

# Network and System Security

A Bottom Up Approach 

Practical Network and System Security	<a href="mailto:nerdock@engineered-net.com">nerdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 1

---

---

---

---

---

---

---

---

## Why Bother?

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

Practical Network and System Security	<a href="mailto:nerdock@engineered-net.com">nerdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 2

---

---

---

---

---

---

---

---

## 10,000 Foot View<sup>1</sup>

- Assessment
- Protection
- Detection
- Response

Practical Network and System Security	<a href="mailto:nerdock@engineered-net.com">nerdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 3

---

---

---

---

---

---

---

---

## 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

Practical Network and System Security	<a href="mailto:nardock@engineered-net.com">nardock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 4

---

---

---

---

---

---

---

---

---

---

## Assessment - Techniques

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

Practical Network and System Security	<a href="mailto:nardock@engineered-net.com">nardock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 5

---

---

---

---

---

---

---

---

---

---

## 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

Practical Network and System Security	<a href="mailto:nardock@engineered-net.com">nardock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 6

---

---

---

---

---

---

---

---

---

---

## 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

Practical Network and System Security	<a href="mailto:nsdock@engineered-net.com">nsdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 7

---

---

---

---

---

---

---

---

## Nessus Windows Frontend



Practical Network and System Security	<a href="mailto:nsdock@engineered-net.com">nsdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 8

---

---

---

---

---

---

---

---

## 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](file:///C:/cygwin/home/ssurdock/RPS/rps.20050926/index.html)

Practical Network and System Security	<a href="mailto:nsdock@engineered-net.com">nsdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 9

---

---

---

---

---

---

---

---

## 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

Practical Network and System Security	<a href="mailto:ssurdock@engineered-net.com">ssurdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 10

---

---

---

---

---

---

---

---

## 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

Practical Network and System Security	<a href="mailto:ssurdock@engineered-net.com">ssurdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 11

---

---

---

---

---

---

---

---

## Assessment - Snort Result

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

Practical Network and System Security	<a href="mailto:ssurdock@engineered-net.com">ssurdock@engineered-net.com</a> <a href="mailto:pt@eng@rockford.k12.il.us">pt@eng@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 12

---

---

---

---

---

---

---

---

# Assessment – DMZ Snort Result

subject: IDS Statistics generated on Mon Sep 26 15:27:52 2005  
 The log begins at : Apr 30 09:34:16 The log ends at : May 10 08:41:08  
 Total of Lines in log file : 13101 Total of Logs Dropped : 40 ( 0.31%)  
 Total events in table : 2502 Source IP recorded : 374  
 Destination IP recorded : 242

The distribution of classification method

```

##### 16 of 16 #####
# No Classification Severity
-----
20.94 749 access to a potentially vulnerable web application medium
20.84 524 Misc activity low
18.78 470 A suspicious filename was detected medium
9.11 228 Attempted Administrator Privilege Gain high
7.57 192 Executable code was detected high
4.80 120 Attempted Information Leak medium
3.48 87 Potentially Bad Traffic medium
1.44 36 http_inspect unknown
1.32 33 smcmt_decoder unknown
0.80 20 Generic Protocol Command Decode low
0.72 18 Attempted Denial of Service medium
0.44 11 Web Application Attack high
0.32 8 Attempted User Privilege Gain high
0.12 3 A Network Trojan was detected high
0.08 2 A system call was detected medium
0.04 1 Unknown Traffic low
    
```

Practical Network and System Security	<a href="mailto:network@engineered-net.com">network@engineered-net.com</a>	Date: 10/07/05
Engineered Networks & Rockford Public Schools	<a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	© 2005 Engineered Networks
	<a href="http://www.engineered-net.com">www.engineered-net.com</a>	Rev: 1.0
	<a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Page: 13



# Assessment – DMZ Snort Result

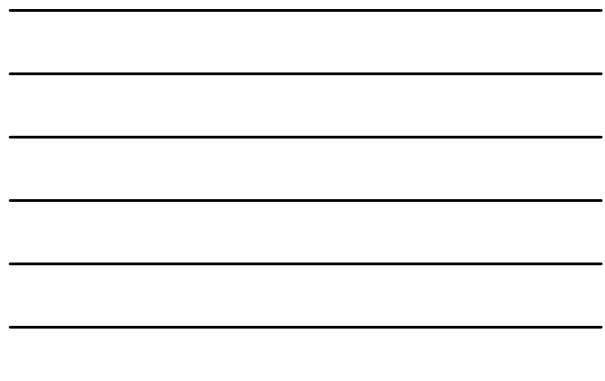
subject: IDS Statistics generated on Mon Sep 26 15:28:35 2005  
 The log begins at : Apr 30 09:34:16 The log ends at : May 10 08:41:08  
 Total events in table : 2502 Source IP recorded : 374  
 Destination IP recorded : 242

The distribution of attack methods

```

##### 70 of 70 #####
# No Attack Priority Severity
-----
13.63 341 VERBOS COMMAND bad file attachment (tcp) 2 medium
12.87 322 WEB-IIS view source via translate header (tcp) 2 medium
8.03 201 (portscan) TCP Portswamp (reserved) 2 medium
6.75 184 POLICY deny relaying denied (tcp) 3 low
7.63 191 INFO web log bad gif attempt (tcp) 3 low
6.52 163 SMTP MAIL FROM overflow attempt (tcp) 1 high
6.35 159 SHMLOCK x86 MOP (tcp) 1 high
5.92 148 WEB-FRONTPAGE cgi_bin/ access (tcp) 2 medium
4.56 114 WEB-IIS spcount access (tcp) 2 medium
3.08 77 (portscan) TCP Portswamp (reserved) 3 low
2.56 64 INFO FTP bad login (tcp) 2 medium
2.14 54 (portscan) TCP Portswamp (reserved) 2 medium
1.96 49 POLICY FTP anonymous login attempt (tcp) 1 low
1.96 49 (portscan) TCP Portswamp (reserved) 1 high
1.80 45 ATTACK HEADERS 403 Forbidden (tcp) 2 medium
0.96 24 WEB-FRONTPAGE admin.exe access (tcp) 2 medium
0.96 24 WEB-FRONTPAGE cgi_bin/ access (tcp) 2 medium
0.96 24 WEB-FRONTPAGE cgi_bin/ access (tcp) 2 medium
0.96 24 WEB-FRONTPAGE cgi_bin/ access (tcp) 2 medium
0.76 19 SHMLOCK x86 int.exe MOP (tcp) 1 high
    
```

Practical Network and System Security	<a href="mailto:network@engineered-net.com">network@engineered-net.com</a>	Date: 10/07/05
Engineered Networks & Rockford Public Schools	<a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	© 2005 Engineered Networks
	<a href="http://www.engineered-net.com">www.engineered-net.com</a>	Rev: 1.0
	<a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Page: 14



# 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
-----
83.30 34862 Attempted Information Leak medium
6.96 2014 access to a potentially vulnerable web application medium
4.07 1704 http_inspect unknown
3.79 1587 Web Application Attack high
0.64 228 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 SOURCE: Get the location high
    
```

Practical Network and System Security	<a href="mailto:network@engineered-net.com">network@engineered-net.com</a>	Date: 10/07/05
Engineered Networks & Rockford Public Schools	<a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	© 2005 Engineered Networks
	<a href="http://www.engineered-net.com">www.engineered-net.com</a>	Rev: 1.0
	<a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Page: 15





## 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

Practical Network and System Security	<a href="mailto:nardock@engineered-net.com">nardock@engineered-net.com</a> <a href="mailto:zfranz@rockford.k12.il.us">zfranz@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 19

---

---

---

---

---

---

---

---

## Detection

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

Practical Network and System Security	<a href="mailto:nardock@engineered-net.com">nardock@engineered-net.com</a> <a href="mailto:zfranz@rockford.k12.il.us">zfranz@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 20

---

---

---

---

---

---

---

---

## 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)

Practical Network and System Security	<a href="mailto:nardock@engineered-net.com">nardock@engineered-net.com</a> <a href="mailto:zfranz@rockford.k12.il.us">zfranz@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 21

---

---

---

---

---

---

---

---

## 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...

Practical Network and System Security	<a href="mailto:nrock@engineered-net.com">nrock@engineered-net.com</a> <a href="mailto:rlw@rockford.k12.il.us">rlw@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 22

---

---

---

---

---

---

---

---

## 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/>

Practical Network and System Security	<a href="mailto:nrock@engineered-net.com">nrock@engineered-net.com</a> <a href="mailto:rlw@rockford.k12.il.us">rlw@rockford.k12.il.us</a>	Date: 10/07/05 © 2005 Engineered Networks
Engineered Networks & Rockford Public Schools	<a href="http://www.engineered-net.com">www.engineered-net.com</a> <a href="http://www.rockford.k12.il.us">www.rockford.k12.il.us</a>	Rev: 1.0 Page: 23

---

---

---

---

---

---

---

---