Design your network to aid forensics investigation

Robert B. Sisk, PhD, CISSP
Senior Technical Staff Member
IBM

Baltimore, Maryland USA
Master Outline

- Introduction
- Incident Management & Investigation
- Network Design
- Consider Risk
- Network Monitoring
- Reporting
- Incorporating Security Monitoring
- Monitoring Examples
- Valuable Assets
- Summary
1. Introduction
Description

This course will review network design and monitoring with the intent of identifying and providing adequate compromise detection, developing appropriate security response to suspicious "events", and increasing readiness for forensics investigation.

The key to success will be participation by all session attendees!
Presentation Dynamics

- Please ask questions
- Discussion
- Share
- Please ask questions
- Storytelling

My goals:
- Stimulate your thought processes
- Learn from your questions
- Send you home with at least one new idea
Who Am I?

- **Employers**
  - Academia
  - Government
  - Business

- **Job Positions**
  - Programming
  - System admin
  - Network admin
  - Security admin
Who Are You?

- **Employers**
  - Academia
  - Government
  - Business

- **Job Positions**
  - Programmers
  - Application admin
  - System admin
  - Network admin
  - Security admin
  - Sales/Marketing
  - Management
  - End User
Origins: Floppy Net to Internet

- In the beginning there was….
  - The computer doesn’t work right!

- Then came…..
  - Where did my file go?
  - Who changed that information?

- Followed by……
  - Why is my computer so slow?
  - Who is using all the bandwidth?

- Today……
  - Hey, my online account holder is asking me for information.
  - My bank emailed me because I have a credit card problem.
  - If I can just help out that poor family in Nigeria.
  - Wow, look at this cool program “Joe Smith” just sent me.
  - Man, IRC is so great. I can trade all sorts of stuff!
First Indications of a Problem

- If you don’t monitor
  - Website defacement
  - File modified or deleted
  - New user account
  - Configuration changes
  - Locked out user ID

- If you do monitor
  - IDS/IPS Alerts
  - Firewall Logs
  - No different from “don’t monitor”
Resolving a Problem

- Is the alert significant?
- Was the penetration successful?
- Did something change?
- Who made the modification?
- How did the change occur?
- What can we do to prevent it from happening again?
- Should we “reinstall”?
The Network is Important

- You can’t hide a flow
- Monitor many devices more easily
- First line of defense
- Most “bang for the buck”
- Best place to begin
What is the Current Status of Your Network?

- Equipment type
- Size
- Age
- Policies
- Diagrams
- Internet connections
- Flows
- Staff
- Management Support

Your network is a valuable asset!
2. Incident Management & Investigation

And now, for something, well, not entirely different.....
What Does “Computer Forensics” Mean?

Definitions of Computer Forensics on the Web:

- Computer Forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage.  

- The investigation of a computer system or any device that contains a processor and memory in order to determine who, what, where, when and how such digital devices temporary or persistent storage to another device.  
  [www.webstonetech.com/page/page/1972572.htm](http://www.webstonetech.com/page/page/1972572.htm)

- Computer forensics deals with the science of determining computer-related conduct - the who, what, when, where, and how of computer and technology use.  
  [www.tecrime.com/0clues.htm](http://www.tecrime.com/0clues.htm)

- Computer forensics is the process of investigating data processing equipment-- typically a home computer, laptop, server, or office workstation-- to determine if the equipment has been used for illegal, unauthorized, or unusual activities. It can also include monitoring a network for the same purpose.  
Typical Attack

- Reconnaissance
- Vulnerability mapping
- Initial attack
- Escalation (if necessary)
- Ensure continuing access
- Utilize the system
- Hide tracks (log files, processes…etc)
Common Avenues of Attack

- Application Vulnerabilities
- Worms and viruses
- Open proxies (Squid, etc…)
- Compromised hosts
- Web and web services
- Email
- Instant messaging
- Etc……
What Do Hackers Do?

- Rootkits
- Backdoors
- Hidden files
- Hidden processes
- Denial of Service
- Steal Information
- Botnets
- Etc……..
Investigation is a Process

- Begin a “Record of Investigation”
- Involvement management
- Set objectives
- Conduct interviews
- Collect evidence
- Analyze evidence
- Establish a “Modus Operandi”
- Document findings in a report
If “Investigation is a Process” What Does That Mean?

- Documented
- Approved by management
- Tested
- Maintained
- Understood
- Practiced
Policy: What’s Your Plan?

- The policy says?
- Can I have a copy of that policy?
- What’s the procedure?
- Can I have a copy of the procedure?
- Do we really do this?
- Who is responsible?
- Where are the results?
- What do we do with the results?
- How do things get fixed?
- Why bother??????

*The best-laid plans of mice and men often go awry.* Robert Burns
Some Objectives of a Process

- Determine the extent of the compromise
- Contain the attack
- Determine the exact mechanism & details of attack
- Stop the attack (maybe)
- Provide recommendations recovering the environment
- Report findings
- Prevention
- Prosecute
What Does “Prosecute” Imply?

- Documentation
- Evidence collection
- Evidence storage
- Rights of individuals
- Local, state, and federal laws
- Interaction with law enforcement
- Interaction with justice system
Report Findings

- Types of reporting
- Appropriate content
- Standardized formats
- Prevention
- Receiving executive
- Policy
Evidence Sources

- Potentially any log file
  - Firewall logs
  - IDS/IPS logs
  - System logs
  - Router logs
  - Application logs (web, e-mail…)
  - Proxy logs
  - Web logs
  - Authentication logs

- Configuration files are good too
  - Router/switch
  - Network appliance
  - And yes firewall
Additional Evidence Sources

- Network session captures (ethereal, tcpdump, NAM, netflow)
- System analysis (binaries, suspect files, malware)
- Network architecture
Summary of Key Elements

- Process
- Documentation
- Evidence collection
- Evidence analysis
- Reporting results
3. Network Design
What Does Your Network Do?

- **What type of network do you have?**
  - Intranet
  - Extranet
  - B2B
  - Internet portal
  - Remote office
  - Remote employee
  - Combination, probably several!

- **What function does your network provide?**
  - Email
  - Web services
  - Business critical applications
  - Financial applications
  - Remote employee
  - Others, probably a lot!
Problems with a Dynamic Infrastructure

- Old documentation
- Aging network infrastructure
- Firewall limitations
- Maintenance contract costs
- Quality control of network changes
- Network management
- IP address management
- Bandwidth usage monitoring
- Ineffective IDS system
- Undependable security logs
- Audit issues
- Increase monitoring and data analysis
- Reactive vs. proactive posture
- Team expertise
- Professional development
Network Topology: Layer/Zone Method
Design your network to aid forensics investigation

Topology: Layer/Zone Method

Internet

© 2006 Robert B. Sisk

18th Annual FIRST Conference Baltimore, Maryland
General Network Flows

TCP/IP inbound flow initiation

TCP/IP outbound flow initiation
Zone Specific Network Flows

TCP/IP flow initiation

Internal

Internet
Specialized Network Flows

- SSH / SSL required
- Strong authentication (required)
- Encryption of application flows (required)
- Requirements enforced
Documentation

- Having adequate documentation for the network is critical to security
- As the network becomes larger the documentation becomes more critical
- Items to document include:
  - Internet connections
  - Firewall locations
  - Flows
  - Much more….
4. Consider Risk
Define: Network Security

**Network security** is the effort to create a secure computing platform, designed so that agents (users or programs) cannot perform actions that they are not allowed to perform, but can perform the actions that they are allowed to. The actions in question can be reduced to operations of access, modification and deletion. Network security can be seen as a subfield of security engineering, which looks at broader security issues in addition to network security.*

*Source unknown*
Risk: Flow Diagram

Owners

value

wish to minimize

impose

Safeguards

to reduce

may be reduced by

may possess

Vulnerabilities

leading to

Risk

may be aware of

give rise to

Threats

exploit

increase

effects

Threat Agents

Assets

wish to abuse and/or damage
Risk: The Goal
Design your network to aid forensics investigation

"Security is a journey not a destination"
Summary of Key Elements

- Risk can never be eliminated
- Managing risk is a continuous process
- Low impact and low likely hood is the goal
- Law of diminishing returns
5. Network Monitoring
Logging

- Centralized log collection
- Redundant collection devices
- How many messages can you send to a collector
  - Std syslog
  - Syslog NG
- Secure storage area
File Modifications

- Device configuration files (network and system)
- Binaries
- Specific files
- Change control – enforced
- Review
- Audit
- Alerting
- Reporting
Security: Discovery……..

- Location (inside / outside)
- Software variety
- Scan activity
  - Daily
  - Monthly
  - Quarterly
- Known / unknown
- Data review
- Reporting
Patch Management

- **Business Objective**
  - Ensure appropriate security patches are installed on all servers and network devices within the designated timeframes

- **Business Risk**
  - If this process is not executed effectively and efficiently, the result could lead to a vulnerable server and/or unnecessary downtime.
Authentication

- Business Objective
  - Each user's identity must be verified (authenticated) when the user attempts to logon to a system or application.

- Business Risk
  - If this process is not executed effectively and efficiently, the result could lead to a compromise.
Advanced Monitoring

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Cisco Network Analysis Module (NAM) Data
- Cisco Monitoring, Analysis & Response System (MARS)
- Honeypots
6. Reporting
Reporting

- Why provide reports?
- What do we report?
- How much information do we provide?
- Tools?
- Opportunity?
Management Reporting

- Security more than a problem
- They want specific information
- We can show attacks
- Demonstrate prevention
- Support policies
- Security can help
Design your network to aid forensics investigation

Security Reporting

- Email
- Paging
- IRC
7. Incorporating Security Monitoring into the Network
Network Depicted as Security Domains
Centralized Logging

Design your network to aid forensics investigation
Attack Detection and Mitigation

- Automatic Attack Detection
- Automatic Attack Mitigation
- Alert Notification
- Report Generation
Design your network to aid forensics investigation

Monitoring File Change

**Tripwire Server**
- Change Management
- Configuration Monitoring
- Compromise Detection
- Policy Compliance Monitoring
- Alert Notification
- Report Generation
Honeypot

- Intrusion Detection
- Alert Notification
- Report Generation
Design your network to aid forensics investigation

Security Technical Testing

**Security Technical Testing Server**
- Penetration Testing
- Patch Monitoring
- Policy Compliance Monitoring
- Report Generation
Design your network to aid forensics investigation

Cisco Security Monitoring, Analysis, and Response System (MARS)

- Advanced Data Analysis
- Automatic Attack Detection/Mitigation
- Alert Notification
- Report Generation

Cisco MARS Server

Security Technical Testing Server

Tripwire Server

Attack Detection and Mitigation System

Internet

Database Servers

Web Servers

Honeypot

© 2006 Robert B. Sisk

18th Annual FIRST Conference Baltimore, Maryland
Design your network to aid forensics investigation

Security Web Portal

- Database Servers
- Web Servers
- Internet

- Security Technical Testing
- Tripwire Server
- Attack Detection and Mitigation System
- Cisco MARS Server
- Honeypot

© 2006 Robert B. Sisk
18th Annual FIRST Conference Baltimore, Maryland
8. Monitoring Examples
Network Diagram

Network Graphic Removed: Not intended for general distribution.
Design your network to aid forensics investigation

Sessions in 24 Hours
Example 1: Identifying an Attack

- Customer with a business requirement for Secure Shell, SSH, access from the Internet.
- Several User IDs are constantly being locked out as the result of too many failed logins.
- Sometimes the user IDs are relocked out as fast as they can be unlocked.
Total Traffic for One Week
Total Attacks During Week
Secure Shell (SSH) Attacks During Week
Another Possible Solution.....
Example 2: Attack Diagram
Example 3: Flow Tracking

Network Graphic Removed: Not intended for general distribution.
Example 4: Identifying Misconfigured Devices

- Security monitoring can help identify misconfigured devices
- Saves money in reduced bandwidth cost
Design your network to aid forensics investigation

Misconfigured Device 1
Design your network to aid forensics investigation

Misconfigured Device 2

Activity: All Events and Netflow - Top Destination Ports, last 1d-0h

Chart resolution: 30Min

<table>
<thead>
<tr>
<th>Color</th>
<th>Recent / Minute</th>
<th>Total Count</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>73.92</td>
<td>121,824</td>
<td>53</td>
</tr>
<tr>
<td>Orange</td>
<td>49.07</td>
<td>96,999</td>
<td>657</td>
</tr>
<tr>
<td>Yellow</td>
<td>36.63</td>
<td>66,752</td>
<td>25</td>
</tr>
</tbody>
</table>
Design your network to aid forensics investigation

Misconfigured Device 3
Example 4: Internal Scanning

<table>
<thead>
<tr>
<th>Rank</th>
<th>Total Sessions</th>
<th>Average / Minute</th>
<th>Raw Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>731,461</td>
<td>72.49</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>605,080</td>
<td>59.97</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>572,525</td>
<td>56.74</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>216,958</td>
<td>21.7</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>80,549</td>
<td>7.98</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>80,543</td>
<td>7.90</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>80,535</td>
<td>7.95</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>78,946</td>
<td>7.82</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>76,713</td>
<td>7.6</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>75,083</td>
<td>7.44</td>
<td></td>
</tr>
</tbody>
</table>
9. Valuable Assets: People
Team Skills

- Knowledge
- Experience
- Training
- Certifications
- Practice
- Get involved
10. Summary

The Take Home Message

Baltimore, Maryland USA
Summary

- Policy and procedure
- Understand the purpose of your network
- Manage risk (simplify, remove what you don’t need)
- Logs are important
- Network flow analysis critical
- Collect as much **good** data as you can
- Develop good data analysis
- Efficient reporting
- Team skills (technical for sure but communication too)
- Be prepared (be prepared)
- Stay in front of management (visibility)
- Future World – physical to virtual (On Demand)