SBSEG'08

VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais

DIBSet: Um Detector de Intrusão por Anomalias Baseado em Séries Temporais

Universidade Federal de Santa Maria - Centro de Tecnologia
GMICRO/INPE

Roben Castagna Lunardi, Bruno L. Dalmazo, Erico M. H. do Amaral , Raul Ceretta Nunes
rclunardi@inf.ufrgs.br, {dalmazo, erico, ceretta}@inf.ufsm.br

informática
Universidade Federal de Santa Maria

SBSEG'08

Sumário

- Introdução
- Caracterização
- Séries Temporais
- Solução Conceitual
- Implementação
- Estudos de Caso
- Resultados
- Conclusões e Trabalhos Futuros

informática
Universidade Federal de Santa Maria

Introdução (1)

- Atualmente a utilização da internet é parte do cotidiano de uma grande gama de usuários
- Diversos serviços são disponibilizados para estes usuários
- Usuários maliciosos podem tirar proveito de possíveis falhas e/ou mal configurações de destes serviços/usuários
- Uma das medidas para a garantia do bom funcionamento é a utilização de Sistemas de Detecção de Intrusão

Introdução (2)

- Sistemas de Detecção de Intrusão são compostos de 3 partes fundamentais: dados, análise e resposta
- Embora existam diversos estudos na área, ainda não existe uma forma eficiente de analisar os dados capturados
- Por este motivo, o trabalho se concentrou no processo de análise, com a utilização do DIBSet para realizar alguns estudos de caso.

Caracterização

- Ataques Caracterizáveis: ocorrem sempre da mesma forma
  - Filtráveis
  - Não-Filtráveis
- Ataques Não-Caracterizáveis: não possuem um padrão de ocorrência
- Detecção por Assinaturas: busca por atividades suspeitas (conhecidas) e por erros na semântica de protocolos
- Detecção por Anomalias: independe do conhecimento de características específicas de ataques, mas pode gerar muitos falsos positivos

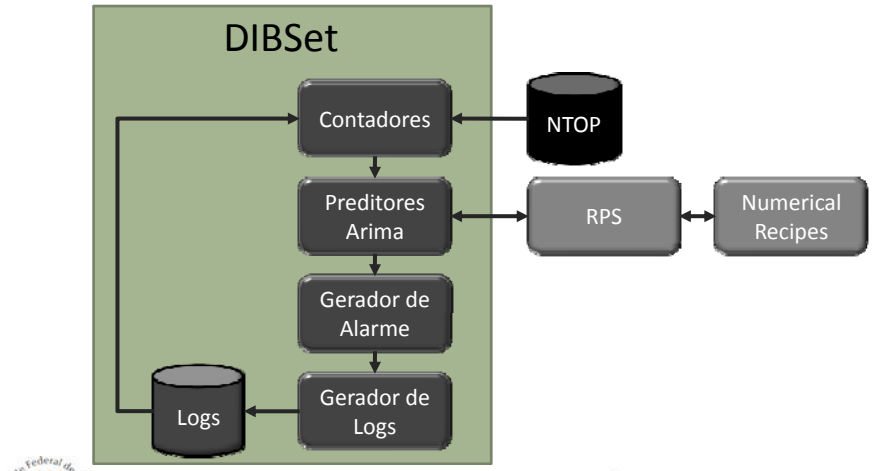
Séries Temporais

- Séries Temporais é um conjunto de observações de uma dada variável, ordenadas no tempo, geralmente em tempos eqüidistantes
- O modelo ARIMA incorpora os modelos:
  - AR(p): puramente autoregressivo de ordem *p*
  - MA(q) puramente médias móveis de ordem *q*
  - ARMA(p,q): autoregressivo e de médias móveis de ordem *p* e *q*
  - ARIMA(p,d,q): autoregressivo integrado e de médias móveis de ordem *p*, *d* e *q* (ARIMA(*p*,*d*,*q*))
  - onde *d* representa a ordem de integração, ou seja, o número de diferenças necessárias para transformar a série temporal não estacionária em estacionária.

Solução Conceitual

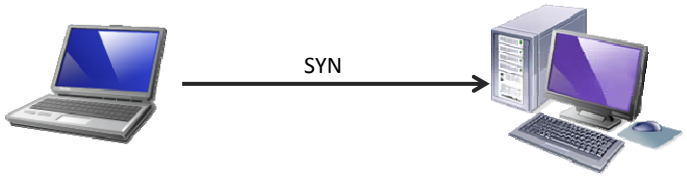
- A Solução é baseado em Detecção de Intrusões por Anomalias
- Foram Utilizadas Séries Temporais para a predição do comportamento esperado
- Estabeleceu-se limites (thresholds) superiores e inferiores
- Os alarmes gerados são diferenciados para a extrapolação dos limiares inferiores e superiores
- Os dados capturados e os alarmes são registrados para realimentação do sistema e conferência das principais ocorrências.

Implementação



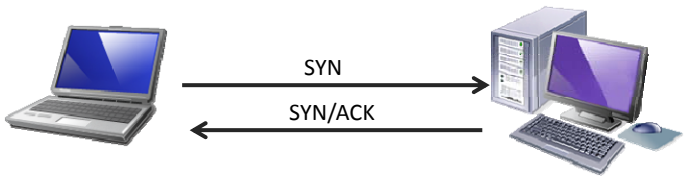
Estudos de Caso (1.1)

Three-way Handshake



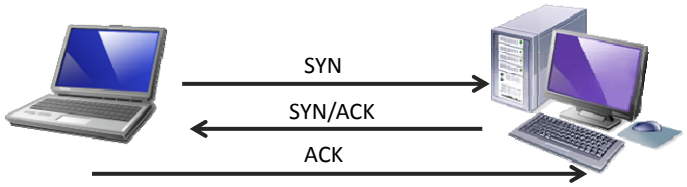
Estudos de Caso (1.2)

Three-way Handshake



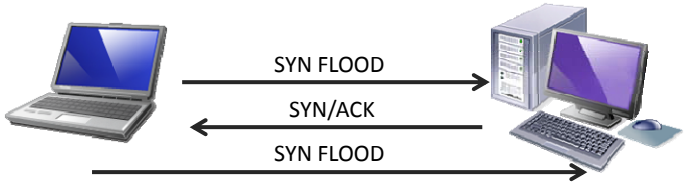
Estudos de Caso (1.3)

Three-way Handshake



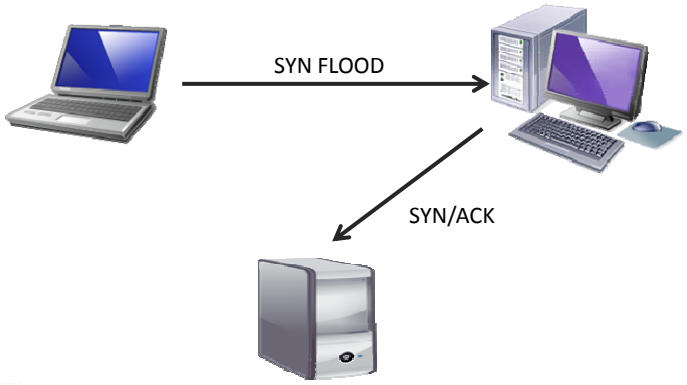
Estudos de Caso (1.4)

Syn Attack



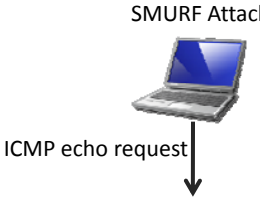
Estudos de Caso (1.5)

SYN Attack com Spoofing

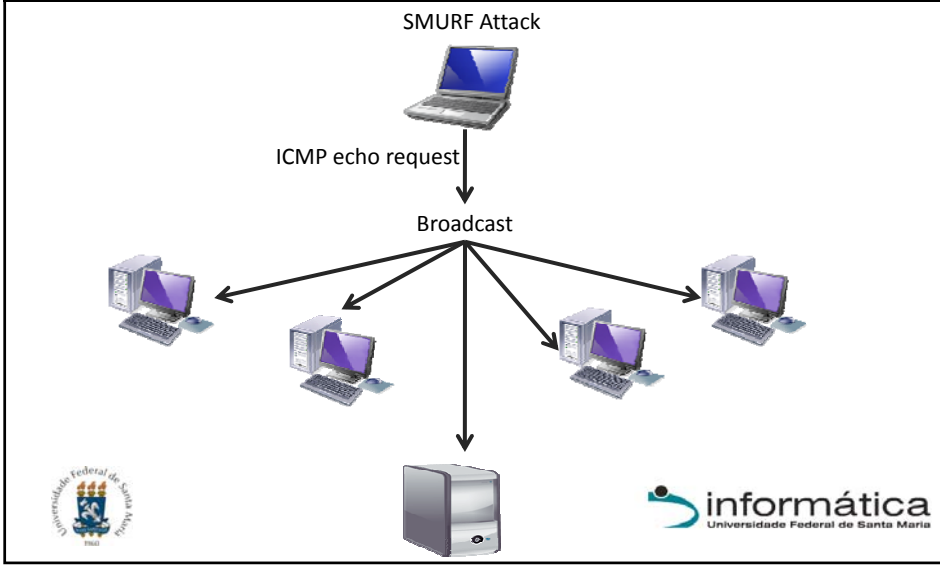


Estudos de Caso (2.1)

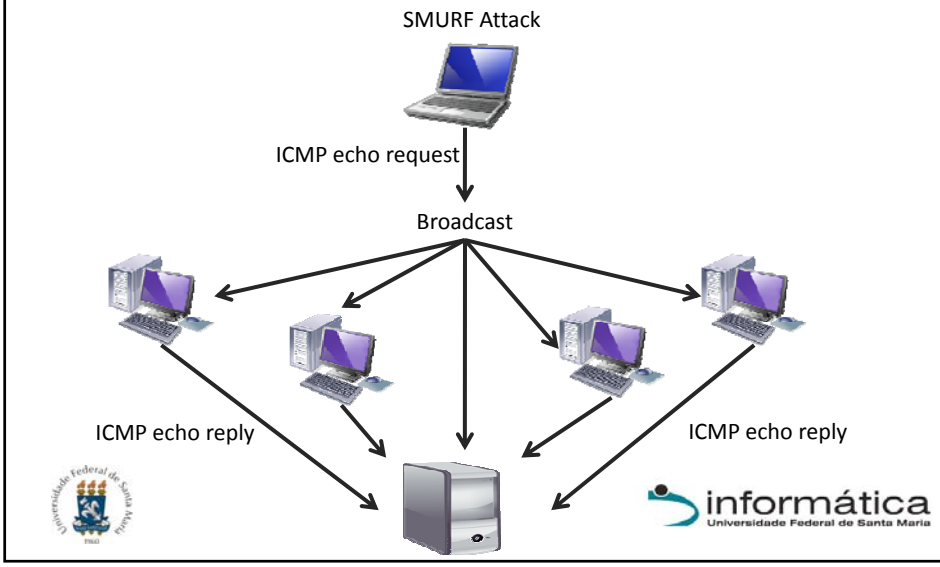
SMURF Attack



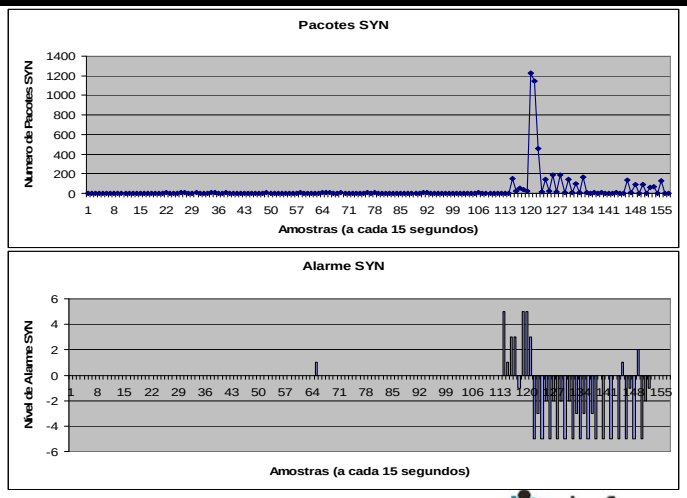
Estudos de Caso (2.2)



Estudos de Caso (2.3)

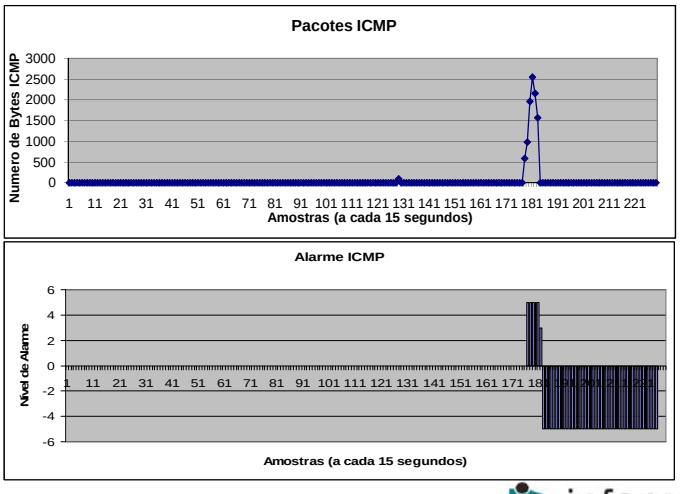


Resultados (1)



informática
Universidade Federal de Santa Maria

Resultados (2)



informática
Universidade Federal de Santa Maria

Conclusões e Trabalhos Futuros

- Utilizamos séries temporais para detectar intrusões
- Empregamos níveis inferiores e superiores de *thresholds*
- Apresentamos a implementação do DIBSet como sistema de detecção de intrusões
- Para suportar a nossa solução, utilizamos dois ataques e os respectivos níveis de alarmes
- Os resultados foram suportaram as idéias apresentadas

informática
Universidade Federal de Santa Maria

Conclusões e Trabalhos Futuros

- Como continuação deste trabalho estão sendo adaptadas as funções de coletas para utilizar os dados do IAS (*Internet Analysis System)* – parceria FHGe e UFSM
- Além disso, está sendo aperfeiçoado o algoritmo de geração de alarmes para diminuir o número de falsos positivos
- Serão realizados outros ataques para verificar o desempenho do DIBSet

informática
Universidade Federal de Santa Maria

Referências

•Pohlmann, N. and Proest M. (2006) "Internet Early Warning System: The Global View". In: Vieweg, Securing Eletronic Business Process, pages 377 – 386.

•Dwyer, D. (2003) "Network Intrusion Detection." 3rd Edition, New Riders Publishing.

•Kompella, R. R., Singh, S. E Varghese, G. (2007) "On Scalable Attack Detection in the Network". In: IEEE/ACM TRANSACTIONS ON NETWORKING, Vol. 15, No. 1.

•Levchenko, K., Paturi, R. e Varghese, G. (2004) "On the Difficulty of Scalably Detecting Network Attacks". CCS-ACM.

•Peng, T., Leckie, C. e Ramamohanarao, K. (2007) "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems". In: ACM Computing Surveys, Vol. 39, No 1, Article 3.

•Maselli, G., Deri, L. e Suin, S. (2003) "Design and Implementation of an Anomaly Detection System: an Empirical Approach". Proceedings of Terena Networking Conference (TNC 03), Zagreb, Croatia.

•Lunardi, R. (2008) "Um analisador de intrusões baseado em Séries Temporais". Trabalho de Graduação n°255, Curso de Ciência da Computação, UFSM.

•Kumar, S. (2007) "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet". Second International Conference on Internet Monitoring and Protection (ICIMP IEEE 2007).

•Bowerman, Bruce L. and O'Connel, Richard T. Forecasting and Time Series: an Applied Approach. Belmont: Duxbury Press. 1993.

•Goodall, J. (2006) "Visualizing Network Traffic For Intrusion Detection" In: ACM Symposium on Designing Interactive Systems, pages 363-364.

informática
Universidade Federal de Santa Maria