Glenon Mateus Barbosa Araújo

Análise de IDPSs

Brasil

2017

Glenon Mateus Barbosa Araújo

Análise de IDPSs

Trabalho de Conclusão de Curso submetida a graduação em Ciência da Computação da UFPA

Universidade Federal do Pará – UFPA

Faculdade de Computação

Bacharelado em Ciência da Computação

Orientador: Dr. Roberto Samarone dos Santos Araújo

Brasil

2017

Glenon Mateus Barbosa Araújo
Análise de IDPSs/ Glenon Mateus Barbosa Araújo. – Brasil, 2017-
39 p. : il. (algumas color.) ; 30 cm.

Orientador: Dr. Roberto Samarone dos Santos Araújo

Trabalho de Conclusão de Curso – Universidade Federal do Pará – UFPA
Faculdade de Computação
Bacharelado em Ciência da Computação, 2017.

1. Suricata. 2. Snort. 3. IDPS. I. Orientador. II. Universidade Federal do Pará. III. Faculdade de Computação. IV. Análise de IDPSs

Errata

Elemento opcional da **??**, 4.2.1.2). Exemplo:

FERRIGNO, C. R. A. **Tratamento de neoplasias ósseas apendiculares com reimplantação de enxerto ósseo autólogo autoclavado associado ao plasma rico em plaquetas**: estudo crítico na cirurgia de preservação de membro em cães. 2011. 128 f. Tese (Livre-Docência) - Faculdade de Medicina Veterinária e Zootecnia, Universidade de São Paulo, São Paulo, 2011.

Folha	**Linha**	**Onde se lê**	**Leia-se**
1	10	auto-conclavo	autoconclavo

Glenon Mateus Barbosa Araújo

Análise de IDPSs

Trabalho de Conclusão de Curso submetida a graduação em Ciência da Computação da UFPA

Trabalho aprovado. Brasil, 24 de novembro de 2012:

Dr. Roberto Samarone dos Santos Araújo
Orientador

Brasil
2017

Agradecimentos

Resumo

Palavras-chave: Segurança, Suricata, Snort, Sistema de Detecção de Intrusão, Sistema de Prevenção de Intrusão, IDS, IPS.

Abstract

Keywords: Security, Suricata, Snort, Intrusion Detection System, Intrusion Prevention System, IDS, IPS.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*

Sumário

Introdução

0.1 Objetivos

0.2 Trabalhos Relacionados

0.3 Motivação

1 Segurança de Redes de Computadores

1.1 Cenário Geral

1.2 Ataques

1.2.1 Exploração de Vulnerabilidades

1.2.2 Varredura de Redes

1.2.3 Força Bruta

1.2.4 Desfiguração de páginas

1.2.5 Negação de Serviços

1.2.6 Worm

1.2.7 Trojan

1.2.8 Fraudes - Direitos Autorais

2 Sistemas de Detecção e Prevenção de Intrusão

2.1 Tipos de IDS/IPS

2.2 Snort

2.3 Suricata

3 Detecção de Intrusão em um Cenário Real

No ambiente de teste foi usado uma máquina Dell com 134G de memória RAM e 40 núcleos. Usou-se XenServer (XENSERVER, 2017) versão 7, sistema operacional *opensource* da Citrix voltado para virtualização. Foram testados outros SOs porém somente o XenServer possuía, na época da instalação do ambiente, *firmware* da placa de rede do *host* compatível e que funcionava com instabilidade. Outro fator que pesou na escolha do SO foi a experiência que tinha com a plataforma.

No primeiro momento, foi instalado uma máquina virtual que seria usada como base para instalações de outras máquinas usando o recurso de *snapshot* do sistema. O uso desse recurso foi necessário para criar um ambiente igual para os IDSs.

Foi alocado 8 GB de memória RAM, 4 processadores e 100 GB de espaço em disco para o *snapshot*. Esses valores foram definidos com base em um estudo (LOCOCO, 2011) que considerava vários fatos, como largura da rede, localização do IDS e versão e tipo do capturador de tráfego para dimensionar os recursos, aplicado especificamente ao Snort. A mesma regra foi aplicada ao Suricata.

Posteriormente criou-se três máquinas virtuais, duas usadas para instalação dos IDSs (Suricata e Snort) e a terceira para instalação das ferramentas usadas para simular ataques a rede. Optou-se pela instalação do sistema Kali (KALI, 2017) para geração de ataques pois nele existe várias ferramentas nativas para testes de penetração e auditoria de segurança.

Para coleta das informações de uso de recurso de hardware como memória e processamento das máquinas com os IDSs foi usado o *daemon* Collectd (COLLECTD, 2017).

Figura 1

Tabela 1

3.1 Métricas de Comparação

Consumo dos Recursos de Hardware (Memória, Processamento)

Taxa de Detecção

	último	min	méd	máx
média	29,34 Mbps	0 bps	5,45 Mbps	107,25 Mbps

Tabela 1 – Estatística do trafego da rede selecionada para teste

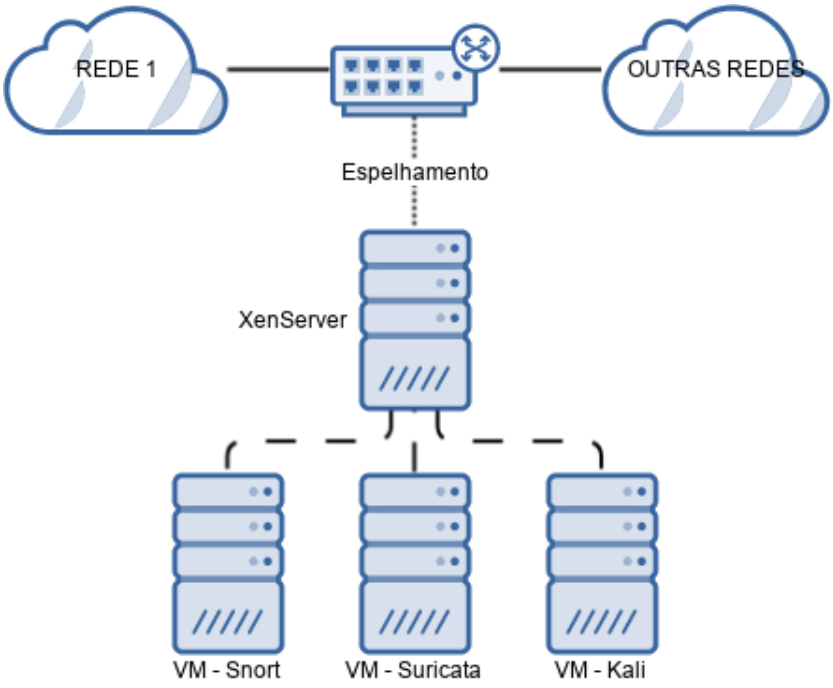

Figura 1 – Infraestrutura do Ambiente de teste

Número de Falsos Positivos/Negativos

4 Considerações Finais

Parte I

Referenciais teóricos

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Referências

COLLECTD. 2017. Disponível em: <https://collectd.org/>. Citado na página 31.

KALI. 2017. Disponível em: <http://docs.kali.org/introduction/what-is-kali-linux>. Citado na página 31.

LOCOCO, M. *Capacity Planning for Snort IDS*. 2011. Disponível em: <http://mikelococo.com/2011/08/snort-capacity-planning/>. Citado na página 31.

XENSERVER. 2017. Disponível em: <https://xenserver.org/about-xenserver-open-source.html>. Citado na página 31.