relatório obtido na análise.	+ -	+ -	Gera um relatório apresentando as vulnerabilidade encontradas e links para atualizações que possam resolver o problema.	Também apresenta um relatório, contendo as vulnerabilidades e links para possíveis atualizações que possam resolver o problema.
F	Analisar a importância da vulnerabilidade destacada pelo scanner.	+ -	++	Foram analisadas 12 vulnerabilidades de médio e alto risco, não identificou uma vulnerabilidade grave sobre o servidor que poderia garantir ao atacante acesso remoto a máquina.	Encontrou 16 vulnerabilidades de médio e alto risco.

Os tópicos referentes a Tabela 1 foram avaliados de acordo com a sua importância utilizando-se os símbolos ++ e --, simulando a utilização em uma empresa de pequeno e médio porte. As comparações (A) e (D) tem menos relevância, comparadas com as demais, pois no cenário do experimento, a empresa tem poucos computadores e o tempo gasto a mais ou não, tanto para instalação quanto para operação do sistema não faria uma grande diferença. O tópico (B) é relevante pois o Nessus está disponível para Windows e Linux, enquanto o OpenVas só pode ser executado no Linux, vale lembrar que nesse caso basta ter o Linux, que em geral é gratuito, instalado. O tópico (C) é muito importante para o nosso cenário já que o valor gasto com o Nessus para uma empresa com muitos ou poucos computadores seria o mesmo. Da mesma forma o OpenVas é gratuito independentemente da quantidade de computadores. Os tópicos (F) e (G) são os de maior relevância pois vão decidir a qualidade da análise e correção das vulnerabilidades e o tempo gasto para isso.

7. Conclusão

Com o decorrer deste estudo observou-se a importância da análise de vulnerabilidades para garantir a segurança da informação em sistemas computacionais. Os resultados obtidos com a utilização do OpenVas e Nessus foram muito próximos, quase que equivalentes. Pode-se observar que o Nessus é um software simples e seus resultados são obtidos em menos tempo, ao contrário do OpenVas que exige um maior esforço e conhecimento técnico para a sua aplicação. Contudo, considerando o cenário adotado, o qual simula uma organização de pequeno porte, com um número pequeno de computadores conectados e em produção, conclui-se que não é justificável o investimento com a licença do Nessus. Diante deste panorama é possível afirmar que o uso do OpenVas é o mais indicado para ambientes com poucos computadores em rede, pois embora seu nível de complexidade seja maior, a compreensão do seu funcionamento e sua utilização permite uma análise e correção efetiva de vulnerabilidades de um ambiente computacional.

Referencias

ABNT. NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da Informação. Rio de Janeiro: ABNT, 2005.

Alencar, G.Dias; Queiroz, A. Lira; Queiroz, R. J. Guerra Barretto; *Um FatorAtivonaSegurança da Informação,* IX SimposioBrasileiro de Sistemas de Informação, UFPB, João Pessoa, 2013.

Beal, Adriana. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações – São Paulo: Atlas, 2005.

Dantas, Marcus. Segurança da Informação: uma abordagem focada em gestão de riscos, Livro Rápido, 2011.

Giavaroto, Sílvio César Roxo; Santos, Gerson Raimundo. Backtrack Linux Auditoria e Teste de Invasão em Redes de Computadores, Ciência Moderna, 2013.

Laboratory for Systems and Signals (LSS), "Nessus/OpenVAS Comparison Test", version 1.02, *Faculty of Electrical Engineering and Computing University of Zagreb*, 2009.

Muniz, Joseph; Lakhani, Aamir. *Web Penetration Testing with Kali Linux*, Packt Publishing, 2013.

Oost, D.*A potential loss of trust as a result of the conflicting messages within information security research*, IEEE International Symposium on Technology and Society (ISTAS), 2010.

StatCounter Global Stats, Top 8 Operating Systems, http://gs.statcounter.com/, acessado em 15 de dezembro de 2013.

Sourcefire, http://www.sourcefire.com/br, acessado em 12 de dezembro de 2013.

Vachek, Pavel. *Audit system at CESNET-CERTS*, *WSEAS Transactions on Computers*, 2009.

Wang, Yong,*Research of Network Vulnerability Analysis Based on Attack Capability Transfer*. IEEE - International Conference on Computer and Information Technology (CIT), 2012.

Willie L. Pritchett; David De Smet. Kali Linux Cookbook, Packt Publishing, 2013.