Network Security Monitoring Theory and Practice

Michael Boman
IT Security Researcher and Developer
proxy@11a.nu | http://proxy.11a.nu

About Me

- Born in Sweden, been working in Singapore for the last 6 years
- Spent the last 5 years specializing in IT Security
- Currently working for KPMG Singapore

Agenda

- Network Security Monitoring (NSM) Theory
- Network Security Monitoring (NSM) Practice

Assumptions

- Some intruders are smarter than you
- Intruders are unpredictable
- Prevention eventually fails

Limitations of Alert Based Approach

1)IDS generates an alert when a packet is matched

2)Analyst's interface displays the offending packet

3)Analyst trying to make decision regarding if the event is a false positive or if the incident response team needs to be informed

4)Usually no other information is easily available to the analyst to make a more informed judgement (if any was collected in the first place)

History of NSM

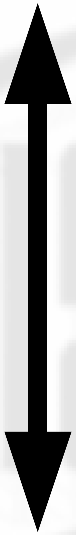
- 1980 – “Computer Security Threat Monitoring and Surveillance” (James P. Anderson)
- 1990 – “A Network Security Monitor” (L. Todd Heberlein et al.)
- 2002 – “Network Security Monitoring” (Bamm Visscher & Richard Bejtlich)
  - Defined NSM as “the collection, analysis and escalation of indications and warnings (I&W) to detect and respond to intrusions”

What is NSM?

- Collection
- Analysis
- Escalation

NSM Data Types

- Alert data
- Statistical
- Session
- Full content



Less

Storage requirement

More

Data Collection

- Collect as much data you legally and technically can

Data Collection

- Sometimes you can't collect everything, but consider this:
  - Data sampling is better than nothing
  - Traffic analysis is better than nothing

NSM's role in Incident Response

- What else did the intruder potentially compromise?
- What tools did he download?
- Who else do we need to inform?

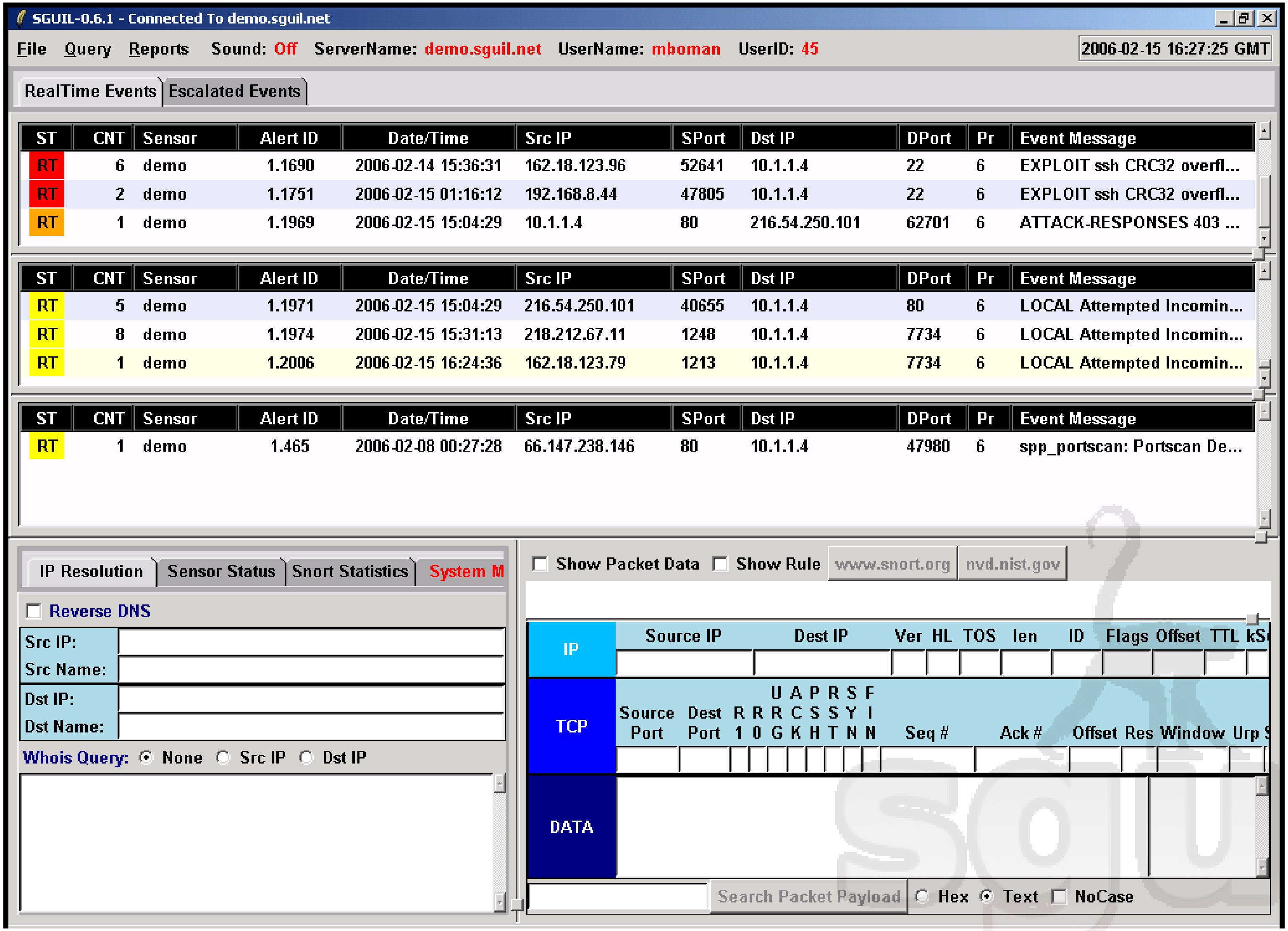
NSM in practice - Sguil

- Sguil is an open source project whose tag line is “For Analysts - By Analysts”
- Written in TCL/TK by Bamm Visscher, with many contributors (including myself)
- Sensor / Server / Client architecture

History of Sguil

- SPREG – Proprietary in-house ancestor of Sguil developed in Perl/TK, around 2000-2001
- Sguil development started late 2002
- First public release was 0.2, May 2003
- Current version is 0.6.1

Sguil Analyst Console



Sound: Off ServerName: demo.sguil.net UserName: mboman UserID: 45

2006-02-15 16:27:25 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	6	demo	1.1690	2006-02-14 15:36:31	162.18.123.96	52641	10.1.1.4	22	6	EXPLOIT ssh CRC32 overfl...
RT	2	demo	1.1751	2006-02-15 01:16:12	192.168.8.44	47805	10.1.1.4	22	6	EXPLOIT ssh CRC32 overfl...
RT	1	demo	1.1969	2006-02-15 15:04:29	10.1.1.4	80	216.54.250.101	62701	6	ATTACK-RESPONSES 403 ...

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	5	demo	1.1971	2006-02-15 15:04:29	216.54.250.101	40655	10.1.1.4	80	6	LOCAL Attempted Incomin...
RT	8	demo	1.1974	2006-02-15 15:31:13	218.212.67.11	1248	10.1.1.4	7734	6	LOCAL Attempted Incomin...
RT	1	demo	1.2006	2006-02-15 16:24:36	162.18.123.79	1213	10.1.1.4	7734	6	LOCAL Attempted Incomin...

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	demo	1.465	2006-02-08 00:27:28	66.147.238.146	80	10.1.1.4	47980	6	spp_portscan: Portscan De...

☐ Reverse DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☐ Show Packet Data ☐ Show Rule

○ Hex ● Text ☐ NoCase

Sguil Framework Demo

Future of Sguil

- PADS (Passive Asset Detection System) Integration
- SnortSAM Integration
- Snort rule management

NSM in the Real World

- Who is using it
  - Fortune 500 Companies
  - US Government Labs
  - Universities
  - MSSPs

NSM in the Real World

- Real life success stories
  - Charles Tomlin used Sguil to track down a recent compromise
    - http://www.ecs.soton.ac.uk/~cet/2006-01-01.html

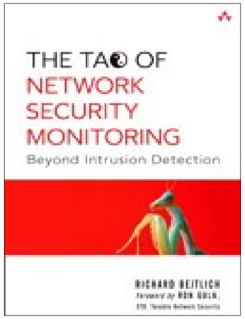
NSM in the Real World

- NSM Products / Projects
  - Apparently Sguil is the only public available product / project that utilizes NSM methodology

What NSM is Not

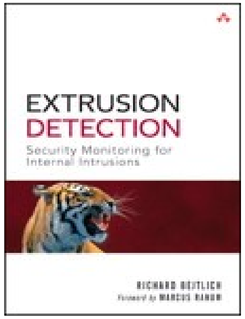
- NSM Is Not Device Management
- NSM Is Not Security Event Management
- NSM Is Not Network-Based Forensics
- NSM Is Not Intrusion Prevention

Books



THE TAO OF NETWORK SECURITY MONITORING
Beyond Intrusion Detection
RICHARD BEJTLICH
Foreword by RON GULA,
CTO, Tenable Network Security

- The Tao of Network Security Monitoring: Beyond Intrusion Detection
  - By Richard Bejtlich
  - Publisher: Addison-Wesley; ISBN: 0321246772



EXTRUSION DETECTION
Security Monitoring for Internal Intrusions
RICHARD BEJTLICH
Foreword by MARCUS RANUM

- Extrusion Detection: Security Monitoring for Internal Intrusions
  - By Richard Bejtlich
  - Publisher: Addison-Wesley; ISBN 0321349962

Thank You

Questions?

There is no secure end-state
– only eternal vigilance

My Website is at http://proxy.11a.nu

Sguil can be downloaded at http://www.sguil.net