**XVIII SEMINÁRIO DE INICIAÇÃO CIENTÍFICA DA PUCPR**

**26 e 27 de outubro de 2010**

|  |  |  |  |
| --- | --- | --- | --- |
| **AVALIADOR** | | **CÓDIGO** | |
| **Fulano da Silva** |  | | 342-3 | |
| **TÍTULO DO TRABALHO** | | **ID TRABALHO** | |
| AMBIENTE VIRTUAL PARA ESTUDO COMPORTAMENTAL DE INTRUSOS EM WEB SERVICES |  | | COMP01 | |

Introdução: Um honeypot é um recurso computacional de segurança que pode ser atacado ou comprometido, sem que a segurança efetiva de uma máquina seja colocada em risco. Isto é possível, porque honeypots são programas que simulam os serviços de rede, mas não são serviços reais. Para quem está atacando o honeypot deve parecer real, se for de alta interatividade, e emular serviços vulneráveis. Pode-se usar honeypots para registrar as tentativas ou as ações de um acesso, incluindo os comandos executados. Essas informações podem fornecer alertas antecipados sobre ataques. Há sistemas como IDS (Sistema de Detenção de Intrusão) que podem detectar ataques sem precisar ser vulneráveis. Porém, para aprender a estratégia do ataque que será programada no IDS é necessário aprendê-la antes usando um honeypot, por exemplo. O problema de IDS para Serviços Web é que esse precisa conhecer detalhes da aplicação para detectar eficientemente o ataque. Então, se for possível filtrar o tráfego que chega nos Serviços Web de forma a direcioná-lo para aplicação ou inspeção, o trabalho do IDS poderia ser simplificado e mais eficiente. Objetivos: O objetivo deste projeto é simular um ambiente virtual para atrair ataques a Serviços Web. Se os ataques não acontecerem, serão simulados usando ferramentas de auditoria para que a estratégia do ataque fique registrada nos logs do honeypot e sirvam como fonte para posterior identificação do mesmo. Método: Foi instalado o aplicativo Honeyd® e, por meio dele, foram criados ambientes virtuais para que estes pudessem servir como Sistemas Vulneráveis. O Honeyd® foi configurado para receber ataques no servidor web. Usando o pacote WSDigger® lançamos ataques XpathInjection, XSSInjection e XQueryInjection sobre o honeypot para que a estratégia dos ataques ficasse logada. Resultados: A partir da analise dos logs ficou evidente que a estratégia de ataque agora é conhecida em seus menores detalhes, sendo que quando se identificar uma sequência parecida de ações haverá forte suspeita de que o ataque esta acontecendo. Conclusão: O emprego do método trouxe informações que softwares como IDS geralmente são conseguem capturar; por exemplo, observou-se que o atacante não consulta a WSDL para descobrir a interface dos Serviços Web antes de atacá-los, quando o normal seria consultar a WSDL e depois acessar o serviço. Assim, quando os serviços web receberem um pedido de uma origem que não conhecem e adicionalmente for identificado que não foi feita consulta anterior à WSDL é muito possível que seja um ataque. Nós desejamos automatizar esta tarefa de detecção para que seja automática. Se isto acontecer, o pacote ingressantes nos Serviços Web já pode ser direcionado para uma inspeção mais criteriosa, desta maneira os tráfegos potencialmente mais danosos seriam filtrados dos normais e o IDS poderia ser mais eficiente, pois haveria menos dados para inspeção, mas com maior probabilidade de serem maliciosos.

|  |  |  |
| --- | --- | --- |
| **(A)RESUMO** |  |  |
| Clareza | Poder de Síntese | Contribuição para formação científica |
| ➀ ➅ ➆ ➇ ➈ ➉ | ➀ ➅ ➆ ➇ ➈ ➉ | ➀ ➅ ➆ ➇ ➈ ➉ |

|  |  |  |
| --- | --- | --- |
| **(B)Apresentação oral** |  |  |
| Conteúdo | Qualidade Visual | Desempenho do Aluno |
| ➀ ➅ ➆ ➇ ➈ ➉ | ➀ ➅ ➆ ➇ ➈ ➉ | ➀ ➅ ➆ ➇ ➈ ➉ |

|  |  |  |
| --- | --- | --- |
| **(C)Pôster** |  |  |
| Conteúdo | Qualidade Visual | Desempenho do Aluno |
| ➀ ➅ ➆ ➇ ➈ ➉ | ➀ ➅ ➆ ➇ ➈ ➉ | ➀ ➅ ➆ ➇ ➈ ➉ |

**PREENCHIMENTO OBRIGATÓRIO**

|  |  |
| --- | --- |
| Atribua uma nota geral de 0 a 100  Nota: (\_\_\_\_\_) | Indicado como um dos dez melhores trabalhos para representar a PUCPR na 63º Reunião Anual da SBPC: ( 1 ) sim ( 2 ) não |