PLANO DE TRABALHO PARA BOLSA PCI/CTI

TÍTULO: Visualização de dados de honeypots

PROJETO: Infraestrutura distribuída de honeypots para coleta de programas maliciosos

LOCAL: Centro de Pesquisa Renato Archer – CTI

Divisão: DSSI

Coordenador: André Ricardo Abed Grégio

Orientador: André Ricardo Abed Grégio

Bolsista: Alexandre Or Cansian Baruque

Modalidade: ITI 1-A

OBJETIVO

O presente projeto tem por objetivo a implantação de uma arquitetura Web para tratamento e visualização de dados distribuídos geograficamente, provenientes de sensores participantes de uma infraestrutura de coleta de programas maliciosos. O projeto envolverá a representação de diversos tipos de dados com dimensão temporal, incluindo arquivos binários, registros de auditoria de honeypos e informações extraídas de tráfego de rede.

PALAVRAS-CHAVES

Segurança computacional; visualização de dados; honeypots; malware

INTRODUÇÃO

Programas maliciosos (*malware*) representam uma das maiores ameaças aos usuários e sistemas conectados à Internet. A facilidade da geração de novos exemplares a partir de *malware* já existente, as chamadas variantes, faz com que a atuação dos mecanismos de defesa seja dificultada, seja na criação de vacinas, seja no processamento das centenas de milhares de variantes em operação. Por exemplo, no caso de antivírus com detecção baseada em assinaturas, é necessário em geral a atividade de um analista humano que descubra um modo de detecção para um dado *malware* e produza a assinatura em questão. Para tanto, o analista precisa ter em mãos a variante ainda não detectada.

A fim de obter programas maliciosos e suas variantes, necessita-se de uma infraestrutura de coleta distribuída. A motivação principal para tal infraestrutura é a de obter e armazenar exemplares de *malware* em circulação no Brasil para análise posterior. Com isso, pretende-se obter informações acerca dos tipos de *malware* que

atacam as redes que possuem um sensor de coleta (*honeypot*) a fim de agregar dados que permitam mostrar as tendências de ataques de uma maneira local (em cada rede) e global (conjunto das redes com sensores instalados).

As informações obtidas desses *honeypots* de coleta incluem tráfego de rede, registros de auditoria (*logs*) das vulnerabilidades exploradas e tipos de ataques utilizados no comprometimento dos serviços/sistemas, e do binário que representa o programa malicioso. De posse de tais informações, é possível representá-las por meio de técnicas de visualização e disponibilizá-las por meio de uma arquitetura Web, permitindo a observação de tendências e geração de estatísticas.

ATIVIDADES

O plano de atividades consiste das seguintes etapas:

A. Estudo sobre conceitos de visualização, Web services e tipos de dados gerados por *honeypots*.

B. Definição da infraestrutura básica e projeto da topologia.

C. Instalação e configuração do servidor Web e busca dos dados nos sensores.

D. Desenvolvimento de procedimentos para tratamento dos dados e interface de visualização via Web.

E. Documentação do projeto e confecção de relatórios (parcial, final).

BIBLIOGRAFIA

Provos, N. Holz, T. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley. 2007.

Grégio, A. R. A., Oliveira, I. L., Santos, R. D. C., Cansian, A. M., Geus, P. L. Malware Distributed Collection and Pre-Classification

System using Honeypot Technology. Proceedings of SPIE Defense, Security and Sensing. Orlando, FL. 2009.

Spitzner, L. “Honeypots: Tracking Hackers”. Addison-Wesley. 2002.

Zhuge, J.; Holz, T.; Han, X.; Song, C. and Zou, W. “Collecting Autonomous Spreading Malware Using High-interaction Honeypots”. Proceedings of 9th International Conference on Information and Communications Security (ICICS'07), Zhengzhou, China, December 2007.

Seifert, C.; Steenson, R.; Holz, T.; Yuan, B. and Davis, M.A. “Know Your Enemy: Malicious Web Servers”. Disponível em: http://www.honeynet.org/papers/mws. (Acesso em outubro/2013).

CERT.br. Distributed Honeypots Project. Disponível em: http://honeytarg.cert.br/honeypots/. (Acesso em outubro/2013).

Santos, R., Grégio, A. R. A. Análise e Visualização de Logs de Segurança. In: Computer on the Beach 2010: Livro de Minicursos. 1 ed. São Jose/SC: Uniali, 2010, PP. 85–114.

Axelsson, S. Visualisation for Intrusion Detection – Hooking the Worm. In Einar Snekkenes and Dieter Gollmann, editors, Computer Security – ESORICS 2003, 8th European Symposium on Research in Computer Security, Gjøvik, Norway, October 13-15, 2003, Proceedings (LNCS 2808)), 2003, pp. 309–325.

Conti, G., Dean, E., Sinda, M., Sangster, B. Visual Reverse Engineering of Binary and Data Files. In John R. Goodall, Gregory Conti, and Kwan-Liu Ma, editors, Visualization for Computer Security – 5th International Workshop, VizSec 2008, Cambridge, MA, USA, September 15, 2008, Proceedings (LNCS 5210), pages 1–17, 2008.

Marty, R.. Applied Security Visualization. Addison Wesley, 2008.

Tufte, E. R. The Visual Display of Quantitative Information. Graphic Press, 2nd edition, 2001.

METODOLOGIA

As ferramentas utilizadas serão todas baseadas em software livre e todo o código desenvolvido será feito em linguagem de orientação a objetos multiplataforma (Python, Java) ou linguagens para Web (Javascript, PHP). Será dada preferência às metodologias atuais de desenvolvimento com a utilização de frameworks disponíveis e reutilização de componentes.

Para o desenvolvimento dos protótipos, será utilizado um desktop adequado disponibilizado pelo orientador. Como referência para estudos iniciais, será utilizado material publicado do orientador e artigos científicos de periódicos e congressos reconhecidos na área.

CRONOGRAMA DO PLANO DE TRABALHO

Os itens definidos na tabela a seguir são descritos na Seção “ATIVIDADES” deste documento:

Tabela I: Plano de atividades com duração de 24 meses

Item/Trimestre	1º	2º	3º	4º	5º	6º	7º	8º
A	X							
B		X						
C			X	X	X			
D					X	X	X	
E	X	X	X	X	X	X	X	X