Vulnerabilidades em Aplicações Web: uma Análise Baseada nos Dados Coletados em Honeypots

João M. Ceron[1], Leonardo L. Fagundes[2], Glauco A. Ludwig[2], Liane Tarouco[1] Leandro Bertholdo[1]

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS) Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

[2]Universidade do Vale do Rio dos Sinos (UNISINOS) - Av. Unisinos, 950 - Bairro Cristo Rei - CEP 93.022-000 São Leopoldo - RS - Brasil

{jmceron,liane,berthod}@inf.ufrgs.br,{llemes,glauco1}@unisinos.br

1. Ameaças em aplicações web

Ataques contra aplicações disponíveis na Internet representam uma grande parte dos incidentes de segurança ocorridos nos últimos anos. O avanço das tecnologias voltadas para a web e a falta da devida preocupação com requisitos de segurança tornam a Internet um ambiente repleto de vulnerabilidades e alvo de freqüentes ataques. O problema torna-se ainda mais grave com a utilização dos mecanismos de busca como uma ferramenta para localizar sites vulneráveis. Dessa maneira, este trabalho tem por objetivo realizar uma avaliação experimental das sondagens a aplicativos web vulneráveis. Para desempenhar essa tarefa, o nosso trabalho usa o conceito de honeypots que são sistemas desenvolvidos para serem comprometidos.

Segundo um estudo apresentado por [Holz 2006] a maioria dos ataques voltados a aplicações web buscam explorar vulnerabilidades de *Cross Site Scripting*, *SQL injection*, *Directory Transversal* [Mavrommatis 2008]. Essas vulnerabilidades estão presentes em uma grande quantidade de aplicações web, como por exemplo, webmail, aplicativos de gerenciamento remoto, fórum de discussões entre outros. Ataques a esses aplicativos vulneráveis podem ser realizados de diferentes formas: ferramentas automatizadas [Zou 2005], worms [Levy 2005], ataques interativos. Atualmente, ferramentas vêm sendo projetadas para analisar as técnicas de ataques às aplicações baseadas na web. Ferramentas como o PHP Honeypot Project (PHP.HoP) [PHP.HoP 2008] emulam aplicações web vulneráveis e coletam informações sobre os acessos. Com base a isso, este trabalho implementou uma estrutura para a observação e monitoração dos ataques a aplicações web.

2. Ambiente de ataque

Com o intuito de obter informações necessárias para a análise das atividades intrusivas, uma infra-estrutura de honeypots foi implantada. Valendo-se de ferramentas como *honeyd* [honeyd 2008] – que cria honeypots virtuais – em conjunção com a ferramenta (PHP.HoP) foram emuladas 8 maquinas virtuais. Cada máquina executava as seguintes aplicações vulneráveis: phpBB 2.0 [phpBB 2008], Horde webmail [Horde 2008],

SquirrelMail [SquirrelMail 2008], phpshell 1.7 [phpshell 2008], phpsysinfo 1.06 [phpsysinfo 2008] e phpMyAdmin 2.1 [phpMyAdmin 2008].

A partir dos dados coletados no período de 53 dias percebeu-se uma grande quantidade de acessos aos serviços web, totalizando 4902 acessos (uma média de 92 acessos por dia). Também foi possível traçar comparativos e observar diferentes métodos de sondagem: **scanners *(70%)***: acessos ao servidor de forma direta, computados através do número de conexões TCP; **buscadores (28%)**: acessos ou varreduras às aplicações por meio de mecanismos de buscas; **outros (2%)**: acessos principalmente realizados por robôs. Outra análise constatou quais aplicações emuladas haviam sido mais acessadas no período de coleta dos dados. A aplicação de administração remota PHP-Shell destacou-se com 84.8% do total de acessos; seguida pela ferramenta de fórum PHP-BB com 5,1%; e pelo sistema de gerencia remoto PHP-Sysinfo com 4.7% dos acessos.

3. Conclusões

Após a análise dos resultados foi observado uma grande quantidade de acessos as aplicações emuladas, o que sinaliza uma alta procura por aplicações web vulneráveis. Também foi constatado que cada vez mais os mecanismos de busca, como google e yahoo, são utilizados como ferramentas para sondagens de portas e aplicações. Essa técnica de sondagem é bastante eficiente, pois não pode ser detectada por mecanismos de segurança tradicionais. Da mesma forma, essa técnica é bastante acessível, uma vez que se necessita apenas de um navegador. No decorrer do trabalho constatou-se (através de assinaturas de acesso), que alguns malwares estão utilizando os buscadores como ferramentas para localizar alvos vulneráveis, delineando assim uma tendência para a nova geração de ataque web.

Referências

Mavrommatis P. and Provos N. (2008). Ghost Turns Zombie: Exploring the Life Cycle of Web-based Malware. In *First USENIX Workshop on Large-Scale Exploits and Emergent Threats (USENIX)*.

Holz, T., Marechal, S. and Raynal, F. (2006). New threats and attacks on the World Wide Web. In: *IEEE Security & Privacy Magazine*.

Zou, C., Weibo G.; Towsley, D. and Lixin G. (2005). The monitoring and early detection of Internet worms, In: *IEEE/ACM Transactions on Networking*.

Levy, E. (2005). **Worm propagation and generic attacks**. In: *Security & Privacy Magazine.*

PHP-SHELL (2008). Remote administration tool. *http://phpshell.sourceforge.net.*

PHP-SYSINFO (2008). PHP system information. *http://phpsysinfo.sourceforge.net*.

SQUIRRELMAIL (2008). WebMail SquirrelMail. *http://www.squirrelmail.org*.

PHP.HoP (2008). PHP HoneyPot Project. *http://www.rstack.org/phphop.*

PHPBB (2008). PHPBB forum system. *http://www.phpbb.com.*

PHPMYADMIN (2008). Database administration tool. *http://www.phpmyadmin.net.*