

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-
35 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

Figura 1 – Infraestrutura do Ambiente de teste	32
--	----

Lista de tabelas

Tabela 1 – Estatística do trafego da rede selecionada para teste	31
--	----

Lista de abreviaturas e siglas

IDS	<i>Intrusion Detection System</i>
IPS	<i>Intrusion Prevention System</i>

Sumário

	Introdução	25
0.1	Objetivos	25
0.2	Trabalhos Relacionados	25
0.3	Motivação	25
1	SEGURANÇA DE REDES DE COMPUTADORES	27
1.1	Cenário Geral	27
1.2	Ataques	27
1.2.1	Exploração de Vulnerabilidades	27
1.2.2	Varredura de Redes	27
1.2.3	Força Bruta	27
1.2.4	Desfiguração de páginas	27
1.2.5	Negação de Serviços	27
1.2.6	Worm	27
1.2.7	Trojan	27
1.2.8	Fraudes - Direitos Autorais	27
2	SISTEMAS DE DETECÇÃO E PREVENÇÃO DE INTRUSÃO	29
2.1	Tipos de IDS/IPS	29
2.2	Snort	29
2.3	Suricata	29
3	DETECÇÃO DE INTRUSÃO EM UM CENÁRIO REAL	31
3.1	Métricas de Comparação	32
4	CONSIDERAÇÕES FINAIS	33
	Referências	35

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.

A rede selecionada para ser monitorada tem os valores especificados na tabela 1. Podemos verificar que seu pico de tráfego chega a 107,25 Mbps em um determinado período do dia, valores considerados ideais para o experimento, inclusive para tentar validar os recursos alocados.

Para o *host* conseguir pegar o pacotes destinados a rede selecionada foi necessário uma configuração de espelhamento que consiste na copia dos pacotes que saem pela porta dessa rede no *switch* para a porta conectada no *host*. A interface de rede do *host* precisou ser configurado no modo *promisc*.

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, processamento e I/O das máquinas com os IDSs foi usado o *daemon* Collectd ([COLLECTD](#),

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

Tabela 1 – Estatística do tráfego da rede selecionada para teste

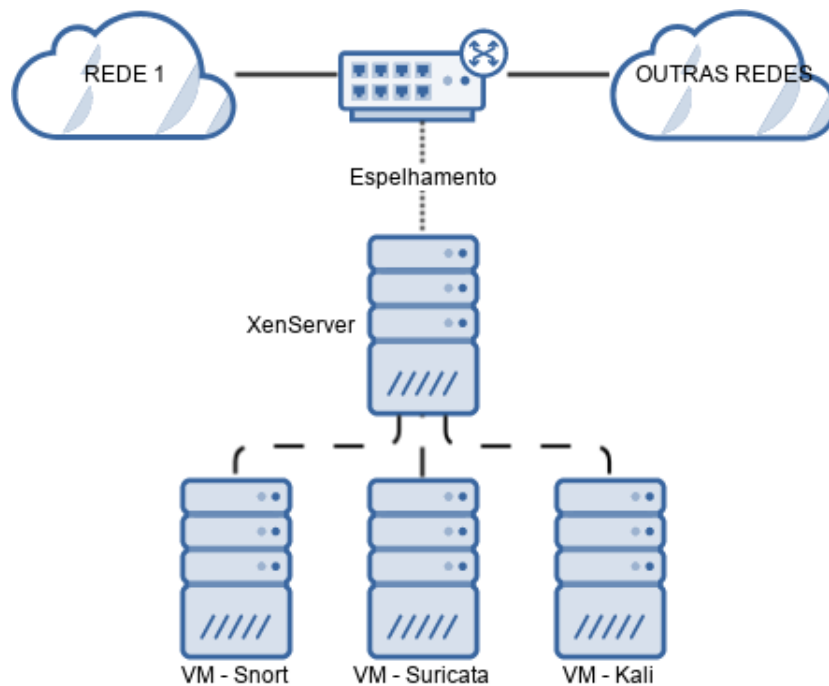


Figura 1 – Infraestrutura do Ambiente de teste

2017). Outra opção para esse fim foi a utilização de um servidor de monitoramento com o *Zabbix* (ZABBIX, 2017). A ideia de usar duas ferramentas para análise é fazer um comparativo e validar as informações coletadas.

Figura 1

3.1 Métricas de Comparação

Consumo dos Recursos de Hardware (Memória, Processamento)

Taxa de Detecção

Número de Falsos Positivos/Negativos

4 Considerações Finais

Referências

COLLECTD. 2017. Disponível em: <<https://collectd.org/>>. Citado na página 32.

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.

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

ZABBIX. 2017. Disponível em: <<http://www.zabbix.com/>>. Citado na página 32.