Análise e Interpretação de *logs*

Cristine Hoepers

cristine@nic.br

Klaus Steding-Jessen

jessen@nic.br

NIC BR Security Office – NBSO

Comitê Gestor da Internet no Brasil

http://www.nbso.nic.br/

NBSO – NIC BR Security Office

- Mantido pelo Comitê Gestor da Internet no Brasil;
- Grupo de Resposta a Incidentes para a Internet Brasileira:
  - desenvolve documentação;
  - dá suporte ao processo de análise e recuperação de sistemas invadidos;
  - trabalha na conscientização sobre os problemas de segurança;
  - ajuda na criação de novos CSIRTs.

NBSO (cont.)

- Membro do FIRST (Forum of Incident Response and Security Teams)
  - Reúne CSIRTs de todo o mundo;
  - Desenvolve e dissemina práticas de segurança;
  - Promove e facilita a comunicação entre seus membros.

Objetivos deste Tutorial

- Destacar a importância de *logs* para administração e segurança de redes;
- Ajudar a priorizar *logs*;
- Apresentar ferramentas para auxílio na análise.

Material disponível em:

`http://www.nbso.nic.br/docs/palestras/`

Roteiro

- Definições
- Exemplos e Falsos Positivos
- Sanitização
- Ferramentas
- Backup e Rotação
- Estudos de Casos

Definições

Definições

Geração de *logs*

- Geração de registros de eventos ou estatíticas para prover informações sobre a utilização e performance de um sistema.

Definições (cont.)

Auditoria de *logs*

- Análise de *logs*, de forma a apresentar informações sobre um sistema de forma clara e compreensível;
- Técnica para determinar *a posteriori* violações de segurança.

Definições (cont.)

Logs

- Provêem mecanismos para:
  - Analisar o estado de segurança de um sistema;
  - Determinar uma seqüência de eventos que possa ter comprometido o sistema.

Definições (cont.)

Tipos de *Logs*:

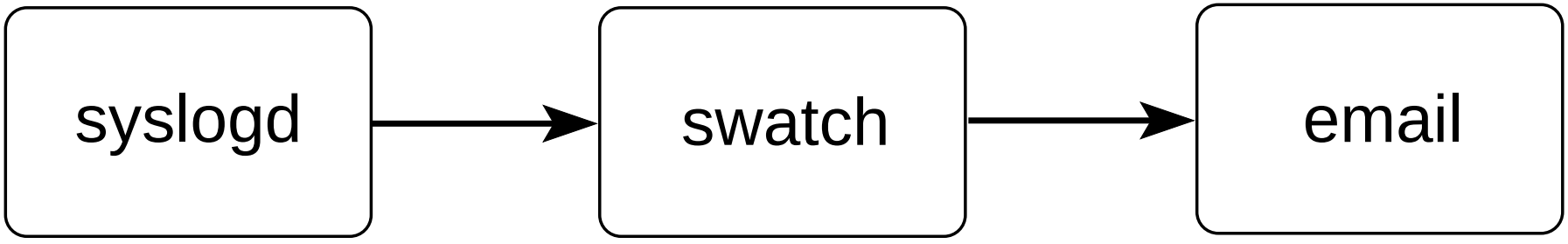
- do sistema;
- de aplicativos;
- de *firewalls*;
- de Sistemas de Detecção de Intrusão.

Definições (cont.)

Sistema de Auditoria de *Logs*

Definições (cont.)

Exemplo de um Sistema de Auditoria de *Logs*



Considerações

Considerações

- Que tipos de *logs* gerar
  - políticas da instituição;
- Objetivos dos *logs* sendo gerados;
- Qual o volume de dados gerado pelos *logs*;
- Topologia a utilizar
  - servidor centralizado;
- Quais ferramentas utilizar.

Considerações (cont.)

Informações contidas nos *logs*:

- Horário sincronizado;
- Máximo de informações possível;
- *Logs* relativos a tráfego de rede:
  - TTL, *flags*, protocolo, conteúdo do tráfego, etc.

Exemplos

Exemplos

```
INDICATOR: NETBIOS SMB C access
PACKETTIME: 12/19/02-16:23:08.814432
SOURCEADDRESS: 10.151.86.184
DESTINATIONADDRESS: 192.0.2.78
SOURCEPORT: TCP:1923
DESTINATIONPORT: TCP:139
EXTENDEDDATA: IP Header:    TCP Header:
  IP Ver: 4                   S Port: 1923
  HLen:   5                   D Port: 139
  Len:    107                 Seq:    49120462
  ID:     43203               Ack:    387121738
  TTL:    112                 Offset: 5
  Proto:  6                   Flags:  ACK PSH  (24)
  CSum:   38932               Window: 8572
                              CSum:   14650
```

Exemplos (cont.)

```
Information regarding the event(s) ORIGINATOR

_____________________________________________________

Details on ORIGINATOR:
Best Name: UNKNOWN
NetBIOS: UNKNOWN
DNS Name: UNKNOWN
Network Address: 10.176.213.12
MAC: UNKNOWN

_____________________________________________________

Information regarding the AFFECTED SYSTEM(S)

_____________________________________________________

Alert List:
Issue: FTP port probe
Parameter: port=21,reason=RSTsent
Time Stamp: 1/6/02 3:25:36 AM (GMT)
Count: 1
Target: TLC3
Target IP: 192.0.2.5
Detector: TLC3
Detector IP: 192.0.2.5
```

Exemplos (cont.)

```
Jan  2 21:38:06 host Feb 06 2080 02:32:53: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4516 dst inside:192.0.2.81/21
Jan  2 21:38:07 host Feb 06 2080 02:32:54: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4527 dst inside:192.0.2.85/21
Jan  2 21:38:07 host Feb 06 2080 02:32:54: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4534 dst inside:192.0.2.87/21
Jan  2 21:38:08 host Feb 06 2080 02:32:55: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4551 dst inside:192.0.2.88/21
Jan  2 21:38:08 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4557 dst inside:192.0.2.89/21
Jan  2 21:38:08 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4561 dst inside:192.0.2.90/21
Jan  2 21:38:09 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4566 dst inside:192.0.2.91/21
Jan  2 21:38:09 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4516 dst inside:192.0.2.81/21
```

Exemplos (cont.)

```
Jan 6 23:59:48 host PR4000 - [FILTER] Denied incomming TCP packet
from Slot #2 Port #1 Filter Name "Main" Rule 87 Source address
(10.229.133.67) Source Port 3746 Destination address (192.0.2.188)
Destination Port 80
Jan 6 23:59:48 host PR4000 - [FILTER] Denied incomming TCP packet
from Slot #2 Port #1 Filter Name "Main" Rule 87 Source address
(10.229.133.67) Source Port 3412 Destination address (192.0.2.28)
Destination Port 80
Jan 6 23:59:48 host PR4000 - [FILTER] Denied incomming TCP packet
from Slot #2 Port #1 Filter Name "Main" Rule 87 Source address
(10.229.133.67) Source Port 3426 Destination address (192.0.2.31)
Destination Port 80
Jan 6 23:59:49 host PR4000 - [FILTER] Denied incomming TCP packet
from Slot #2 Port #1 Filter Name "Main" Rule 87 Source address
(10.229.133.67) Source Port 3808 Destination address (192.0.2.65)
Destination Port 80
```

Exemplos (cont.)

```
"183578"  "4Jan2002"  "16:03:31"  "eth-
s2p1c0"  "192.0.2.252"  "log" =
 "drop"  "domain-
tcp"  "10.213.171.212"  "192.0.2.30"  "tcp"  "177"  =
"1356"  ""  ""  ""  ""  ""  ""  ""  ""  ""  "firewall"  " len 60" =20
"183579"  "4Jan2002"  "16:03:34"  "eth-
s2p1c0"  "192.0.2.252"  "log" =
 "drop"  "domain-
tcp"  "10.213.171.212"  "192.0.2.16"  "tcp"  "177"  =
"1342"  ""  ""  ""  ""  ""  ""  ""  ""  ""  "firewall"  " len 60" =20
"183580"  "4Jan2002"  "16:03:34"  "eth-
s2p1c0"  "192.0.2.252"  "log" =
 "drop"  "domain-
tcp"  "10.213.171.212"  "192.0.2.17"  "tcp"  "177"  =
"1343"  ""  ""  ""  ""  ""  ""  ""  ""  ""  "firewall"  " len 60" =20
"183581"  "4Jan2002"  "16:03:34"  "eth-
s2p1c0"  "192.0.2.252"  "log" =
 "drop"  "domain-
tcp"  "10.213.171.212"  "192.0.2.18"  "tcp"  "177"  =
```

Exemplos (cont.)

```
Jan  6 22:34:07 host screend[14398]: REJECT: UDP
[10.154.68.106]->[192.0.2.130](31790->31789) src interface RED dst
interface GREEN
Jan  6 22:34:07 host screend[14398]: REJECT: UDP
[10.154.68.106]->[192.0.2.133](31790->31789) src interface RED dst
interface GREEN
Jan  6 22:34:07 host screend[14398]: REJECT: UDP
[10.154.68.106]->[192.0.2.131](31790->31789) src interface RED dst
interface GREEN
Jan  6 22:34:07 host screend[14398]: REJECT: UDP
[10.154.68.106]->[192.0.2.132](31790->31789) src interface RED dst
interface GREEN
Jan  6 22:34:07 host screend[14398]: REJECT: UDP
[10.154.68.106]->[192.0.2.135](31790->31789) src interface RED dst
interface GREEN
Jan  6 22:34:07 host screend[14398]: REJECT: UDP
[10.154.68.106]->[192.0.2.137](31790->31789) src interface RED dst
interface GREEN
```

Exemplos (cont.)

```
230559;5Jan2002;12:10:33;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.96.1;ftp;1042;60;72;;;;;;;;;;;;;;;;;;;;
230580;5Jan2002;12:10:54;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.97.1;ftp;1301;60;72;;;;;;;;;;;;;;;;;;;;
230648;5Jan2002;12:11:13;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.98.1;ftp;1559;60;72;;;;;;;;;;;;;;;;;;;;
230782;5Jan2002;12:11:32;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.99.1;ftp;1815;60;72;;;;;;;;;;;;;;;;;;;;
230797;5Jan2002;12:11:53;192.168.3.1;log;drop;;sbif2;inbound;tcp;
10.132.68.10;207.5.100.1;ftp;2070;60;72;;;;;;;;;;;;;;;;;;;;
230812;5Jan2002;12:12:12;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.101.1;ftp;2328;60;72;;;;;;;;;;;;;;;;;;;;
230837;5Jan2002;12:12:32;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.102.1;ftp;2591;60;72;;;;;;;;;;;;;;;;;;;;
230851;5Jan2002;12:12:53;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.103.1;ftp;2846;60;72;;;;;;;;;;;;;;;;;;;;
230871;5Jan2002;12:13:13;192.168.3.2;log;drop;;sbif9;inbound;tcp;
10.132.68.10;207.5.104.1;ftp;3101;60;72;;;;;;;;;;;;;;;;;;;;
```

Exemplos (cont.)

```
< Jan  7 14:36:20  ipmon[51]: 14:36:20.173630 de0 @0:2 b
10.175.94.110,1872 -> xxx.xxx.xxx.xxx,79 PR tcp len 20 12288 -S IN
< Jan  7 14:36:21  ipmon[51]: 14:36:20.742919 de0 @0:2 b
10.175.94.110,1874 -> xxx.xxx.xxx.xxx,110 PR tcp len 20 12288 -S IN
< Jan  7 14:36:21  ipmon[51]: 14:36:20.934602 de0 @0:2 b
10.175.94.110,1877 -> xxx.xxx.xxx.xxx,113 PR tcp len 20 12288 -S IN
< Jan  7 14:36:22  ipmon[51]: 14:36:21.597870 de0 @0:2 b
10.175.94.110,1881 -> xxx.xxx.xxx.xxx,1080 PR tcp len 20 12288 -S IN
< Jan  7 14:36:22  ipmon[51]: 14:36:21.667955 de0 @0:2 b
10.175.94.110,1882 -> xxx.xxx.xxx.xxx,3128 PR tcp len 20 12288 -S IN
< Jan  7 14:36:22  ipmon[51]: 14:36:21.713096 de0 @0:2 b
10.175.94.110,1883 -> xxx.xxx.xxx.xxx,5741 PR tcp len 20 12288 -S IN
< Jan  7 14:36:23  ipmon[51]: 14:36:23.166470 de0 @0:2 b
10.175.94.110,1872 -> xxx.xxx.xxx.xxx,79 PR tcp len 20 12288 -S IN
< Jan  7 14:36:24  ipmon[51]: 14:36:23.672768 de0 @0:2 b
10.175.94.110,1874 -> xxx.xxx.xxx.xxx,110 PR tcp len 20 12288 -S IN
```

Exemplos (cont.)

Timestamp	Protocol	Source IP:Port	Destination IP:Port
Jan 7 13:18:35	UDP	10.45.32.134:32870	TARGET:33474
Jan 7 13:18:40	UDP	10.45.32.134:32870	TARGET:33475
Jan 7 13:18:45	UDP	10.45.32.134:32870	TARGET:33476
Jan 7 13:18:50	UDP	10.45.32.134:32870	TARGET:33477
Jan 7 13:18:55	UDP	10.45.32.134:32870	TARGET:33478
Jan 7 13:19:00	UDP	10.45.32.134:32870	TARGET:33479
Jan 7 13:19:05	UDP	10.45.32.134:32870	TARGET:33480
Jan 7 13:19:10	UDP	10.45.32.134:32870	TARGET:33481
Jan 7 13:19:15	UDP	10.45.32.134:32870	TARGET:33482
Jan 7 13:19:20	UDP	10.45.32.134:32870	TARGET:33483
Jan 7 13:19:25	UDP	10.45.32.134:32870	TARGET:33484
Jan 7 13:19:30	UDP	10.45.32.134:32870	TARGET:33485
Jan 7 13:19:35	UDP	10.45.32.134:32870	TARGET:33486
Jan 7 13:19:40	UDP	10.45.32.134:32870	TARGET:33487
Jan 7 13:19:45	UDP	10.45.32.134:32870	TARGET:33488
Jan 7 13:19:50	UDP	10.45.32.134:32870	TARGET:33489

Exemplos (cont.)

```
12/30/2001 19:54:41 -> 12/30/2001 19:54:42    6  11 192.0.2.122
22 <->  01 10.190.39.99          3433 4         243         00 FS-PA-
12/30/2001 19:54:41 -> 12/30/2001 19:54:42    6  101 10.190.39.99
3346 <->  02 192.0.2.35           22 4          216         00 FS--A-
12/30/2001 19:54:41 -> 12/30/2001 19:54:42    6  101 10.190.39.99
3351 <->  02 192.0.2.40           22 5          244         00 FSR-A-
12/30/2001 19:54:41 -> 12/30/2001 19:54:42    6  101 10.190.39.99
3352 <->  02 192.0.2.41           22 5          244         00 FSR-A-
12/30/2001 19:54:41 -> 12/30/2001 19:54:42    6  101 10.190.39.99
3385 <->  02 192.0.2.74           22 3          164         00 FS--A-
12/30/2001 19:54:41 -> 12/30/2001 19:54:42    6  101 10.190.39.99
3415 <->  02 192.0.2.104          22 4          216         00 FS--A-
12/30/2001 19:54:41 -> 12/30/2001 19:54:42    6  101 10.190.39.99
3433 <->  02 192.0.2.122          22 6          284         00 FSR-A-
12/30/2001 19:54:42 -> 12/30/2001 19:54:42    6  11 192.0.2.74
22 <->  01 10.190.39.99          3385 2         119         10 F--PA-
12/30/2001 19:54:42 -> 12/30/2001 19:54:42    6  01 10.190.39.99
3385 <->  11 192.0.2.74           22 2          80          10 --R---
```

Exemplos (cont.)

```
Jan 14 05:51:00.169312 rule 2/0(match): block in on fxp0:
10.206.132.12 > xx.xx.xx.xx: icmp: echo request

Jan 14 05:51:00.170933 rule 2/0(match): block in on fxp0:
10.206.132.12 > xx.xx.xx.xx: icmp: address mask request

Jan 14 05:51:00.182242 rule 2/0(match): block in on fxp0:
10.206.132.12 > xx.xx.xx.xx: icmp: time stamp request

Jan 14 05:51:00.192393 rule 2/0(match): block in on fxp0:
10.206.132.12 > xx.xx.xx.xx: icmp: information request

Jan 14 05:51:00.205672 rule 2/0(match): block in on fxp0:
10.206.132.12 > xx.xx.xx.xx: icmp: echo request
```

Exemplos (cont.)

```
Jan 07 17:57:38.346281 10.0.32.23 > 224.0.0.2: igmp
leave 224.0.0.9 [ttl 1]
Jan 07 17:57:38.346311 10.0.32.23 > 224.0.0.2: igmp
leave 224.0.0.9 [ttl 1]
Jan 07 19:29:24.514578 10.0.32.16 > 224.0.0.2: igmp
leave 224.0.0.9 [ttl 1]
Jan 07 19:29:24.514609 10.0.32.16 > 224.0.0.2: igmp
leave 224.0.0.9 [ttl 1]
Jan 08 08:25:28.961183 10.0.32.16 > 224.0.0.9: igmp
nreport 224.0.0.9 [ttl 1]
Jan 08 08:25:28.961209 10.0.32.16 > 224.0.0.9: igmp
nreport 224.0.0.9 [ttl 1]
Jan 08 08:26:06.833689 10.0.32.23 > 224.0.0.9: igmp
nreport 224.0.0.9 [ttl 1]
Jan 08 08:26:06.833716 10.0.32.23 > 224.0.0.9: igmp
nreport 224.0.0.9 [ttl 1]
Jan 08 08:32:44.073313 10.0.32.11 > 224.0.0.9: igmp
nreport 224.0.0.9 [ttl 1]
```

Exemplos (cont.)

```
Jan 8 23:13:33 srv [797]: attackalert: Host: 10.195.7.80 is
already blocked. Ignoring
Jan 8 23:13:33 srv [797]: attackalert: Connect from host:
10.195.7.80/10.195.7.80 to TCP port: 79
Jan 8 23:12:11 srv [797]: attackalert: Host: 10.195.7.80 is
already blocked. Ignoring
Jan 8 23:12:11 srv [797]: attackalert: Connect from host:
10.195.7.80/10.195.7.80 to TCP port: 119
Jan 8 23:11:58 srv [797]: attackalert: Connect from host:
10.195.7.80/10.195.7.80 to TCP port: 79
```

Exemplos (cont.)

```
Jan  8 08:02:41 192.0.2.129 500466: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1053) -> 192.0.2.1(27374), 1 packet
Jan  8 08:03:26 192.0.2.129 500469: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1054) -> 192.0.2.2(27374), 1 packet
Jan  8 08:04:11 192.0.2.129 500471: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1055) -> 192.0.2.3(27374), 1 packet
Jan  8 08:04:56 192.0.2.129 500473: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1059) -> 192.0.2.4(27374), 1 packet
Jan  8 08:05:41 192.0.2.129 500475: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1063) -> 192.0.2.5(27374), 1 packet
Jan  8 08:06:26 192.0.2.129 500479: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1064) -> 192.0.2.6(27374), 1 packet
Jan  8 08:07:11 192.0.2.129 500480: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1065) -> 192.0.2.7(27374), 1 packet
Jan  8 08:07:46 192.0.2.129 500481: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1053) -> 192.0.2.1(27374), 3 packets
Jan  8 08:07:56 192.0.2.129 500484: 14w0d: %SEC-6-IPACCESSLOGP: list
150 denied tcp 10.158.52.28(1075) -> 192.0.2.8(27374), 1 packet
```

Exemplos (cont.)

```
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.102  1149
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.128  1176
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.131  1179
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.133  1181
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.136  1184
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.139  1187
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.141  1189
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.144  1192
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.147  1195
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.149  1197
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.153  1201
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.156  1204
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.159  1207
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.161  1209
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.164  1212
10-Jan-02   2:34:16   sunrpc  10.216.242.242 xxx.xx.xx.167  1215
```

Exemplos (cont.)

```
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.217 s_port 2237 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.212 s_port 2232 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.209 s_port 2229 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.206 s_port 2226 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.203 s_port 2223 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.214 s_port 2234 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.198 s_port 2218 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.223 s_port 2243 rule 74
14Jan2002 12/30/99 12:30:52 drop vitima.net >qfe0 tcp src
10.216.242.242 service sunrpc dst 192.0.2.193 s_port 2213 rule 74
```

Exemplos (cont.)

```
Jan 12 17:16:27 host1 Message forwarded from host1: sshd2[10294]:
refused connect from 10.193.138.129
Jan 12 17:16:29 host1 Message forwarded from host1: sshd2[18626]:
refused connect from 10.193.138.129
Jan 12 18:38:37 host2 Message forwarded from host2: sshd2[18832]:
refused connect from 10.193.138.129
Jan 12 18:38:42 host3 Message forwarded from host3: sshd2[39712]:
refused connect from 10.193.138.129
Jan 12 18:38:42 host3 Message forwarded from host3: sshd2[42548]:
refused connect from 10.193.138.129
Jan 12 18:39:04 host4 Message forwarded from host4:
sshd2[33580]: refused connect from 10.193.138.129
Jan 12 18:06:38 host5 sshd[19771]: refused connect from 10.193.138.129
Jan 12 18:06:39 host5 sshd[19772]: refused connect from 10.193.138.129
```

Exemplos (cont.)

```
4,1617990,2001/07/03,06:33:49,2001/07/02,23:33:49,10008,1,
2003,OUT,IN,1,3000,80,TCP/IP,10.195.224.3,xxx.xx.xxx.xx,
42085,80,0.0.0.0,2072962083
4,1617992,2001/07/03,06:33:49,2001/07/02,23:33:49,10008,1,
2003,OUT,IN,4,5081,0,TCP/IP,10.195.224.3,xxx.xx.xxx.xx,
42085,80,0.0.0.0,/system32/cmd.exe,474554202F6D736164632F2
E2E2535632E2E2535632E2E2535632E2E2535632E2E2535632E2E25356
32E2E2535632E2E2535632E2E2535632E2E2535632E2E2535632E2E253
56377696E6E742F737974656D33322F636D642E6578653F2F632B646
9722048545450ZZ
3,1618010,2001/07/03,06:33:54,2001/07/02,23:33:54,10003,1,
2003,10008,1,2003,EXEC ShunHost 10.195.224.3 1440
```

Exemplos (cont.)

```
Mar 26 20:49:27 host spamd[20373]: 10.137.225.30:
-> <helloseed@hotpop.com>
Mar 28 03:39:24 host spamd[20373]: 10.137.244.50:
-> <helloseed@hotpop.com>
Apr  3 00:13:41 host spamd[20373]: 10.70.153.112:
-> <ameill@19.com.cn>
```

Exemplos (cont.)

```
15:52:55.642713 10.150.134.123.2191 > 192.0.2.78.135: udp 724
0x0000   4500 02f0 312d 0000 6a11 8c0b 0a96 867b      E...1-..j.......
0x0010   c000 024e 088f 0087 02dc 0fc1 0400 0800      Dd.N............
0x0020   1000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   0000 0000 f891 7b5a 00ff d011 a9b2 00c0      .......Z........
0x0040   4fb6 e6fc b102 9b00 bbff af4d af0f 13a0      O..........M....
0x0050   a442 5c67 0000 0000 0100 0000 0000 0000      .B.g............
0x0060   0000 ffff ffff 8402 0000 0000 0900 0000      ................
0x0070   0000 0000 0900 0000 5745 4250 4f50 5550      ........WEBPOPUP
0x0080   0000 0000 0100 0000 0000 0000 0100 0000      ................
0x0090   0000 0000 4f02 0000 0000 0000 4f02 0000      ....O.......O...
0x00a0   5520 4e20 4920 5620 4520 5220 5320 4920      U.N.I.V.E.R.S.I.
0x00b0   5420 5920 2020 4420 4920 5020 4c20 4f20      T.Y...D.I.P.L.O.
0x00c0   4d20 4120 530d 0a0d 0a4f 6274 6169 6e20      M.A.S....Obtain.
0x00d0   6120 7072 6f73 7065 726f 7573 2066 7574      a.prosperous.fut
0x00e0   7572 652c 206d 6f6e 6579 2065 6172 6e69      ure,.money.earni
0x00f0   6e67 2070 6f77 6572 2c0d 0a61 6e64 2074      ng.power,..and.t
0x0100   6865 2061 646d 6972 6174 696f 6e20 6f66      he.admiration.of
```

Sanitização de *Logs*

Sanitização de Logs

- Várias informações sensíveis: IPs, hostnames, interfaces, endereços MAC, regras do *firewall*, *uptime*, topologia, etc;
- Importante na notificação de incidentes e postagem de *logs* em listas públicas;
- Pode ser necessária segundo a política da instituição.

Sanitização de Logs (cont.)

```
Dec 18 12:17:55 manjuba kernel: Packet log: input
DENY eth2 PROTO=6 10.195.155.18:61767 192.0.2.1:22
L=60 S=0x00 I=62979 F=0x4000 T=51 SYN (#66)

Mar 26 18:35:21.944042 rule 4/0(match): block in on fxp0:
220.117.130.143.22 > 192.0.2.10.22: tcp 0
```

Sanitização de Logs (cont.)

```
Mar  4 08:12:19 192.0.2.70 5532: 2d14h: %SEC-6-IPACCESSLOGP:
list 150 denied tcp 210.119.136.41(111) -> 192.0.2.75(111),
1 packet

Dec 15 06:23:24 intranet kernel: IN=eth1 OUT=
MAC=ff:ff:ff:ff:ff:ff:00:c0:05:03:38:24:08:00
SRC=10.163.48.193 DST=192.0.2.255 LEN=60
TOS=0x10 PREC=0x00 TTL=52 ID=5942 DF PROTO=TCP
SPT=1859 DPT=21 WINDOW=5840 RES=0x00 SYN URGP=0
```

Sanitização de Logs – ASCII

- Substituição de informações sensíveis por “xxx”, “xxx.xxx.xxx.xxx”, “a.b.c.d”, “192.168.xxx.xxx”, etc;
- Simples, se envolver apenas informações do cabeçalho;
- Pode ser automatizado com um *script*;
- Pode gerar um formato de saída genérico;
- Suporte em algumas ferramentas (`snort -0`).

Sanitização de Logs – ASCII (cont.)

Ocultação de um /24:

```
Jun  9 07:32:20 10.248.155.75:22 -> xx.xx.xx.38:22 SYNFIN
Jun  9 07:32:20 10.248.155.75:22 -> xx.xx.xx.39:22 SYNFIN
Jun  9 07:32:20 10.248.155.75:22 -> xx.xx.xx.51:22 SYNFIN
Jun  9 07:32:21 10.248.155.75:22 -> xx.xx.xx.101:22 SYNFIN
Jun  9 07:32:21 10.248.155.75:22 -> xx.xx.xx.103:22 SYNFIN
Jun  9 07:32:21 10.248.155.75:22 -> xx.xx.xx.104:22 SYNFIN
```

Sanitização de Logs – ASCII (cont.)

Várias informações removidas:

```
Dec 15 06:23:24 host kernel: IN=if_name OUT= MAC=xxx
SRC=10.163.48.193 DST=xxx.xxx.xxx.xxx LEN=60 TOS=0x10
PREC=0x00 TTL=52 ID=5942 DF PROTO=TCP SPT=1859 DPT=21
WINDOW=5840 RES=0x00 SYN URGP=0
```

Tráfego bidirecional. Uso de rede reservada:

```
Mar 25 05:53:59 host ipmon[xxxxx]: 05:53:59.065060 if_name
@xx:xx p 10.227.161.161 -> 192.168.0.1 PR icmp len 20 60
icmp echo/0 K-S IN
Mar 25 05:53:59 host ipmon[xxxxx]: 05:53:59.065149 if_name
@xx:xx p 192.168.1.1 -> 10.227.161.161 PR icmp len 20 60
icmp echoreply/0 K-S OUT
```

Sanitização de Logs – ASCII (cont.)

Erro comum:

```
Mar 25 16:19:24.854670 10.248.245.122.999 > xxx.xxx.xxx.xxx.1024:  udp
  0000: 4500 0450 6855 0000 3611 0000 0af8 f57a  ................
  0010: c000 0201 03e7 0400 043c 30d1 50c3 0302  ................
  0020: 0000 0000 0000 0002 0001 86b8 0000 0001  ................
  0030: 0000 0001 0000 0001 0000 0020 3e80 a122  ................
  0040: 0000 0009 6c6f 6361 6c68 6f73 7400 0000  ....localhost...
  0050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
  0060: 0000 0000 0000 03e7 18f7 ffbf 18f7 ffbf  ................
  0070: 1af7 ffbf 1af7 ffbf 2538 7825 3878 2538  ........%8x%8x%8
  0080: 7825 3878 2538 7825 3878 2538 7825 3878  x%8x%8x%8x%8x%8x
  00c0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
```

Sanitização de Logs – ASCII (cont.)

Erro comum: sanitizar o cabecalho ASCII e esquecer do cabecalho hexa:

```
Mar 25 16:19:24.854670 10.248.245.122.999 > xxx.xxx.xxx.xxx.1024:  udp
  0000: 4500 0450 6855 0000 3611 0000 0af8 f57a  ...............
  0010: c000 0201 03e7 0400 043c 30d1 50c3 0302  ...............
  0020: 0000 0000 0000 0002 0001 86b8 0000 0001  ...............
  0030: 0000 0001 0000 0001 0000 0020 3e80 a122  ...............
  0040: 0000 0009 6c6f 6361 6c68 6f73 7400 0000  ....localhost...
  0050: 0000 0000 0000 0000 0000 0000 0000 0000  ...............
  0060: 0000 0000 0000 03e7 18f7 ffbf 18f7 ffbf  ...............
  0070: 1af7 ffbf 1af7 ffbf 2538 7825 3878 2538  ........%8x%8x%8
  0080: 7825 3878 2538 7825 3878 2538 7825 3878  x%8x%8x%8x%8x%8x
  00c0: 9090 9090 9090 9090 9090 9090 9090 9090  ...............
```

0xC000 0201 == 192.0.2.1

Sanitização de Logs – binários

- Geralmente em formato libpcap;
- Algumas ferramentas sanitizam apenas IPs do cabecalho (`snort -B mask`);
- Sanitização efetiva pode não ser trivial;
  - recálculo de checksum;
  - o conteúdo dos pacotes pode conter endereços IP (ICMP de erro, por exemplo);
  - *banners* de SMTP, HTTP, etc;
  - pura substituição hexa pode destruir conteúdo.

Ferramentas

Ferramentas de Análise de Logs

Problemas da análise de *logs*:

- Volume muito grande
  - servidores e *hosts*;
  - roteadores;
  - *firewalls*;
  - IDSs;
- Tarefa pode ser muito tediosa.

Ferramentas de Análise de Logs

AI (Artificial Ignorance)

- Idéia de Marcus Ranum. Detalhes em:

  `http://archives.neohapsis.com/archives/nfr-wizards/1997/09/0098.html`

- Condensar linhas de *logs* iguais;
- Filtrar os eventos que não são de interesse;
- Inicialmente proposto para *logs* de *syslog*, mas pode ser usado também com outros *logs*, como alertas de *snort*.

Ferramentas de Análise de Logs

AI (Exemplo)

```
1  postfix/smtpd: reject: RCPT from unknown[10.49.117.227]:
   554 <china9988@21cn.com>: Relay access denied;
1  named: client 10.54.164.132#1956: query 'VERSION.BIND/CH' denied
1  login: 1 LOGIN FAILURE ON ttyC0, l;'
1  /bsd: aac0: ** Battery is Charging
1  /bsd: aac0: ** Battery charge is now OK
2  sshd: Did not receive identification string from 10.194.124.207
```

- Uma ferramenta que usa esse princípio: `syslog-summary`.

Ferramentas de Análise de Logs

Ferramentas podem facilitar:

- *Parser* e sumário de *logs* de *firewall*: `fwlogwatch`, `pixlog`;
- Sumário de *logs* de mail: `pflogsumm`, `smtpstats`;
- Sumário de *logs* de servidores web: `analog`;
- Alertas: `logsurfer`, `swatch`;
- Algumas podem ser integradas com *scripts* de notificação diária (`/etc/daily`, etc).

Ferramentas de Análise de Logs

Muitas ferramentas e documentação em:

http://www.counterpane.com/log-analysis.html

Rotação e Backups

Rotação

Ferramentas como `newsyslog`.
Importância:

- Comprimir arquivos grandes de *log*;
- Conveniência: rotação por tamanho, idade, etc;
- Não lotar *filesystems*.

Riscos:

- Sobreescrita de *logs*.

Backup

- Armazenar *logs* off-line, conforme política da instituição.

Confidencialidade:

- Segurança física;
- Criptografar *logs* sensíveis.

Estudo de Caso 1

Estudo de Caso 1

Logs:

```
Date-Time                Proto Source Address          Destination Address
12/30-01:52:59.201441 TCP 10.174.165.2:3916 -> 192.0.2.1:80
12/30-01:52:59.201489 TCP 10.174.165.2:3916 -> 192.0.2.1:80
12/30-01:52:59.321365 TCP 10.174.165.2:3917 -> 192.0.2.1:80
12/30-01:52:59.321411 TCP 10.174.165.2:3917 -> 192.0.2.1:80
12/30-01:52:59.441386 TCP 10.174.165.2:3918 -> 192.0.2.1:80
12/30-01:52:59.441432 TCP 10.174.165.2:3918 -> 192.0.2.1:80
12/30-01:52:59.561826 TCP 10.174.165.2:3919 -> 192.0.2.1:80
12/30-01:52:59.561874 TCP 10.174.165.2:3919 -> 192.0.2.1:80
12/30-01:52:59.681380 TCP 10.174.165.2:3920 -> 192.0.2.1:80
12/30-01:52:59.681426 TCP 10.174.165.2:3920 -> 192.0.2.1:80
12/30-01:52:59.799026 TCP 10.174.165.2:3921 -> 192.0.2.1:80
12/30-01:52:59.799091 TCP 10.174.165.2:3921 -> 192.0.2.1:80
12/30-01:52:59.921438 TCP 10.174.165.2:3922 -> 192.0.2.1:80
12/30-01:52:59.921483 TCP 10.174.165.2:3922 -> 192.0.2.1:80
12/30-01:53:00.062038 TCP 10.174.165.2:3923 -> 192.0.2.1:80
```

Estudo de Caso 1 (Cont.)

Conteúdo dos pacotes vindos de 10.174.165.2:

```
000 : 47 45 54 20 2F 2F 2F 65 64 69 74 5F 69 6D 61 67   GET ///edit_imag
010 : 65 2E 70 68 70 3F 64 6E 3D 31 26 75 73 65 72 66   e.php?dn=1&userf
020 : 69 6C 65 3D 2F 65 74 63 2F 70 61 73 73 77 64 26   ile=/etc/passwd&
030 : 75 73 65 72 66 69 6C 65 5F 6E 61 6D 65 3D 25 32   userfile_name=%2
040 : 30 3B 6C 73 3B 25 32 30 20 48 54 54 50 2F 31 2E   0;ls;%20 HTTP/1.
050 : 30 0D 0A 56 69 61 3A 20 31 2E 30 20 70 72 6F 78   0..Via: 1.0 prox
060 : 79 2E 78 78 78 2E 78 78 78 2E 62 72 3A 33 31 32   y.xxx.xxx.br:312
070 : 38 20 28 53 71 75 69 64 2F 32 2E 34 2E 53 54 41   8 (Squid/2.4.STA
080 : 42 4C 45 37 29 0D 0A 58 2D 46 6F 72 77 61 72 64   BLE7)..X-Forward
090 : 65 64 2D 46 6F 72 3A 20 20 31 30 2E 32 30 38 2E   ed-For:  10.208.
0a0 : 32 34 39 2E 33 32 0D 0A 48 6F 73 74 3A 20 31 39   249.32..Host: 19
0b0 : 32 2E 30 2E 30 2E 32 2E 2E 0D 0A 20 20 43 61 63   2.0.2.1..    Cac
0c0 : 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20 6D 61 78 2D   he-Control: max-
0d0 : 61 67 65 3D 32 35 39 32 30 30 0D 0A 43 6F 6E 6E   age=259200..Conn
0e0 : 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69   ection: keep-ali
0f0 : 76 65 0D 0A 0D 0A                                 ve....
```

Estudo de Caso 1 (Cont.)

Logs:

```
12/30-01:50:47.839101 TCP 10.208.249.32:1393 -> 192.0.2.1:21
12/30-01:50:47.839181 TCP 10.208.249.32:1393 -> 192.0.2.1:21
12/30-01:50:47.877629 TCP 10.208.249.32:1393 -> 192.0.2.1:21
12/30-01:50:47.877733 TCP 10.208.249.32:1393 -> 192.0.2.1:21
12/30-01:51:06.697551 TCP 10.208.249.32:1395 -> 192.0.2.1:21
12/30-01:51:06.697575 TCP 10.208.249.32:1395 -> 192.0.2.1:21
12/30-01:51:06.749194 TCP 10.208.249.32:1395 -> 192.0.2.1:21
12/30-01:51:06.749303 TCP 10.208.249.32:1395 -> 192.0.2.1:21
12/30-01:51:06.817425 TCP 10.208.249.32:1395 -> 192.0.2.1:21
12/30-01:51:06.817531 TCP 10.208.249.32:1395 -> 192.0.2.1:21
12/30-01:51:13.788340 TCP 10.208.249.32:1397 -> 192.0.2.1:21
12/30-01:51:13.788393 TCP 10.208.249.32:1397 -> 192.0.2.1:21
12/30-01:51:13.829628 TCP 10.208.249.32:1397 -> 192.0.2.1:21
12/30-01:51:13.829735 TCP 10.208.249.32:1397 -> 192.0.2.1:21
12/30-01:51:13.888751 TCP 10.208.249.32:1397 -> 192.0.2.1:21
12/30-01:51:13.888858 TCP 10.208.249.32:1397 -> 192.0.2.1:21
```

Estudo de Caso 1 (Cont.)

Logs:

```
000 : 75 73 65 72 20 61 6E 6F 6E 79 6D 6F 75 73 0D 0A   user anonymous..
010 : 70 61 73 73 20 6D 69 61 61 61 61 61 61 0D 0A 75   pass miaaaaaa..u
020 : 73 65 72 20 61 6E 6F 6E 79 6D 6F 75 73 0D 0A 70   ser anonymous..p
030 : 61 73 73 20 6E 69 61 61 61 61 61 61 0D 0A 75 73   ass niaaaaaa..us
040 : 65 72 20 61 6E 6F 6E 79 6D 6F 75 73 0D 0A 70 61   er anonymous..pa
050 : 73 73 20 6F 69 61 61 61 61 61 61 0D 0A 75 73 65   ss oiaaaaaa..use
060 : 72 20 61 6E 6F 6E 79 6D 6F 75 73 0D 0A 70 61 73   r anonymous..pas
070 : 73 20 70 69 61 61 61 61 61 61 0D 0A 75 73 65 72   s piaaaaaa..user
080 : 20 61 6E 6F 6E 79 6D 6F 75 73 0D 0A 70 61 73 73    anonymous..pass
090 : 20 71 69 61 61 61 61 61 61 0D 0A 75 73 65 72 20    qiaaaaaa..user
0a0 : 61 6E 6F 6E 79 6D 6F 75 73 0D 0A 70 61 73 73 20   anonymous..pass
0b0 : 72 69 61 61 61 61 61 61 0D 0A 75 73 65 72 20 61   riaaaaaa..user a
0c0 : 6E 6F 6E 79 6D 6F 75 73 0D 0A 70 61 73 73 20 73   nonymous..pass s
0d0 : 69 61 61 61 61 61 61 0D 0A 75 73 65 72 20 61 6E   iaaaaaa..user an
0e0 : 6F 6E 79 6D 6F 75 73 0D 0A 70 61 73 73 20 74 69   onymous..pass ti
0f0 : 61 61 61 61 61 61 0D 0A 75 73 65 72 20 61 6E 6F   aaaaaa..user ano
```

Estudo de Caso 2

Estudo de Caso 2

Logs disponíveis:

```
[**] IDS246 - MISC - Large ICMP Packet [**]
06/23-20:48:34.516346 x.x.x.x -> x.x.x.x
ICMP TTL:239 TOS:0x0 ID:15191  DF
ID:39612   Seq:57072  ECHO
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Estudo de Caso 2 (cont.)

Primeiras conclusões:

- TTL 239 – Unix?
- pacotes grandes de ICMP – DoS? Outro ataque?

Estudo de Caso 2 (cont.)

Observações posteriores:

- Pacotes vinham de servidores de *email*;
- Poucos pacotes;
- Horário próximo ao de troca de mensagens;

Estudo de Caso 2 (cont.)

Após contactar responsáveis pelas redes:

- Servidores AIX 4.3.3;
- Com *path mtu discovery* habilitado:
  - `udp_pmtu_discover = 1`;
  - `tcp_pmtu_discover = 1`;
- TTL inicial do AIX:
  - 60 para UDP e TCP;
  - 255 para ICMP.

Estudo de Caso 3

Estudo de Caso 3

Fatos iniciais:

- Fulano acusado de ter tentado um *defacement* e, não conseguindo, ter apagado informações do sevidor;
- Evidências: *logs* de IIS da empresa A e *logs* de acesso do provedor X;
- Fulano confirma que estava conectado na data e hora apontadas pela empresa A, mas nega participação.

Estudo de Caso 3 (cont.)

Logs do IIS:

- *Logs* de um *defacement* feito no dia 11;
- *Logs* de ataques que envolviam o IP de Fulano são do dia 19;
- os *Logs* indicavam um ataque vindo de uma pessoa usando *Windows*. Fulano é usuário de *Mac*.

Estudo de Caso 3 (cont.)

Trechos dos *logs* com o IP de Fulano:

```
yyyy-mm-19 06:19:03 atacante - vitima 80 GET /msadc/../
../../../../../../..//winnt/system32/cmd.exe/c%20 dir 200
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)

yyyy-mm-19 06:19:05 atacante - vitima 80 GET /cgi-bin/../
../../../../../../..//winnt/system32/cmd.exe/c%20 dir 200
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)

yyyy-mm-19 06:26:30 atacante - vitima 80 GET /form.asp
own=grupo 200 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;
+DigExt)
```

Estudo de Caso 3 (cont.)

Informações **não** fornecidas pela empresa A:

- Timezone dos *logs*;
- Confirmação sobre a sincronia do relógio da máquina comprometida.

Estudo de Caso 3 (cont.)

Processo de identificação do usuário pelo provedor X:

- Assumiu todos os horários como *localtime*;
- Não considerou atrasos de seu próprio servidor:
  - Fulano possuía NTP na máquina;
  - Horário do provedor X estava 12 minutos adiantado.

Estudo de Caso 3 (cont.)

Logs do IIS da empresa A estavam em formato "W3C Extended".

"W3C Extended format is a customizable ASCII format with a variety of different fields. You can include fields important to you, while limiting log size by omitting unwanted fields. Fields are separated by spaces. Time is recorded as UTC (Greenwich Mean Time)."

`http://www.iisfaq.com/default.aspx?View=A435`

Estudo de Caso 3 (cont.)

Provavelmente houve uma identificação incorreta:

- Não foi levado em conta o timezone;
- Não havia evidências de sincronização de relógio no provedor X nem na empresa A;
- O ataque deve ter ocorrido aproximadamente 2 horas antes do horário afirmado pela empresa A.

Estudo de Caso 3 (cont.)

Resultados da investigação:

- Empresa A continuou afirmando que seus horários estavam em localtime;
- Empresa A não se pronunciou sobre sincronia de relógio, nem o provedor X;
- Juiz arquivou o caso por falta de evidências do crime;
- Fulano, mesmo não sendo processado, ficou visto pelos conhecidos como alguém que já se envolveu com atividades ilícitas.

Estudo de Caso 4

Estudo de Caso 4

Problema:

- Instituição A não conseguia enviar emails para Instituição B;
- Demais emails da Instituição A eram entregues sem problemas.
  (com algumas excessões sem diagnóstico claro. . .)

Estudo de Caso 4 (Cont.)

Logs gerados pela Inst. B:

```
Sep 18 23:27:06.465595 rule xx/xx(match): block in on int0:
x.x.x.x.56409 > smtp.25: SWE 2848068646:2848068646(0)

Sep 18 23:43:44.555285 rule xx/xx(match): block in on int0:
x.x.x.x.56726 > smtp.25: SWE 3898219082:3898219082(0)

Sep 19 00:00:33.508330 rule xx/xx(match): block in on int0:
x.x.x.x.56804 > smtp.25: SWE 650122741:650122741(0)
```

Estudo de Caso 4 (Cont.)

ECN (Explicit Congestion Notification):

```
[tcpdump/print-tcp.c]

if (flags & TH_CWR)
   putchar('W');   /* congestion _W_indow reduced (ECN) */
if (flags & TH_ECNECHO)
   putchar('E');   /* ecn _E_cho sent (ECN) */
```

Mais detalhes sobre ECN em:

http://www.icir.org/floyd/ecn.html

Estudo de Caso 4 (Cont.)

Regra de *firewall* Inst. B:

```
block return-rst in log on $interface proto tcp all

pass in quick on $interface proto tcp
from any to $smtpserver
port = smtp flags S keep state
```

Estudo de Caso 4 (Cont.)

Solução:

- Inst. A tinha ECN habilitado por *default* nesta máquina;
- Inst. A desabilitou o uso de ECN;
- Inst. B “flexibilizou” o seu filtro, deixando passar as *flags* de “WE”.

Considerações Finais

Considerações Finais

- *Logs* precisam ter um mínimo de informações úteis;
- Cuidado ao enviar *logs* para fora da sua instituição;
- Ferramentas são essencias;
- Cruzar informações ao analisar *logs*.

Sites de Interesse (cont.)

- NBSO

  http://www.nbso.nic.br/

- Log Analysis Resources

  http://www.counterpane.com/log-analysis.html

- Forum of Incident Response and Security Teams

  http://www.first.org/