Building a Security Operations Center

Randy Marchany
VA Tech IT Security Office and Lab
marchany@vt.edu
CyberSecurity Operations Center

- Security Operations Center (SOC) term is being taken over by physical surveillance companies
- We’re building a Cyber Security Operations Center (CSOC) that doesn’t have any physical surveillance capability.
- It could be a component of a SOC in the future
(C)SOC vs. NOC

- Network Operations Center usually responsible for monitoring and maintaining the overall network infrastructure. Its primary function is to ensure uninterrupted network service.
- CSOC leverages security related network activity to refine security incidents response.
- CSOC and NOC should complement each other and work in tandem.
Why?

• We’ve been collecting security related data for a number of years and needed a focal point to help us see the big picture
• Data from
  • Security Reviews
  • Vulnerability scans (push/pull)
  • IPS/IDS data
  • System logs
• We want to build a “security history” for a host
Why?

- The CSOC is a logical place to collect, analyze and distribute data collected to support our Defense in Depth Strategy
  - Preventing **Network Based** Attacks
  - Preventing **Host Based** Attacks
  - Eliminating Security **Vulnerabilities**
  - Supporting **Authorized Users**
  - Providing tools for **Minimizing Business Loss**
Why?

• We want to measure and report compliance with our IT policies, state/federal laws and regulations
  • FERPA, HIPAA, PCI, ITAR, GLB, SOX
  • VT Policies
    • 7010 Policy for Securing Technology Resources and Services 1/22/2007
    • 7025 Safeguarding Nonpublic Customer Information 5/12/2004
    • 7035 Privacy Policy for Employees' Electronic Communications 3/14/2005
    • 7040 Personal Credentials for Enterprise Electronic Services 4/01/2008
    • 7100 Administrative Data Management and Access Policy 4/01/2008
    • 7105 Policy for Protecting University Information in Digital Form 7/1/2008
    • 7200 University IT Security Program 6/12/2006
    • 7205 IT Infrastructure, Architecture and Ongoing Operations 6/12/2006
    • 7210 IT Project Management 6/12/2006
    • 7215 IT Accessibility 6/12/2006
Where?

- OS Syslog/event logs, IDS logs, IPS logs, PID logs, Firewall logs, Pen Test Logs, PCI, netflow
- CSOC needs to be able to analyze and display this data quickly
- Data resides on separate, distributed servers
- CSOC pulls data from these servers as needed
- CSOC lives in the IT Security Office & Lab
What?

- Provides real-time view of the VT network’s security status
- Provides info to assess risk, attacks, mitigation
- Provides metrics
  - Executive
  - Operational
  - Incident
What?

• Event Generators (E boxes)
  • Any form of IDS sensor (firewalls, IPS, IDS, Snort, Active Directory servers, Remedy, vulnerability scanners, TACACS, application software

• Most are Polling Generators
  • Generate specific event data in response to a specific action
  • Example: IDS or firewall
What?

• Events Databases (D boxes)
  • Provide basic storage, search and correlation tools for events collected and sent to the CSOC
  • Vulnerability databases contain info about security breaches, etc.
What?

• Events Reactions (R boxes)
• SOC Console
  • Used for internal analysis
  • Real-time monitors (Snort, Base, IPS, Dshield)
  • Incident Handling
  • Remedy trouble ticket system
  • Location tools
  • Statistical analysis
• End User Portals
  • Multi level reporting for various target audiences
    • Sysadmin, management
What?

- Analysis Engines (A Boxes)
  - Helps ID Analyst determine if an incident has occurred, its spread, its impact, etc.

- Knowledge Base Engines (K boxes)
  - Store security configs of critical assets, tips/tricks and effective solutions to previous problems

- Reaction and Report Engines (R boxes)
  - Switches, routers, IPS and associated management tools
Putting the Pieces Together

- RDWEB – locate any device in our network
- DSHIELD – Collect Firewall logs
- SNORT – Sensors monitoring for patterns
- VULNSCAN – “pull” vulnerability scanner
- CHECKNET – “push” vulnerability scanner
- REMEDY – Trouble Ticket system used by Help Desk
- CENTRAL SYSLOG – collects syslogs
IDS Infrastructure

- Campus Systems
  - VT Dshield
    - Dshield MySQL DB
  - Central Syslog Servers
  - CheckNet WWW
  - Nessus, Comm Scanners
  - Remedy Trouble Ticket System
    - CIRT
    - Help Desk
- MySQL DB
  - Snort BASE
    - CheckNet Failure DB
- User Vuln Scanner
  - MySQL DB
- IPS
- SNORT Sensors
Virginia Tech DShield
Distributed Intrusion Detection System

DShield Reports and Database Summaries

Top 10 Most Wanted
Top 10 offenders according to the DShield database.

   Top 10 Ports
   Top 10 most probed ports.

   Port Report
   Provides a thirty day history of a user selected port.

   Attacker IP Info
   Get a summary of recent activity from an attacker IP address

   Target IP Info
   Get a summary of recent activity from a target IP address

   Subnet Report
   Get a summary of recent activity from a Subnet

   Search DShield
   Search the DShield database.

   Block List
   List of IP address ranges that you might want to block.

---

[ Home | Login | Whats New | Intro | Submit | Clients | Web Submission | All Reports | Links | About | Privacy ]

last update: 04/Nov/2008 17:52
DShield is a Servicemark of Euclidian Consulting
Some Common VT Server Counts
Welcome to IT Security at VT

Welcome to the Virginia Tech IT Security website, the gateway to protecting your computer. This site provides the University community with the links, tools, and resources needed to protect your network and data from break-ins and virus attacks. As well as providing detailed information about system access through Information Resource Management (IRM).

Getting Started

Whether you are a student or an employee at Virginia Tech, the links below will assist you in securing your network and computer.

- Students
- Faculty/Staff
- System Administrators

Common Tools

- Social Security Number and Credit Card Number Scan - Searches for SSNs and

News & Alerts

1. **NEW** Check out the October 2008 issue of the IT Security Quarterly Hot Sheet
2. **Updated** Phishing Email Alert - Click Here for Info
3. Notice for password change sent to selected account holders .... See notice
4. For more information on how to handle sensitive information please click here.
5. Download and learn about the VTnet CD here. A very useful resource for all users that is updated regularly.
## HAWK-i 6.0

### ALL ASSETS

<table>
<thead>
<tr>
<th>Asset Name</th>
<th>IP Address</th>
<th>Application</th>
<th>Asset Type</th>
<th>Location</th>
<th>Criticality</th>
</tr>
</thead>
</table>
|            | 198.82.01  | Vendor Maintenance  
Tuition Remission for Graduate School  
Travel Reimbursement  
Student Accounts  
Sponsored Programs  
Purchasing (SciQuest,eVA)  
Processing to report to the state  
Payment Gateway (InfNet)  
General Accounting  
Fund Management  
Fixed Assets and Inventory Control  
Effort Reporting  
Cash Receipts  
Budgeting  
Banner Student  
Accounts Receivable  
Accounts Payable  
Travel Reimbursement  
Student Accounts  
Sponsored Programs  
Purchasing (SciQuest,eVA)  
Processing to report to the state  
Payment Gateway (InfNet) | Production Linux Server | AIST | 4.29 |
# IDS Logs - Attacks that Originate from VT's Network

<table>
<thead>
<tr>
<th>Date</th>
<th>Primary NL</th>
<th>Attacker</th>
<th>Previous Attacker?</th>
<th>Victim</th>
<th>Attack</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-09-20</td>
<td>128.173.3</td>
<td>N/A</td>
<td>216.35.75.103</td>
<td>HTTP_POST_Script</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>2008-09-21</td>
<td>128.173.3</td>
<td>N/A</td>
<td>222.231.41.69</td>
<td>HTTP_UserAgentToo_Long</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>2008-09-21</td>
<td>128.173.3</td>
<td>N/A</td>
<td>121.254.193.190</td>
<td>HTTP_UserAgentToo_Long</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>2008-09-21</td>
<td>128.173.3</td>
<td>N/A</td>
<td>76.13.220.11</td>
<td>HTTP_repeated_character</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>2008-09-21</td>
<td>128.173.3</td>
<td>N/A</td>
<td>158.105.194.209</td>
<td>HTTP_UserAgentToo_Long</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>2008-09-21</td>
<td>128.173.3</td>
<td>N/A</td>
<td>76.13.220.11</td>
<td>HTTP_repeated_character</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>2008-09-21</td>
<td>128.173.3</td>
<td>N/A</td>
<td>211.115.109.43</td>
<td>HTTP_UserAgentToo_Long</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>
### Lookup New Host or PID

<table>
<thead>
<tr>
<th>Host IP Address</th>
<th>Host MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS Name</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Associated PID</th>
<th>Liaison</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outlet</th>
<th>Local Hub</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### VPN
- N/A

### Wireless
- N/A

**Tests**
- Ping
- Trace Route
- Full Scan
- NetFlow

### Nessus
- Last Scan: 
- Results: 

### Departmental Review
- Last Review: 
- Results: 

### Daily Scan
- Open Ports: 
- Vulnerabilities: 
- Details: 

---

**Done**

---

**cand1.cit.vt.edu**
Futures

- There are commercial tools that do all of this
- They cost lots of $$$
- We don’t have lots of $$$
- Had to grow our own
- Improves our skill set, proactive and reactive capabilities
- We can better evaluate commercial products because of our experience
Reference

- Reference paper “Security Operation Center Concepts & Implementation” by Renaud Bidou
- We used this as our blueprint
Contact Information

- Randy Marchany
- VA Tech IT Security Office & Lab
- 1300 Torgersen Hall
- VA Tech
- Blacksburg, VA 24060
- 540-231-9523
- marchany@vt.edu
- http://security.vt.edu