Intrusion Detection Systems

(IDS)

What are They and How do They Work?

By
Wayne T Work

Security Gauntlet Consulting
56 Applewood Lane
Naugatuck, CT 06770
203.217.5004

1. Introduction

Intrusion Detection Systems, also known as IDS, were developed to analyze and make determinations, given set criteria, on administratively defined levels looking for ANOMOLIES or POSSIBLE intrusions within a network or computer system. There are two basic types of IDS, they are:

Host	Network
Host Based	Networked and Network Node
Hybrid	Hybrid
File Integrity	Honeypots

Figure 1-1

a. Host Based IDS

Host based IDS consists of software or AGENT components, which exist on a Server, Router, Switch or Network appliance. The agent versions must report to a console or can be run together on the same Host. This is NOT the preferred method though. The ideal method is illustrated in Figure 1.2

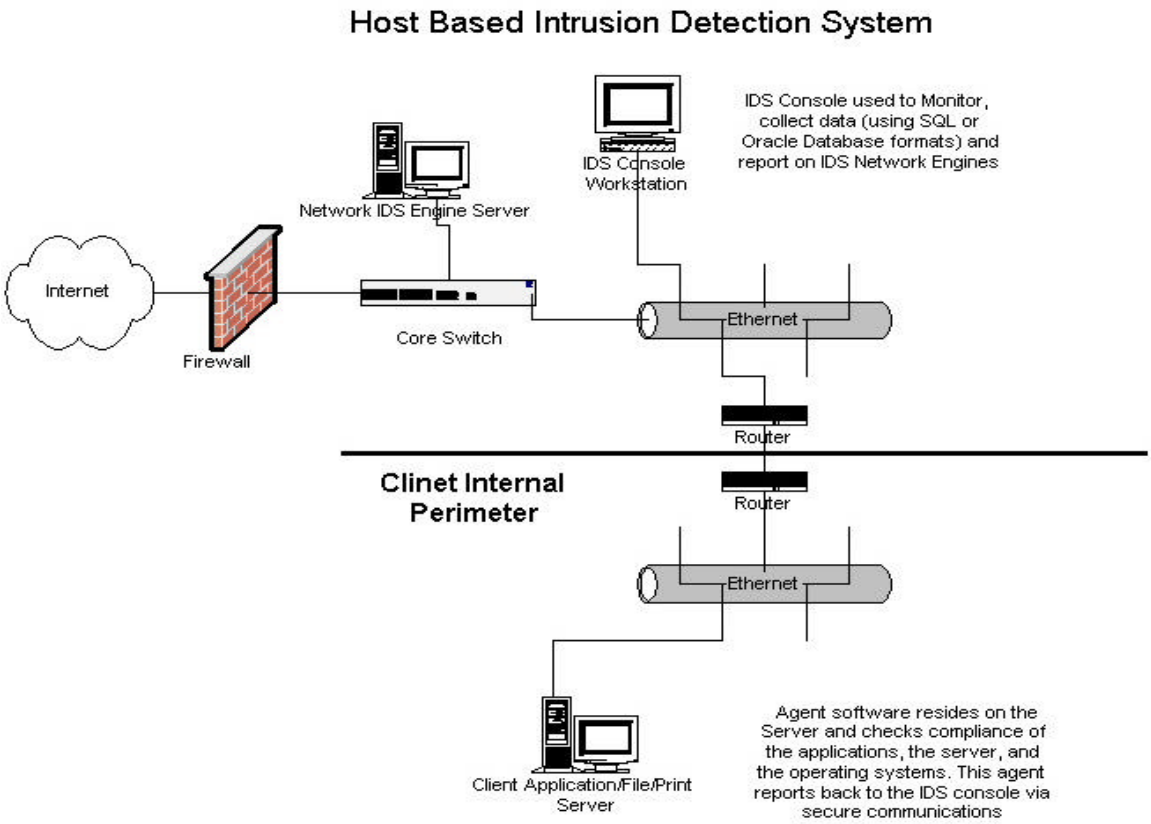


Figure 1-2

The above model allows for remote monitoring, remote storage of event logs and the ability to PUSH agents to new or existing Hosts.

b. Network Based IDS

Network based IDS captures network traffic packets (TCP, UDP, IPX/SPX, etc.) and analyzes the content against a set of **RULES** or **SIGNATURES** to determine if a POSSIBLE event took place. False positives are common when an IDS system is not configured or "tuned" to the environment traffic it is trying to analyze. **Network Node** is merely an extended model of the networked IDS systems adding segregated and dedicated IDS servers on each NODE of a network in order to capture all the networked traffic not visible to other IDS servers. Switched or "Gig-a-Bit" networks have brought with them an inherent problem, standard network based IDS are unreliable at "Gig-a-Bit" speeds on more than one segment, dropping a HI percentage of the network packets. Switched networks often prevent a network IDS from seeing passing packets promiscuously from segment to segment. Network Node IDS delegates the network IDS function down to individual hosts alleviating the problems of both switching and "Gig-a-Bit" speeds. **Personal Software Firewall** systems such as "Black Ice" and "Tiny Firewall" are examples of these IDS.

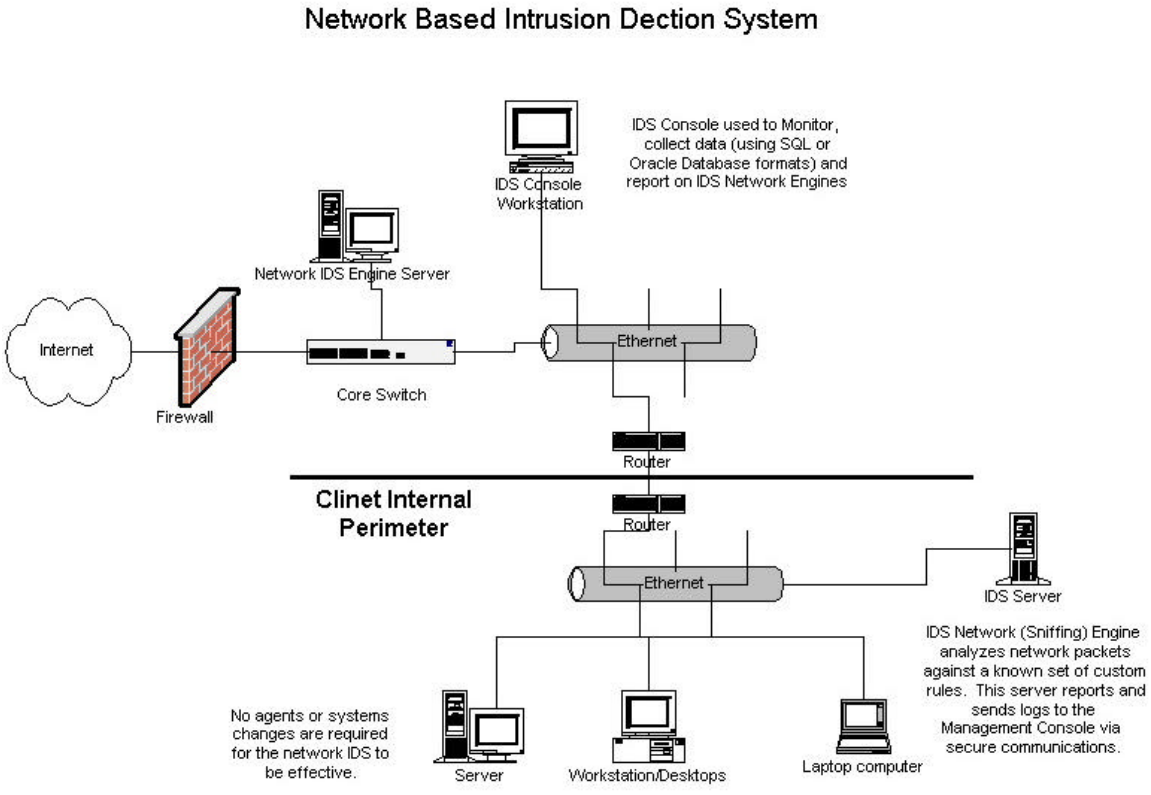


Figure 1-3

c. Honeypot IDS

Honeypot Intrusion Detection Systems are utilized as a "Bait" and "Trap" methodology. They can **emulate** numerous operating systems, multiple operating systems, dedicated "services" (File Transfer Protocol (FTP), Hyper Text Transfer

Protocol (HTTP), etc.) and most importantly, **TRACK** the 'finger print" of an intruder. This allows the tracing of intruders to the source or origin of the attack. Obviously there are inherent risks in using Honeypot technology, the allowing of a "Hacker" onto a computer is a dangerous but if placed correctly in and environment this is limited to the Honeypot Server and the fact that you have "available" services or operating systems noticeable on your network can bring more "hackers" to snoop the network. Again, this is avoidable if placed in the right location and isolated from all other "Operational" systems.

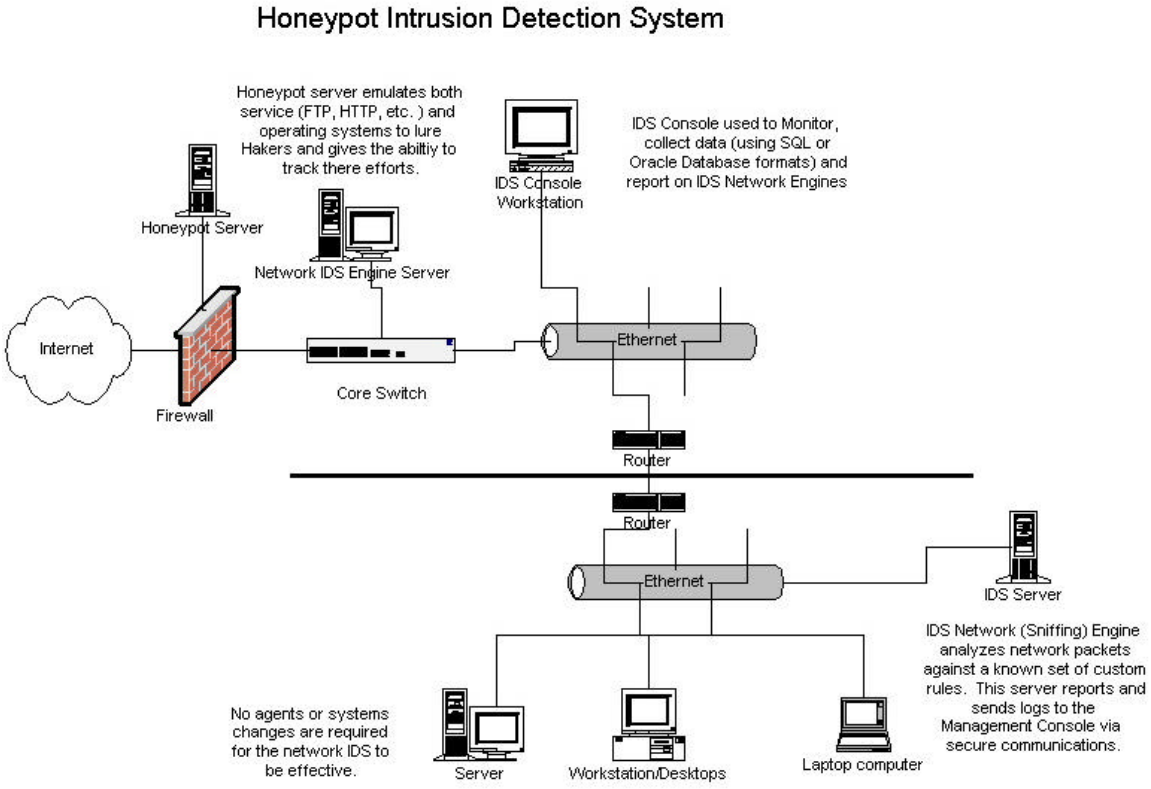


Figure 1-4

d. Hybrid IDS

Hybrid Intrusion Detection Systems are the "IDS of the Future". They exist in a limited form but are still on the cutting edge of technologies for IDS itself. They are based on a model which brings multiple agents of multiple types such as Simple Network Message Protocol (SNMP), Packet "sniffers", TCPdump (a Unix based network packet capture and filtering software), Cybercop Scanner, ISS Security Scanner, Snort IDS and other multi-vendor IDS systems all of which come into a **Centralized Management Console** and are analyzed by its centralized processors. Typically these product multi-vendor products are accumulated into a central Database Program or Engine such as SQL or Oracle. The purpose of this technology is to bring more flexibility, expandability and most important to cross-check anomalies against other systems to enhance there accuracy of the alerts and reduce "False Positives".

e. File Integrity Checking

Another use of Intrusion Detection is the File Integrity checking software. These programs develop a "Baseline" snapshot of the current file system or systems. Most create a MD5 hash (an encrypted algorithm used to verify integrity and consistency) of the file system and use this to do periodic scans of the file system to check for changes, file corruption, etc. Some of these products also check and update when service packages become available, are updated or changed. This type of program is very specific in nature and very specific to the operating systems in which they are placed upon. User or management intervention and monitoring are required. Also, for the most part these systems run on an "as schedule" basis. This software also requires "Super User" or "Administrative" rights on the systems to run, be installed, or modified. This software is installed locally on a computer and modifies that current file system if required. In very few cases this is run externally, in a remote type of check. This method of remote monitoring has been developed for some routers and switches to reduce the effect on the hardware and software requirements of the appliance.

2. A More Detailed Look at the FULL Snort IDS Architecture

The **Open Snort Sensor** is the powerful, industrial-strength, network based, intrusion detection system that performs real-time traffic analysis and packet logging. The full software package or "Snort-Bloat" version is complied with numerous added features called "processors". These processors perform unique analysis functions and can be turned "ON" or "OFF". This software is completely configurable for the client's environment. The Open Snort Sensor can perform intrusion detection for 100 Mbps+ networks with over 1,000 rules loaded, automatically generating real-time alerts to the Open Snort Sensor client user interface. ACID (**A**dvanced **C**onsole for **I**ntrusion **D**etection) is the graphical **Front End** for the Snort Sensor. This product displays a logical and sensible look at the data, which is captured by the Snort Sensor and placed in several MySQL database tables. This product is developed and supported by the CERT Coordination Center and the AIRCERT project located at Carnegie Melon University.

Refer to URL: **http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html**

a. Benefits of Network Based IDS

Some of the detailed benefits of the SNORT product and generally of most Networked Based IDS systems are as follows:

- It is passive so intruders are unaware of its presence.
- It requires no modifications to the hosts that it is monitoring.
- It analyzes data either as it is collected or after it is passed to the Management Console.

- It can provide real-time alert notification for intrusive behavior via Email or paging and several other methods.
- It can begin data gathering upon detection of intrusive behavior.
- It can terminate data gathering upon continued absence of intrusive behavior.
- It can replay data that flowed between computers so that intrusive behavior may be observed.
- It provides a full suite of analytical tools.
- It provides support for either command line or graphical user interface.
- It provides an interface for secure communications.
- It is highly user-customizable.

b. Snort Command Line ONLY Version Description

Snort command line only version is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug in architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or Win Popup messages to Windows clients using Samba's smb client. Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or as a full-blown network intrusion detection system. Snort logs packets in either tcpdump binary format or in Snort's decoded ASCII format to logging directories that are named based on the IP address of the "foreign" host

3. A Pictorial Presentation of Snort IDS

The following pictures are direct outputs from a Snort Sensor and presented using ACID Front End. Figure 3-1 is a presentation of the main page displayed by ACID. As one can note, there is a great deal of information on this page. Also note that these different selections on this page represent Hyper Link addresses to more detailed analysis or an in depth look at a particular of group of events. One selection directly under the mail “BAR” graph allows you to develop a graphic output of timed data for analysis. Other key factors are the presence of the total number of events, unique events and so on. An IP Packet is displayed in Figure 3-2 for analysis. Figure 3-3 displays a consolidated Snortreport output from a MySQL database developed by the Snort Sensor output. Figure 3-4 is a basic flow diagram for Snort with ACID data flow. Figure 3-5 is a description and cost analysis of Host based IDS. Figure 3-6 is a description and cost analysis of Network Based IDS Systems.

ACID Console Main Screen

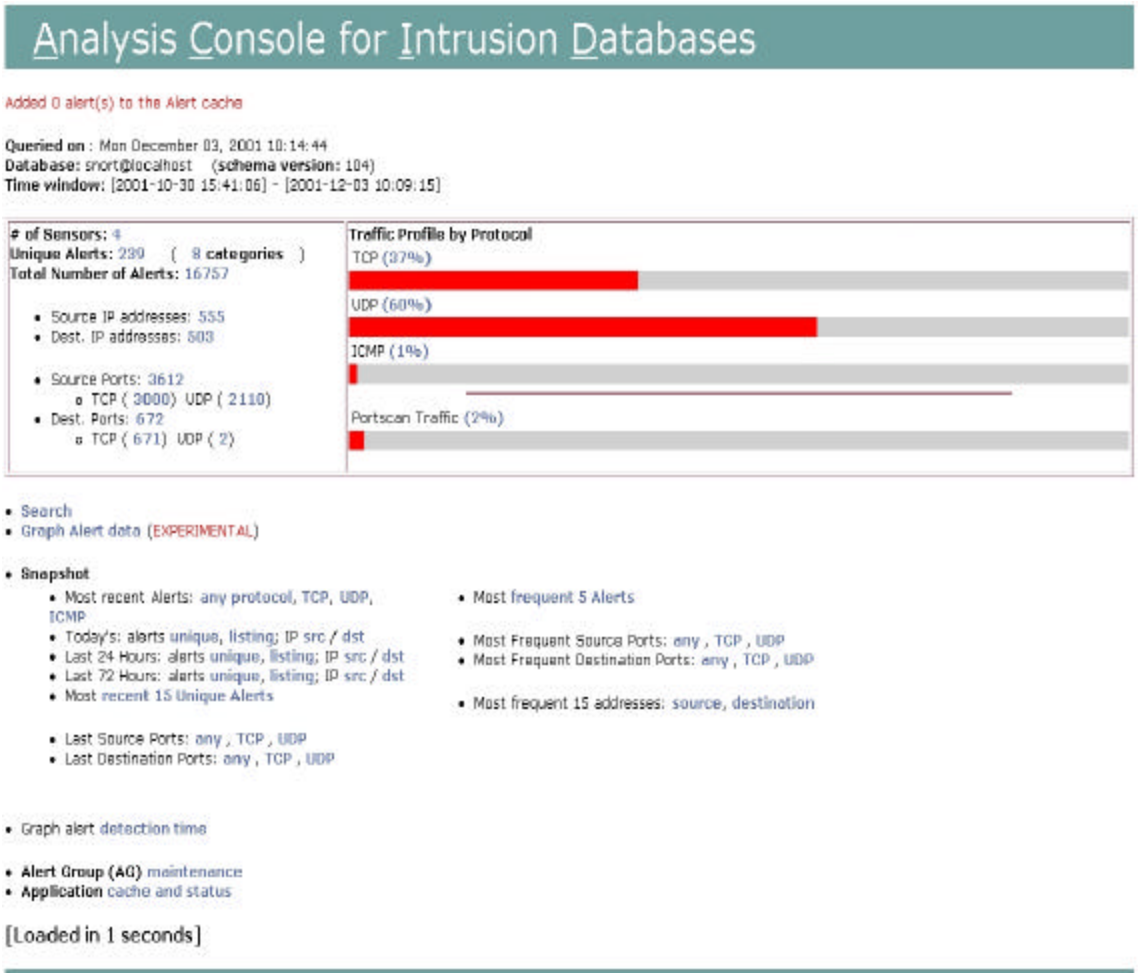
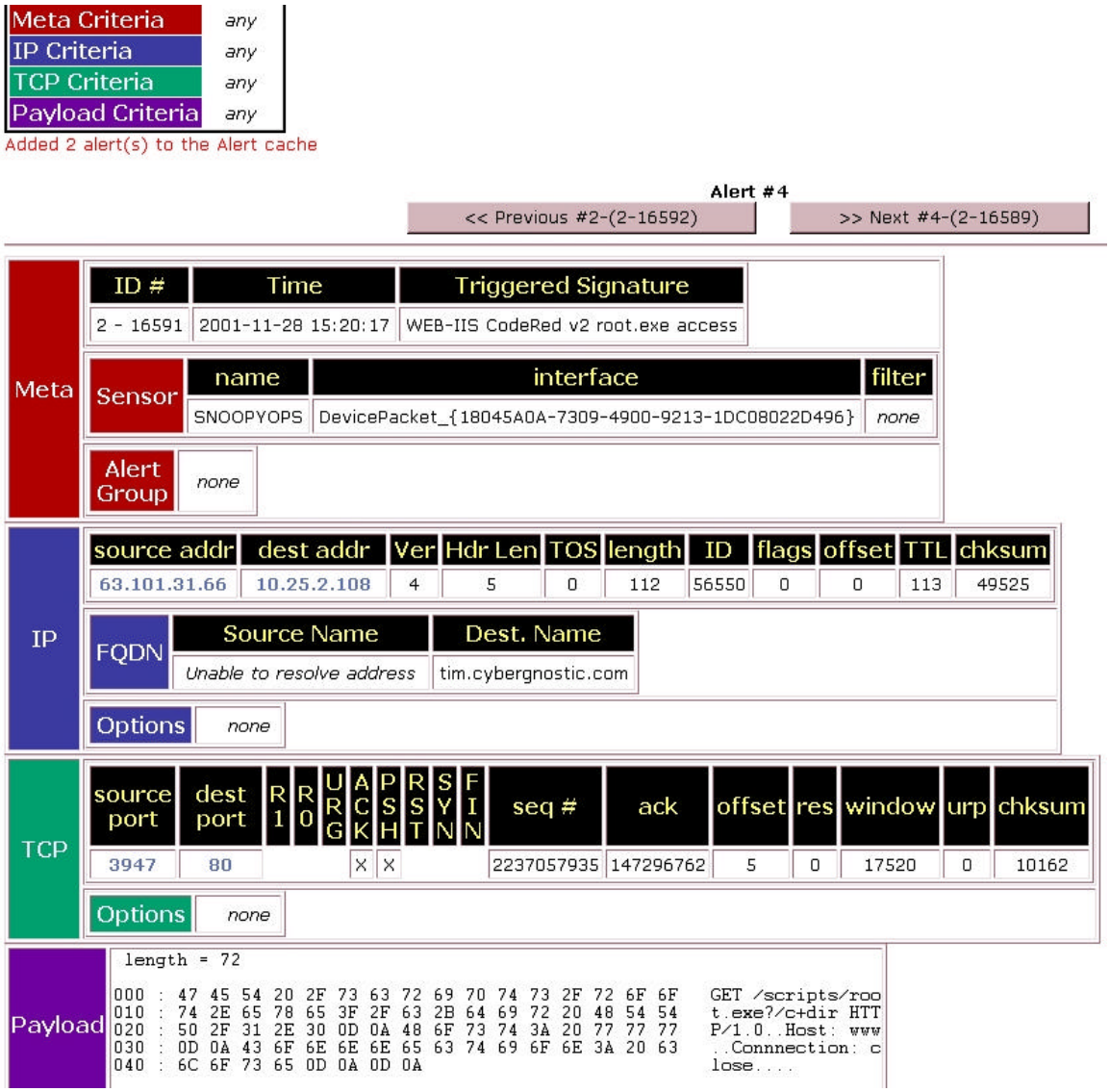


Figure 3-1

IP Packet Analysis of and Alert



Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

Added 2 alert(s) to the Alert cache

Alert #4

<< Previous #2-(2-16592) >> Next #4-(2-16589)

Meta

ID #	Time	Triggered Signature
2 - 16591	2001-11-28 15:20:17	WEB-IIS CodeRed v2 root.exe access

Sensor	name	interface	filter
	SNOOPYOPS	DevicePacket_{18045A0A-7309-4900-9213-1DC08022D496}	none

Alert Group: none

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
63.101.31.66	10.25.2.108	4	5	0	112	56550	0	0	113	49525

FQDN	Source Name	Dest. Name
	Unable to resolve address	tim.cybergnostic.com

Options: none

TCP

source port	dest port	R1	R0	URG	ACK	PSH	RST	SYN	FIN	seq #	ack	offset	res	window	urp	chksum
3947	80				X	X				2237057935	147296762	5	0	17520	0	10162

Options: none

Payload

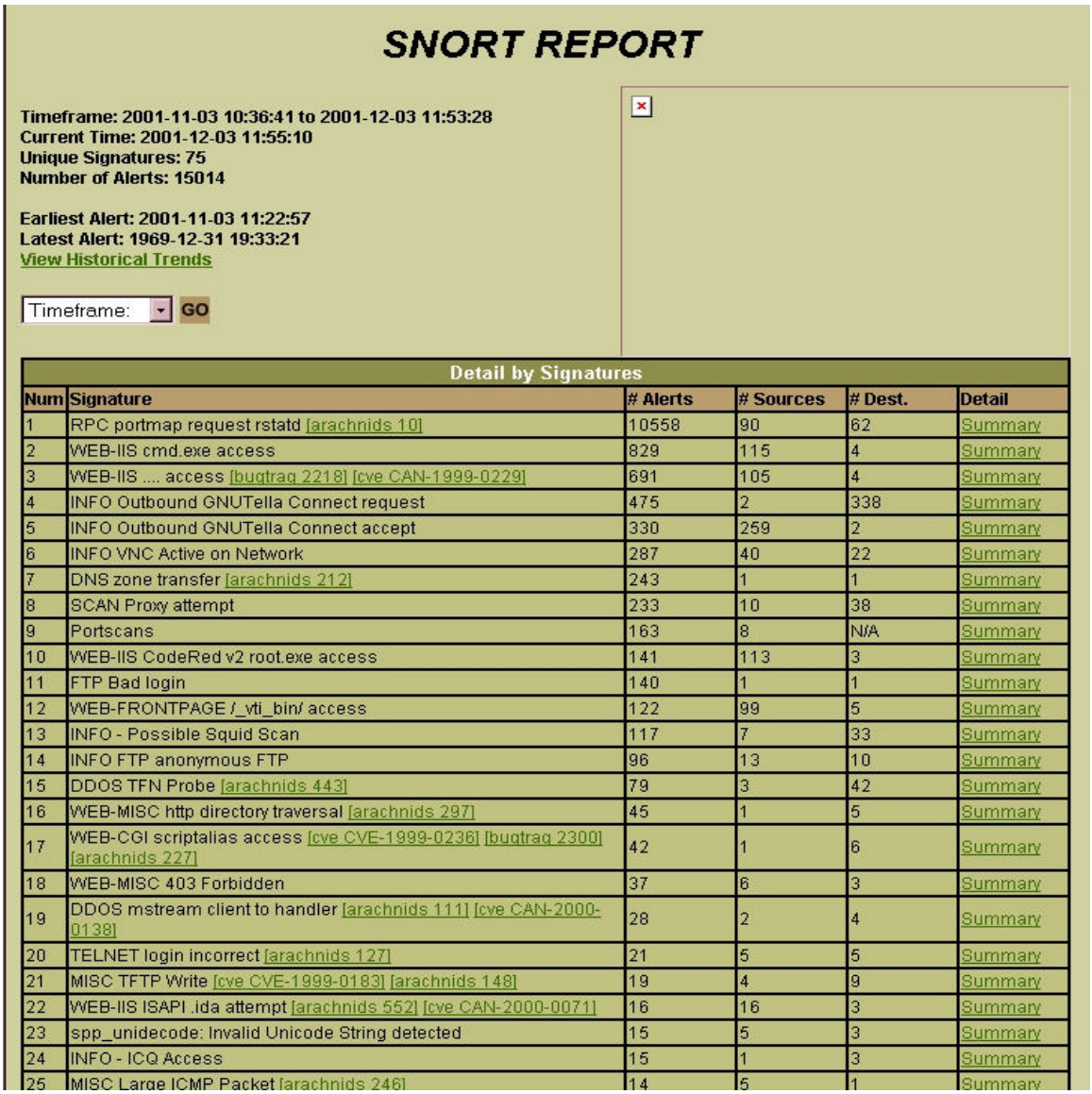
```
length = 72

000 : 47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F   GET /scripts/roo
010 : 74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54   t.exe?/c+dir HTT
020 : 50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77   P/1.0..Host: www
030 : 0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63   ..Connnection: c
040 : 6C 6F 73 65 0D 0A 0D 0A                           lose....
```

Figure 3-2

Snort Reports

Snortreports is a web based PHP scripted analysis and compilation of the "MySQL" database developed and stored by SNORT. This program can be run on and Microsoft IIS Web Server or an Apache Web server setup to interpret PHP scripted files.



SNORT REPORT

Timeframe: 2001-11-03 10:36:41 to 2001-12-03 11:53:28
Current Time: 2001-12-03 11:55:10
Unique Signatures: 75
Number of Alerts: 15014

Earliest Alert: 2001-11-03 11:22:57
Latest Alert: 1969-12-31 19:33:21
View Historical Trends

Timeframe: GO

Detail by Signatures

Num	Signature	# Alerts	# Sources	# Dest.	Detail
1	RPC portmap request rstatd [arachnids 10]	10558	90	62	Summary
2	WEB-IIS cmd.exe access	829	115	4	Summary
3	WEB-IIS .... access [bugtraq 2218] [cve CAN-1999-0229]	691	105	4	Summary
4	INFO Outbound GNUTella Connect request	475	2	338	Summary
5	INFO Outbound GNUTella Connect accept	330	259	2	Summary
6	INFO VNC Active on Network	287	40	22	Summary
7	DNS zone transfer [arachnids 212]	243	1	1	Summary
8	SCAN Proxy attempt	233	10	38	Summary
9	Portscans	163	8	N/A	Summary
10	WEB-IIS CodeRed v2 root.exe access	141	113	3	Summary
11	FTP Bad login	140	1	1	Summary
12	WEB-FRONTPAGE /_vti_bin/ access	122	99	5	Summary
13	INFO - Possible Squid Scan	117	7	33	Summary
14	INFO FTP anonymous FTP	96	13	10	Summary
15	DDOS TFN Probe [arachnids 443]	79	3	42	Summary
16	WEB-MISC http directory traversal [arachnids 297]	45	1	5	Summary
17	WEB-CGI scriptalias access [cve CVE-1999-0236] [bugtraq 2300] [arachnids 227]	42	1	6	Summary
18	WEB-MISC 403 Forbidden	37	6	3	Summary
19	DDOS mstream client to handler [arachnids 111] [cve CAN-2000-0138]	28	2	4	Summary
20	TELNET login incorrect [arachnids 127]	21	5	5	Summary
21	MISC TFTP Write [cve CVE-1999-0183] [arachnids 148]	19	4	9	Summary
22	WEB-IIS ISAPI .ida attempt [arachnids 552] [cve CAN-2000-0071]	16	16	3	Summary
23	spp_unidecode: Invalid Unicode String detected	15	5	3	Summary
24	INFO - ICQ Access	15	1	3	Summary
25	MISC Large ICMP Packet [arachnids 246]	14	5	1	Summary

Figure 3-3

Generic SNORT Process Flow Diagram used with
ACID and Snortreports

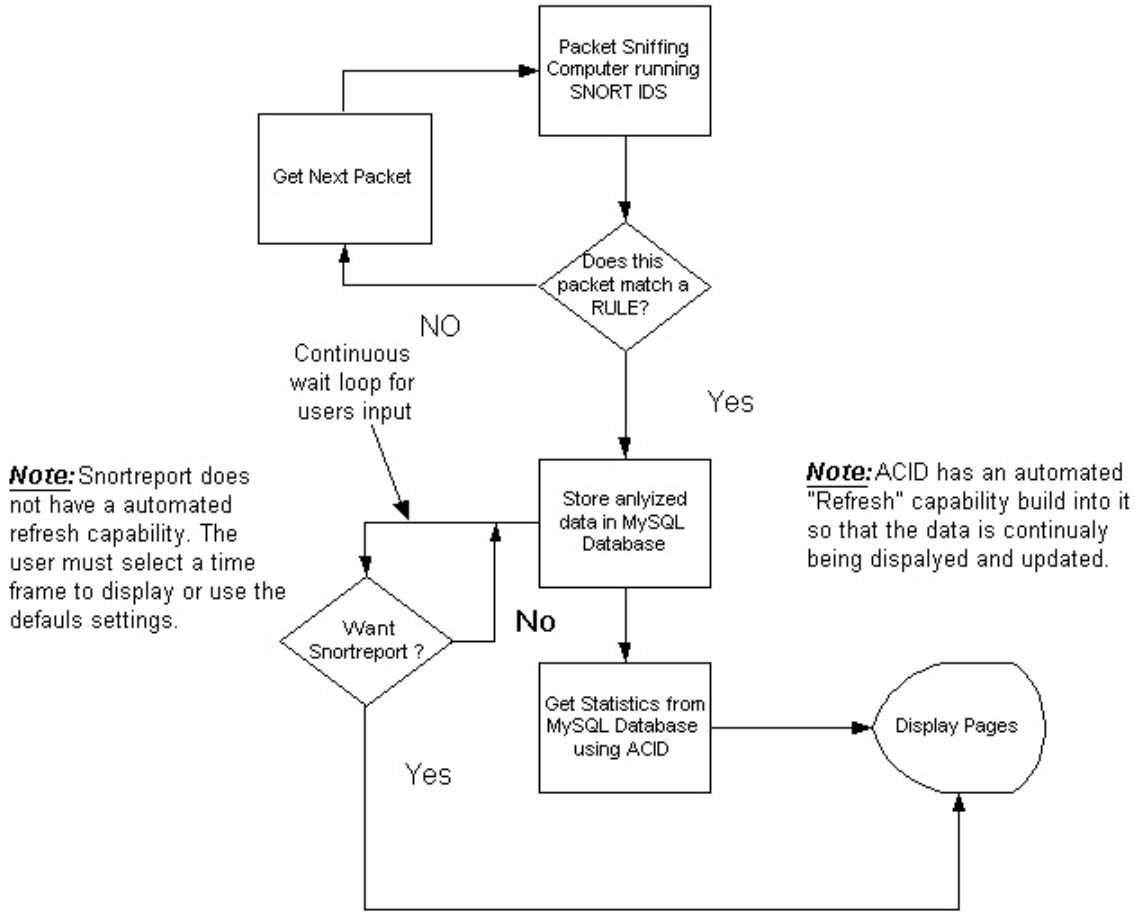


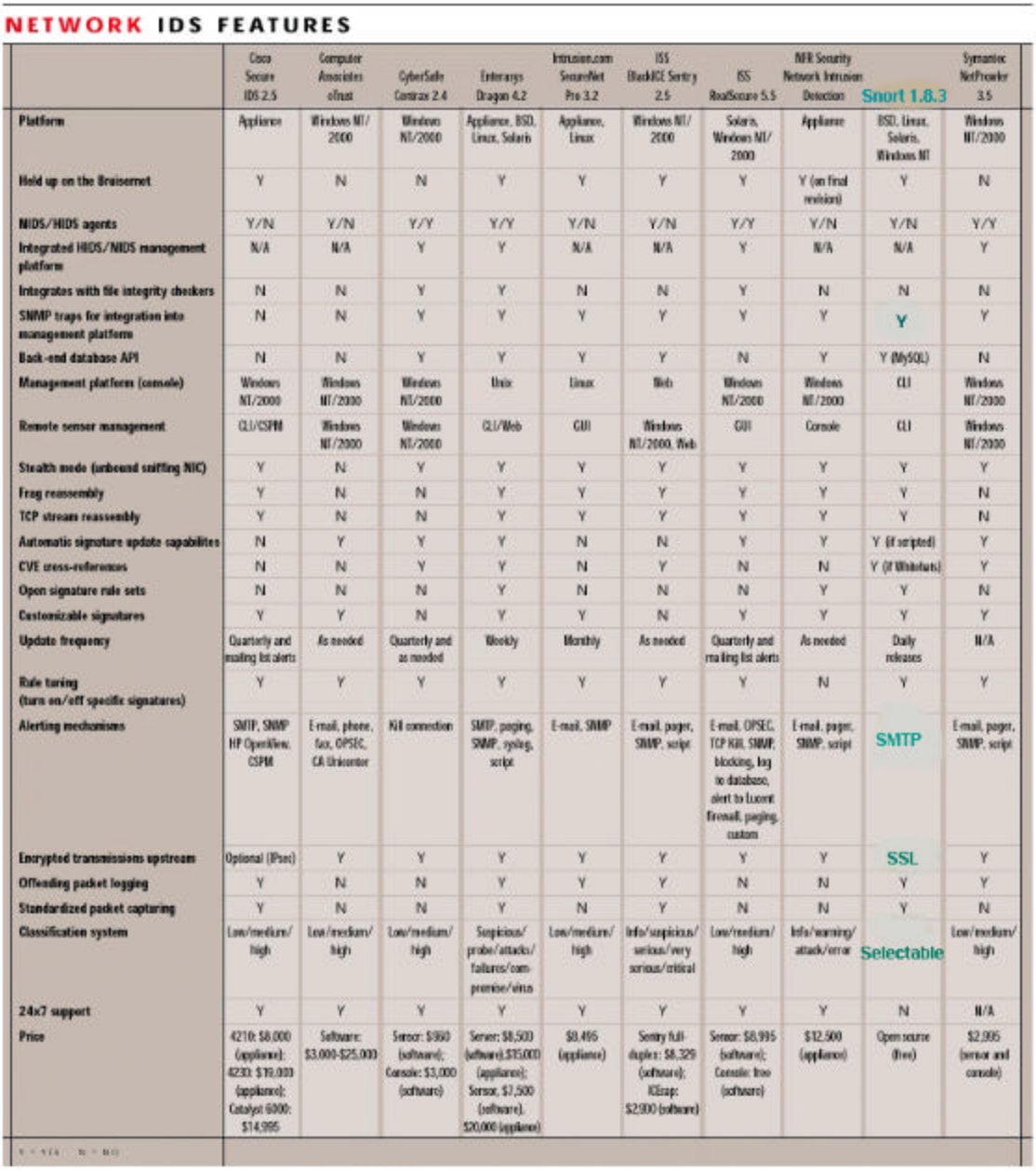
Figure 3-4

HOST-BASED IDS FEATURES

	CyberSafe Centrax 2.4	Enterasys Dragon 4.2	ISS RealSecure 5.5	Symantec Intruder Alert
Platform	AIX, HP/UX, Solaris, Windows NT/2000	BSD, HP-UX, Linux, Solaris	AIX, HP-UX, Linux, Solaris, Windows NT/2000	AIX, Digital Unix, HP-UX, Irix, NCR, NetWare, Solaris, SVR 4, Windows NT/2000
System log-based signatures	Y	Y	Y	Y
Web log-based signatures	N	N	N	N
Binary integrity checking	Y	Y	N	Y
Process monitoring	N	N	N	N
Centralized event/system logs	Y	N	Y	Y
Ties into unified console	Y	Y	Y	Y
Customizable signatures	Y	Y	Y	Y
Price (software only)	Agent: $960, Console: $3,000	Agent: $650, Console: $8,500	Licence: $750, Maintenance: $150	Agent: $995, Console: $1,995

Y = YES N = NO

Figure 3-5



NETWORK IDS FEATURES

	Cisco Secure IDS 2.5	Computer Associates eTrust	CyberSafe Centrax 2.4	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security Network Intrusion Detection	Snort 1.8.3	Symantec NetProwler 3.5
Platform	Appliance	Windows NT/2000	Windows NT/2000	Appliance, BSD, Linux, Solaris	Appliance, Linux	Windows NT/2000	Solaris, Windows NT/2000	Appliance	BSD, Linux, Solaris, Windows NT	Windows NT/2000
Hold up on the Brainernet	Y	N	N	Y	Y	Y	Y	Y (on final revision)	Y	N
NIDS/HIDS agents	Y/N	Y/N	Y/Y	Y/Y	Y/N	Y/N	Y/Y	Y/N	Y/N	Y/Y
Integrated HIDS/NIDS management platform	N/A	N/A	Y	Y	N/A	N/A	Y	N/A	N/A	Y
Integrates with file integrity checkers	N	N	Y	Y	N	N	Y	N	N	N
SNMP traps for integration into management platform	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Back-end database API	N	N	Y	Y	Y	Y	N	Y	Y (MySQL)	N
Management platform (console)	Windows NT/2000	Windows NT/2000	Windows NT/2000	Unix	Linux	Web	Windows NT/2000	Windows NT/2000	CLI	Windows NT/2000
Remote sensor management	CLI/CSPM	Windows NT/2000	Windows NT/2000	CLI/Web	GUI	Windows NT/2000, Web	GUI	Console	CLI	Windows NT/2000
Stealth mode (unbound sniffing NIC)	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Frag reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
TCP stream reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
Automatic signature update capabilities	N	Y	Y	Y	N	N	Y	Y	Y (if scripted)	Y
CVE cross-references	N	N	Y	Y	N	Y	N	N	Y (if Whitehats)	Y
Open signature rule sets	N	N	N	Y	N	N	N	Y	Y	N
Customizable signatures	Y	Y	N	Y	Y	N	Y	Y	Y	Y
Update frequency	Quarterly and mailing list alerts	As needed	Quarterly and as needed	Weekly	Monthly	As needed	Quarterly and mailing list alerts	As needed	Daily releases	N/A
Rule tuning (turn on/off specific signatures)	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Alerting mechanisms	SMTP, SNMP HP OpenView, CSPM	E-mail, phone, fax, OPSEC, CA Unicenter	Kill connection	SMTP, paging, SNMP, syslog, script	E-mail, SNMP	E-mail, pager, SNMP, script	E-mail, OPSEC, TCP Kill, SNMP, blocking, log to database, alert to Lucent firewall, paging, custom	E-mail, pager, SNMP, script	SMTP	E-mail, pager, SNMP, script
Encrypted transmissions upstream	Optional (IPsec)	Y	Y	Y	Y	Y	Y	Y	SSL	Y
Offending packet logging	Y	N	N	Y	Y	Y	N	N	Y	Y
Standardized packet capturing	Y	N	N	Y	N	Y	N	N	Y	N
Classification system	Low/medium/high	Low/medium/high	Low/medium/high	Suspicious/probe/attacks/failures/compromise/virus	Low/medium/high	Info/suspicious/serious/very serious/critical	Low/medium/high	Info/warning/attack/error	Selectable	Low/medium/high
24x7 support	Y	Y	Y	Y	Y	Y	Y	Y	N	N/A
Price	4210: $8,000 (appliance); 4230: $19,000 (appliance); Catalyst 6000: $14,995	Software: $3,000-$25,000	Sensor: $960 (software); Console: $3,000 (software)	Server: $8,500 (software), $15,000 (appliance); Sensor, $7,500 (software), $20,000 (appliance)	$8,495 (appliance)	Sentry full-duplex: $8,329 (software); IDSnap: $2,900 (software)	Sensor: $8,995 (software); Console: free (software)	$12,500 (appliance)	Open source (free)	$2,995 (sensor and console)

Figure 3-6 **Note:** Graph was altered to reflect the latest update information and abilities of Snort 1.8.3

Figures 3-5 and 3-6 are courtesy of **http://www.networkcomputing.com/**