Advanced Hacking Techniques & Intrusion Detection Experiences with Snort

LinuxWorld 2003, San Francisco
Thursday, August 7, 2003, 1:00 pm-2:15 pm, S82
Thorsten Weigl, weigl interservice

Overview #1

1. Introduction
1.1 What is Intrusion Detection?
1.2 What is a Intrusion Detection System
1.3 What is the status quo
1.4 Typically used Systems

2. Snort
2.1 What is Snort?
2.2 Architecture of Snort 2.0
2.3 Which Features has Snort 2.0?
2.4 Plug-ins for Snort?
2.5 Option: Make your own Snort Rules

Overview #2

3. Advanced Hacking Techniques and Experiences
3.1 The Automated Hacking Techniques
3.2 Simple Hacking Techniques
3.3 "Better" Hacking Techniques (Part 1)
3.4 "Better" Hacking Techniques (Part 2)
3.5 "Advanced" Hacking Techniques
3.6 Really Dangerous Hacking Techniques

4. Experiences with Snort
4.1 My Experiences with Snort
4.2 Behavior of Snort
4.3 Conclusion

Appendix 1: Abbreviations
Appendix 2: Snort Rules – Advanced Example

1.1 What is Intrusion Detection?

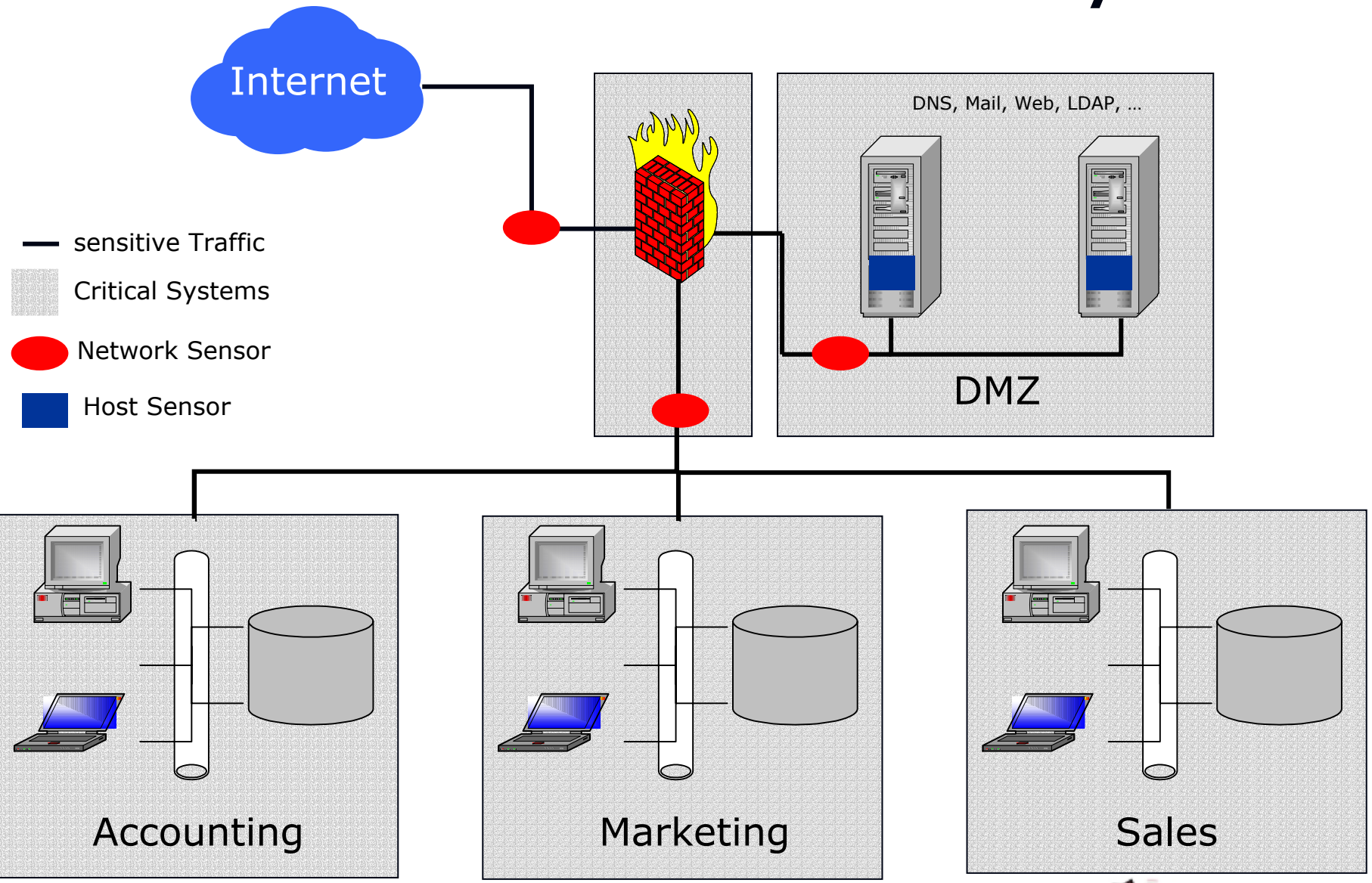
Example Log 1

2002-05-08 22:27:29 131.128.2.170 - 123. 123.123.123 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u90
90%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd
3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078
%u0000%u00=a 200 -

Example Log 2

195.219.147.75 - - [13/May/2002:00:12:56 +0200] "GET /MSADC/root.exe?/c+dir HTTP/1.0" 404 276
195.219.147.75 - - [13/May/2002:00:12:58 +0200] "GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 286
195.219.147.75 - - [13/May/2002:00:13:01 +0200] "GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 286
195.219.147.75 - - [13/May/2002:00:13:03 +0200] "GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 300
195.219.147.75 - - [13/May/2002:00:13:08 +0200] "GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 317

1.2 What is a Intrusion Detection System?



1.3 What is the status quo

Network-based and host-based intrusion prevention systems:

Dynamic Attack Responses: RST Packets, Updates of IP Chain Rules, Email to abuse …

Inspecting Gigabit Networks without packet loss

IP defragmentation and TCP stream reassembly

Stateful protocol analysis

1.4 Typically used Systems

For those how can afford up to possibly US $ 100,000 in License Fees …

- ISS Real Secure
- Enterasys Dragon
- Okena StormWatch
- Forescout ActiveScout

For those how need the source files …

- Snort (http://www.snort.org/)
- Prelude-IDS (http://www.prelude-ids.org/)
- Hogwash (http://hogwosh.sourceforge.net/)

2.1 What is Snort?

A lightweight (800 kB) IDS which is under the Gnu Public License

Absolutely comparable with commercial IDS:

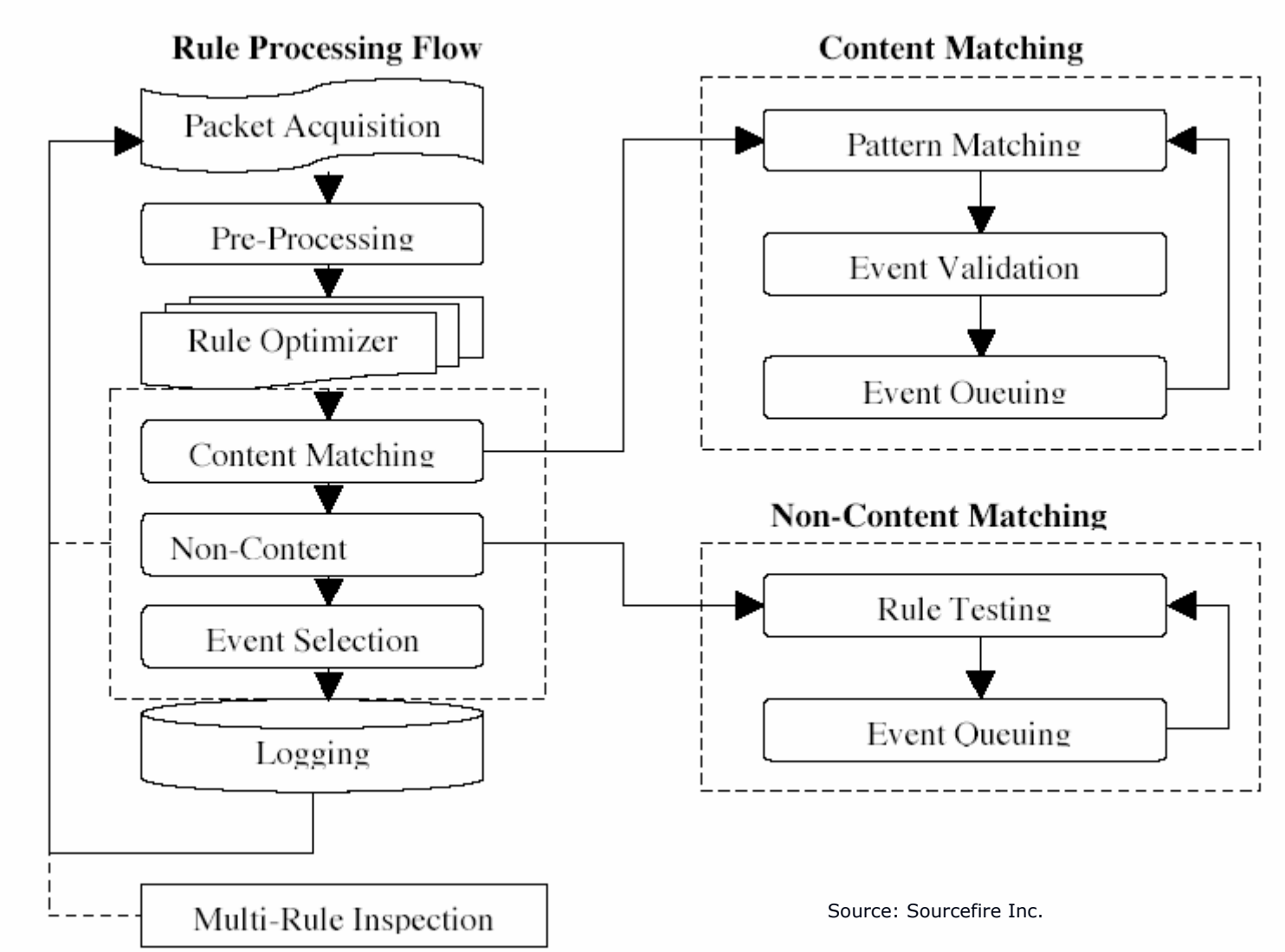
- 2,000 rules

- Event logging in gigabit environment (winner in several benchmark tests against commercial systems) is now possible

- Intrusion response with RST, Scripts, …

- Supports all Major DBs and OS

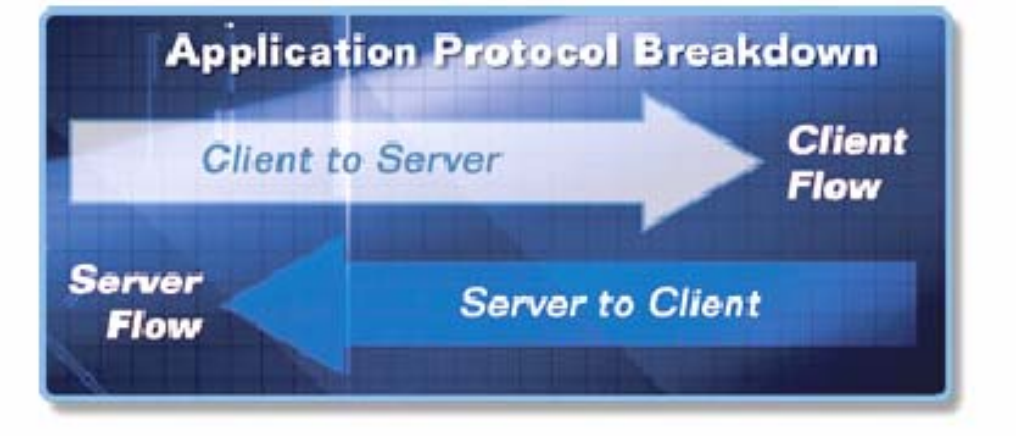
2.2 Architecture of Snort 2.0



Source: Sourcefire Inc.

2.3 Features of Snort 2.0

Protocol Flow Analyzer



Source: Sourcefire Inc.

Rule Optimizer

Enhanced processing Speed through multi-rule inspection algorithms

2.4 Plug-ins for Snort

ACID: Powerful web based GUI for analysis and visualizing

Guardian: Configures automatically IP Chains Rules

SnortNet: A distributed IDS approach

SnortSam: Automated blocking of IP Addresses in a Firewall (Checkpoint, Cisco, Netscreen, Watchguard)

SnortCenter: Web based Rule and Sensor Management

2.5 Option: Make your own Snort Rules Example 1

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”;)

2.5 Option: Make your own Snort Rules Example 2

Example

Alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS cmd.exe access"; Flow:to_server, established; content:"cmd.exe"; nocase; Classtype:web-application-attack;sid:1002;rev:5;)

Description

See if someone is trying to access port 80 and send the string „cmd.exe"

3.1 The Automated Hacking Techniques ...

Worms
Slammer
Code Red

Dos and DDos
Trin00
Stacheldraht
TFN

some false-positives ... for example if the sequence number is 674711609

3.2 Simple Hacking Techniques

Backdoors for Trojans
BackOrifice, SubSeven, NetBus, DeepThroat

Backdoors for Rootkits
HidePak

lots of false-positives

3.3 “Better” Hacking Techniques (Part 1)

Exploits (1)

sendmail 8.6.9 Exploit
no false-positives and no false-negatives

Ptrace bug ...
better patch your kernel or set
/proc/sys/kernel/modprobe to /cannot/own/me,
no signature exists

3.4 “Better” Hacking Techniques (Part 2)

Exploits (2)

Large ICMP Packet

99% are hits … false-negatives with some load balancers that send 1.500 byte packets to measure the latency for best routing

Fin Scan

100% strikes

3.5 “Advanced” Hacking Techniques

XSS – Cross Site Scripting

phpinfo() Attack

http://target/info.php?SERVER_ADDR="><script>alert('test');</script>

http://target/info.php?SERVER_ADDR=<script>alert(document.cookie);</script>

But there are only 8140 sites vulnerable ...

http://consult.cern.ch/xwho/people/<script>alert(,hallo cern');</script>

Cgi Attack

http://www.openbsd.org/cgi-bin/man.cgi/source

few signatures

3.6 Really Dangerous Hacking Techniques

Sniffer & Hijacker

Dsniff
no signature available

Hunt
no signature available

Ettercap
no signature available – only for root exploit

4.1 My Experiences with Snort

Noise Generators can fool snort
Stick or Snot

Code Morphing can fool snort also
http://secinf.net/info/ids/idspaper/idspaper.html

And remember even Snort cannot see ...
Social engineering
Other "Layer 8*)" related stuff …

*) where do you keep the passwords

4.2 Behavior of Snort

Technique	Detection
Worms, Dos, DDos	☺
Backdoors	☺
Packet Anomalies	😐
Port Scans	☺
XSS	😐
Sniffer & Hijacker	☹
Noise Generator	☹
Code Morphing	☹

4.3 Conclusion #1

Intrusion Detection only makes sense …

if security policies are deployed enterprise wide

and the ids is configured very good.

4.3 Conclusion #2

1. **No Signatures for Sniffer**
2. **Few Signatures for XSS**
3. **Very good alerting for Worms**

Please send questions and comments to

t.weigl@weigl.de

If you are in Munich do participate in the

Munich Snort Users Group Meeting

in any case visit

http://mucsnug.weigl.de

Appendix 1: Abbreviations

Cross Site Scripting: Malicious HTML Tags Embedded in Client Web Requests

Appendix 2:
Snort Rules – Advanced Example

Rule

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"RPC tooltalk TCP overflow attempt"; flow: To_server,established; content:"|00 01 86 F3|"; content:"|00 00 00 07|"; distance:4;within4; byte_jump: 4,12,relative,align;byte_test:4,>,128,20,relative:reference:cve, CVE-1999-0003,reference:bugtraq,122; Classtype:misc-attack;sid:1965;rev:2;)

Description

After getting a content of 4 bytes 0x00 0x00 0x00 0x07, go 12 bytes further into the packet and read 4 bytes and then move up. Then read 4 bytes from the payload and compare them to 128 with the > Operator 20 more bytes into the packet.