

Network and System Security

A Bottom Up Approach 

Practical Network and System Security

Engineered Networks & Rockford Public Schools

ssurdock@engineered-net.com

PJYoung@rockford.k12.mi.us

www.engineered-net.com

www.rockford.k12.mi.us

Date: 10/07/05

© 2005 Engineered Networks

Rev: 1.0

Page: 1

Why Bother?

- Information
 - Confidentiality
 - Integrity
 - Availability
- Lawsuits
- Your Job

10,000 Foot View¹

- Assessment
- Protection
- Detection
- Response

Assessment – Bottom Up

- What are the vulnerabilities?
- What are the threats?
- What are the assets?
 - What is their value?
- What is the risk?
 - Risk = threat x vulnerability x asset value

Assessment - Techniques

- Identify the vulnerabilities
- Identify the threats
- Develop a plan & policies
- Methodologies
 - OCTAVE - <http://www.cert.org/octave/>



Assessment - Tools

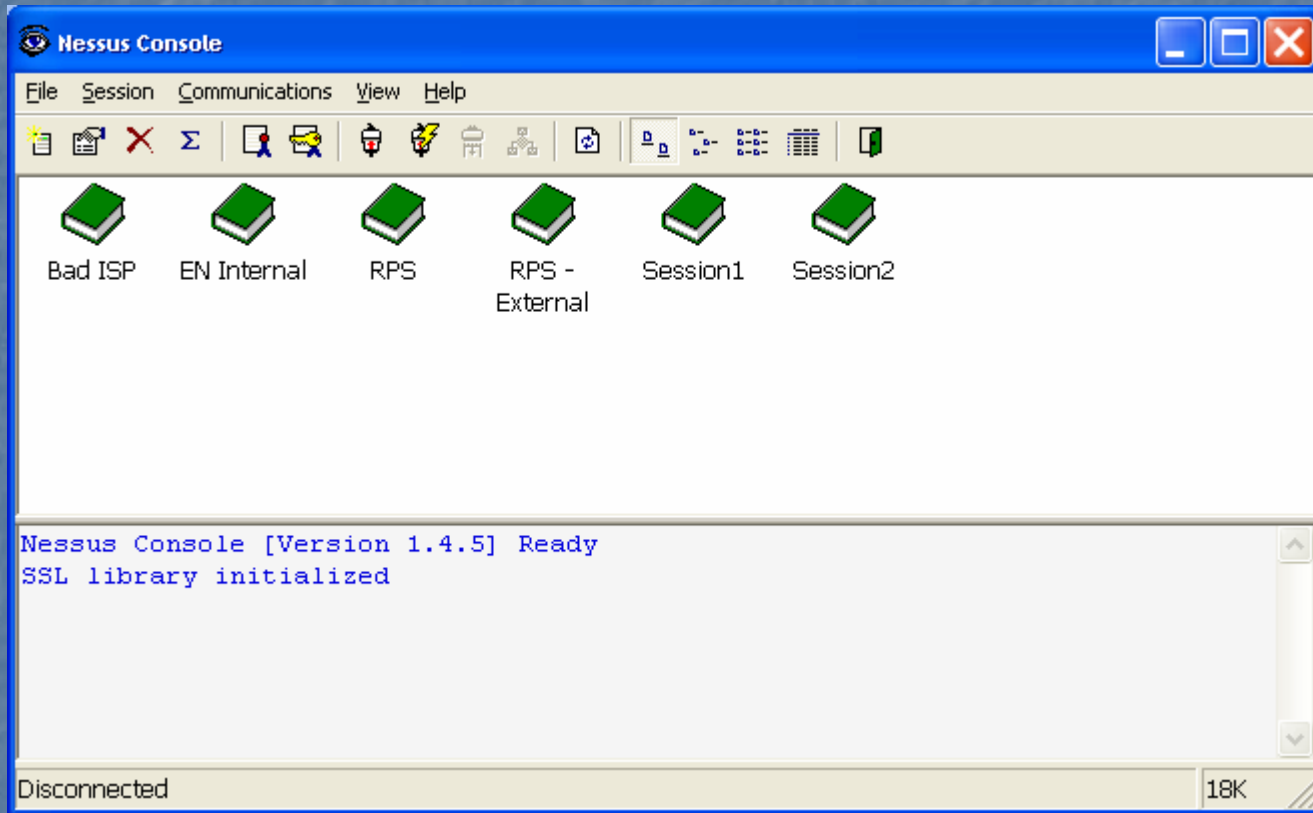
- We had a good idea of how the network is laid out
- We used Nessus to find vulnerabilities
- We used Snort find "bad" traffic & help identify threats

Assessment Tools - Nessus

■ Nessus Setup

- Intel Celeron 333 Mhz, 256 MB RAM
- OpenBSD 3.6 (Nessus installed as package)
- Download Nessus
<http://www.nessus.org/download/>
- Register Nessus to obtain lots of rules
- We ran it against the outside and the inside of the network

Nessus Windows Frontend



Assessment - Nessus Result

- External Scan Result – RPS 9/26, 11:18
 - 5 security holes found
 - 19 security warnings found
 - 62 security notes found
 - <File:///C:/cygwin/home/ssurdock/RPS/rps.20050926/index.html>

Assessment - Nessus Result

- Internal Scan Result – 10.1.0.0/21
 - 79 security holes found
 - 128 security warnings found
 - 626 security notes found
 - <File:///C:/cygwin/home/ssurdock/RPS/rps.10.1.0.0/index.html>

Assessment Tools - Snort

- What “bad” traffic on the DMZ now?
- Using Snort
 - 333 MHz Celeron with 256 MB RAM
 - OpenBSD 3.6
 - Download Snort <http://www.snort.org/dl/binaries/>
 - Register Snort to obtain lots of rules
 - Create a span/mirror/monitor port and plug in your sensor
 - Enabled almost all signatures

Assessment - Snort Result

- Easily handled dual Internet T-1's
 - 10% CPU typical
- Session Result – Lots of false positives.
 - DMZ
 - Internal Internet Link

Assessment – DMZ Snort Result

subject: IDS Statistics generated on Mon Sep 26 15:28:35 2005
The log begins at : Apr 30 09:34:16 The log ends at : May 10 08:41:08

Total events in table : 2502 Source IP recorded : 374
Destination IP recorded : 242

The distribution of attack methods

```
=====
### 70 of 70 ###
%   No   Attack                                     Priority Severity
=====
```

%	No	Attack	Priority	Severity
13.63	341	VIRUS OUTBOUND bad file attachment {tcp}	2	medium
12.87	322	WEB-IIS view source via translate header {tcp}	2	medium
8.03	201	(portscan) TCP Portsweep {reserved}	2	medium
7.75	194	POLICY SMTP relaying denied {tcp}	3	low
7.63	191	INFO web bug 0x0 gif attempt {tcp}	3	low
6.51	163	SMTP MAIL FROM overflow attempt {tcp}	1	high
6.35	159	SHELLCODE x86 NOOP {tcp}	1	high
5.92	148	WEB-FRONTPAGE /_vti_bin/ access {tcp}	2	medium
4.56	114	WEB-IIS fpcount access {tcp}	2	medium
3.08	77	(portscan) TCP Portsweep {reserved}	3	low
2.56	64	INFO FTP Bad login {tcp}	2	medium
2.16	54	(portscan) TCP Portsweep {reserved}	2	medium
1.96	49	POLICY FTP anonymous login attempt {tcp}	3	low
1.96	49	(portscan) TCP Portsweep {reserved}	1	high
1.80	45	ATTACK-RESPONSES 403 Forbidden {tcp}	2	medium
0.96	24	WEB-FRONTPAGE shtml.exe access {tcp}	2	medium
0.96	24	WEB-FRONTPAGE _vti_rpc access {tcp}	2	medium
0.96	24	WEB-FRONTPAGE _vti_inf.html access {tcp}	2	medium
0.76	19	SHELLCODE x86 inc ebx NOOP {tcp}	1	high

Assessment – Internal Snort Result

subject: IDS Statistics generated on Thu Sep 29 14:37:03 2005

The log begins at : Sep 24 13:00:02

The log ends at : Sep 29 12:59:55

Total of Lines in log file : 242342

Total of Logs Dropped : 318 (0.13%)

Total events in table : 41852

Source IP recorded : 332

Destination IP recorded : 861

The distribution of classification method

```
=====
### 15 of 15 ###
%   No      Classification                               Severity
=====
```

%	No	Classification	Severity
83.30	34862	Attempted Information Leak	medium
6.96	2914	access to a potentially vulnerable web application	medium
4.07	1704	http_inspect	unknown
3.79	1587	Web Application Attack	high
0.54	228	Potentially Bad Traffic	medium
0.34	144	Misc activity	low
0.33	139	Misc Attack	medium
0.27	112	Detection of a non-standard protocol or event	medium
0.17	73	A suspicious filename was detected	medium
0.09	38	Attempted Administrator Privilege Gain	high
0.05	20	Attempted Denial of Service	medium
0.03	13	Generic Protocol Command Decode	low
0.02	9	Attempted User Privilege Gain	high
0.01	5	Potential Corporate Privacy Violation	high
0.01	4	SCORE! Get the lotion!	high

Practical Network and System Security

Engineered Networks & Rockford Public Schools

ssurdock@engineered-net.com

PJYoung@rockford.k12.mi.us

www.engineered-net.com

www.rockford.k12.mi.us

Date: 10/07/05

© 2005 Engineered Networks

Rev: 1.0

Page: 15

Assessment – Internal Snort Result

subject: IDS Statistics generated on Thu Sep 29 14:44:20 2005
The log begins at : Sep 24 13:00:02 The log ends at : Sep 29 12:59:55
Total of Lines in log file : 242342 Total of Logs Dropped : 318 (0.13%)

Total events in table : 41852 Source IP recorded : 332
Destination IP recorded : 861

The distribution of attack methods

```
=====
### 128 of 128 ###
%   No   Attack                                     Priority Severity
=====
```

38.98	16315	SNMP request udp {udp}	2	medium
38.69	16193	SNMP public access udp {udp}	2	medium
4.98	2085	WEB-IIS %2E-asp access {tcp}	2	medium
2.33	974	ATTACK-RESPONSES 403 Forbidden {tcp}	2	medium
1.68	702	ICMP L3retriever Ping {icmp}	2	medium
1.52	636	(http_inspect) BARE BYTE UNICODE ENCODING {tcp}	2	unknown
1.23	515	WEB-MISC weblog/tomcat .jsp view source attempt {tcp}	1	high
1.00	417	WEB-MISC jigsaw dos attempt {tcp}	1	high
0.91	380	(http_inspect) OVERSIZE REQUEST-URI DIRECTORY {tcp}	2	unknown
0.79	332	WEB-MISC RBS ISP /newuser access {tcp}	2	medium
0.63	265	WEB-ATTACKS mail command attempt {tcp}	1	high
0.55	232	(portscan) TCP Portsweep {reserved}	2	medium
0.54	225	WEB-CGI redirect access {tcp}	2	medium
0.44	183	ICMP redirect host {icmp}	2	medium
0.36	151	ATTACK-RESPONSES Invalid URL {tcp}	2	medium

Threats

- Identify the threats
 - Where to start???
- Where are your valuable assets?
 - Student Information System, Computational Resources, Employee Data?
- Where are your vulnerabilities?

Assessment Results

- Risk = threat x vulnerability x asset value
- Fill in the holes
- Apply necessary patches
- Upgrade your protection & detection systems

Protection

- ...will eventually fail
- Defense in depth
- Carefully use "ANY" in a firewall rule
- Secure the host
 - Limit available services
 - Review file/folder permissions
 - Enforce permissions
 - Patch, patch, patch

Detection

- Looking for violations of the security policy
- Logging
- Statistical Data
- Session Data
- Packet Data

Security Framework

- Assessment
 - Calculate risk & create plan
- Protection
 - Enforce the traffic you want
- Detection
 - Logging and alerting
- Response
 - Make sure it doesn't happen (again)

The End

- Thank you for coming!
- Please fill out a speaker evaluation sheet to enter the drawing.
- The Presentation can be found at:
<http://www.engineered-net.com/Library>
- The winner is...

Bibliography

- 1) Richard Bejtlich, *The Tao of Network Security Monitoring – Beyond Intrusion Detection*. (Addison-Wesley, 2004)
- 2) Steve A. Rouiller, Virtual LAN Security: weaknesses and countermeasures,
<http://www.sans.org/rr/whitepapers/networkdevs/1090.php>
- 3) Nessus, <http://www.nessus.org/>
- 4) Snort, <http://www.snort.org/>
- 5) Snortalog, <http://jeremy.chartier.free.fr/snortalog/>