ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

INFORMÁTICA

UM COMPARATIVO ENTRE FERRAMENTAS DE SCANNER DE VULNERABILIDADES

2º SGT HUMBERTO PEREIRA DIAS

RESUMO: Aplicações Web têm sido produzidas sob grande demanda atualmente, e a acirrada concorrência do mercado de produção de software aliada a complexidade de desenvolvimento, trouxe à tona, o surgimento de brechas de segurança e crescimento de vulnerabilidades no cenário mundial. Por consequência, a necessidade de buscar equilíbrio perfeito entre disponibilidade e segurança, ocasionou uma crescente produção de ferramentas de escaneamento de redes, que visam expor a quem o utilize, todas as vulnerabilidades do ambiente testado. Portanto, a credibilidade dos resultados das ferramentas de scanner tornou-se algo de grande valia. Logo, este artigo propõe um comparativo entre ferramentas que realizam esse tipo de serviço, altamente requisitados nos dias atuais.

Palavras Chaves: REDES DE COMPUTADORES. SEGURANÇA. VULNERABILIDADE.

1 INTRODUÇÃO

A internet tornou-se indispensável à grande maioria da população. Ela é utilizada para realizar diversas atividades do dia a dia, tais como: fazer transações bancárias, compras online, redes sociais, entre outras atividades. O alto grau de conectividade além de grandes benefícios inseriu em ambientes virtuais incidentes que comprometem a segurança das redes, fazendo com que massivos investimentos em ferramentas de proteção contra invasores acompanhem este crescimento (KUROSE, 2006).

Para Nakamura e Geus (2007), ambientes de redes, quando não bem configurados, podem apresentar falhas passíveis de ataques internos ou externos que podem comprometer o seu bom funcionamento, tornando-o mais lento e acessível às pessoas não autorizadas, através da exploração de vulnerabilidades, que são bugs na implementação. Ataques exploram 'brechas' existentes em qualquer nível relacionado à proteção da informação que são: sistema operacional, serviços e protocolos, rede e telecomunicações, aplicação, usuários e organização (NAKAMURA; GEUS, 2007).

Para estruturação de um ambiente de rede seguro é preciso analisar alguns pontos básicos na configuração das políticas de segurança. Estas, por sua vez, fornecem um conjunto de regras, leis e práticas destinadas à gestão da segurança. Criptografia, assinatura digital, autenticação e controle de acesso são alguns dos mecanismos utilizados para implementação destas políticas, pois provém um conjunto de ferramentas gerenciáveis (DUMONT, 2006).

Às ferramentas citadas anteriormente, pode-se somar ainda os sistemas de detecção de intrusão (IDS) que monitoram o tráfego da rede, e equipamentos de restrição e controle de tráfego como firewall, utilizados para reforçar a segurança e deixar o ambiente mais seguro. De acordo com Kurose (2006), proteger a comunicação e os recursos da rede é o fator primordial para definir uma comunicação segura. Sendo assim, a segurança da rede não envolve apenas sua proteção, mas também a detecção de falhas, ataques à infraestrutura e reações a serem tomadas. O monitoramento das ameaças torna-se necessário para que se detectem mudanças na rede. Através de scanners detectores de vulnerabilidades é possível realizar diversos testes na rede e procurar falhas de segurança. Os Scanners são programas de varredura de rede utilizados para detectar vulnerabilidades em sistemas, sua funcionalidade consiste em procurar por

falhas de segurança na rede para corrigi-las antes que sejam exploradas por intrusos, obtendo alguma vantagem ou causando prejuízo (MOREIRA et al., 2008).

O presente artigo tem como objetivo principal, apresentar um comparativo entre softwares de varredura de redes de computadores com ênfase nas suas funcionalidades principais.

2 DESENVOLVIMENTO

Apesar da existência de inúmeros scanners, que tem como objetivo detectar vulnerabilidades de sistemas Web, estudos demonstram que há disparidade entre as ferramentas existentes em termos de abrangência e níveis de exploração das vulnerabilidades [Rocha et al. 2012, Doup´e et al. 2010, Vieira et al. 2009].

A função de monitoramento continuo em aplicações e dispositivos, em busca de pontos vulneráveis, além de reportar esses erros em detalhes, demonstra a importância da escolha certa do scanner de rede para atuar em ativos da iniciativa pública ou privada. Sendo assim, é possível a escolha perfeita de "um" scanner dentre os disponíveis no mercado? Ou a escolha certa, se daria por um conjunto de ferramentas de scanner, para se ter um resultado fidedigno das análises de vulnerabilidades?

2.1 HIPÓTESE

Em face da disparidade entre as ferramentas de scanner, no que diz respeito às suas funções e capacidades, a melhor escolha seria por um conjunto de ferramentas que se complementam.

2.2 OBJETIVO GERAL

O presente artigo tem como objetivo principal, apresentar um comparativo entre softwares de varredura de redes de computadores com ênfase nas suas funcionalidades principais.

2.3 OBJETIVOS ESPECÍFICOS

Identificar e corrigir brechas em sistemas que possam comprometer sua funcionalidade, desempenho e segurança;

Alterar e melhorar a configuração de softwares visando torná-los mais seguros e eficientes;

Visualizar e implantar novas soluções de segurança de acordo com as necessidades encontradas;

2.4 JUSTIFICATIVA

Analisar vulnerabilidades não é atacar um sistema, mas sim realizar verificações de portas para conhecer possíveis aplicações e atualizações identificando falhas e vulnerabilidades. 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. 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”. Por Vachek (2009).

2.5 REFERENCIAL TEÓRICO

Segundo Nakamura e Geus (2007, p. 56) “A defesa é mais complexa do que o ataque”, pois, para o atacante, basta que ele consiga explorar um ponto de falha da organização. 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.

Caso uma determinada técnica não funcione, ele pode tentar explorar outras, até que seus objetivos sejam atingidos. Já para as organizações, a defesa é muito mais complexa, pois exige que todos os pontos de ataque sejam defendidos. A falta de conhecimento sobre as vulnerabilidades do próprio sistema e os mecanismos apropriados de defesa geram várias falácias relacionadas com a problemática da segurança. Algumas falácias são: “tenho um firewall, então meu sistema está seguro” ou “meu sistema é totalmente seguro”. Na verdade, negligenciar um único ponto de defesa faz com que todos os esforços dispensados na segurança dos outros pontos sejam em vão se este ponto vulnerável for descoberto e explorado. Profissionais mal qualificados tendem a mal dimensionar ou ignorar as reais fragilidades e supervalorizar os dispositivos de segurança implementados. Com isso, a 12 organização passa a correr riscos ainda maiores, que são o resultado da negligência dos profissionais responsáveis. Isso acontece, comumente, com os firewalls ou antivírus, que podem não proteger a organização contra diversos tipos de ataques. (WHITAKER; NEWMAN, 2005).

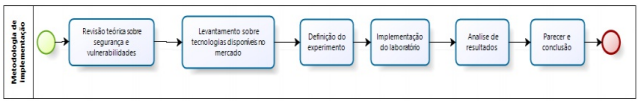
Novas tecnologias trazem consigo novas vulnerabilidades e é preciso ter em mente que novas vulnerabilidades surgem diariamente. O aumento da conectividade resulta em novas possibilidades de ataques visto que a facilidade de acesso traz como consequência o aumento de novos curiosos. Entender a natureza dos ataques é fundamental. Muitos ataques são resultado da exploração de vulnerabilidades que podem ser uma falha no projeto ou na implementação de um protocolo, aplicação, serviço, sistema. Erros de configuração e administração de recursos computacionais e falhas humanas também geram brechas de segurança (NAKAMURA; GEUS, 2007).

Em particular, alguns fatores, como a utilização de serviços remotos e as frequentes atualizações de software fazem com que as redes sejam mais vulneráveis ao passo que ferramentas maliciosas estão tornando-se a cada dia, mais simples e mais acessíveis. (WHITAKER; NEWMAN, 2005).

2.6 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. (Dantas, Marcus,2011). O infográfico representado na Figura 3 apresenta as etapas adotadas para a pesquisa.

FIGURA 1 - Etapas adotadas na pesquisa



Fonte: Autor

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.

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 and Signals (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 usouse 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.

Para a realização dos experimentos deste estudo implementou-se, um laboratório feito a partir de quatro máquinas virtuais, utilizando virtual box rodando sistemas operacionais Windows 7 logicamente conectados por meio da rede NAT. Dois dos sistemas desta rede foram analisados pelo Open VAS e o Nessus, em tempo de produção.

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 e Windows XP. A adoção do Windows se justifica pela sua utilização em grande escala em ambientes de pequenas e médias empresas.

Os resultados das comparações dos testes estão representados na Tabela 1, a justificativa para cada resultado pode ser observado na tabela 2, nesta se encontram as características avaliadas nos programas. Tabela 1. Itens avaliados e suas respectivas notas de acordo com os programas. (TABELA NO ANEXO A).

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 Open Vas 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 Open Vas 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. (Beal, Adriana.2005).

3 CONCLUSÃO

Após análise dos scanners Open Vas e Nessus, verificou-se que a importância dos softwares de varredura de vulnerabilidades em ambientes corporativos é vital, posto que falhas de segurança, podem facilmente

comprometer toda a estrutura e organização de uma instituição. O comparativo entre os softwares supracitados, deixou clara, a necessidade de trabalho em conjunto das ferramentas, mesmo com a diferença em termos de resultados não tenha sido substancial. É de se notar que foi comparado um software de código aberto com um proprietário, e o ambiente de teste e o cenário adotado simulam uma organização de pequeno porte, com um número pequeno de computadores conectados e em produção. Logo, diante dos resultados obtidos, conclui-se que em se tratando de segurança, não se pode haver brechas, e a pequena diferença de resultados obtidos através da utilização de ambos os softwares demonstram que houveram resultados diferentes, o que sugere que a utilização isolada não cobriria todo o necessário para se ter uma rede o mais segura possível.

ANEXO A – RESULTADOS DAS COMPARAÇÕES DOS TESTES

Cod	Itens Avaliados	Avaliação Nessus	Avaliação OpenVas	Justificativa Nessus	Justificativa OpenVas
A	Facilidade de Instalação	++	+_-	Seu download é rápido e pode ser feito no site oficial do programa; sua instalação também é rápida, porém, 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	Download também pode ser feito no site oficial; sua instalação é complexa, pois é preciso configurar em linhas de comando, apesar disso houve facilidade de 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, porém o cliente pode ser acessado pelo browser em todos os sistemas operacionais
C	Custo de instalação	--	++	O Nessus é um software pago custa em torno de $1500,00 por ano, mas cota 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 licença GPL.
D	Facilidade de operação do sistema	++	+-	Fácil operação á tem uma seleção de testes prontos com conjuntos de pluguins selecionados para diferentes tipos de cenários	Apresenta interface gráfica, sua configuração é mais completa 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 soluções pelo relatório obtido na análise	+-	+-	Gera um relatório apresentado as vulnerabilidades encontradas e lis para atualizações que possam resolver os problemas.	Também apresenta relator, 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	Encontrou 16 vulnerabilidade de médio e alto risco.

REFERÊNCIAS

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 Fator Ativo na Segurança da Informação. IX Simpósio Brasileiro de Sistemas de Informação, João Pessoa, PB: UFPB, 2013.

ALVES, Maria Bernardete Martins; ARRUDA, Suzana Margret de. Como elaborar um Artigo Científico. Disponível em: <http://www.bu.ufsc.br/design/ ArtigoCientifico.pdf>. Acesso em: 18 maio 2017.

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

BAUER, C. A. Política de segurança da informação para redes corporativas. Trabalho de conclusão de curso – Centro Universitário Feevale, 2006.

BRASIL. Tribunal de Contas da União. Boas Práticas de Segurança da Informação/ Tribunal de Contas da União. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

BORGES, A. Ataque de fixação de sessão. Revista Linux. 2014. Disponível em: < http://www.linux-magazine.com.br/images/uploads/pdf_aberto/LM_92_14_15_02_colalexborges.pdf >. Acessado em: 2 Jun. 2014.

BROWN, T; GALITZ, G. O farejador de vulnerabilidades OpenVAS. Linux Magazine, São Paulo, , Abr. 2010.

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

GALEGALE, Gustavo Perri e Col. Internet das Coisas aplicada a negócios - Um estudo bibliométrico. Revista de Gestão da Tecnologia e Sistemas de Informação. v. 13, no 3, Set/Dez., 2016, pp. 423-438. Disponível em: <http://www.jistem.fea.usp.br/index.php/jistem/article/viewFile/10.4301%25S 1807-17752016000300004/616>. Acesso em: 18 maio 2017.

GONÇALVES, Adriana Aguillera. A proteção do conhecimento e a inovação na Universidade Estadual de Londrina. 2012. Dissertação (Mestrado em Gestão da Informação) - Universidade Estadual de Londrina, Londrina. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/337>. Acesso em:18 maio 2017.

MORAES, A. F. de. Redes de computadores: fundamentos. 7. Ed. São Paulo: Editora Érica, 2010.

MOREIRA et al. Scanners de Vulnerabilidades Aplicados a Ambientes Organizacionais. Revista Eletrônica da Faculdade Metodista Granbery: Jul/Dez, 2008. 63

MORENO, D. Tipos de PenTest. Disponível em: < http://www.100security.com.br/tipos-de-pentest/ >. Acessado em: 7 Mai. 2014.

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