IV Semana de Tecnologia da Informação - 8 a 10 de novembro de 2017, Paranavaí, PR - ISSN: 2526-1924

Análise de Desempenho de Scanners de Vulnerabilidades

Willian Cligor de Souza de Oliveira[1], André Ricardo Zavan[1]

[1]Campus Paranavaí - Instituto Federal do Paraná (IFPR)
Paranavaí– PR – Brasil

williancligor@gmail.com, andre.zavan@ifpr.edu.br

O *pentest*, ou teste de invasão, corresponde a metodologia, ao processo e aos procedimentos usados pelos *pentesters* de acordo com diretrizes específicas e aprovadas para tentar burlar as proteções de um sistema de informação em busca de falhas de segurança [Broad e Bindner 2014]. A metodologia mais utilizada para testes de invasão é a proposta pelo programa EC C|EH (*EC – Council Certified Ethical Hacker*), que divide o *pentest* em 5 fases principais: (1) *Reconnaissance*: fase de reconhecimento do ambiente que será atacado; (2) *Scanning*: varreduras na rede e sistemas do alvo, que são divididas em *network scanning* (varredura de rede), *port scanning* (varredura de portas) e *vulnerability scanning* (varredura de vulnerabilidades); (3) *Gaining Access*: Execução dos ataques ao sistema; (4) *Maintaining Access*: implantação de softwares que garantem acesso posterior ao sistema invadido; (5) *Covering Tracks*: limpando os rastros da invasão [Broad e Bindner 2014].

Na fase de *Scanning*, no momento de varrer *hosts* em busca de vulnerabilidades, são utilizadas algumas ferramentas chamadas *scanners* de vulnerabilidades. Este artigo objetiva testar e analisar os *scanners Nessus*, *Nmap* e *OpenVAS*. As métricas de comparação aplicadas serão: tempo gasto com a varredura e o número de vulnerabilidades encontradas que podem ser exploradas.

O *Nessus* é um dos *scanners* de vulnerabilidade mais populares, criado e distribuído pela empresa *Tenable*. Inicialmente foi gratuito e de código aberto, porém seu código-fonte foi fechado em 2005. Hoje em dia possui uma versão gratuita chamada "*Nessus Home*" e uma versão completa que custa US $ 2.190 por ano [Sectools 2012].

O *Nmap* é uma ferramenta de código aberto criada por Gordon Lyon em 1997. Sua principal função é varrer portas de *hosts*, podendo examinar mais de 1600 portas do alvo. Atualmente o *Nmap* ganhou novas funções com o *NSE* (*Nmap Scripting Engine*), ferramenta acoplada ao *Nmap* que permite a execução de *scripts* com variadas funções, inclusive a descoberta de vulnerabilidades [Lyon 2009].

OpenVAS é um *scanner* de vulnerabilidade gratuito e de código aberto que foi desenvolvido a partir da última versão de código aberto do *Nessus* em 2005 [Sectools 2012].

Para o ambiente de testes, foram utilizadas as seguintes máquinas: (1) Alvo-*Metasploitable*: máquina propositalmente vulnerável utilizada para aprendizagem de *pentest* que foi configurada pela empresa *Rapid7* de forma que possua diversas falhas para serem exploradas de maneira segura; (2) Alvo-*Windows*: máquina que utiliza o sistema operacional *Windows XP*, com os seguintes softwares instalados: *Adobe Reader*

8, *Firefox* 17.0.1, *Java Runtime Environment* 7u6, SLMail 5.5 e Xampp 1.7.2.; (3) Atacante: máquina que utiliza o sistema operacional *Kali Linux Rolling*.

Na fase de exploração (*Gainning Access*), é muito comum a utilização da ferramenta *Metasploit Framework*. Esta ferramenta carrega consigo recursos associados a anos de conhecimentos e experimentos efetuados por *hackers*, *pentesters*, governos e pesquisadores do mundo todo, possuindo centenas de *scripts* diferentes para encontrar, explorar e/ou auxiliar na exploração de vulnerabilidades existentes que já são de conhecimento da comunidade de segurança [Broad e Bindner 2014]. Este *framework* será utilizado para validar se as vulnerabilidades encontradas pelos *scanners* são passíveis de exploração.

Referências

ABNT (2005) NBR ISO/IEC 17799 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. ABNT.

Assunção, M. F. A. (2009) Honeypots e Honeypots: aprenda a detectar e enganar invasores. 1. ed. Florianópolis: Visual Books.

Broad, J.; Bindner, A. (2014) Hacking com Kali Linux: técnicas práticas para testes de invasão. 3. ed. São Paulo: Novatec.

Lyon, G. (2009) Nmap Network Scanning. 1. ed. Estados Unidos da América: Nmap Project.

Verde, E. V. (2012) “Mini Curso – Pentest – UniVem”, http://aberto.univem.edu.br/bitstream/handle/11077/mini_pen_univem.pdf?sequence=1, Maio.

Sectools (2012) “Sectools.org: top 125 network security tools”, sectools.org, Outubro.

Sêmola, M. (2003) Gestão da Segurança da Informação: uma visão executiva. 1. ed. Rio de Janeiro: Elsevier.

Santo, A. F. S. E. (2010) “Segurança da Informação”. Cuiabá: Instituto Cuiabano de Educação.

Weidman, G. (2014) Testes de Invasão: uma introdução prática ao hacking. 1. ed. São Paulo: Novatec.