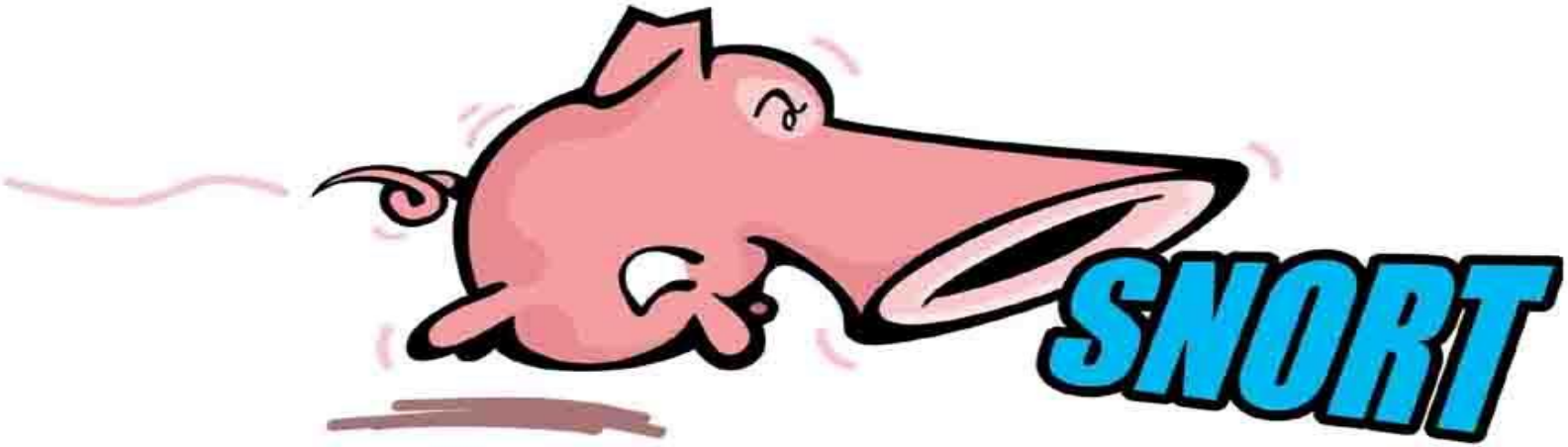
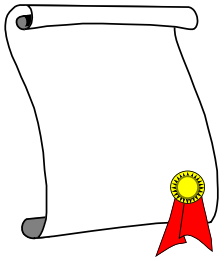


SNORT

Topics

- Background
  - What is Snort?
- Using Snort
- Snort Architecture
- Third-Party Enhancements

Background – Policy



- Successful intrusion detection depends on policy and management as much as technology
  - Security Policy (defining what is acceptable and what is being defended) is the first step
  - Notification
    - Who, how fast?
  - Response Coordination

Intro to Snort

- What is Snort?
  - Snort is a multi-mode packet analysis tool
    - Sniffer
    - Packet Logger
    - Forensic Data Analysis tool
    - Network Intrusion Detection System
- Where did it come from?
  - Developed out of the evolving need to perform network traffic analysis in both real-time and for forensic post processing

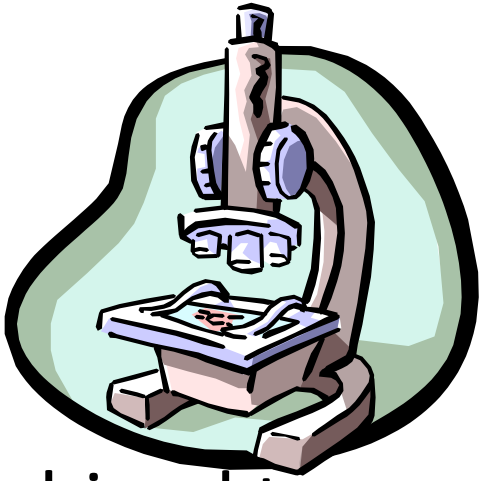
Snort “Metrics”

- Portable (Linux, Windows, MacOS X, Solaris, BSD, IRIX, Tru64, HP-UX, etc)
- Fast (High probability of detection for a given attack on 100Mbps networks)
- Configurable (Easy rules language, many reporting/logging options
- Free (GPL/Open Source Software)

Snort Design

- Packet sniffing “lightweight” network intrusion detection system
- Libpcap-based sniffing interface
- Rules-based detection engine
- Plug-in system allows endless flexibility

Detection Engine

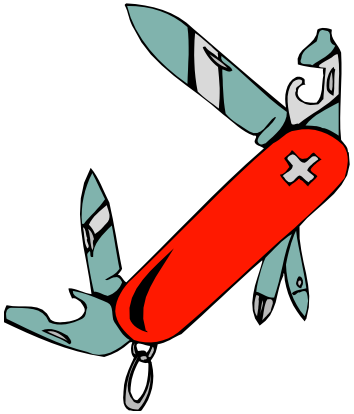


- Rules form “signatures”
- Modular detection elements are combined to form these signatures
- Wide range of detection capabilities
  - Stealth scans, OS fingerprinting, buffer overflows, back doors, CGI exploits, etc.
- Rules system is very flexible, and creation of new rules is relatively simple

Plug-Ins

- Preprocessor
  - Packets are examined/manipulated before being handed to the detection engine
- Detection
  - Perform single, simple tests on a single aspect/field of the packet
- Output
  - Report results from the other plug-ins

Using Snort



- Three main operational modes
  - Sniffer Mode
  - Packet Logger Mode
  - NIDS Mode
  - (Forensic Data Analysis Mode)
- Operational modes are configured via command line switches
  - Snort automatically tries to go into NIDS mode if no command line switches are given, looks for snort.conf configuration file in /etc

Using Snort – Sniffer Mode

- Works much like tcpdump
- Decodes packets and dumps them to stdout
- BPF filtering interface available to shape displayed network traffic

What Do The Packet Dumps Look Like?

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/09-11:12:02.954779 10.1.1.6:1032 -> 10.1.1.8:23
TCP TTL:128 TOS:0x0 ID:31237 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x16B6DA  Ack: 0x1AF156C2  Win: 0x2217  TcpLen: 20
FF FC 23 FF FC 27 FF FC 24 FF FA 18 00 41 4E 53  ..#..'..$....ANS
49 FF F0                                         I..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/09-11:12:02.956582 10.1.1.8:23 -> 10.1.1.6:1032
TCP TTL:255 TOS:0x0 ID:49900 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1AF156C2  Ack: 0x16B6ED  Win: 0x2238  TcpLen: 20
0D 0A 0D 0A 53 75 6E 4F 53 20 35 2E 37 0D 0A 0D  ....SunOS 5.7...
00 0D 0A 0D 00                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Packet Logger Mode

- Gee, it sure would be nice if I could save those packets to disk…
- Multi-mode packet logging options available
  - Flat ASCII, tcpdump, XML, database, etc available
- Log all data and post-process to look for anomalous activity

NIDS Mode

- Wide variety of rules available for signature engine (~1300 as of June 2001, grow to ~2900 at May 2005, now ~6000 rules)
- Multiple detection modes available via rules and plug-ins
  - Rules/signature
  - Statistical anomaly
  - Protocol verification

Snort Rules

Snort Rules

- Snort rules are extremely flexible and are easy to modify
- Sample rule to detect SubSeven trojan:

```
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR
   subseven 22"; flags: A+; content: "|0d0a5b52504c5d3030320d0a|";
   reference:arachnids,485; reference:url,www.hackfix.org/subseven/;
   sid:103; classtype:misc-activity; rev:4;)
```

- Elements before parentheses comprise ‘rule header’
- Elements in parentheses are ‘rule options’

Snort Rules

```
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR
   subseven 22"; flags: A+; content:
   "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;
   reference:url,www.hackfix.org/subseven/; sid:103;
   classtype:misc-activity; rev:4;)
```

- **alert** action to take; also **log, pass, activate, dynamic**
- **tcp** protocol; also **udp, icmp, ip**
- **$EXTERNAL_NET** source address; this is a variable – specific IP is ok
- **27374** source port; also **any**, negation (**!21**), range (**1:1024**)
- **->** direction; best not to change this, although **<>** is allowed
- **$HOME_NET** destination address; this is also a variable here
- **any** destination port

Snort Rules

```
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR
   subseven 22"; flags: A+; content:
   "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;
   reference:url,www.hackfix.org/subseven/; sid:103;
   classtype:misc-activity; rev:4;)
```

- **`msg:"BACKDOOR subseven 22";`** message to appear in logs
- **`flags: A+;`** tcp flags; many options, like `SA, SA+, !R`
- **`content: "|0d0…0a|";`** binary data to check in packet; content without | (pipe) characters do simple content matches
- **`reference…;`** where to go to look for background on this rule
- **`sid:103;`** rule identifier
- **`classtype: misc-activity;`** rule type; many others
- **`rev:4;`** rule revision number
- other rule options possible, like **`offset, depth, nocase`**

Snort Rules

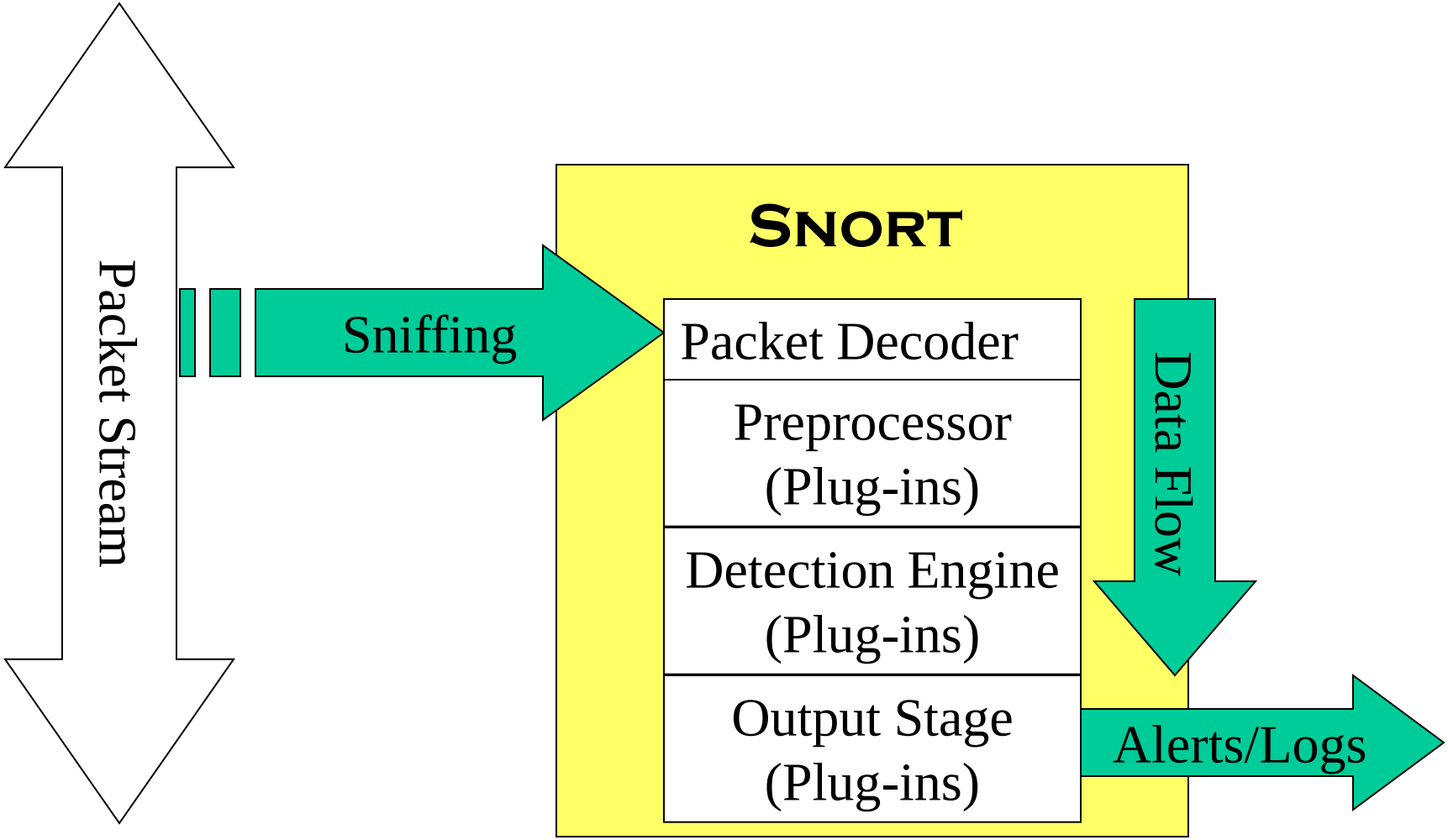
- bad-traffic.rules exploit.rules scan.rules
- finger.rules ftp.rules telnet.rules
- smtp.rules rpc.rules rservices.rules
- dos.rules ddos.rules dns.rules
- tftp.rules web-cgi.rules web-coldfusion.rules
- web-frontpage.rules web-iis.rules web-misc.rules
- web-attacks.rules sql.rules x11.rules
- icmp.rules netbios.rules misc.rules
- backdoor.rules shellcode.rules policy.rules
- porn.rules info.rules icmp-info.rules
- virus.rules local.rules attack-responses.rules

Snort Rules

- Rules which actually caught intrusions
  - **`alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"MS-SQL xp_cmdshell - program execution"; content: "x|00|p|00|_|00|c|00|m|00|d|00|s|00|h|00|e|00|l|00|l|00| "; nocase; flags:A+; classtype:attempted-user; sid:687; rev:3;)`** caught compromise of Microsoft SQL Server
  - **`alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS cmd.exe access"; flags: A+; content:"cmd.exe"; nocase; classtype:web-application-attack; sid:1002; rev:2;)`** caught Code Red infection
  - **`alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"INFO FTP \"MKD / \" possible warez site"; flags: A+; content:"MKD / "; nocase; depth: 6; classtype:misc-activity; sid:554; rev:3;)`** caught anonymous ftp server

Snort Architecture

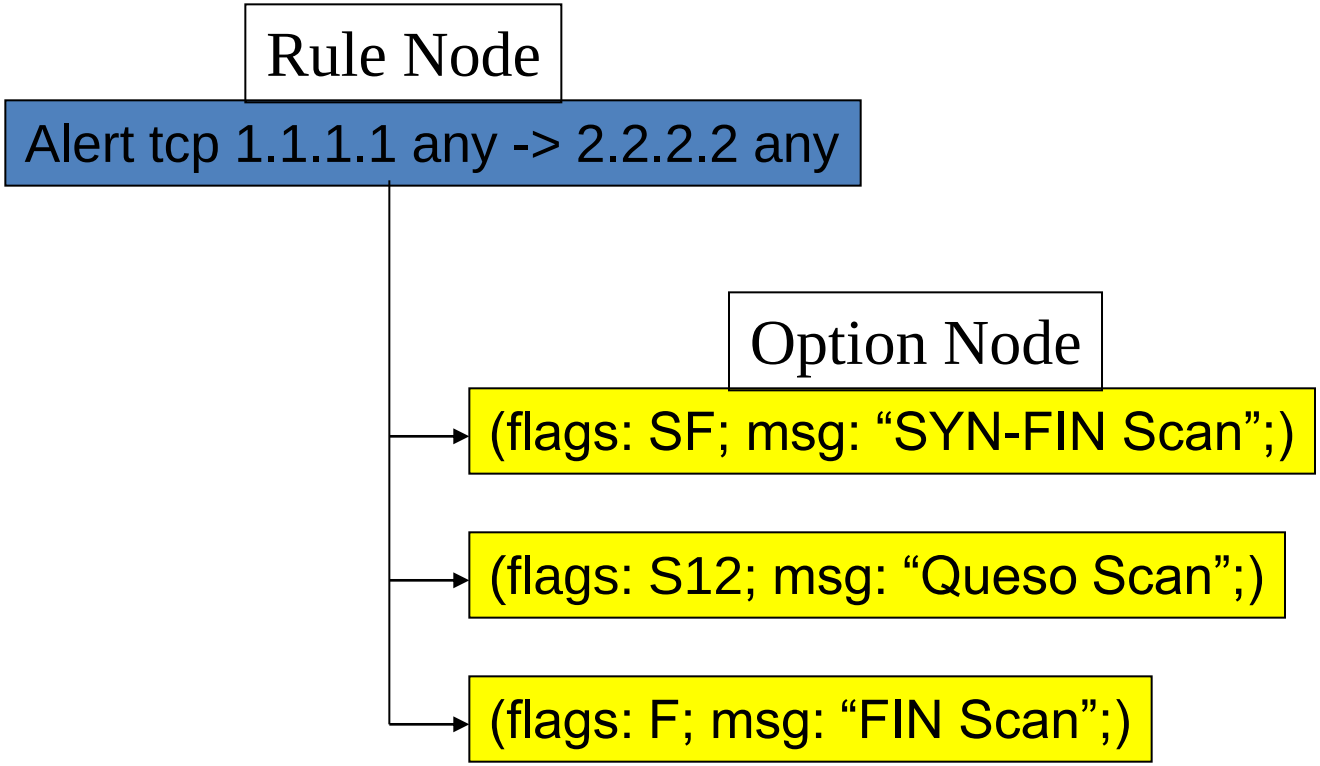
Data Flow


Packet Stream
Sniffing
SNORT
Packet Decoder
Preprocessor
(Plug-ins)
Detection Engine
(Plug-ins)
Output Stage
(Plug-ins)
Data Flow
Alerts/Logs

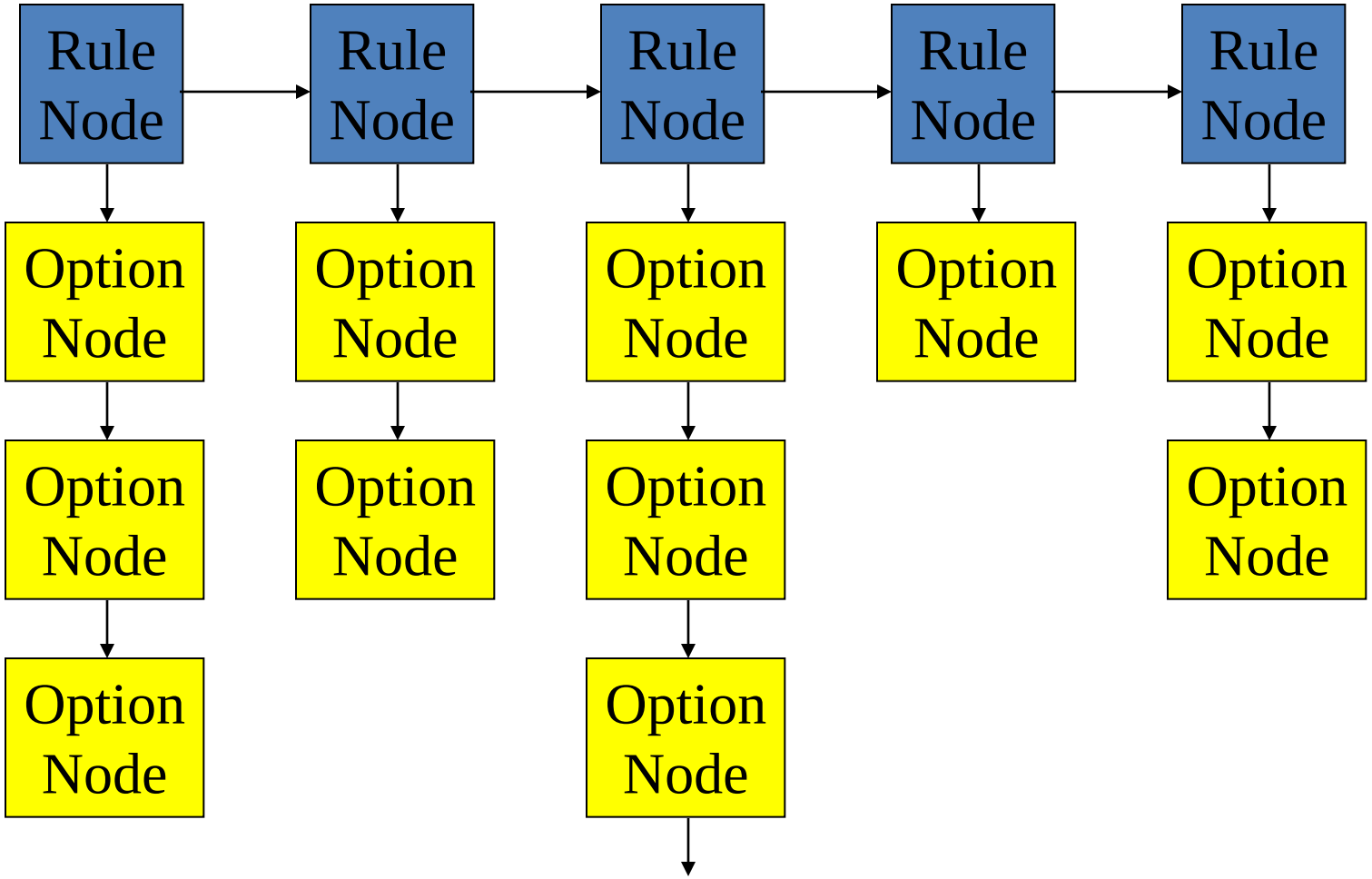
Detection Engine: Rules

Rule Header	Rule Options
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: SF; msg: “SYN-FIN Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: S12; msg: “Queso Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: F; msg: “FIN Scan”;)

Detection Engine: Internal Representation



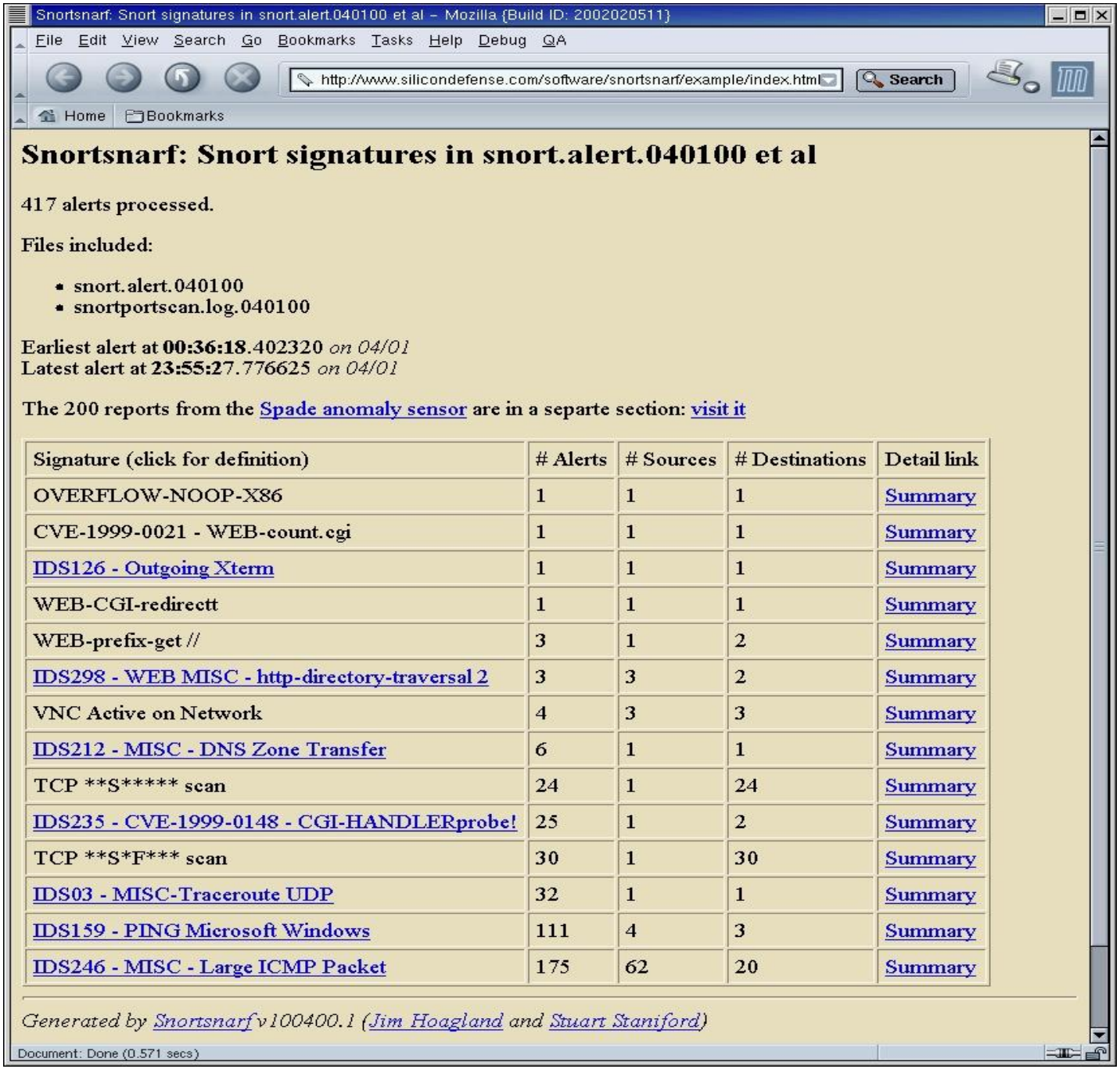
Detection Engine: Fully Populated



Third-Party Enhancements

SnortSnarf

- http://www.snort.org/dl/contrib/data_analysis/snortsnarf/
- SnortSnarf is a Perl program to take files of alerts from the Snort to produce HTML reports
- Output intended for diagnostic inspection
- Used to have commercial support from SiliconDefense



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*

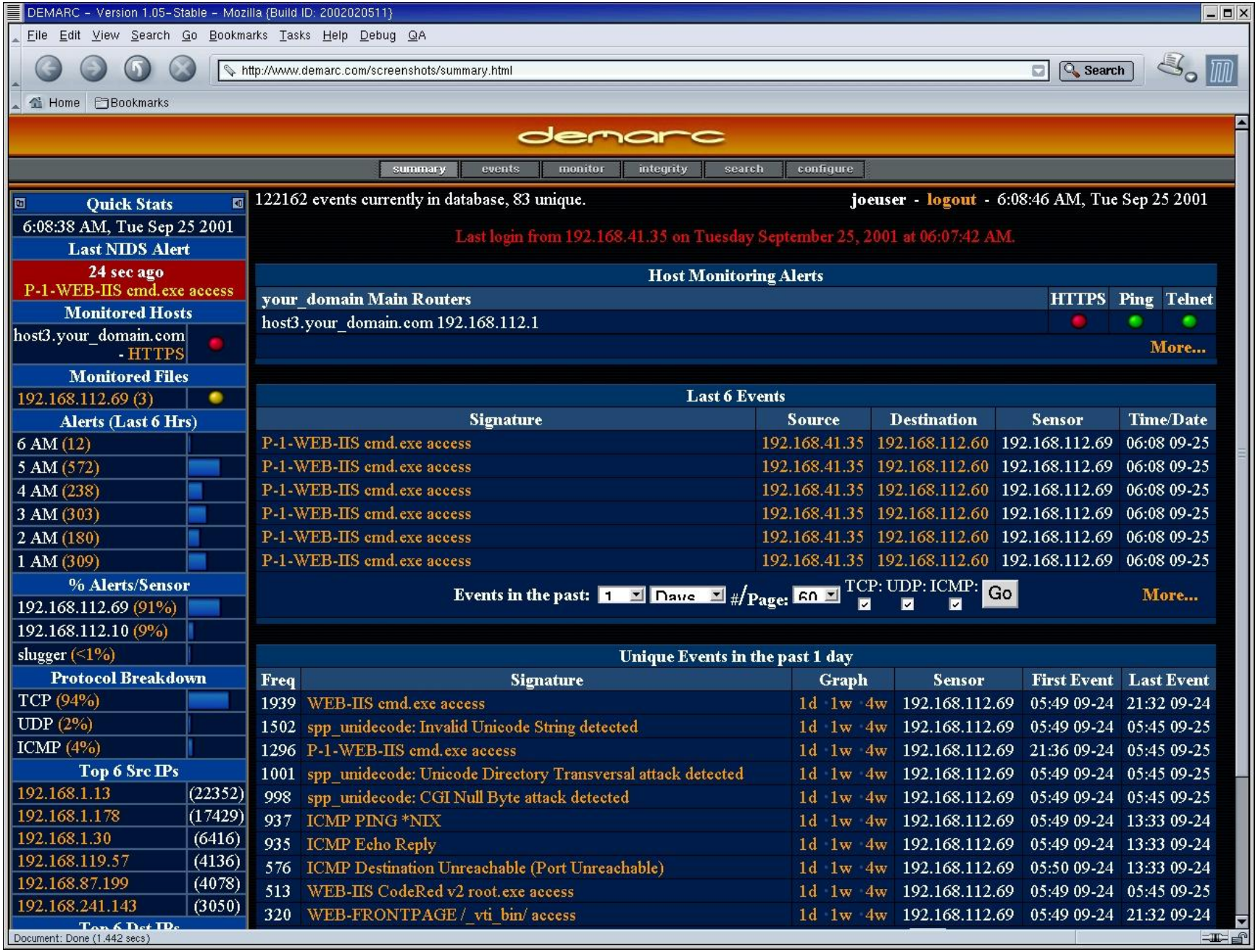
The 200 reports from the Spade anomaly sensor are in a separte section: visit it

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)

Demarc

- www.demarc.com
- NIDS management console, integrating Snort with the convenience and power of a centralized interface for all network sensors
- Commercialized by *Applied Watch* for **Enterprise Open Source Security Management**
  - Snort® (IDS)
  - Snort-Inline (IPS)
  - Labrea Tarpit (Sticky Honeypot)
  - ClamAV (Antivirus)
  - Nessus (Vulnerability Management)



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)

Conclusion

- Snort is a powerful tool, but maximizing its usefulness requires a trained operator
- Becoming proficient with network intrusion detection takes 12 months; “expert” 24-36?
- Snort is considered a very good NIDS when compared to most commercial systems
- Managed network security providers should collect enough information to make decisions without calling clients to ask what happened