Curso Superior de Tecnologia em Redes de Computadores

Projeto Integrador

1º Seminário de Andamento

Gabriel Jesus Pereira
gabroot.pereira@gmail.com.br

Análise dos Sistemas de IDS/IPS em Redes

Sumário

- Introdução
- Objetivos
  - Geral
  - Específicos
- Projeto
  - Situação atual
  - Próximos passos
- Cronograma
- Referências Bibliográficas
- Wiki
- Perguntas

Introdução

- IDS - *Intrusion Detection Systems*

Sistema de Detecção de Intrusão.

- IPS - *Intrusion Prevention Systems*

Sistema de Prevenção de Intrusão.

Motivação/Justificativa

- Alcançar os *pilares da segurança da informação*;
- Conhecer e estudar novas ferramentas;
- Implementar como solução para um ambiente em produção.

Objetivo Geral

- Conhecer de forma teórica e prática duas ferramentas de IDS/IPS. Identificar os diferenciais, testar em ambiente controlado, comprovar a eficácia e concluir qual pode ser mais assertiva.

Objetivos Específicos

- Realizar pesquisa bibliográfica;
- Instalar e identificar a funcionalidade das ferramentas;
- Elaborar um cenário para a realização dos testes;
- Utilizar as funcionalidades das ferramentas para prevenir e detectar intrusões;
- Instalar e configurar os serviços para os quais serão direcionados os ataques;

Objetivos Específicos

- Realizar ataques aos serviços/rede;
- Monitorar e gerar gráfico de desempenho de hardware e rede no momento dos ataques;
- Documentar o comportamento das ferramentas de detecção e prevenção de intrusões;
- Comparar assertividade das ferramentas;
- Escrever artigo.

Situação Atual

- Levantamento bibliográfico;
- Estudando as ferramentas;
- Familiarização com o ambiente;
- Definindo o cenário à ser montado;
- Definindo serviços à serem atacados.

Próximos Passos

- Instalar os sistemas e serviços à serem explorados;
- Definir as regras à serem utilizadas pelo Snort e Suricata;
- Definição do cenário;
- Montagem do cenário;
- Realizar testes iniciais;
- Iniciar a escrita do artigo.

	MAR	ABR	MAI	JUN	JUL
Realizar pesquisa bibliográfica sobre as ferramentas	X	X			
Instalar e identificar a funcionalidade de cada ferramenta	X	X			
Definir e montar o cenário para a realização dos testes		X	X		
Utilizar as funcionalidades das ferramentas para prevenir e detectar intrusões			X	X	
Instalar e configurar os serviços para os quais serão direcionados os ataques			X	X	
Realizar ataques aos serviços/rede			X	X	
Monitorar e gerar gráfico de desempenho de hardware e rede no momento dos ataques			X	X	
Documentar o comportamento das ferramentas de detecção e prevenção de intrusões				X	X
Comparar assertividade das ferramentas				X	X
Escrever artigo		X	X	X	X

Referências

- Snort. Disponível em: <https://www.snort.org/>. Acesso em: 25/03/2017
- Suricata. Disponível em: <https://suricata-ids.org/>. Acesso em: 25/03/2017
- Suricata. Disponível em: <https://oisf.net/suricata/>. Acesso em: 25/03/2017

Wiki

- LINK PROPOSTA “EXTERNO”: http://187.7.106.14/wiki2017_1/doku.php?id=projeto08:proposta
- LINK PROPOSTA “INTERNO”: http://192.168.200.3/wiki2017_1/doku.php?id=projeto08:proposta

Dúvidas