



Ministério da Fazenda

Serviço Federal de Processamento de Dados (SERPRO)

Mineração de Dados em Sistemas de Detecção de Intrusão e Antivírus



Palestrante: Daniel Araújo Melo – Grupo de Resposta a Ataques da Intranet

00/00/0000

Serviço Federal de Processamento de Dados



Ministério da Fazenda



www.serpro.gov.br



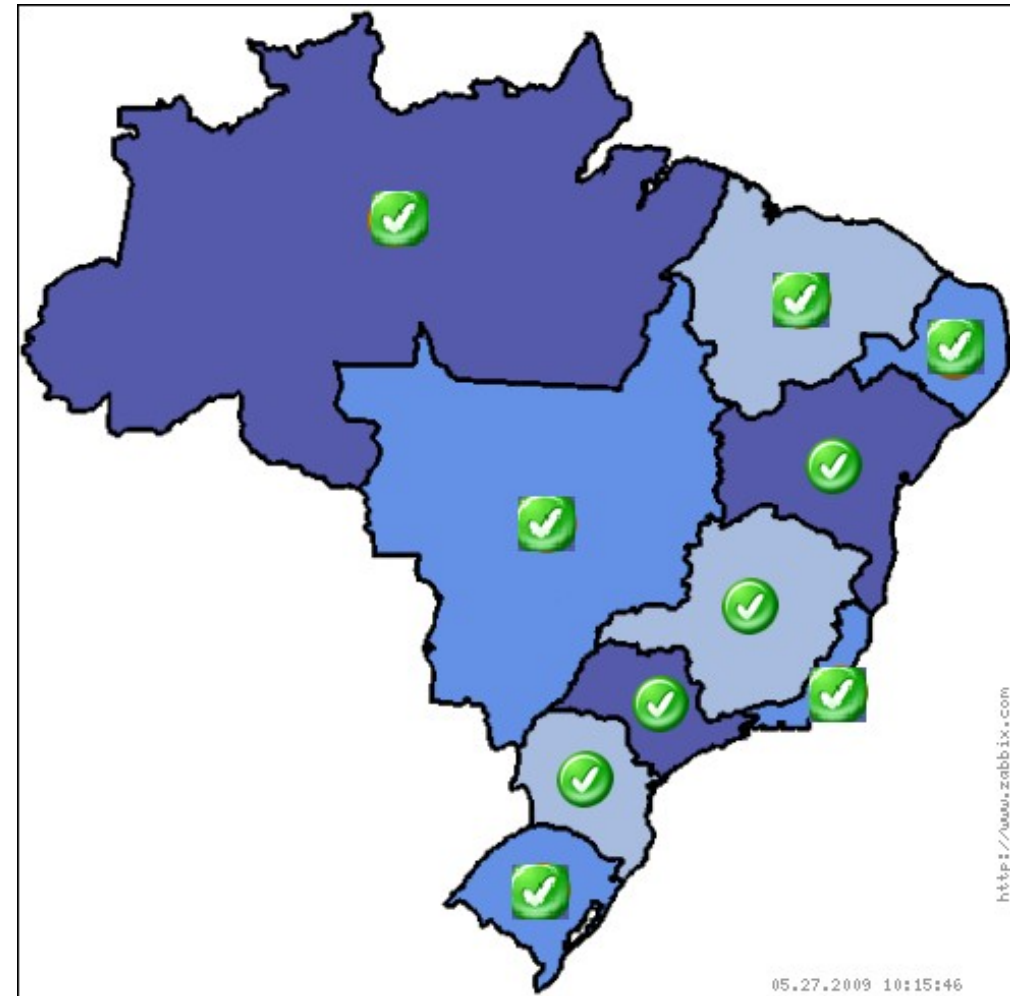
Introdução

- Serpro - Serviço Federal de Processamento de Dados
- Empresa do Ministério da Fazenda
- Criado inicialmente para atender às necessidades da Receita Federal
- Atualmente desenvolve sistemas para todo o Governo do Brasil
 - MINISTÉRIO DO DESENVOLVIM. INDUSTRIA E COMÉRCIO EXTERIOR , MINISTÉRIO DO TRABALHO E EMPREGO, MINISTÉRIO DA EDUCAÇÃO, POLÍCIA FEDERAL, etc
- Presente nas 10 Regiões Fiscais do Brasil
 - 10 Regionais + 1 Sede
- Aproximadamente 8.000 estações de trabalho na Intranet



Introdução

- TIGRA – Grupo de Resposta a Ataques da Intranet
- Possui NIDS nas 10 Regionais e Sede
- Monitoramento interno
- Aproximadamente 30.000.000 de alertas por mês
- Dificuldade em identificar ataques verdadeiros ou significativos.





Introdução

- Pesquisa de Mestrado
 - Área: Inteligência Computacional
- UFPE - Universidade Federal de Pernambuco
 - CIN – Centro de Informática
- Orientadores:
 - Paulo Adeodato – pjla@cin.ufpe.br
 - Paulo Gonçalves – pasg@cin.ufpe.br
- Alunos:
 - Daniel A. Melo – daniel.melo@serpro.gov.br, dam2@cin.ufpe.br
 - Paulo Mauricio – pmgj@cin.ufpe.br
 - Davi Carnaúba – dclv@cin.ufpe.br



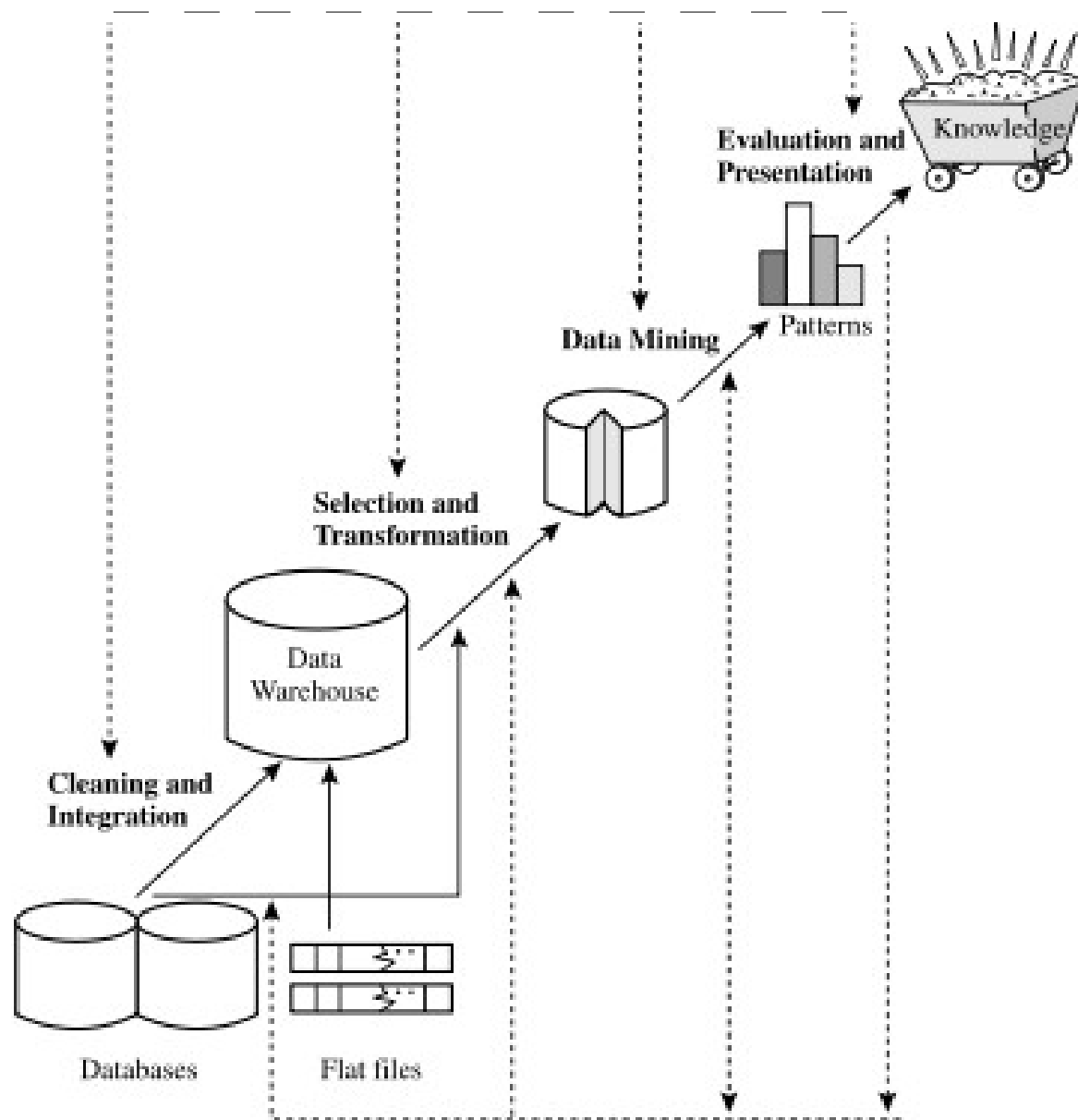
Introdução

- Modelos de correlação foram propostos para minimizar incidências de falsos positivos, de acordo com as classes:
 - (1) Utilizando cenários de ataques especificados por especialistas ou aprendidos através de conjuntos de treinamento;
 - (2) Com base na similaridade entre atributos de um alerta;
 - (3) Com base em pré-condições e consequências de ataques.
- **Foco da Pesquisa: Classe (1)**



Mineração de Dados

- Mineração de Dados
 - Etapa do KDD
 - Knowledge Discovery in Databases





Análise dos Dados

- **NIDS e AV do SERPRO**
 - 10 Regionais
 - 8.000 estações de trabalho
 - NIDS – 30.000.000 alertas/mês
 - AV – 2.500 alertas/mês
- **Dados coletados**
 - 1 Regional
 - 400 estações
 - 90 dias
 - 12.165.461 alertas NIDS
 - 2220 alertas do AV



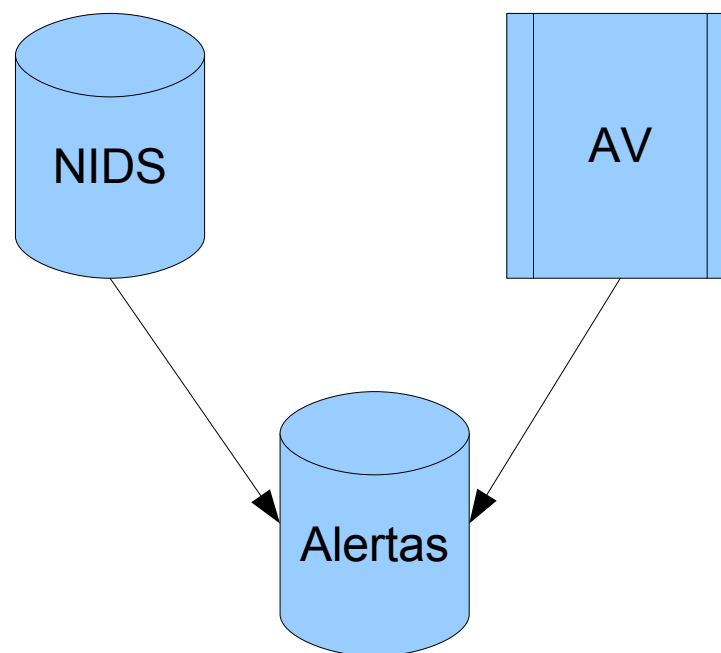
Análise dos Dados

- **Dimensões do NIDS**
 - Evento
 - Assinatura
 - classificação da assinatura
 - cabeçalho IP
 - cabeçalho TCP
 - cabeçalho UDP
 - cabeçalho ICMP
- **Como AV será classificador:**
 - Timestamp
 - End. IP Fonte
- **Granularidade: Evento**



Pré-processamento

- União de duas bases distintas e ordenadas pelo timestamp;
 - NIDS – Banco normalizado
 - AV – plain text - CSV
- End. IP – campo de 32 bits:
 - Necessário para relacionar eventos
 - NIDS – integer
 - AV: String com notação de 4 octetos





Pré-processamento

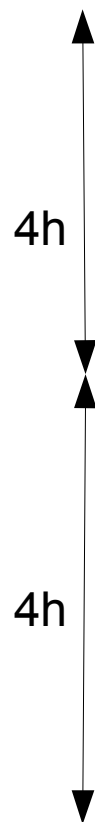
- **Heurística**
 - Eventos do NIDS relacionados com um alerta do AV, para um hospedeiro, numa janela de 4 horas, foram considerados influenciadores
 - Eventos da janela que resultaram em alertas do AV
 - *Classe 1 – Classe alvo*
 - Eventos da janela que não resultaram em alerta do AV, apenas NIDS
 - *Classe 0 – Classe não-alvo*



Janelas

Classe 1

Timestamp	Host	Alerta
1	A	NIDS
2	A	NIDS
3	A	AV
4	A	NIDS
5	A	AV
6	B	NIDS
7	B	NIDS
8	B	NIDS
9	B	NIDS
10	B	NIDS
11	B	AV



Classe 0

Timestamp	Host	Alerta
1	A	NIDS
2	A	NIDS
3	A	NIDS
4	A	NIDS
5	A	NIDS
6	B	NIDS
7	B	NIDS
8	B	AV
9	B	NIDS
10	B	NIDS
11	B	NIDS



Pré-processamento

- **Principal Dificuldade**
 - Cross join de eventos:
 - *aprox. 6.000.000 de registros – classe 1*
 - *aprox 126.000.000 de registros – classe 0*
- **Após agrupamento:**
 - Aprox. 2.200 eventos da classe 1
 - Aprox. 10.000 eventos eventos da classe 0
 - *Selecionados aleatoriamente entre os hospedeiros*



Variáveis

- **Nids**

- *Timestamp;*
- *ip_src;*
- *ip_dst;*
- *sig_id;*
- *sig_class_id;*
- *ip_proto;*
- *Sport;*
- *Dport;*
- *icmp_type;*
- *icmp_code;*
- *Tamanho;*
- *id;*

- **Antivírus**

- *Timestamp e ip_src*



Variáveis

- A partir do Conhecimento do especialista e agrupamento:
 - 96 variáveis
 - *Moda de variáveis categóricas*
 - *Media de variáveis numéricas*
 - *Total de variáveis no período*
 - Considerando eventos gerados e destinados ao hospedeiro
- Cálculo do ganho de informação para selecionar variáveis
 - GainInformationRatio
 - *Avalia entropia de cada variável e ordena de acordo com maior ganho de informação*
 - 15 variáveis restaram com ganho significativo



Variáveis

- **Src_bad_unknown**
 - Quantidade de alertas do tipo “bad_unknown” gerados pelo hospedeiro.
- **Dst_bad_unknown**
 - Quantidade de alertas do tipo “bad_unknown” direcionados ao hospedeiro.
- **Qtde_sigs_dest**
 - Quantidade de assinaturas distintas de alertas direcionados ao hospedeiro
- **Qtde_sigs_fonte**
 - Quantidade de assinaturas de alertas gerados pelo hospedeiro
- **Moda_sig_fonte**
 - Moda das assinaturas de alertas gerados pelo hospedeiro.
- **Media_tamanho**
 - Média do tamanho dos pacotes que disparam alertas no intervalo



Variáveis

- **Qtde_udp_dest**
 - Quantidades de portas UDP distintas em alertas direcionados ao hospedeiro.
- **Qtde_tcp_fonte**
 - Quantidade de segmentos TCP em alertas disparados pelo hospedeiro
- **Qtde_tcp_sport_fonte**
 - Quantidade de portas fonte TCP distintas em alertas disparados pelo hospedeiro
- **Qtde_tcp_sport_dest**
 - Quantidade de portas fonte TCP distintas em alertas direcionados ao hospedeiro
- **Qtde_tcp_dport_dest**
 - Quantidade de portas destino TCP distintas em alertas direcionados ao hospedeiro



Variáveis

- **Qtde_icmp_dest**
 - Quantidade de mensagens ICMP direcionadas ao hospedeiro, que disparam alertas.
- **Qtde_icmp_fonte**
 - Quantidade de mensagens ICMP geradas pelo hospedeiro, que disparam alertas.
- **Moda_icmp_type_fonte**
 - Moda dos tipos de mensagens ICMP gerados pelo hospedeiro que disparam alertas.



Rede Neural

- Utilizada para construir classificador
- Multi Layer Perceptron com algoritmo de aprendizagem Backpropagation
 - Escolha devido a capacidade de generalização
 - Aprendizagem supervisionada
- **Parâmetros:**
 - Taxa de Aprendizado – 0.01
 - Momentum – 0.1
 - Quantidade de Camadas Escondidas - 1
 - Número de Neurônios na Camada Escondida – 2
- **Validação do classificador validado com método hold-out:**
 - 50% treinamento
 - *Replicação de eventos da classe 1 para balancear proporção*
 - 50% testes



Resultados

- Matriz de confusão
 - 3933 registros analisados na fase de testes
 - 3882 corretamente classificados
 - 51 classificados errados
 - 98,7% de acerto

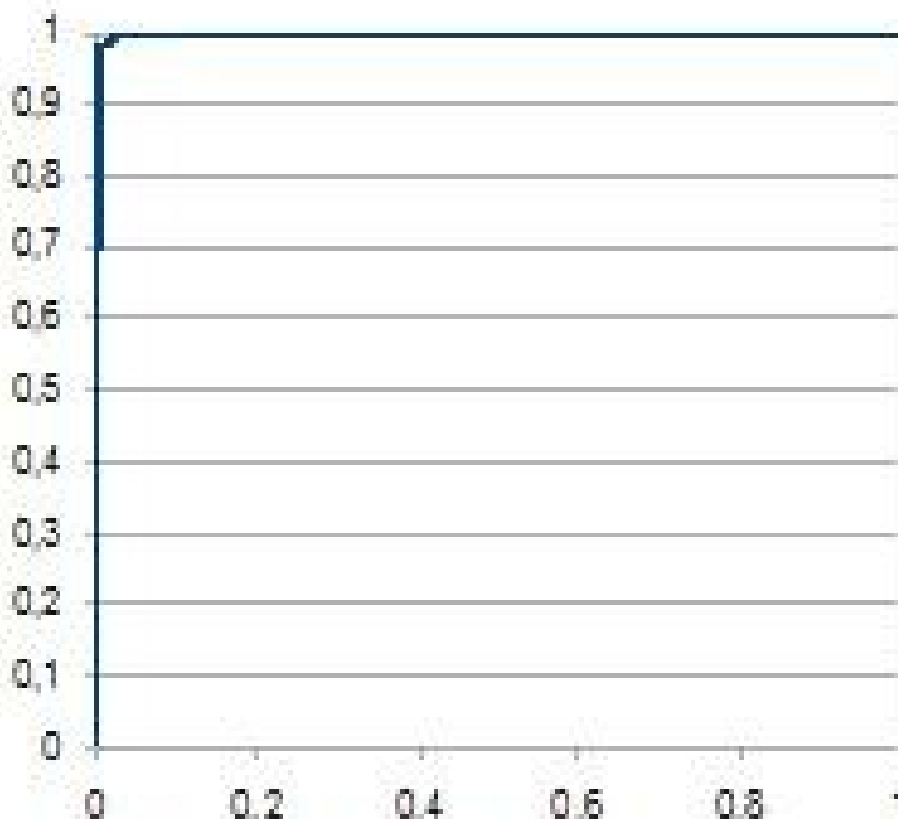
Classe/Predição	Classe 1	Classe 0
Classe 1	1330	15
Classe 0	36	2552



Avaliação de Desempenho

- Curva ROC

AUC=0,998





Conclusão

- A formalização do conhecimento em um modelo computacional permite uma série de vantagens como, por exemplo:
 - resposta automática,
 - suporte ao analista de detecção de intrusão;
- A diminuição da quantidade de alertas levantados pelo NIDS;
- **Trabalhos Futuros**
 - Verificar a independência das amostras;
 - Realizar testes com outras regionais;
 - Implementar DW em tempo real;
 - Construir classificador em tempo hábil;



FIM

Obrigado