SISTEMA DE PONTUAÇÃO PARA AVALIAÇÃO DE *HONEYPOTS*. ESTUDO DE CASO: *VALHALA*

Alexandre William Batista da Silva[1], Paulo Henrique de Morais Silva[1], Murilo da Silva Dantas[1,2]
[1]Faculdade de Tecnologia de São José dos Campos-SP, FATEC, Tecnologia em Informática
[2]Instituto Nacional de Pesquisas Espaciais, INPE
alexandrewbs@hotmail.com, murilodantas06@gmail.com

1. Introdução

Com o desenvolvimento da informática e sua inserção nos mais diversos setores corporativos e de entretenimento, além da importância da informação nos negócios, tornou-se crescente a atenção na segurança da informação.

A preocupação é ampliada quando o sistema possui conexão com a Internet. Neste contexto cabe ao administrador de rede aplicar medidas de seguranças que previnam o acesso de ameaças e pessoas não autorizadas a seus sistemas. Essas medidas tornam-se cada vez mais complexas, visto que o número de ataques cresce em larga escala.

Uma das soluções existentes para o monitoramento de redes é o conceito de *honeypots* [1]. Essa tecnologia permite acompanhar invasões podendo interagir com o invasor e até inibir completamente o ataque.

O objetivo deste trabalho foi implementar um sistema de pontuação para avaliação de *honeypots*. Avaliamos o Valhala como estudo de caso, futuramente outros serão analisados, seguindo critérios estabelecidos em nossa pesquisa atual, que tem como foco principal obter um panorama de ferramentas *honeypots.*

2. Valhala Honeypot

O Valhala Honeypot é uma ferramenta gratuita, produzida em português e opera nos sistemas Windows®. Ele é capaz de emular os seguintes serviços: WEB, FTP, TFTP, POP3, ECHO, DAYTIME, SMTP, PORT FORWARDING e FINGER. Além disso, é possível simular arquivos e enviar respostas às solicitações.

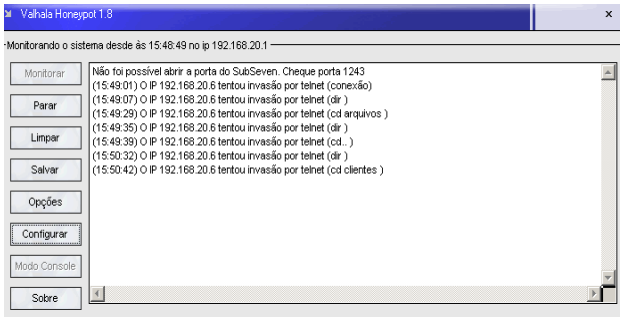

Figura 1 - Valhala Honeypot 1.8

3. Método de Pontuação

Foi criado um mecanismo de pontuação para cada item, de acordo com a disponibilidade do serviço em atender ou não os requisitos que foram baseados em [1] e [2], pontuando de 0 a 10 cada item. A tabela I mostra a métrica adotada para este artigo.

Tabela I – Tabela de Avaliação

Critério de avaliação	Conceito	Valor
Atende às Necessidades	Ótimo	8 - 10
Atende Parcialmente	Bom	6 - 8
Limitado	Regular	3 - 6
Não Atende	Ruim	0 - 3

"Atender às necessidades" significa disponibilizar serviços satisfatoriamente; já "atender parcialmente" é disponibilizar o recurso, porém não atender completamente às necessidades; ser "limitado" é não oferecer mais opções de sistema operacional e, por fim, "não atender às necessidades" significa apresentar falhas em pontos importantes para a proposta *honeypot*.

4. Resultado

A tabela II apresenta o resultado da avaliação aplicada sobre o Valhala Honeypot versão 1.8.

Tabela II – Avaliação do *honeypot Vallhala*

Critério de avaliação	Nota	Resultado
Plataforma	4	Regular
Layout	10	Ótimo
Configuração	8	Ótimo
Gerenciamento	10	Ótimo
Confiabilidade	10	Ótimo
Eficiência do Log	10	Ótimo
Opção de Entrega	10	Ótimo
Rastreamento	10	Ótimo
Invisibilidade	6	Regular
Realidade Honeypot	10	Ótimo

5. Conclusão

O sistema avaliado apresenta interface amigável e fácil configuração, assim como seu gerenciamento e acompanhamento de ataques, mas não reconhece alguns comandos básicos quando invadido. Sua avaliação média ficou em 8,8 pontos, o que o classifica em "Ótimo", apresentando-se como uma boa solução para empresas que utilizam de servidores Windows.

6. Referências Bibliográficas

[1] SPTIZER, L. Disponível em: http://www.tracking-hackers.com/papers/honeypots.html

[2] SOMMERVILLE, I. **Engenharia de Software,** 8ª Edição. São Paulo, 2007

[3] Valhala Honeypot. Disponível em: http://valhalahoneypot.sourceforge.net/