Trabalho de conclusão de Segurança em Sistemas de Informação: motivacional para a construção de um módulo de detecção de *ARP spoofing*

Ewerton Carlos de Araújo Assis

25 de Junho de 2013

Resumo

O presente trabalho, que comporá nota parcial na disciplina de Segurança em Sistemas de Informação, ministrada pelo professor Hailton Lemos, no Instituto de Informática da Universidade Federal de Goiás, tem como objetivo apresentar motivações para a construção de um módulo de detecção de ataques de *ARP spoofing*.

1 Introdução

Muitas técnicas de intrusão são utilizadas com o fim de pertubar o uso decente de uma rede de computadores [2]. Sejam técnicas que comprometam a acessibilidade e a disponibilidade, a confidencialidade ou a integridade de um sistema baseado em redes de computadores, detectar e superar estas ameaças e ataques nem sempre é uma tarefa fácil.

Dentre as ameaças que podem acometer uma rede de computadores está o *ARP spoofing*, que consiste em uma técnica de enganar os computadores de uma rede local (LAN) ao enviar mensagens ARP (*Address Resolution Protocol*) falsas com o fim de associar um endereço MAC a um certo IP com fins maliciosos. Embora seja uma técnica simples e bem documentada, essa técnica é geralmente usada como precedente para ataques de negação de serviço, *man-in-the-middle* e sequestro de sessão [2].

Embora esse tipo de ataque não pode ser impedido, por características inerentes do protocolo ARP [3], ele pode ser detectado e superado, o que o presente trabalho tem por finalidade desenvolver.

A seguir são apresentadas as motivações para desenvolver esse projeto e quais serão as linhas gerais de desenvolvimento.

2 Por que desenvolver um módulo de detecção de ataque de *ARP spoofing*?

Embora seja um ataque simples, ele se mostra poderoso, por direcionar mensagens para determinado *host* (hospedeiro — qualquer computador de borda que implemente as cinco camadas da arquitetura TCP/IP [1]), colocando em risco a disponibilidade e a integridade de sistemas computacionais, abrindo brechas para que outras ameaças sejam colocadas sobre uma rede de computadores.

Em termos didáticos, detectar e superar esse tipo de ataque tem por base conhecimentos nos fundamentos da arquitetura TCP/IP e em como fazer para interceptar e capturar pacotes em uma rede local, o que corrobora para estabelecer um conhecimento para que outros módulos de detecção de intrusões em uma rede sejam construídos.

3 Linhas gerais de desenvolvimento

O presente trabalho será desenvolvido em ambiente Linux por apresentar um ambiente de programação mais robusto e melhor documentado, na visão daqueles que desenvolverão o projeto; e por um maior domínio de programação em ambientes GNU/POSIX. Os pacotes de uma rede local serão capturados com o fim de fazer a instrumentalização destes e identificar o comportamento da rede, além de outras características que deverão ser apresentadas em apresentação à parte, com o fim de realizar a detecção do ataque.

4 Conclusão

Motivações para o desenvolvimento de um módulo de detecção de ataques de *ARP spoofing* foram apresentados bem como as linhas gerais de desenvolvimento do trabalho de conclusão. A data prevista para a apresentação da solução final está marcada para 4 de Julho de 2013, com aviso prévio ao professor ou por este em caso de modificação desta data.

Referências

[1] Kurose, J. F.; Ross, K. **Computer Networking: A Top-Down Approach Featuring the Internet**. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition, 2002.

[2] Lockhart, A. **Network Security Hacks**. O'Reilly, Sebastopol, CA, 2nd edition, 2006.

[3] Plummer, D. C. **An ethernet address resolution protocol or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware**. `http://tools.ietf.org/html/rfc826`, November 1982.