# *Metodologia de Monitoração Remota de Logs de Segurança*

Carlos Henrique P. C. Chaves
Lucio Henrique Franco
Antonio Montes

{carlos.chaves,lucio.franco,antonio.montes}@cenpra.gov.br

CenPRA
Centro de Pesquisas
Renato Archer

Honeynet.BR

# *Sumário*

- Análise de Logs
- Fontes de Log
- Redução do Volume de Logs
- Metodologias para Análise
- Conclusão
- Contatos

# *Análise de Logs*

- Monitoramento e análise de vários tipos de registros (logs).
- Diferentes tipos: firewalls, roteadores, IDS, servidores, ...
- Log > /dev/null
- Não registra tudo ⇒ capacidade de armazenamento limitada, utilização da banda, limitações de aplicações.

# *Análise de Logs*

- Milhares de US$ gastos com IDS e firewalls.
- E a ameaça interna?
- Configuração segura de máquinas (registrando tudo).
- Por quanto tempo armazenar?
- Por que ocupar espaço em disco?
- Quantidade de registros gerados por IDS, Firewalls, sistema operacional, aplicativos, etc.

# *Análise de Logs*

- Invasão!!!! Onde estão meus logs?
  - Descobrir os passos do atacante.
  - Reparar a brecha de segurança.
  - Descobrir quais outras máquinas foram comprometidas.

Objetivo: correlacionar e processar o conteúdo de múltiplos logs.

# *Fontes de Log*

- Boa prática de segurança: registrar tudo.
- IDS, firewall, syslog, aplicativos, etc.
- Soma de todos os logs = centenas de milhares ou milhões de linhas / dia.

Se ((logar tudo = (+ seguro)) &&
(linhas/dia >= 1000000))
então Dia de trabalho = Análise de Logs

# *Fontes de Log*

- Problema: Dia de trabalho = Análise de Logs

Solução: Diminuir número de linhas/dia!!!

- Mas como?

# *Redução do Volume de Logs*

- *Artificial Ignorance (AI):* técnica de processamento de logs que determina o que ignorar.
- O que é considerado normal deve ser desconsiderado.
- Exemplos:
  - Logs de HTTP: acessos a páginas estáticas que retornaram código 200.
  - Alertas de IDS: alertas de ataques contra IIS quando existem apenas Apache na minha rede.

# *Redução do Volume de Logs*

- Utilizar a Ignorância artificial para reduzir o número de registros.
- Agora: linhas/dia << 1000000
- Se pararmos aqui, o problema continua, então:

Pergunta: Como analisar os Logs?

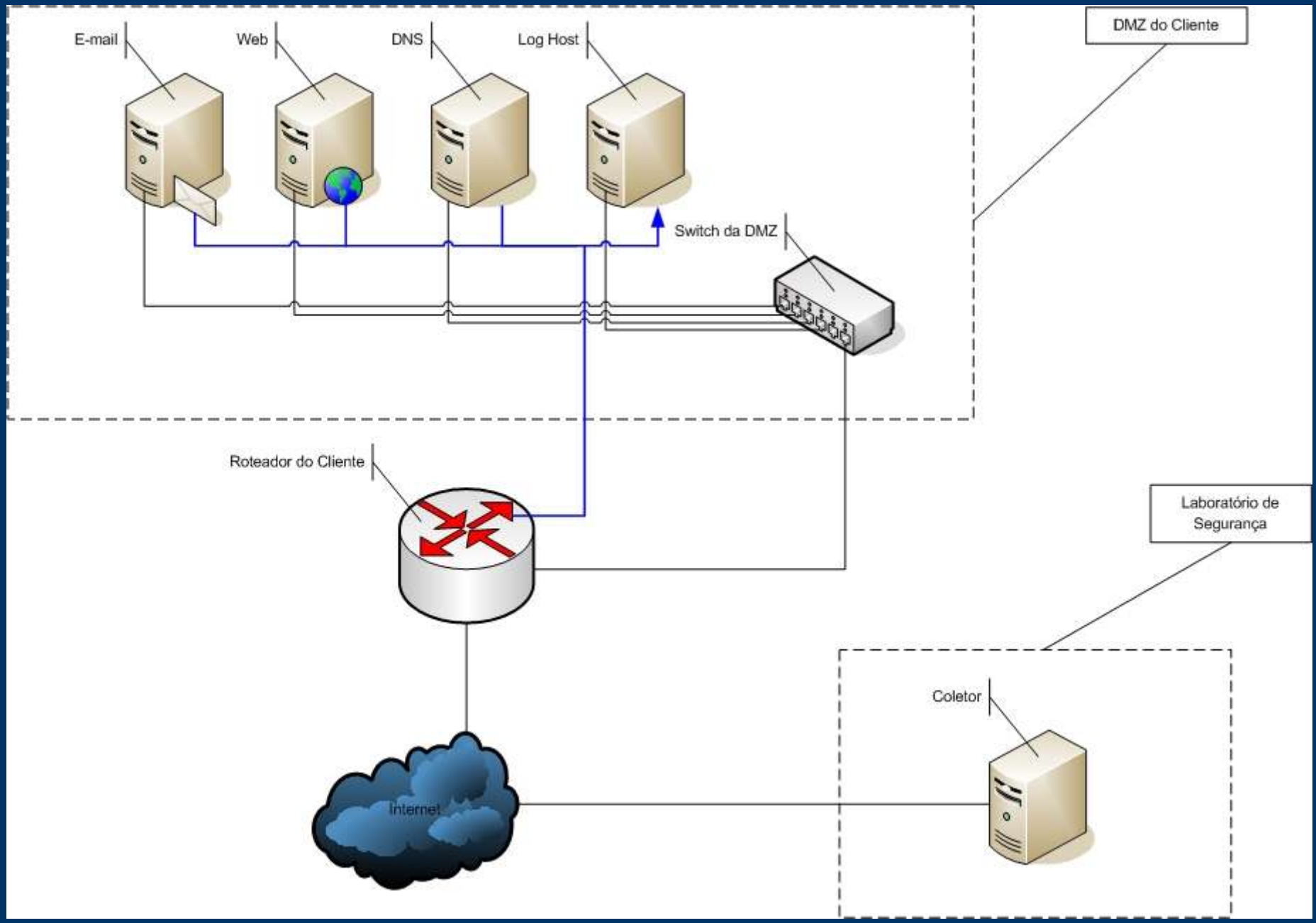
# *Metodologia para Análise*

- Relembrando:
  - Servidores, firewall, IDS, roteador, syslog, aplicativos ⇒ registrando tudo.
  - Volume de logs reduzido pela AI.
- Problema: Cada máquina armazena seus logs.

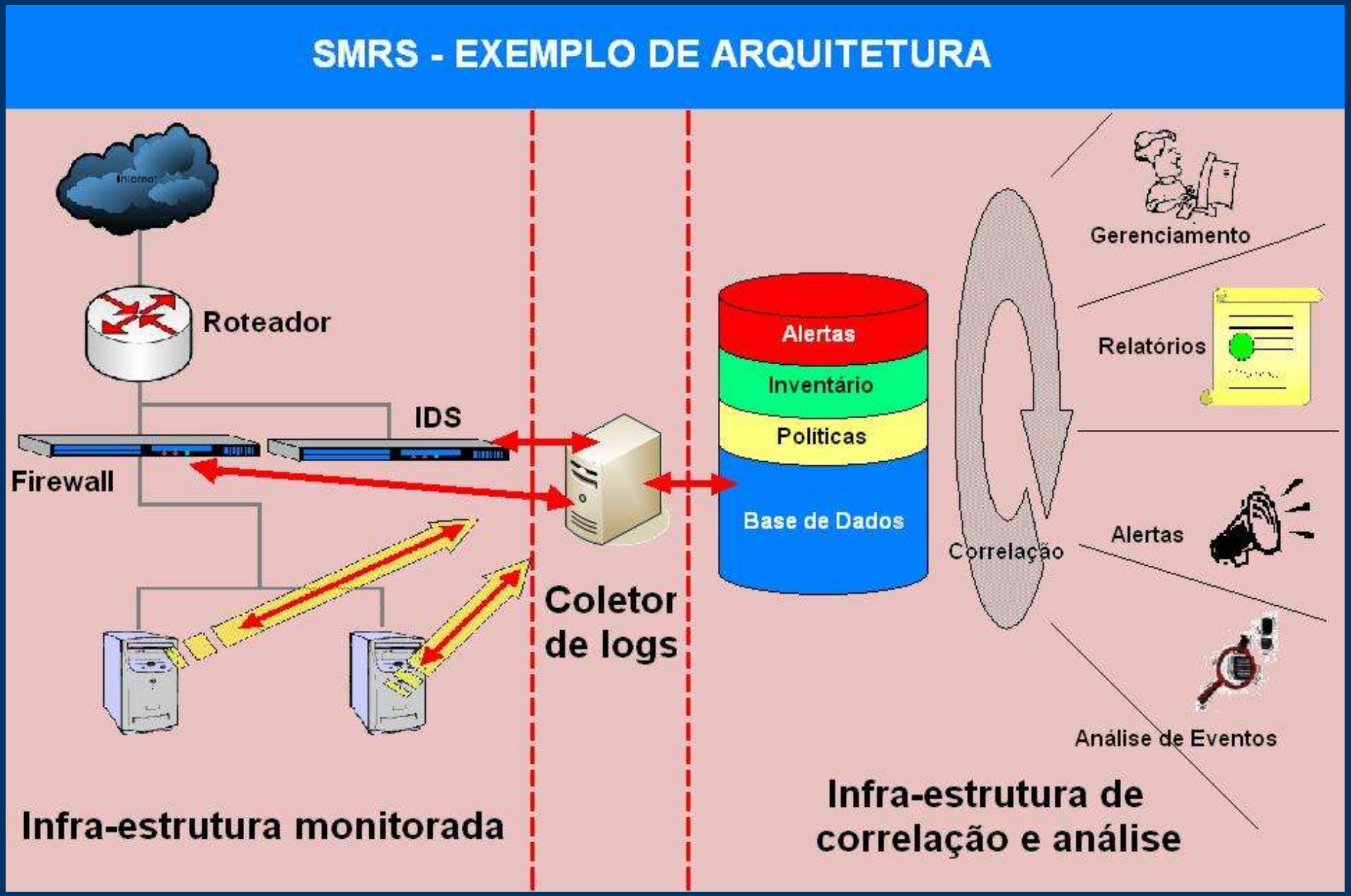
Solução: centralização dos logs.

- Como?

# Metodologia para Análise



# Metodologia para Análise



# *Metodologia para Análise*

- Metodologia para redução do número de logs

  - Ferramentas desenvolvidas
    - artificial_ignorance
      - Utiliza arquivo de configuração.
      - Informa a ocorrências de vários padrões não tratados.
    - logs_counter
      - Contabiliza a quantidade de linhas de logs a serem analisadas.
    - ...

# *Metodologia para Análise*

- Metodologia para geração de estatísticas
  - Acesso indevidos a servidores
  - Host Scans
  - Port Scans
  - Ferramentas desenvolvidas
    - port_counter
    - protocol_counter
    - ip_counter
    - access_by_country
    - ...

# *Metodologia para Análise*

- Metodologia para correlação de logs
  - Firewall-IDS-syslog
  - Syslog-syslog
  - Ferramentas desenvolvidas
    - http_correlator
    - pid_correlator
    - snort_http_correlator
    - iptables_summary
    - pf_summary
    - …

# *Metodologia para Análise*

- Metodologia para geração de relatórios
  - Um documento é gerado por um script.
  - O resultado de todas as análises é adicionado ao documento.
  - Os logs não descartados pela metodologia de redução devem ser avaliados.
  - Finalmente o relatório deve ser enviado para o responsável pela rede.

# Metodologia para Análise

```
ORGANIZACAO: ABC.com.br - ABC Network Consulting

##########################################
# Numero de registros examinados: 461858 #
##########################################

##############################################
# Servidores: 192.168.105.7 | 192.168.105.9 #
# Periodo: Tue May 30 0:00-24:00 2005       #
##############################################

############################
# Acessos aos servidores #
############################

- Total de Acessos:              9101  (100.00%)
- Acessos do Protocolo TCP:       442   (04.86%)
- Acessos do Protocolo UDP:       930   (10.22%)
- Acessos do Protocolo ICMP:     7726   (84.89%)
- Acessos do Protocolo IPv6:        0   (00.00%)
- Acessos de outros Protocolos:     3   (00.03%)
```

# Metodologia para Análise

```
##########################################
# Endereços IPs que mais acessaram a rede #
##########################################

 1.-   192.168.129.1:    343
 2.-  200.223.82.141:     14
 3.-   131.215.102.1:      9
 4.-   65.54.190.158:      6
 5.-      64.4.50.29:      5
 6.-   65.54.252.145:      5
 7.-     64.4.50.166:      4
 8.- 200.136.224.207:      4
 9.-  192.168.156.16:      4
 10.-   200.154.55.2:      4

################################################
# Portas de destino TCP mais acessadas na rede #
################################################

 1.-  113:    393
 2.- 3477:      6
 3.- 2168:      5
 4.- 1100:      5
 5.- 2499:      4
(...)
```

# Metodologia para Análise

```
##########################
# Eventos de baixo risco #
##########################

Servidor: 192.168.105.7
Servico : CONSOLE
--------------------------------
Numero de linhas de log analisadas     : 3
Numero de linhas analisadas manualmente: 0

Servidor: 192.168.105.7
Servico : CRON
--------------------------------
Numero de linhas de log analisadas     : 726
Numero de linhas analisadas manualmente: 0

Servidor: 192.168.105.7
Servico : HTTP
--------------------------------
Numero de linhas de log analisadas     : 123277
Numero de linhas analisadas manualmente: 92

Servidor: 192.168.105.7
Servico : HTTP_ERROR_LOG
(...)
```

# Metodologia para Análise

```
--------------------------------
Numero de linhas de log analisadas     : 2139
Numero de linhas analisadas manualmente: 72

Servidor: 192.168.105.7
Servico : MAILLOG
--------------------------------
Numero de linhas de log analisadas     : 2905
Numero de linhas analisadas manualmente: 137

Servidor: 192.168.105.7
Servico : MESSAGES
--------------------------------
Numero de linhas de log analisadas     : 376
Numero de linhas analisadas manualmente: 51

Servidor: 192.168.105.9
Servico : CONSOLE
--------------------------------
Numero de linhas de log analisadas     : 2
Numero de linhas analisadas manualmente: 0

Servidor: 192.168.105.9
Servico : CRON
(...)
```

# Metodologia para Análise

```
--------------------------------
Numero de linhas de log analisadas     : 792
Numero de linhas analisadas manualmente: 0

Servidor: 192.168.105.9
Servico : MAILLOG
--------------------------------
Numero de linhas de log analisadas     : 2111
Numero de linhas analisadas manualmente: 14

Servidor: 192.168.105.9
Servico : MESSAGES
--------------------------------
Numero de linhas de log analisadas     : 108
Numero de linhas analisadas manualmente: 2

###############
# Correlacoes #
###############

Servidor: 192.168.105.7
Servico : Snort
--------------------------------
Alertas  Descricao
(...)
```

# Metodologia para Análise

```
      34  WEB-IIS asp-dot attempt (Ref: bugtraq,1814, nessus,10363)
       4  WEB-IIS scripts-browse access (Ref: nessus,11032)
       2  WEB-MISC TrackerCam overly long php parameter overflow attempt
   (Ref: cve,2005-0481, bugtraq,12592)

Servidor: 192.168.105.7
Servico : HTTP
---------------------------------
IP de Origem: 10.0.0.1

HTTP ACCESS
10.0.0.1 - - [29/May/2005:23:22:58 -0300] "GET /
   default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%
   u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%
   u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0" 404 209

ASSINATURA DO ATAQUE: WEB-IIS ISAPI .ida attempt (Ref: arachnids,552,
   bugtraq,1065, cve,2000-0071)

HTTP ERROR
[Sun May 29 23:22:58 2005] [error] [client 10.0.0.1] File does not
   exist: /home/httpd/cenpra/default.ida
```

# Metodologia para Análise

```
Rede   : 192.168.0.0/16
Servico: Host Scan (ip: # de hosts diferentes acessados)
---------------------------------
 1.-   192.168.156.16:   2980
 2.-    61.129.81.223:   2723
 3.-    218.83.155.79:   2188
 4.-   61.143.210.214:   2072
 5.-      82.89.37.59:   1977
 6.-    64.94.239.228:   1101
 7.-     71.11.223.62:   1043
 8.-     67.159.5.193:    809
 9.-     192.168.2.91:    665
 10.- 202.111.175.191:    612

Rede   : 192.168.0.0/16
Servico: Port Scan (ip: # de portas diferentes acessadas)
---------------------------------
 1.-   61.129.81.223:   2878
 2.-  61.143.210.214:   2203
(...)
```

# Metodologia para Análise

```
 3.- 202.111.175.191:    636
 4.-     218.5.72.20:    500
 5.-  202.107.60.150:    459
 6.-   61.136.58.229:    427
 7.-   61.152.144.14:    308
 8.-   220.249.97.20:    289
 9.-    202.96.209.5:    227
 10.-  211.115.194.3:    203


##########################
# Eventos de Alto Risco #
##########################

Nenhum evento de alto risco observado.

####################
# Conclusao do dia #
####################

Nenhum ataque significativo observado.
```

# *Conclusão*

- Necessário armazenar os logs de forma segura para que eles possam ser analisados periodicamente.
- Redução do volume a ser analisado através de filtros.
- Uso e desenvolvimento de ferramentas para auxiliar as tarefas.
- Nem todos os logs podem ser correlacionados da mesma maneira.

# *Referências Bibliográficas*


[1] http://www.loganalysis.org

[2] http://ntsyslog.sourceforge.net

[3] S. Northcutt, L. Zeltser, S. Winters, K. K. Frederic, R. W. Ritcher. Inside Network Perimeter Security. New Riders. 2003.

[4] A. Lockhart. Network Security Hacks. O'Reilly. 2004.

[5] C. Peikari, A. Chuvakin. Security Warrior. O'Reilly. 2004

[6] K. Mandia, C. Prosise, M. Pepe. Incident Response & Computer Forensics. Mc Graw Hill. 2003.

# Contatos


Carlos Henrique P C Chaves
carlos.chaves@cenpra.gov.br

Lucio Henrique Franco
lucio.franco@cenpra.gov.br

Antonio Montes
antonio.montes@cenpra.gov.br


CenPRA
Centro de Pesquisas
Renato Archer

Honeynet.BR