

Network and System Security

A Bottom Up Approach

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 1

Why Bother?

- Information Security
 - Confidentiality
 - Integrity
 - Availability
- Lawsuits

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 2

10,000 Foot View¹

- Assessment
- Protection
- Detection
- Response

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 3

Risk Assessment

- Focus priorities based on (potential) loss
- Quantitative or qualitative
- Organizational buy-off
- First step for Business Continuity (Disaster Recovery) Plan
 - Business Impact Analysis

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurlock@engineered-net.com	Page: 4

Assessment – Bottom Up

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

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurlock@engineered-net.com	Page: 5

Assessment - Techniques

- Identify mitigation techniques
- Identify residual risk
- Develop a plan & policies
- Methodologies
 - OCTAVE - <http://www.cert.org/octave/>

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurlock@engineered-net.com	Page: 6

Assessment - Tools

- Use Nessus to find systems & vulnerabilities
 - Backtrack– Linux LiveCD with Security Tools
 - <http://www.remote-exploit.org/index.php/BackTrack>
 - Register Nessus to obtain recent tests
 - <http://www.nessus.org/plugins/index.php?view=register>
 - Initialize & start Nessus server
 - Start the Nessus client.
 - Run it against the outside and the inside

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
ssurdock@engineered-net.com	Page: 7

Nessus Windows Frontend



Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
ssurdock@engineered-net.com	Page: 8

Assessment - Nessus Result

- Sample External Scan Result
 - 5 security holes found
 - 19 security warnings found
 - 62 security notes found
 - [File:///C:/cygwin/home/ssurdock/client/them.20050926/index.html](file:///C:/cygwin/home/ssurdock/client/them.20050926/index.html)

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
ssurdock@engineered-net.com	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	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
ssurdock@engineered-net.com	Page: 10

Formalize results

- Nessus helps identify systems and vulnerabilities, it doesn't identify information assets
- Use the Nessus results to derive information assets
- Create groups of assets
 - Network infrastructure, e-mail, HR, Payroll, accounting...

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
ssurdock@engineered-net.com	Page: 11

Formalize results

- Identify the loss value for each asset group & vulnerability
 - Productivity loss
 - Reputation loss
 - Support (rebuild) loss
- Consider "other" vulnerabilities
 - E.g. Age of server/components

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
ssurdock@engineered-net.com	Page: 12

Threats

- Identify the threats
 - Where to start??
- What entities can take advantage of vulnerabilities to affect data
 - Availability
 - Confidentiality
 - Integrity

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 13

Threats

- Security threats
 - Ex-staff
 - Students
 - External threats
- Natural threats
 - Fire
 - Flood
 - Wind
- Use Snort to help identify network threats

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 14

Assessment Tools - Snort

- Existing "bad" traffic?
- Using Snort
 - Favorite OS (OpenBSD) or LiveCD
 - 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
 - Enable signatures

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 15

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
3.11 228 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	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 16



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 VERB OSSTRONG 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
7.75 184 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 smb ncsp (tcp) 1 high
5.92 148 WEB-FRONTPAGE _vsl_inif 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 HEADERSIZE 403 Forbidden (tcp) 2 medium
0.96 24 WEB-FRONTPAGE sbml.exe access (tcp) 2 medium
0.96 24 WEB-FRONTPAGE _vsl_rpc access (tcp) 2 medium
0.96 24 WEB-FRONTPAGE _vsl_inif.html access (tcp) 2 medium
0.76 19 SHMLOCK smb_ini.exe ncsp (tcp) 1 high
    
```

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 17



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	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 18



Assessment Results

- Fix low hanging fruit (patches)
- Fill in the holes for highest risk first
- Determine protection & detection systems that costs less than the loss value (cost justification)
- Determine residual risk

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 22

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	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 23

Detection

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

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 24

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	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 25

The End

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

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 26

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) Risk Management Guide for Information Technology Systems, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

Practical Network and System Security	Date: 03/10/06
Engineered Networks	© 2006 Engineered Networks
http://www.engineered-net.com	Rev: 1.0
gsurdock@engineered-net.com	Page: 27
