

# Sistema de Monitoramento Remoto de Segurança

Tiago Barabasz<sup>1,2</sup> Vitor Monte Afonso<sup>1,2</sup> Antonio Montes<sup>1</sup>

<sup>1</sup>Cenpra - Divisão de Segurança de Sistemas de Informação

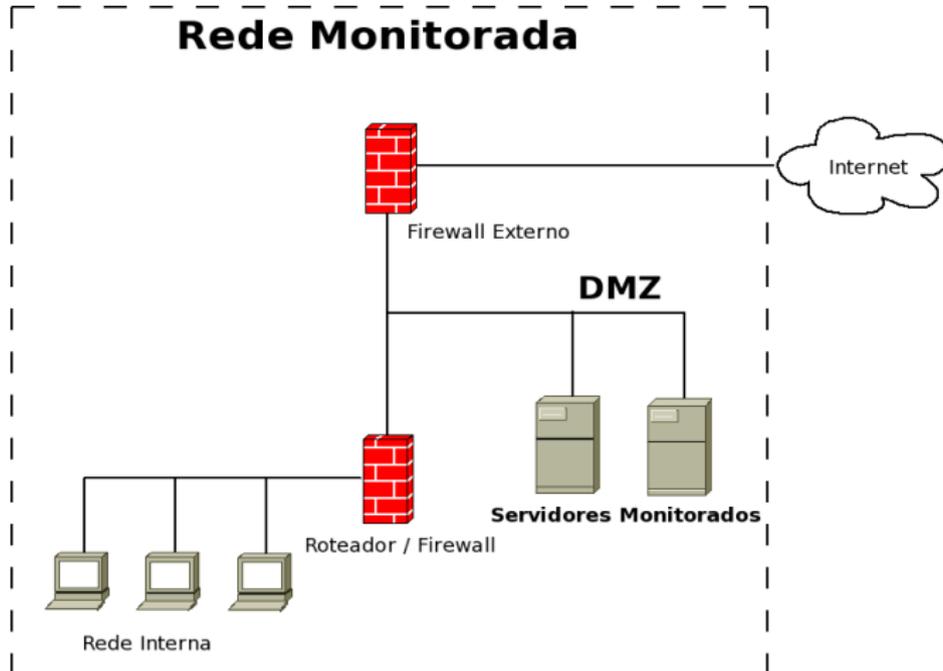
<sup>2</sup>Universidade Estadual de Campinas

GTS-10 2007

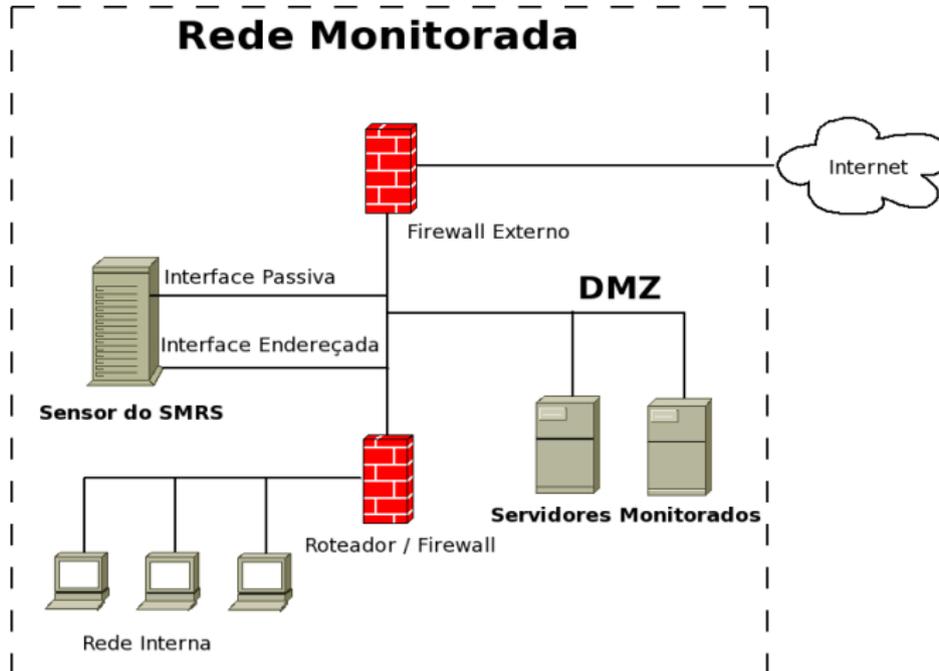
# Introdução

- Motivação
  - Prover sistema de monitoramento remoto de redes, que permita a analistas detectar problemas de segurança

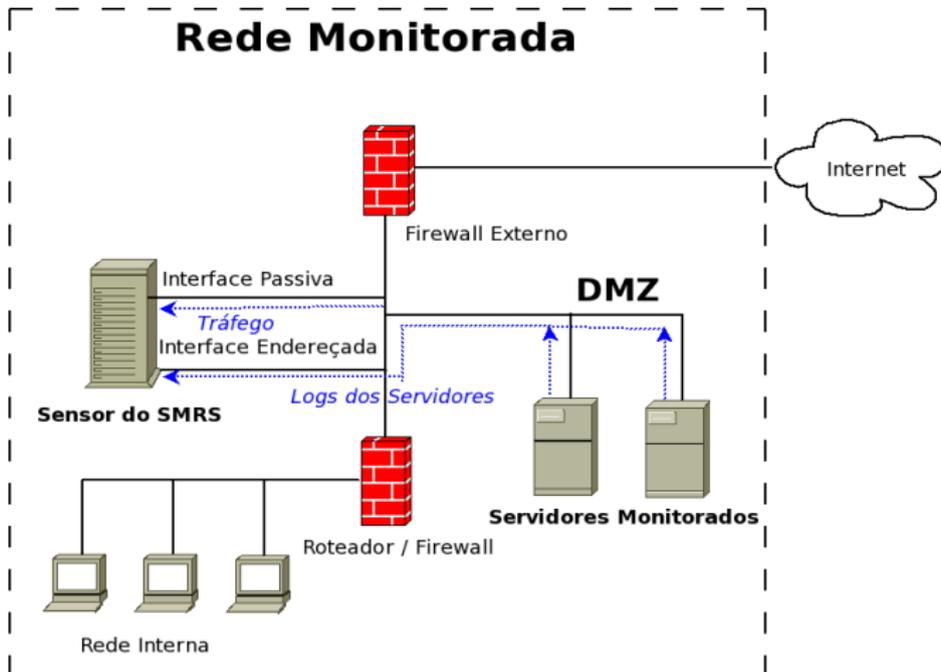
# Estrutura



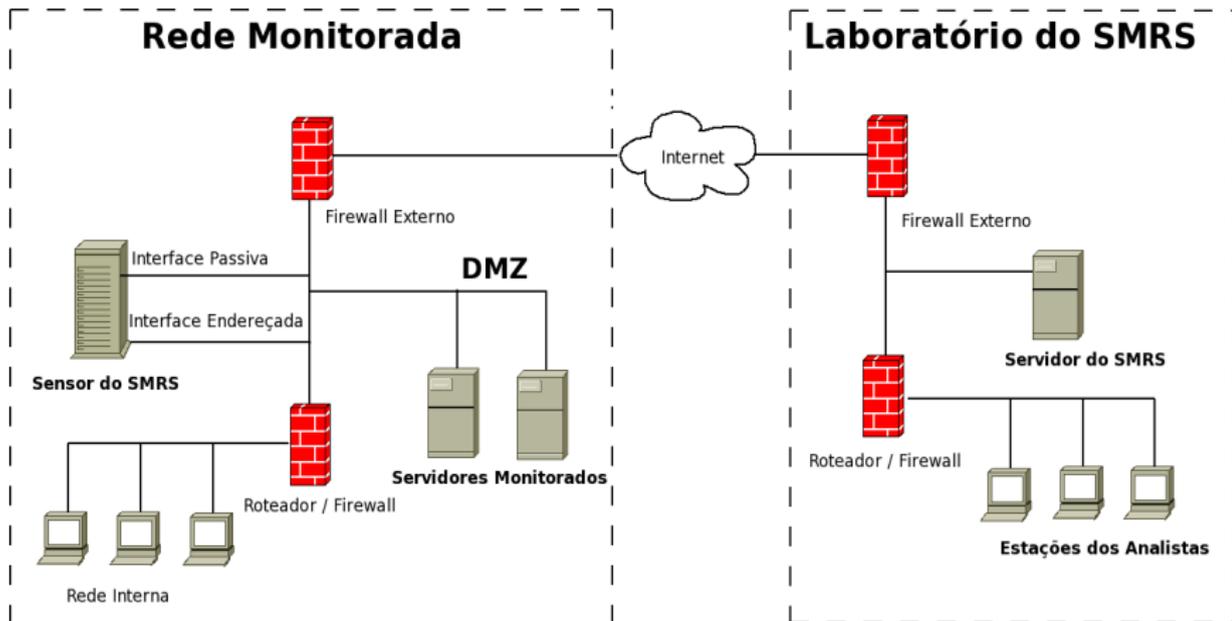
# Estrutura



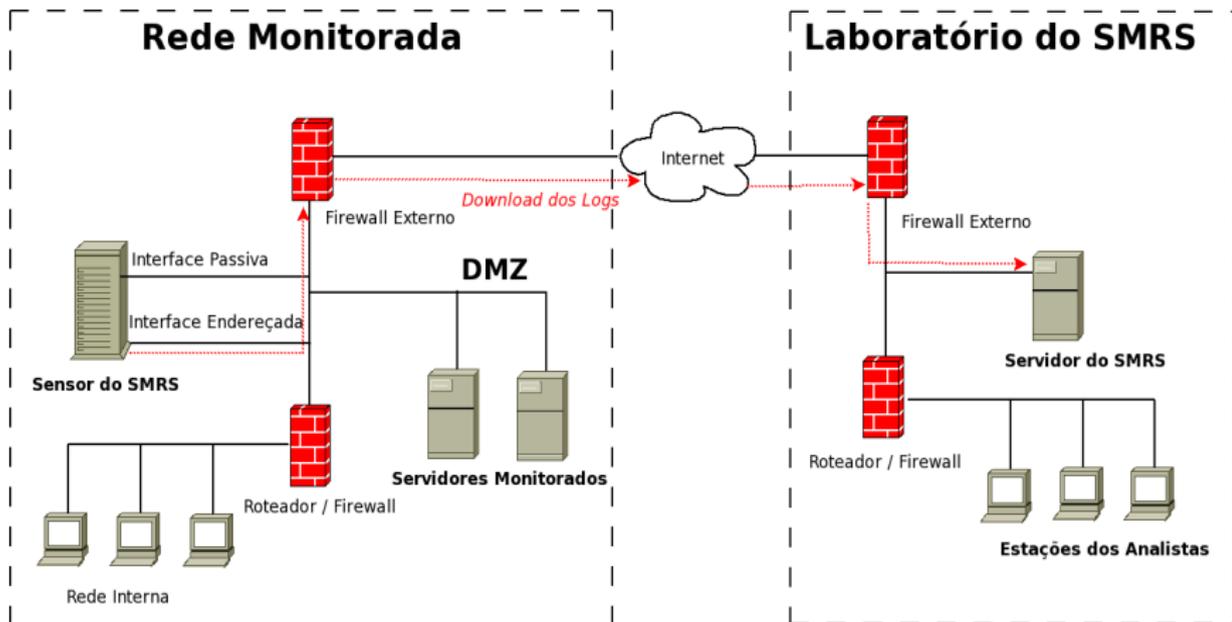
# Estrutura



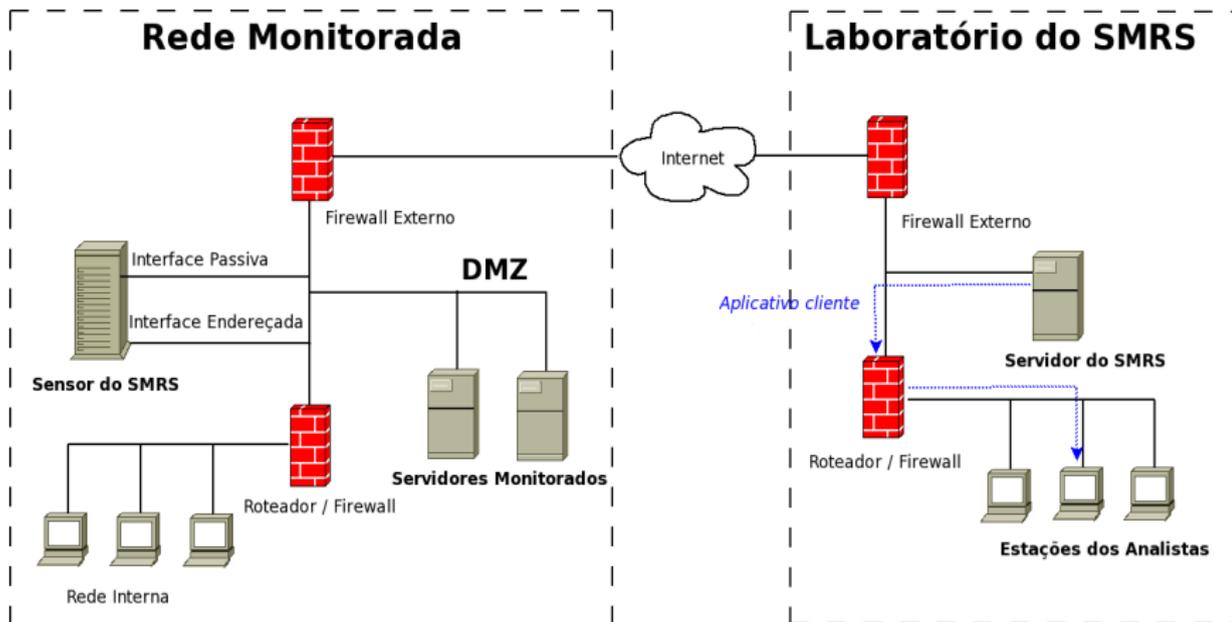
# Estrutura



# Estrutura



# Estrutura



# Processo de análise

- Seleção de escopo
- Visualização de relatórios estatísticos
- Verificação de alertas de segurança
- Geração de relatórios

# Seleção de escopo

The screenshot displays a web-based interface for a security monitoring system. On the left, a sidebar menu includes 'MENU', 'Options', and 'Admin'. The main content area is divided into several sections:

- Analyst:** A tree view showing a hierarchy with 'dssi' as the root, 'vitor' as a child, and '1' as a sub-child of 'vitor'.
- Local Time:** 12:58:16
- GMT Time:** 12:58:16
- Calendar:** A calendar for October 2007. The days of the week are Sun, Mon, Tue, Wed, Thu, Fri, Sat. The dates 23, 24, 25, 26, 27, 28, 29 are visible in the first row.
- Buttons:** 'Start Analysis' and 'Logout' buttons are located at the bottom of the sidebar.

The right side of the interface features a main panel with tabs for 'Reports', 'NIDS', 'Session', and 'Analyzed Report'. The 'Reports' tab is active, showing sub-tabs for 'Attacks per time' and 'Ports'. Below these are several data entry fields:

- Attacks Report:** A large empty text area with the label 'number of attacks :'.
- Attacker Hosts:** A large empty text area with the label 'number of source hosts :'.
- Targeted Ports:** A large empty text area with the label 'number of destination ports :'.
- Targeted Hosts:** A large empty text area with the label 'number of destination hosts :'.

At the bottom of the main panel, there are fields for 'Analyst :', 'Inst :', 'Site :', 'Sensor :', 'From :', and 'To :'. On the far right, there are navigation icons for back, forward, and search.

# Seleção de escopo

The screenshot displays a web-based interface for configuring a security analysis. On the left, a sidebar menu includes 'MENU', 'Options', and 'Admin'. The main content area is titled 'Analyst: smrs\_server' and features a tree view with nodes for 'dssi', 'vitor', and '1'. Below this, it shows 'Local Time 11:25:21' and 'GMT Time 11:25:21'. A calendar for October 2007 is visible, with dates 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, and 30 highlighted in red. At the bottom of the sidebar are 'Start Analysis' and 'Logout' buttons.

The main panel has a navigation bar with 'Reports', 'NIDS', 'Session', and 'Analyzed Report'. The 'Reports' section is active, showing 'Attacks per time' and 'Ports' tabs. The 'Attacks per time' tab is currently empty. To the right, there are sections for 'Attacks info' and 'Src hosts info'. The 'Attacks info' section includes fields for 'Attacks:', 'Class Name:', 'Priority:', 'Sid:', and 'Reference:'. Below this are 'Targeted Ports' and 'Targeted Hosts' sections, each with a 'number of destination ports:' and 'number of destination hosts:' label respectively. At the bottom of the main panel, there are 'Attacker Hosts' and 'Attacks Report' sections, each with a 'number of source hosts:' label. The 'Attacks Report' section is currently empty.

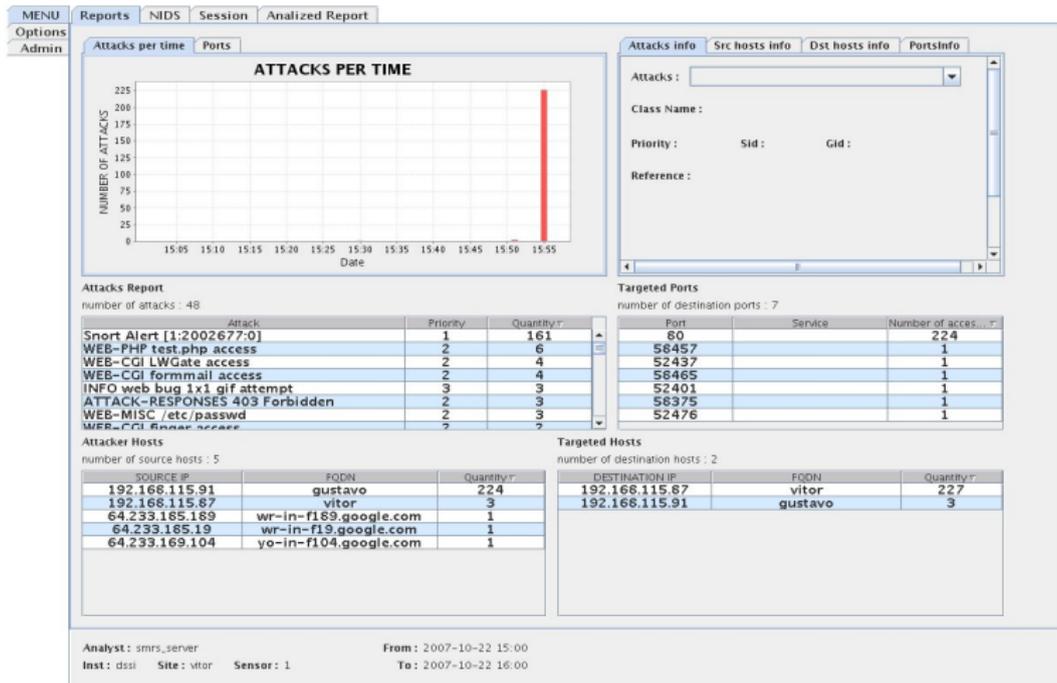
At the bottom of the interface, there are fields for 'Analyst:', 'Inst:', 'Site:', 'Sensor:', 'From:', and 'To:'.

# Seleção de escopo

The interface is divided into several sections:

- Left Panel:** Contains a menu with 'MENU', 'Options', and 'Admin'. Below it, the analyst's name is 'dssi' and the sensor is 'vitor'. It shows local and GMT times (11:26:33) and a calendar for October 2007. The calendar highlights the 22nd. Below the calendar is an 'Hours' grid from 00 to 23. At the bottom are 'Start Analysis' and 'Logout' buttons.
- Top Panel:** Navigation tabs for 'Reports', 'NIDS', 'Session', and 'Analyzed Report'.
- Main Content Area:** A large empty box for 'Attacks per time' and 'Ports'.
- Right Panel:** A sidebar with 'Attacks info' and 'Src hosts info' tabs. It contains fields for 'Attacks:', 'Class Name:', 'Priority:', 'Sid:', and 'Reference:'. Below this are sections for 'Targeted Ports' (number of destination ports) and 'Targeted Hosts' (number of destination hosts).
- Bottom Panel:** Fields for 'Attacker Hosts' (number of source hosts) and 'Attorney Hosts' (number of destination hosts). At the very bottom, there are fields for 'Analyst:', 'Inst:', 'Site:', 'Sensor:', 'From:', and 'To:'.

# Visualização de relatórios estatísticos



# Gráfico de alertas X tempo

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

**Attacks Report**  
number of attacks : 48

Attack	Priority	Quantity
Snort Alert [1:2002677:0]	1	161
WEB-PHP test.php access	2	6
WEB-CGI LWGate access	2	4
WEB-CGI formmail access	2	4
INFO web bug 1x1 gif attempt	3	3
ATTACK-RESPONSES 403 Forbidden	2	3
WEB-MISC /etc/passwd	2	3
WEB-CGI /etc/passwd	2	3

**Attacker Hosts**  
number of source hosts : 5

SOURCE IP	FQDN	Quantity
192.168.115.91	gustavo	224
192.168.115.87	vitor	3
64.233.165.189	wr-in-f189.google.com	1
64.233.165.19	wr-in-f19.google.com	1
64.233.169.104	yo-in-f104.google.com	1

**Attacks info** Src hosts info Dst hosts info PortsInfo

Attacks :

Class Name :

Priority : Sid : Gid :

Reference :

**Targeted Ports**  
number of destination ports : 7

Port	Service	Number of acces
80		224
58457		1
52437		1
58465		1
52401		1
58375		1
52476		1

**Targeted Hosts**  
number of destination hosts : 2

DESTINATION IP	FQDN	Quantity
192.168.115.87	vitor	227
192.168.115.91	gustavo	3

Analyst : smrs\_server From : 2007-10-22 15:00  
Inst : dssl Site : vitor Sensor : 1 To : 2007-10-22 16:00

# Informações extras

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

**Attacks Report**  
number of attacks : 48

Attack	Priority	Quantity
Snort Alert [1:2002677:0]	1	161
WEB-PHP test.php access	2	6
WEB-CGI LWGate access	2	4
WEB-CGI formmail access	2	4
INFO web bug 1x1 gif attempt	3	3
ATTACK-RESPONSES 403 Forbidden	2	3
WEB-MISC /etc/passwd	2	3
WEB-CGI /etc/passwd	2	3

**Attacker Hosts**  
number of source hosts : 5

SOURCE IP	FQDN	Quantity
192.168.115.91	gustavo	224
192.168.115.87	vitor	3
64.233.165.189	wr-in-f189.google.com	1
64.233.165.19	wr-in-f19.google.com	1
64.233.169.104	yo-in-f104.google.com	1

**Attacks info** Src hosts info Dst hosts info PortsInfo

Attacks :

Class Name :

Priority : Sid : Gid :

Reference :

**Targeted Ports**  
number of destination ports : 7

Port	Service	Number of access
80		224
58457		1
52437		1
58465		1
52401		1
58375		1
52476		1

**Targeted Hosts**  
number of destination hosts : 2

DESTINATION IP	FQDN	Quantity
192.168.115.87	vitor	227
192.168.115.91	gustavo	3

Analyst : smrs\_server From : 2007-10-22 15:00  
Inst : dssi Site : vitor Sensor : 1 To : 2007-10-22 16:00

# Tabela com alertas

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

Attacks Report  
number of attacks : 48

Attack	Priority	Quantity
Snort Alert [1:2002677:0]	1	161
WEB-PHP test.php access	2	6
WEB-CGI LWGate access	2	4
WEB-CGI formmail access	2	4
INFO web bug 1x1 gif attempt	3	3
ATTACK-RESPONSES 403 Forbidden	2	3
WEB-MISC /etc/passwd	2	3
WEB-CGI Basic access	2	3

Attacker Hosts  
number of source hosts : 5

SOURCE IP	FQDN	Quantity
192.168.115.91	gustavo	224
192.168.115.87	vitor	3
64.233.165.189	wr-in-f189.google.com	1
64.233.165.19	wr-in-f19.google.com	1
64.233.169.104	yo-in-f104.google.com	1

Attacks info Src hosts info Dst hosts info PortsInfo

Attacks :

Class Name :

Priority : Sid : Gid :

Reference :

Targeted Ports  
number of destination ports : 7

Port	Service	Number of access
80		224
58457		1
52437		1
58465		1
52401		1
58375		1
52476		1

Targeted Hosts  
number of destination hosts : 2

DESTINATION IP	FQDN	Quantity
192.168.115.87	vitor	227
192.168.115.91	gustavo	3

Analyst : smrs\_server From : 2007-10-22 15:00  
Inst : dssl Site : vitor Sensor : 1 To : 2007-10-22 16:00

# Tabela com portas de destino

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

Attacks Report  
number of attacks : 48

Attack	Priority	Quantity
Snort Alert [1:2002677:0]	1	161
WEB-PHP test.php access	2	6
WEB-CGI LWGate access	2	4
WEB-CGI formmail access	2	4
INFO web bug 1x1 gif attempt	3	3
ATTACK-RESPONSES 403 Forbidden	2	3
WEB-MISC /etc/passwd	2	3
WEB-CGI /etc/passwd	2	3

Attacker Hosts  
number of source hosts : 5

SOURCE IP	FQDN	Quantity
192.168.115.91	gustavo	224
192.168.115.87	vitor	3
64.233.165.189	wr-in-f189.google.com	1
64.233.165.19	wr-in-f19.google.com	1
64.233.169.104	yo-in-f104.google.com	1

Attacks info Src hosts info Dst hosts info PortsInfo

Attacks : [dropdown]  
Class Name :  
Priority : Sid : Gid :  
Reference :

Targeted Ports  
number of destination ports : 7

Port	Service	Number of access
80		224
58457		1
52437		1
58465		1
52401		1
58375		1
52476		1

Targeted Hosts  
number of destination hosts : 2

DESTINATION IP	FQDN	Quantity
192.168.115.87	vitor	227
192.168.115.91	gustavo	3

Analyst : smrs\_server From : 2007-10-22 15:00  
Inst : dssl Site : vitor Sensor : 1 To : 2007-10-22 16:00

# Tabela com endereços de origem

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

Attacks Report  
number of attacks : 48

Attack	Priority	Quantity
Snort Alert [1:2002677:0]	1	161
WEB-PHP test.php access	2	6
WEB-CGI LWGate access	2	4
WEB-CGI formmail access	2	4
INFO web bug 1x1 gif attempt	3	3
ATTACK-RESPONSES 403 Forbidden	2	3
WEB-MISC /etc/passwd	2	3
WEB-CGI /etc/passwd	2	3

Attacker Hosts  
number of source hosts : 5

SOURCE IP	FQDN	Quantity
192.168.115.91	gustavo	224
192.168.115.87	vitor	3
64.233.165.189	wr-in-f189.google.com	1
64.233.165.19	wr-in-f19.google.com	1
64.233.169.104	yo-in-f104.google.com	1

Attacks info Src hosts info Dst hosts info PortsInfo

Attacks :

Class Name :

Priority : Sid : Gid :

Reference :

Targeted Ports  
number of destination ports : 7

Port	Service	Number of access
80		224
58457		1
52437		1
58465		1
52401		1
58375		1
52476		1

Targeted Hosts  
number of destination hosts : 2

DESTINATION IP	FQDN	Quantity
192.168.115.87	vitor	227
192.168.115.91	gustavo	3

Analyst : smrs\_server From : 2007-10-22 15:00  
Inst : dssi Site : vitor Sensor : 1 To : 2007-10-22 16:00

# Tabela com endereços de destino

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

Attacks Report  
number of attacks : 48

Attack	Priority	Quantity
Snort Alert [1:2002677:0]	1	161
WEB-PHP test.php access	2	6
WEB-CGI LWGate access	2	4
WEB-CGI formmail access	2	4
INFO web bug 1x1 gif attempt	3	3
ATTACK-RESPONSES 403 Forbidden	2	3
WEB-MISC /etc/passwd	2	3
WEB-CGI /etc/passwd	2	3

Attacker Hosts  
number of source hosts : 5

SOURCE IP	FQDN	Quantity
192.168.115.91	gustavo	224
192.168.115.87	vitor	3
64.233.165.189	wr-in-f189.google.com	1
64.233.165.19	wr-in-f19.google.com	1
64.233.169.104	yo-in-f104.google.com	1

Attacks info Src hosts info Dst hosts info PortsInfo

Attacks :

Class Name :

Priority : Sid : Gid :

Reference :

Targeted Ports  
number of destination ports : 7

Port	Service	Number of access
80		224
58457		1
52437		1
58465		1
52401		1
58375		1
52476		1

Targeted Hosts  
number of destination hosts : 2

DESTINATION IP	FQDN	Quantity
192.168.115.87	vitor	227
192.168.115.91	gustavo	3

Analyst : smrs\_server From : 2007-10-22 15:00  
Inst : dssi Site : vitor Sensor : 1 To : 2007-10-22 16:00



# Informações do snort.org sobre o alerta

MENU Reports NIDS Session Analyzed Report  
Options Admin

Attacks per time Ports

## ATTACKS PER TIME

Attacks info Src hosts info Dst hosts info Portsinfo  
Attacks: WEB-PHP test.php access

Information from snort.org :

GEN-SID: 1:2152  
 Message: WEB-PHP test.php access  
 Summary: This event is generated when an attempt is made to access a script not normally used in a production environment.  
 Impact: Information gathering.  
 Detailed Information: This event indicates that an attempt has been made to access a test script (test.php) that would not normally be used in a production environment.  
 The attacker may be trying to gain information on the php implementation on the host, this may be the prelude to an attack against that host using that information.  
 In applications such as Horde or IMP, the test.php script may reveal valuable server information to the attacker.  
 Affected Systems: Any host using php applications such as Horde or IMP.  
 Other php applications may use a file named test.php also.  
 Attack Scenarios: An attacker can retrieve a sensitive file containing information on the php application on the host. The attacker might then gain administrator access to the site or database.  
 Ease of Attack: Simple.  
 False Positives: If the script test.php exists and is normally used, this rule will generate an event.  
 If you think this rule has a false positives, please help fill it out. False Negatives: None Known.  
 If you think this rule has a false negatives, please help fill it out. Corrective Action: Check the php implementation on the host. Ensure all measures have been taken to deny access to sensitive files.  
 Check the host for signs of compromise.  
 Contributors: Sourcefire Vulnerability Research Team  
 Brian Caswell &lt;bmc@sourcefire.com>;  
 Nigel Houghton &lt;nigel.houghton@sourcefire.com>;  
 Additional References: ; Rule References: Error: Unknown reference type: nessus,11617

Attacks Report  
number of attacks : 48

Snort Alert [1:20026]  
 WEB-PHP test.php acc  
 WEB-CGI LWGate acc  
 WEB-CGI formmail ad  
 INFO web bug 1x1 gi  
 ATTACK-RESPONSES  
 WEB-MISC /etc/passw  
 WEB-CGI formmail acc

Attacker Hosts  
 number of source hosts : 5

SOURCE IP
192.168.115.91
192.168.115.87
64.233.165.169
64.233.165.19
64.233.169.104

Number of acces
224
1
1
1
1
1
1

Quantity
227
3

Analyst: smrs\_server From: 2007-10-22 15:00  
 Inst: dssi Site: vltor Sensor: 1 To: 2007-10-22 16:00

# Informações sobre determinado host

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

Attacks Info Src hosts info Dst hosts info Ports info

IPs: 64.233.185.19

FQDN: wr-in-f19.google.com

Get whois

set description

**Attacks Report**  
number of attacks : 48

Attack	Priority	Quantity
Snort Alert [1:2002677:0]	1	161
WEB-PHP test.php access	2	6
WEB-CGI LWGate access	2	4
WEB-CGI formmail access	2	4
INFO web bug 1x1 gif attempt	3	3
ATTACK-RESPONSES 403 Forbidden	2	3
WEB-MISC /etc/passwd	2	3
WEB-PHP /etc/passwd	2	3

**Attacker Hosts**  
number of source hosts : 5

SOURCE IP	FQDN	Quantity
192.168.115.91	gustavo	224
192.168.115.87	vitor	3
64.233.185.189	wr-in-f189.google.com	1
64.233.185.19	wr-in-f19.google.com	1
64.233.169.104	yo-in-f104.google.co	1

**Targeted Ports**  
number of destination ports : 7

Port	Service	Number of access
80		224
58457		1
52437		1
58465		1
52401		1
58375		1
52476		1

**Targeted Hosts**  
number of destination hosts : 2

DESTINATION IP	FQDN	Quantity
192.168.115.87	vitor	227
192.168.115.91	gustavo	3

Analyst: smrs\_server From: 2007-10-22 15:00  
Inst: dssi Site: vitor Sensor: 1 To: 2007-10-22 16:00

# Whois do endereço

MENU Options Admin

Reports NIDS Session Analyzed Report

Attacks per time Ports

### ATTACKS PER TIME

Attacks info Src hosts info Dst hosts info Portsinfo

IPs: 64.233.185.19

FOONI wr-in-fl9.google.com

#### Whois

GeekTools Whois Proxy v5.0.4 Ready.  
Checking access for 200.144.115.87... ok.  
Final results obtained from whois.arin.net.  
Results:

OrgName: Google Inc.  
OrgID: GOGL  
Address: 1600 Amphitheatre Parkway  
City: Mountain View  
StateProv: CA  
PostalCode: 94043  
Country: US

NetRange: 64.233.160.0 - 64.233.191.255  
CIDR: 64.233.160.0/19  
NetName: GOOGLE  
NetHandle: NET-64-233-160-0-1  
Parent: NET-64-0-0-0-0  
NetType: Direct Allocation  
NameServer: NS1.GOOGLE.COM  
NameServer: NS2.GOOGLE.COM  
NameServer: NS3.GOOGLE.COM  
NameServer: NS4.GOOGLE.COM  
Comment:  
RegDate: 2003-08-18  
Updated: 2007-04-10  
RTechHandle: ZG39-ARIN  
RTechName: Google Inc.  
RTechPhone: +1-650-318-0200  
RTechEmail: arin-contact@google.com  
OrgTechHandle: ZG39-ARIN  
OrgTechName: Google Inc.

Attacks Report  
number of attacks : 48

Attack
Snort Alert [1:2002677-0]
WEB-PHP test.php access
WEB-CGI LWGate access
WEB-CGI formmail access
INFO web bug 1x1 gif attempt
ATTACK-RESPONSES 403 Forbidden
WEB-MISC /etc/passwd
WEB-CGI formmail access

Attacker Hosts  
number of source hosts : 5

SOURCE IP	FOONI
192.168.115.91	gustav
192.168.115.87	vitor
64.233.185.189	wr-in-fl189.go
64.233.185.19	wr-in-fl19.go
64.233.169.104	yo-in-fl104.go

Number of acces
224
1
1
1
1
1
1
1

Quantity
227
3

Analyst : smrs\_server From : 2007-10-22 15:00  
Inst : dssi Site : vitor Sensor : 1 To : 2007-10-22 16:00

# Verificação de alertas de segurança

MENU  
Options  
Admin

Reports NIDS Session Analyzed Report

Build tree... FILTER

Sort by  Risk  Host  Quantity

SNORT ALERTS

Attacks info Src hosts info Dst hosts info PortsInfo Events Data Packet

IPs: [dropdown]  
FQDN:  
Get whois  
set description

Analyst: smrs\_server From: 2007-10-22 15:00  
Inst: dssi Site: vitor Sensor: 1 To: 2007-10-22 16:00

# Verificação de alertas de segurança

The screenshot displays a web-based interface for security monitoring. At the top, there are navigation tabs: MENU, Options, Admin, Reports, NIDS, Session, and Analyzed Report. The 'Reports' tab is active, showing a 'Build tree...' section with a 'FILTER' button and several dropdown menus. A tree structure is visible with 'Attack' selected, and sub-items 'Src' and 'Dst' are shown. Below the tree, there are radio buttons for 'Attack', 'Host', and 'Quantity'. The main content area is empty. At the bottom, there are tabs for 'Attacks info', 'Src hosts info', 'Dst hosts info', 'PortsInfo', 'Events', and 'Data Packet'. The 'Attacks info' tab is active, showing an 'IPs:' dropdown, an 'FQDN:' field, and buttons for 'Get whois' and 'set description'. At the very bottom, there is a status bar with the following information: Analyst: smrs\_server, Inst: dssi, Site: vtor, Sensor: 1, From: 2007-10-22 15:00, To: 2007-10-22 16:00.

# Verificação de alertas de segurança

The screenshot displays a web-based security monitoring interface. At the top, there are navigation tabs: 'MENU', 'Options', and 'Admin'. Below these are report filters: 'Reports', 'NIDS', 'Session', and 'Analyzed Report'. The main area is titled 'Build tree...' and contains a 'FILTER' button and three dropdown menus for 'Dst', 'Src', and 'Attack'. Below the filters, there is a 'Sort by' section with radio buttons for 'Risk', 'Host', and 'Quantity'. A tree view shows a folder icon next to 'SNORT ALERTS'. Below the tree view, there are tabs for 'Attacks info', 'Src hosts info', 'Dst hosts info', 'Portsinfo', 'Events', and 'Data Packet'. The 'Attacks info' tab is active, showing an 'IPs:' dropdown, an 'FQDN:' field, and buttons for 'Get whois' and 'set description'. At the bottom, there is a status bar with the following information: 'Analyst: smrs\_server', 'Inst: dssi', 'Site: vitor', 'Sensor: 1', 'From: 2007-10-22 15:00', and 'To: 2007-10-22 16:00'. The interface is rendered in a light gray color scheme.

# Verificação de alertas de segurança

MENU Options Admin

Reports NIDS Session Analyzed Report

Build tree... FILTER

Dst Src Attack

Sort by Risk Host Quantity

- Dst 192.168.115.91 (3)
- Dst 192.168.115.87 (227)

Attacks info Src hosts info Dst hosts info PortsInfo

IPs: 192.168.115.91

FQDN: gustavo

Get whois

set description

Analyst: smrs\_server From: 2007-10-22 15:00  
Inst: dssl Site: vitor Sensor: 1 To: 2007-10-22 16:00

Edit Mode: Order Scale Translate Brush 0 / 230 Reset Brush Reset All

Time Src Dst Sid Port

status: rendering (quality) 100% 0 s  hist  tooltips  line  Brush Fuzziness: 20%

Events Data Packet

Timestamp	Src IP	Dst IP	Pri	Event Message	Port
22/10/07 15:3...	64.233.169...	192.168.11...	3	INFO web bug 1x1 gif...	583...
22/10/07 15:5...	64.233.185...	192.168.11...	3	INFO web bug 1x1 gif...	584...
22/10/07 15:5...	64.233.185...	192.168.11...	3	INFO web bug 1x1 gif...	584...
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	2	WEB-MISC /--root access	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	2	WEB-MISC oracle web	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80

# Verificação de alertas de segurança

The screenshot displays a security analysis tool interface. At the top, there are menu options: MENU, Options, and Admin. Below these are tabs for Reports, NIDS, Session, and Analyzed Report. The main area is divided into several sections:

- Build tree...:** Includes a FILTER button and dropdown menus for Dst, Src, and Attack. Below this, it shows 'Sort by' options (Risk, Host, Quantity) and a list of destinations: Dst 192.168.115.91 (3) and Dst 192.168.115.87 (227).
- Network Flow Graph:** A line graph showing traffic flow between various nodes. The x-axis represents Time (from 15:00:07 to 16:00:07), Src (0.0.0.0), Dst (192.168.115.87), Sid (0.0), and Port (0.0). The y-axis represents quantity, with values up to 58465. A red box highlights this graph.
- Attacks info:** Shows the IP address 192.168.115.91 and the FQDN gustavo. It includes buttons for 'Get whois' and 'set description'.
- Events Data Packet:** A table listing events with columns for Timestamp, Src IP, Dst IP, Pri, Event Message, and Port. The table contains multiple entries for 'INFO web bug 1x1 gif...' and 'Snort Alert [1:2002677... 80]'. The Snort alerts are highlighted in red.
- Summary:** At the bottom, it shows 'Analyst: smrs\_server', 'Inst: dssl Site: vitor Sensor: 1', 'From: 2007-10-22 15:00', and 'To: 2007-10-22 16:00'.

# Verificação de alertas de segurança

MENU Reports NIDS Session Analyzed Report  
Options Admin

Build tree... FILTER  
Dst Src Attack  
Sort by Risk Host Quantity  
 Dst 192.168.115.91 (3)  
 Dst 192.168.115.87 (227)

Attacks info Src hosts info Dst hosts info PortsInfo  
IPs: 192.168.115.91  
FQDN: gustavo  
Get whois  
set description

status: rendering [quality] 100% 0 s  hist  tooltips  line  Brush Fuzziness: 20%

Events Data Packet

Timestamp	Src IP	Dst IP	Pri	Event Message	Port
22/10/07 15:3...	64.233.169...	192.168.11...	3	INFO web bug 1x1 gif...	584...
22/10/07 15:5...	64.233.185...	192.168.11...	3	INFO web bug 1x1 gif...	584...
22/10/07 15:5...	64.233.185...	192.168.11...	3	INFO web bug 1x1 gif...	584...
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	2	WEB-MISC /-root access	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:5...	192.168.11...	192.168.11...	2	WEB-MISC oracle web	80
22/10/07 15:5...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80

Analyst: smrs\_server From: 2007-10-22 15:00  
Inst: dsssl Site: vitor Sensor: 1 To: 2007-10-22 16:00

# Verificação de alertas de segurança

The screenshot displays a network security analysis tool interface. At the top, there are menu options: MENU, Options, and Admin. Below these are tabs for Reports, NIDS, Session, and Analyzed Report. The main area is divided into several sections:

- Build tree...:** A tree view showing a hierarchy of IP addresses. The selected node is "Dst 192.168.115.87 (227)". Other nodes include Src 64.233.169.104 (1), Src 192.168.115.91 (224), Src 64.233.185.19 (1), and Src 64.233.185.189 (1).
- Graph:** A line graph showing traffic volume over time. The x-axis represents Time (from 22/10/07 15:00:07 to 16:00:07) and the y-axis represents Src (0.0.0.0), Dst (192.168.115.87), Sid (0.0), and Port (0.0). The graph shows a significant spike in traffic at 15:55:00.
- Attacks info:** A section for analyzing the selected IP (192.168.115.87). It includes fields for FQDN (vitor) and buttons for "Get whois" and "set description".
- Events:** A table listing detected events. The table has columns for Timestamp, Src IP, Dst IP, Pri, Event Message, and Port. The events are all "Snort Alert" messages, with the first one being "INFO web bug 1x1 gif ... 583...".

At the bottom of the interface, there is a summary section:

Analyst: smrs\_server  
Inst: dssi Site: vitor Sensor: 1  
From: 2007-10-22 15:00  
To: 2007-10-22 16:00



# Verificação de alertas de segurança

MENU Reports NIDS Session Analyzed Report  
Options Admin

Build tree... FILTER

Dst Src Attack

Sort by Risk Host Quantity

- Dst 192.168.115.91 (3)
- Dst 192.168.115.87 (227)
- Src 64.233.169.104 (1)
- Src 192.168.115.91 (224)
  - Attack WEB-CGI /cgi-bin/ access (1)
  - Attack WEB-CGI echo.bat arbitrary comma (1)
  - Attack Snort Alert [1:2001343:0] (1)
  - Attack WEB-MISC global.inc access (1)
  - Attack Snort Alert [1:2001736:0] (1)
  - Attack Snort Alert [1:2002997:0] (1)
  - Attack WEB-IIS /scripts/samples/ access (1)
  - Attack WEB-COLDFUSION exeveal access (1)
  - Attack WEB-CGI book.cgi arbitrary comma (1)
  - Attack Snort Alert [1:2002677:0] (161)
  - Attack WEB-MISC /~root access (2)

Attacks info Src hosts info Dst hosts info PortsInfo

IPs: 192.168.115.91

FQDN: gustavo

Get whois

set description

Analyst: smrs\_server From: 2007-10-22 15:00  
Inst: dssi Site: vitor Sensor: 1 To: 2007-10-22 16:00

Edit Mode: Order Scale Translate Brush 230 / 230 Reset Brush Reset All

Time 22/10/07 15:00:07 22/10/07 16:00:07

Src 0.0.0.0 255.255.255.255

Dst 192.168.115.87 192.168.115.91

Sid 0.0.0 378.0

Port 80.0 58465

status rendering [quality] 100% 0 s  hist  tooltips  line  Brush Fuzziness: 20%

Events Data Packet

Timestamp	Src IP	Dst IP	Pri	Event Message	Port
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	2	WEB-MISC /~root access	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	2	WEB-MISC oracle web	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80
22/10/07 15:...	192.168.11...	192.168.11...	1	Snort Alert [1:2002677...	80

# Tráfego da sessão associada

MENU	Reports	NIDS	Session	Analyzed Report
Options				
Admin				
Timestamp	Src	Dst	Info	
15:55:32.047456	192.168.115.91.52401	192.168.115.87.80	S 90952375:90952375(0) win 5840 <mss 1460,sackOK,tim...	
15:55:32.047461	192.168.115.87.80	192.168.115.91.52401	S 643153008:643153008(0) ack 90952376 win 5792 <mss...	
15:55:32.047551	192.168.115.91.52401	192.168.115.87.80	. ack 1 win 92 <nop,nop,timestamp 4927127 62570485>	
15:55:32.047836	192.168.115.91.52401	192.168.115.87.80	F 1:123(122) ack 1 win 92 <nop,nop,timestamp 4927127 ...	
15:55:32.047843	192.168.115.87.80	192.168.115.91.52401	. ack 123 win 5792 <nop,nop,timestamp 62570485 49271...	
15:55:32.091780	192.168.115.87.80	192.168.115.91.52401	F 1:518(517) ack 123 win 5792 <nop,nop,timestamp 6257...	
15:55:32.092006	192.168.115.91.52401	192.168.115.87.80	. ack 518 win 108 <nop,nop,timestamp 4927138 6257049...	
15:55:32.092810	192.168.115.91.52401	192.168.115.87.80	F 123:123(0) ack 518 win 108 <nop,nop,timestamp 49271...	
15:55:32.092829	192.168.115.87.80	192.168.115.91.52401	F 518:518(0) ack 124 win 5792 <nop,nop,timestamp 6257...	
15:55:32.092918	192.168.115.91.52401	192.168.115.87.80	. ack 519 win 108 <nop,nop,timestamp 4927138 6257049...	

Data Packet	Who Is...
<div style="border: 1px solid gray; height: 100px;"></div>	<div style="border: 1px solid gray; height: 100px;"></div>

Analyst: smrs_server	From: 2007-10-22 15:00
Inst: dssli Site: vitor Sensor: 1	To: 2007-10-22 16:00



# Verificação de alertas de segurança

MENU Options Admin

Reports NIDS Session Analyzed Report

Build tree... FILTER

Dst Attack Src

Sort by Risk Host Quantity

- Dst 192.168.115.91 (3)
- Dst 192.168.115.87 (3)

Attacks info Src hosts info Dst hosts info Portinfo

IPs: 192.168.115.91

FQDN: gustavo

Get whois

set description

Analyst: smrs\_server From: 2007-10-22 15:00  
Inst: dssi Site: wtor Sensor: 1 To: 2007-10-22 16:00

Edit Mode: Order Scale Translate Brush 0 / 6 Reset Brush Reset All

Time: 22/10/07 15:00:17 Src: 0.0.0.0 Dst: .192.168.115.87 Sld: 2.0 Port: 52301

status: rendering (Quality) 100% 0 s  hist  tooltips  line  Brush fuzziness: 20%

Events Data Packet

Timestamp	Src IP	Dst IP	Pri	Event Message	Port
22/10/07 15:3...	64.233.169...	192.168.11...	3	INFO web bug 1x1 gif a...	583...
22/10/07 15:5...	64.233.185...	192.168.11...	3	INFO web bug 1x1 gif a...	584...
22/10/07 15:5...	64.233.185...	192.168.11...	3	INFO web bug 1x1 gif a...	584...
22/10/07 15:5...	192.168.11...	192.168.11...	2	ATTACK-RESPONSES 4...	524...
22/10/07 15:5...	192.168.11...	192.168.11...	2	ATTACK-RESPONSES 4...	524...
22/10/07 15:5...	192.168.11...	192.168.11...	2	ATTACK-RESPONSES 4...	524...

# Geração de relatórios

MENU Reports NIDS Session Analyzed Report  
Options  
Admin

Analyst: *smrs\_server*

Institution: *dssi*  
Site: *vitor*  
Sensor: 1

From: 22/10/07 15:00:16  
To: 22/10/07 16:00:16  
Risk: *Medium*

General Comment:

Events:

Src IP	Dst IP	Event Message	Risk	Critt
192.168.115.91	192.168.115.87	*	Medium	224
192.168.115.87	192.168.115.91	ATTACK-RESPONSE...	Low	3
3	192.168.115.87	INFO web bug 1x1 ...	False Positive	3

Hosts:  Ports:  Attacks:

Comments:

Analyst: *smrs\_server* From: 2007-10-22 15:00  
Inst: *dssi* Site: *vitor* Sensor: 1 To: 2007-10-22 16:00

# Relatório gerado

## Analysis report from SMRS 15/22/2007

Analyst: smrs\_server

Institution: dssi  
Site: vitor  
Sensor: 1

From : 2007-10-22 15:00  
Until: 2007-10-22 16:00

Risk: Medium

### ### Alert Analysis :

Attack: \*, Risk: Medium  
From : 192,168,115,91 To : 192,168,115,87,  
Quantity: 224,  
Alert Priority: \*,  
Comment:  
Scan attempt.

Attack: ATTACK-RESPONSES 403 Forbidden, Risk: Low  
From : 192,168,115,87 To : 192,168,115,91,  
Quantity: 3,  
Alert Priority: 3,  
Comment:

Attack: INFO web bug IxI gif attempt, Risk: False Positive  
From : \* To : 192,168,115,87  
Quantity: 3,  
Alert Priority: 3,  
Comment:

# Teste realizado com nikto

MENU  
Options  
Admin

Reports NIDS Analyzed Report

Build tree... FILTER

Dst Src Attack

Sort by Risk Host Quantity

- 192.168.115.88 (4531)
  - Attack WEB-ATTACKS /usr/bin/ld command attempt (4)
  - Attack WEB-CGI csSearch.cgi arbitrary command executi
  - Attack WEB-CGI SIX.webboard.generate.cgi attempt (3)
  - Attack Snort Alert [1.2002070:0] (1)
  - Attack Snort Alert [1.2002070:0] (14)
  - Attack WEB-CGI bb-hist.sh attempt (1)
  - Attack WEB-MISC Tomcat servlet mapping cross site scrip
  - Attack WEB-CGI faqmanager.cgi arbitrary file access atte
  - Attack WEB-CGI htsearch arbitrary configuration file alter
  - Attack WEB-PHP Typo3 translations.php file include (1)
  - Attack WEB-MISC oracle web arbitrary command executi
  - Attack WEB-MISC jrun directory.browse attempt (4)
  - Attack WEB-CGI webplus directory.traversal (1)

Edit Mode: Order Scale Translate Brush 4531 / 4531 Reset Brush Reset All

Time Src Dst Sid Port

09/08/07 09:18:45 255.255.255.255 192.168.115.88 500.0 80.0

09/08/07 09:18:33 0.0.0.0 192.168.115.89 0.0 0.0

status: rendering: equality 33% 32 s  hist.  tooltips  line  Brush fuzziness: 20%

Attacks info Src hosts info Dst hosts info Ports info

IPs: 192.168.115.88

FQDN: tiago

Get whois

set description

Events Data Packet

Timestamp	Src IP	Dst IP	Pri	Event Message	Port
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	2	WEB-MISC oracle web applicati.	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	WEB-CGI (cgi-bin) access	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80
09/08/07 09:18:33	192.168.115.91	192.168.115.88	1	Snort Alert [1.2002677:0]	80

# Conclusão

- O sistema atualmente está em fase de testes e estão sendo desenvolvidos programas para automatizar sua instalação.

## Trabalhos futuros

- Incluir suporte a análise do tráfego de rede e de registros de aplicações

# Apoio

