LET'S
BUILD
TOMORROW
TODAY
Cisco Cybersecurity Analyst Specialist Certification

James Risler, CCIE #15412
@JimRisler
jarisler@cisco.com

BRKCRT-2206
Agenda

• Understanding the Problem
• Why a Cybersecurity Analyst Specialist Certification
• Understanding the Job Role of a Security Analyst
• Topics included on the Exam
• How to Prepare for the Certification Exam
• Conclusion
The Problem...

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Ebay
Anthem
JP Morgan Chase
Target
Univ. of MD
Neiman Marcus
TJ Maxx
Sony
Zappos
LinkedIn
Citigroup
There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco
Breaches Happen in Minutes…
But go Undetected for Months or Years

<table>
<thead>
<tr>
<th>Timespan of events by percent of breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 60% of breaches, data is stolen in hours</td>
</tr>
<tr>
<td>Initial Attack to Initial Compromise</td>
</tr>
<tr>
<td>Seconds: 10%</td>
</tr>
<tr>
<td>Initial Compromise to Data Exfiltration</td>
</tr>
<tr>
<td>Seconds: 8%</td>
</tr>
<tr>
<td>Initial Compromise to Discovery</td>
</tr>
<tr>
<td>Seconds: 0%</td>
</tr>
<tr>
<td>Discovery to Containment/Restoration</td>
</tr>
<tr>
<td>Seconds: 0%</td>
</tr>
</tbody>
</table>

In 60% of breaches, data is stolen in hours. 54% of breaches are not discovered for months.
Threat Landscape is Evolving…

Enterprise Response
Antivirus (Host-Based)
IDS/IPS (Network Perimeter) and Sandboxing
Reputation (Global)
Intelligence and Analytics (Cloud)

Worms
2000

Spyware and Rootkits
2005

APTS Cyberwar
2010

Increased Attack Surface
Tomorrow
The Evolution of Cyber Threats

Viruses (1990s)
Defense: Anti-Virus, Firewalls

Worms (2000s)
Defense: Intrusion Detection & Prevention

Botnets (late 2000s to current)
Defense: Reputation, DLP, App.-aware Firewalls

Directed Attacks (APTs) (today)
Strategy: Visibility and Context

ILOVEYOU
Melissa
Anna Kournikova

Nimda
SQL Slammer
Conficker

Tedroo
Rustock
Conficker

Aurora
Shady Rat
Duqu
Why a Security Analyst

• Common Attacks Methods
• Challenges facing Organizations
• Security Analyst Skills
• Security Investigation Process
• Functional Model for Security Analyst
• Examples of Security Analyst Tools
Common Attack Methods

- Social Engineering
- Technical Exploit
- Zero-day Attack
Challenges Facing Organizations

• **Detecting Advanced Persistent Threats.** Malware that makes it past perimeter security can remain in the enterprise waiting to strike as lurking threats. These may be zero day threats that do not yet have an antivirus signature or be hard to detect for other reasons.

• **Uncovering Network Reconnaissance.** Some attacks will probe the network looking for attack vectors to be utilized by custom-crafted Cyber threats.

• **Finding Internally Spread Malware.** Network interior malware proliferation can occur across hosts for the purpose gathering security reconnaissance data, data exfiltration or network backdoors.

• **Identifying BotNet Command & Control Activity.** BotNets are implanted in the enterprise to execute commands to send SPAM, Denial of Service attacks, or other malicious acts.
Perimeter security stops many threats but sophisticated Cyber threats evade existing security constructs.

Fingerprints of threats are often found in network fabric.
Key Challenges: Complex Threat Visibility

• **Breached but How, Where and Who?**
  • Often very difficult to find
  • High value assets – major consequences
  • Network flow analysis is central to this process—throughout the network

• **Context is Critical**
  • No single system provides all data to decipher an attack
  • Related threats, identity, reputation, vulnerability, device type…

• **Disparate Data Sources, Manual Assembly**
  • Analysts collect and assemble contextual information from a variety of systems
  • Requires expensive analysts—round-the-clock coverage
Example - Cisco CSIRT Structure
Security Analyst Skills

What Skills to Develop?

• Four Key Areas of Competency
  1. Monitoring
  2. Data & Traffic Analysis
  3. Event and Alarm Handling
  4. Incident Response

• Foundation/Background
  • Network infrastructure knowledge
  • Diverse device configuration ability
  • Security configuration knowledge
  • Data management & teamwork

• Challenge is Arming Security Investigators
  • Not tied to a product or solution
  • Complex knowledge – Not one specific process is correct or product solution
  • Diverse set of skills are needed
Security Investigation Process

Start

Solutions

1

Vision

Prevent

Detect

Collect

Analyze

Mitigate

Foundations

Solutions Components

2

End
Functional Model for Security Analyst

**Prevent**
- Network IPS
- Host IPS
- Firewall
- Email/Web Proxy
- AntiVirus
- Spam Prevention

**Detect**
- Network IDS
- Adv. Malware
- Behavioral anomaly
- NetFlow anomaly

**Collect**
- NetFlow
- Proxy Logs
- Event Logs
- Web Firewall

**Analyze**
- NetFlow Analyze
- SIEM Analysis
- Malware Analyze
- Other Tools

**Mitigate**
- IP Blackhole
- Adv. ACL’s
- DNS Poisoning

**Skill Foundation**
- Device Config
- Traffic Capture
- Performance Monitoring
- Device Monitoring
Example: Security Analyst Tool

NetFlow Telemetry
Cisco Switches, Routers, and ASA 5500-x

Monitor, collect and analyze network traffic, establish a baseline, and alarm on anomalies and behavior changes

TrustSec Enabled Enterprise Network

NetFlow: Switches, Routers, and ASA 5500-x
Context: NBAR/AVC
Identity Services Engine

Cisco Cyber Threat Detection - enhances efficiency and effectiveness of analysis and provides key insight into internal activity across the network
Example: NetFlow tool identifying a Worm

Alarm indicating this host touched another host which then began exhibiting the same suspicious behavior

Suspicious activity that triggered the alarm
Exam Preparation

• How to Prepare for the Exam

• Exam Blueprint: http://www.cisco.com/web/learning/exams/list/spec_scyber.html#~Topics

• Resources
  • Books
  • Publically available resources
  • Cisco Learning Network
  • Labs “Build your own”
How to Prepare

• Where to Start?
  • Blueprint
  • Create a study plan
  • Study Group on Cisco Learning Network
    • Cyber Security Study Group
    • Posted documents

• Example of Resources
  • NIST Documents
    • [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)
  • NetFlow Overview (see links at end of slide deck)
  • Wireshark Usage
    • [www.wireshark.org/docs/wsug_html_chunked](http://www.wireshark.org/docs/wsug_html_chunked)
600-199 (SCYBER) Securing Cisco Networks with Threat Detection and Analysis—Topics and Weighting

SCYBER (600-199) Exam—Topics and Weighting

13%  1.0  Information Gathering and Security Foundation
16%  2.0  Event Monitoring
16%  3.0  Security Events and Alarms
24%  4.0  Traffic Analysis, Collection and Correlation
16%  5.0  Incident Response
15%  6.0  Operational Communication
1.0 Information Gathering and Security Foundations

1.1 - Describe basic network topologies, application architectures, and host configuration standards
1.2 - Identify the services a network and security operation center offers to an organization
1.3 - Describe traditional hacking techniques
1.4 - Describe basic operational procedures and incident response in a security operation center (SOC)
1.5 – Describe basic network security events
1.6 – Describe mission critical network traffic, applications, services and device behaviors
1.7 – Describe Corporate Security Policies
1.8 – Describe the role of a Network Security Analyst
1.9 – Primary sources of data on Vendor vulnerabilities, current threats, exploits, and active attacks
1.10 – Describe how vulnerability, attack, and threats impact data operations
1.11 – Describe the baseline of a network profile
1.12 – Describe correlation baseline (Normal vs. Non-normal)
1.13 - Describe security around business process, infrastructure and business applications
1.14 – Describe risk analysis mitigation

2.0 Event Monitoring

2.1 – Describe the various sources of data and how they relate to network security issues
2.2 – Monitor the collection of network data as it relates to network security
2.3 – Monitor and validate health state and device availability
2.4 – Monitor DNS Query log output
2.5 – Identify a security incident (single or reoccurring)
2.6 – Describe the best practice for evidence collection and forensic analysis

3.0 Security Event and Alarms

3.1 – Describe the different types of severity of alarms and events
3.2 – Identify and dismiss false positive indicators correctly
3.3 – Describe event correlation within context of the various alarms
3.4 – Assess traffic and events in relation to stated policies
3.5 – Identify actionable events
3.6 – Identify basic incident types
3.7 – Describe event metrics and diagnostic procedures
4.0 Traffic Analysis, Collection, and Correlation

4.1 – Describe IP Packet structures
4.2 – Describe TCP and UDP Header information
4.3 – Analyze network traces or TCP Dumps and trace back actual activities
4.4 – Describe packet analysis in IOS
4.5 – Describe access packets in IOS
4.6 – Acquire network traces
4.7 – Configure packet captures

5.0 Incident Response

5.1 – Describe standard corporate incident response
5.2 – Identify necessary changes to enhance the existing procedure, policy, and decision tree
5.3 – Describe the basic emergency mitigation of high-level threats, exploits, and vulnerabilities
5.4 – Evaluate and recommend responses to vulnerabilities to ensure adequate monitoring response and mitigations
5.5 – Assist the level 2 incident response team
5.6 – Describe best practices for post-event investigation
5.7 – Describe common legal and compliance issues in security event handling

6.0 Operational Communication

6.1 – Describe the communication vehicles related to post-threat remediation
6.2 – Generate incident reports and interpret the information to determine the direction of the escalation
6.3 – Describe the different types of available metrics and
6.4 – Process incident handling communications and provide context awareness for stakeholders
6.5 – Articulate details of problems to remediating teams
6.6 – Maintain awareness of vulnerabilities and critical security patches as a result from incident handling
6.7 – Communicate recurring issues based on incident handling and provide recommendations for architectural changes or modifications.
6.8 – Describe the post-mortem process
More Resources…

Books

• Crafting the InfoSec Playbook by Cisco’s Jeff Bollinger

• The Tao of Network Security Monitoring – by Richard Bejtlich

• Extrusion Detection: Security Monitoring for Internal Intrusions

• Incident Response with NetFlow for Dummies
  http://www.lancope.com/blog/incident-response-for-dummies/

• Real Digital Forensics: Computer Security and Incident Response

• Security Monitoring by Chris Fry and Martin Nystrom
Labs – Strategy is to learn through hands-on

- Lab 1-1: Case Study – Understanding a SOC
- Lab 2-1: Configure AAA and TACACS+ logging
- Lab 3-1: Capturing Packets (Wireshark, SPAN, TCPDump)
- Lab 4-1: Understanding Log Data
- Lab 4-2: Correlating Event Logs
- Lab 5-1: Mapping a Monitored Network Topology
- Lab 5-2: Retrieving Event Data
- Lab 5-3: Understanding Log Data Fields
- Lab 6-1: Assessing Current Security Controls
- Lab 6-2: Assessing Current Monitoring Systems
- Lab 7-1: Manually Correlate Events
- Lab 7-2: Automatically Correlate Events
- Lab 7-3: Identifying a Security Incident
- Lab 8-1: Understanding Flow Data
- Lab 8-2: NetFlow Practical Activity
- Lab 9-1: ACL and CBAC Configuration
- Lab 9-2: Multiple Mitigation Deployment
- Lab 10-1: Documenting an Incident
- Lab 10-2: Recommending Remediation
Lab 1-1: Security Operations Center

- National Institute of Standards and Technology (NIST) SP 800-61 (csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf)


Google – Building a SOC

- Dell SecureWorks – SOC operations center
Roles within the SOC

• Roles and qualifications required for each SOC position
  • Chief Information Security Officer (CISO)
  • SOC Management
  • Analyst
  • Specialist

• Define and compare NOCs and SOCs
  • Network Operations Center (NOC)
    • Services
    • Reporting
    • Authorities
    • Responsibilities
  • Security Operations Center (SOC)
    • Services
    • Reporting
    • Authorities
    • Responsibilities
Attacker Methodology

• Understand what type of Attackers there are.

• What is the methodology an attacker will use
  • Hacking Techniques
  • Basic strategy
  • Public Information
  • Map Information
  • Short-term vs. Long-term attacker goals
Understanding Attacks

Step 1: Attacker sends email to victim
Step 2: Email infects victim, connects to C&C
Step 3: Attacker sends instructions to victim host
Step 4: Victim host copies and encrypts data
Step 5: Victim host uploads encrypted data to FTP
Step 6: Attacker retrieves encrypted data from FTP
Malware and Attacker tools

• Distinguish between general purpose Malware and attacker tools
• Describe roles of each tool in an attacking toolset
• Attacker Exploits – (know the difference between each one of these)
  • Backdoors
  • Downloaders and droppers
  • Rootkits
  • Pivots
  • Keyloggers
  • Exploits
  • Payloads

Polymorphic Malware
“Kimusky” Operation: A North Korean APT

• 4 Key South Korean Targets
  • Phishing against Hyundai Merchant Marine

• Infecting Systems
  • Trojan Dropper – DLL library against Windows 7

• Install Spying Modules
  • Key Stroke Logger, Directory Listing, Remote Control & Execution, Remote Control Access

• Disable Firewall

• Communication
  • Command and control Bot done through a Bulgarian web-based free email server

• Regular Reporting and RC4 Encryption and Exporting of Data
Phases of Attack on Large Retail Chain Outlet

1. Phish HVAC Vendor
   Steal credentials – Attack hosted web server

2. Scan Network – Determine HVAC vendor access shared web server

3. Upload PHP Script to Web Server – Vulnerability in Application

4. Control of Webserver – Scan for relevant targets for propagation (MSSQLSvc/Billing)

5. Attack Microsoft AD Domain – Steal access tokens on Webserver (Pass-the-hash)
6. Create new Admin Account in MS AD Domain

7. Propagate to relevant computers (“Angry IP Scanner”) by pass security solutions (Tunneling with PsExec’s)

8. Attack SQL Server – Steal 70 Million PII records (no credit cards because PCI compliant)
   • Osql.exe
   • Isql.exe
   • Bcp.exe
Phases of Attack – cont.

9. Download POS Malware and install on POS ("Kaptoxa" Malware)

10. Send stolen Credit Card info to network share (FTP transfer)

11. Upload Credit Card information to FTP site

Reference

Example of a Type of Exam Question

Q: Select the correct answers in which a worm may spread?

A) A user clicks on a executable
B) A vulnerability in OS or services allows it to infect the host
C) Privilege level of the local user account
D) Through infected FTP servers
E) Through a USB drive
Example Question - Answers

Q: Select the correct answers in which a worm may spread?

A) A user clicks on a executable
B) A vulnerability in OS or services allows it to infect the host
C) Privilege level of the local user account
D) Through infected FTP servers
E) Through a USB drive
Network Security Analysts

• **Responsibilities of an analyst:**
  - Monitor and defend the network
  - Identify, investigate, and document incidents
  - Present, implement, and document mitigations
  - Stay up-to-date with modern technologies, tools, and threats
  - Conduct technical, security, and operational risk assessments
  - Identify the security needs of a system

• As analysts progress in their career, they may choose to specialize.

• What’s it like to be a Cisco Security Analyst?
  (blogs.cisco.com/security/what-is-it-like-to-be-a-cisco-security-analyst/)
Lab 2 (AAA) and Lab 3 (Packets)

Lab 2
• Cisco Router Configure AAA
• Setup AAA Logging

Lab 3
• Download Wireshark or TCDump (Linux)
• Capture packets – Learn to decode and understand payload
• Critical skill

http://packetlife.net/blog/2010/jun/7/understanding-tcp-sequence-acknowledgment-numbers/
Packet Data – Follow the packet

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>198.51.100.33</td>
<td>192.168.0.117</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; pop3s [SYN] Seq=0 Win=4096 Len=0</td>
</tr>
<tr>
<td>2</td>
<td>0.000007</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; h323hostcall [SYN] Seq=0 Win=4096</td>
</tr>
<tr>
<td>3</td>
<td>0.000010</td>
<td>198.51.100.33</td>
<td>192.168.0.117</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; ssh [SYN] Seq=0 Win=4096 Len=0 MS</td>
</tr>
<tr>
<td>4</td>
<td>0.000014</td>
<td>198.51.100.33</td>
<td>192.168.0.117</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; http [SYN] Seq=0 Win=1024 Len=0</td>
</tr>
<tr>
<td>5</td>
<td>0.000017</td>
<td>198.51.100.33</td>
<td>192.168.0.117</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; pop3 [SYN] Seq=0 Win=3072 Len=0</td>
</tr>
<tr>
<td>6</td>
<td>0.000020</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; rfb [SYN] Seq=0 Win=1024 Len=0 MS</td>
</tr>
<tr>
<td>7</td>
<td>0.000024</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; http-alt [SYN] Seq=0 Win=2048 Len</td>
</tr>
<tr>
<td>8</td>
<td>0.000027</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; submission [SYN] Seq=0 Win=3072 Len</td>
</tr>
<tr>
<td>9</td>
<td>0.000031</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; netbios-ssn [SYN] Seq=0 Win=1024 Len</td>
</tr>
<tr>
<td>10</td>
<td>0.000034</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; ms-wbt-server [SYN] Seq=0 Win=4096</td>
</tr>
<tr>
<td>11</td>
<td>0.000203</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; ms-wbt-server &gt; 48745 [SYN, ACK] Seq=0 Ack=0</td>
</tr>
<tr>
<td>12</td>
<td>0.002038</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; ms-wbt-server [RST] Seq=1 Win=0 E</td>
</tr>
<tr>
<td>13</td>
<td>0.004189</td>
<td>198.51.100.33</td>
<td>192.168.0.117</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; auth [SYN] Seq=0 Win=3072 Len=0 M</td>
</tr>
<tr>
<td>14</td>
<td>0.004194</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; pptp [SYN] Seq=0 Win=4096 Len=0 M</td>
</tr>
<tr>
<td>15</td>
<td>0.004200</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; auth &gt; 40945 [RST, ACK] Seq=1 Ack=1 Win=0</td>
</tr>
<tr>
<td>16</td>
<td>0.006800</td>
<td>198.51.100.33</td>
<td>192.168.0.117</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; smtp [SYN] Seq=0 Win=3072 Len=0 M</td>
</tr>
<tr>
<td>17</td>
<td>0.006803</td>
<td>198.51.100.33</td>
<td>192.168.0.117</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; emap [SYN] Seq=0 Win=2048 Len=0 M</td>
</tr>
<tr>
<td>18</td>
<td>0.006807</td>
<td>198.51.100.33</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; blackjack [SYN] Seq=0 Win=4096 Len</td>
</tr>
<tr>
<td>19</td>
<td>0.006810</td>
<td>198.51.100.33</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; sunrpc [SYN] Seq=0 Win=2048 Len=0 M</td>
</tr>
<tr>
<td>20</td>
<td>0.007071</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>48745 &gt; smtp [SYN, ACK] Seq=1 Ack=1 Win=0</td>
</tr>
<tr>
<td>21</td>
<td>0.007074</td>
<td>192.168.0.117</td>
<td>198.51.100.33</td>
<td>TCP</td>
<td>60</td>
<td>emap &gt; 48745 [SYN, ACK] Seq=0 Ack=1 Win=0</td>
</tr>
</tbody>
</table>
Attack Example – SQL Injection

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000600</td>
<td>192.168.132.1</td>
<td>192.168.132.129</td>
<td>TCP</td>
<td>74</td>
<td>58601 &gt; http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 T</td>
</tr>
<tr>
<td>2</td>
<td>0.006177</td>
<td>192.168.132.129</td>
<td>192.168.132.129</td>
<td>TCP</td>
<td>74</td>
<td>58601 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA</td>
</tr>
<tr>
<td>3</td>
<td>0.0089191</td>
<td>192.168.132.129</td>
<td>192.168.132.129</td>
<td>TCP</td>
<td>66</td>
<td>58601 &gt; http [ACK] Seq=1 Ack=1 Win=5888 Len=0 Tsv1=5619361</td>
</tr>
<tr>
<td>4</td>
<td>0.0162260</td>
<td>192.168.132.129</td>
<td>192.168.132.129</td>
<td>HTTP</td>
<td>250</td>
<td>GET /vuln.php?id=23%20alter%20table%20ids%20add%20column%20fucky%20int HTTP/1.0\r\n</td>
</tr>
<tr>
<td>5</td>
<td>0.0175556</td>
<td>192.168.132.129</td>
<td>192.168.132.129</td>
<td>TCP</td>
<td>66</td>
<td><a href="http://192.168.132.129">http://192.168.132.129</a> HTTP/1.0\r\n</td>
</tr>
<tr>
<td>6</td>
<td>0.0175153</td>
<td>192.168.132.129</td>
<td>192.168.132.129</td>
<td>TCP</td>
<td>675</td>
<td>HTTP/1.0 HTTP/1.0\r\n</td>
</tr>
<tr>
<td>7</td>
<td>0.0179907</td>
<td>192.168.132.129</td>
<td>192.168.132.129</td>
<td>TCP</td>
<td>66</td>
<td>58601 &gt; http [ACK] Seq=188 Ack=610 Win=7104 Len=0 Tsv1=5619361</td>
</tr>
<tr>
<td>8</td>
<td>0.0181818</td>
<td>192.168.132.129</td>
<td>192.168.132.129</td>
<td>HTTP</td>
<td>250</td>
<td>GET /vuln.php?id=23%20alter%20table%20ids%20add%20column%20fucky%20int HTTP/1.0\r\n</td>
</tr>
</tbody>
</table>

GET /vuln.php?id=23%20alter%20table%20ids%20add%20column%20fucky%20int HTTP/1.0\r\n
User-Agent: Wget/1.11.4 (Red Hat modified)\r\n
Accept: */\r\n
Host: 192.168.132.129\r\n
Connection: Keep-Alive\r\n
\r\n

[HTTP request 1/1]
Tcpdump

- `linux@ubuntu:~$ sudo tcpdump -i eth0 -n`
- tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
- listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
- 10:06:57.246670 IP 192.168.28.1.137 > 192.168.28.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
- 10:06:57.665021 ARP, Request who-has 192.168.28.128 (00:0c:29:66:4d:29) tell 192.168.28.1, length 46
- 10:06:57.665041 ARP, Reply 192.168.28.128 is-at 00:0c:29:66:4d:29, length 28
- 10:06:57.996116 IP 192.168.28.1.137 > 192.168.28.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
- 10:06:58.746225 IP 192.168.28.1.137 > 192.168.28.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
- 5 packets captured
- 5 packets received by filter
- 0 packets dropped by kernel
- `linux@ubuntu:~$`

Reading tcpdump output:

```
```

**Timestamp**  **Protocol**  **Source address**  **Source port**  **Destination address**  **Destination port**  **Description**
Lab 3 (ACL) and Lab 4 (Understanding Log Data)

Lab 3
• Configure a Cisco ACL include logging
• Setup free shareware Syslog server

Lab 4
• Use Free Syslog server (turn on timestamp)
• Server logs, DNS logs, DHCP logs – Attempt to correlate

Get Splunk free Syslogger

http://www.openxtra.co.uk/blog/top-5-open-source-event-correlation-tools/
### Syslog Levels and Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence Number</td>
<td>Stamps log messages with a sequence number only if “service sequence-numbers global” is part of the configuration.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Date and time of the event. Requires “service timestamps log”. Formatted as mm/dd hh:mm:ss, or hh:mm:ss, or d h.</td>
</tr>
<tr>
<td>Facility</td>
<td>The facility to which generated the message (for example, SNMP or SYS).</td>
</tr>
<tr>
<td>Severity</td>
<td>Single-digit code from 0 to 7 that is the severity of the message.</td>
</tr>
<tr>
<td>Mnemonic</td>
<td>A unique identifier associated with the category of the event.</td>
</tr>
<tr>
<td>Description</td>
<td>Detailed information about the event.</td>
</tr>
</tbody>
</table>


Description (continued)
Splunk for Cisco Security Suite

Provides increased visibility across Cisco device data such as Cisco reputation data in real time

- Pre-defined dashboards, searches, reports and alerts for all supported devices
- Field definitions to make ad-hoc investigations and custom dashboard creation as simple as a few mouse clicks
- Geographic threat information and visualization
- Reputation trending and monitoring

Supported Cisco Security Devices:

- ASA and PIX Firewalls
- FWSM (Router firewall module)
- Identity Services Engine (ISE)
- IronPort Web Security Agent (WSA)
- IronPort E-mail Security Agent (ESA)
- Sourcefire
DNS Logging: Windows DNS Output

- **Timestamp**: 9/1/2013 5:46:23 PM
- **Requesting IP**: 0e78
- **Requested Domain**: 10.0.0.100
- **Request Type**: UDP
- **Response Type**: Snd
- **Response Time-To-Live**: 0003 R Q [8081 DR NOERROR]
- **Response IP Address**: AAAA (3)www(6)google(3)com(0)
- **QUESTION SECTION**:
  - Offset = 0x000c, RR count = 0
  - Name "(3)www(6)google(3)com(0)"
    - QTYPE AAAA (28)
    - QCLASS 1
- **ANSWER SECTION**:
  - Offset = 0x0020, RR count = 0
  - Name "[C00C](3)www(6)google(3)com(0)"
    - TYPE AAAA (28)
    - CLASS 1
    - TTL 145
    - DLEN 16
    - DATA 2607:f8b0:400c:c02::68
Lab 5 (Event Data) and Lab 6 (Security Controls)

Lab 5
• Download Observium
• Monitor some network devices
• Understand Event data vs. Log data fields

Lab 6
• Security Controls – Run Nmap against your perimeter devices
• Review output of logs
• Freeware Vulnerability scanners
Resource Monitoring with Observium
Lab 7 (Correlation Events) and Lab 8 (Flow Data)

Lab 7
• Read documents on manual correlation
• Download OSSIM
• Learn how to configure automatic correlation between different sources

Lab 8
• NetFlow – Configure Cisco Router or ASA with NetFlow
• Read on NetFlow and the fields
• Free Tools for retrieving NetFlow (link)

http://www.networkmanagementsoftware.com/5-free-NetFlow-analyzer-tools-for-windows
Example – Nmap Output

- Nmap Options
  - TCP
  - UDP
  - OS Detection

- Run it against a router/firewall with logging enabled
  - Enable Decoy option
  - MTU Fragmentation
  - Random order
  - Zombie host

Establishing a Packet Baseline

• To detect intrusions or discover unexpected network activity, a baseline must first be established:
  • Determine what is “normal” and what is an “anomaly”
  • Capture all traffic on the network perimeter for a five-minute span
  • Export the packet capture to a local workstation for analysis

• Baselines are formed by collecting datapoints describing network activity.
  • Use packets capture tools to form these datapoints.
Defining Baselines – Traffic Analysis

• A baseline serves as a basis for rating the performance of a network in real-time situations.

• Baselines are established through testing and reporting of the characteristics of the network during routine load.
Know your IP Packet Fields

• Attackers Know IPv4 and IPv6 and TCP/UDP
  – They know the vulnerabilities
• Know TCP Sequence numbers and Windows size
• Study TCP Ports and range
• Study UDP ports and range
• Know ICMP
  – ICMP Attacks and Types
  – ICMP Tunneling – Send data out of the network
• Learn IPv6
## Internet Protocol version 4 (IPv4) Headers

<table>
<thead>
<tr>
<th>Byte 1</th>
<th>Byte 2</th>
<th>Byte 3</th>
<th>Byte 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Header Length</td>
<td>Service Type</td>
<td>Packet Length</td>
</tr>
<tr>
<td>Identification</td>
<td>Flags</td>
<td>Fragmentation Offset</td>
<td></td>
</tr>
<tr>
<td>Time-to-Live</td>
<td>Protocol</td>
<td>Header Checksum</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Internet Protocol version 6 (IPv6) Headers

<table>
<thead>
<tr>
<th>Byte 1</th>
<th>Byte 2</th>
<th>Byte 3</th>
<th>Byte 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Traffic Class</td>
<td>Flow Label</td>
<td></td>
</tr>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td></td>
<td>Hop Limit</td>
</tr>
</tbody>
</table>

- Source:
  - (16 bytes)

- Destination:
  - (16 bytes)
### User Datagram Protocol (UDP) Headers

<table>
<thead>
<tr>
<th>Byte 1</th>
<th>Byte 2</th>
<th>Byte 3</th>
<th>Byte 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td></td>
<td>Destination Port</td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td></td>
<td>Checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data</td>
</tr>
</tbody>
</table>
Transmission Control Protocol (TCP) Headers

<table>
<thead>
<tr>
<th>Byte 1</th>
<th>Byte 2</th>
<th>Byte 3</th>
<th>Byte 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Destination Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sequence Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acknowledgement Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Header Length</td>
<td>Resv.</td>
<td>Flags (RST, SYN, FIN, ...)</td>
<td>Window Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td></td>
<td></td>
<td>Urgent Pointer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data / Options (optional)</td>
<td></td>
</tr>
</tbody>
</table>
# Internet Control Message Protocol (ICMP) Headers

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Destination network unreachable</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Destination host unreachable</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Destination protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>Destination port unreachable</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>Destination host unreachable</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Destination protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Destination port unreachable</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>Fragmentation required</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>Network administratively prohibited</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>Host administratively prohibited</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>Echo Request</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>Time-To-Live Expired in Transit</td>
</tr>
</tbody>
</table>
Embedded Packet Capture (EPC)

- Embedded packet capture allows IOS devices to perform basic packet analysis on-board.
- Traffic may be displayed, saved, or exported as a PCAP file.
- Differs from SPAN ports or Router IP Traffic Export.
  - Data is stored on the network device, not forwarded
  - Data can be exported through a variety of paths, including:
    - flash:
    - tftp:
    - ftp:
    - scp:
Embedded Packet Capture (EPC)

```plaintext
router# monitor capture buffer name [...] 

router#monitor capture buffer malware
Filter Association succeeded

router#monitor capture buffer malware size 1024

router#monitor capture buffer malware filter access-list 101

router#monitor capture buffer malware export flash:malware.pcap

router#
```
Embedded Packet Capture (EPC)

```bash
router# monitor capture point ip cef name interface direction

[...]
```

```bash
router# monitor capture point ip cef inbound-traffic Gig0/0 in

router# monitor capture point associate inbound-traffic malware

router# monitor capture point start inbound-traffic
Jun 17 23:56:13.951: %BUFCAP-6-ENABLE: Capture point inbound-traffic enabled.

router# monitor capture point stop inbound-traffic
```
Remote Switched Port Analyzer (RSPAN)

- **Example Scenario**
  - A workstation has been reported to be generating excessive connection to a server located elsewhere on the internal network.
  - Use RSPAN to monitor traffic to and from both devices by directing to a dedicated port for detailed, offline analysis.
Log Correlation Engine - Tenable
Alienvault OSSIM

- Unified Security Management
Splunk

• Machine Data Search and Correlation Engine
## Vulnerability Assessments with Nessus

### Vulnerability Summary

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Vendor</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical</td>
<td>Cisco IOS Software Smart Install Remote Code Execution Vulnerability</td>
<td>CISCO</td>
<td>1</td>
</tr>
<tr>
<td>high</td>
<td>Cisco IOS Software Command Authorization Bypass</td>
<td>CISCO</td>
<td>1</td>
</tr>
<tr>
<td>high</td>
<td>Cisco IOS Software DHCP Version 6 Server Denial of Service Vulnerability</td>
<td>CISCO</td>
<td>1</td>
</tr>
<tr>
<td>high</td>
<td>Cisco IOS Software Multicast Source Discovery Protocol Vulnerability</td>
<td>CISCO</td>
<td>1</td>
</tr>
<tr>
<td>high</td>
<td>Cisco IOS Software Network Address Translation Vulnerability</td>
<td>CISCO</td>
<td>1</td>
</tr>
<tr>
<td>high</td>
<td>Cisco IOS Software Smart Install Denial of Service Vulnerability</td>
<td>CISCO</td>
<td>1</td>
</tr>
<tr>
<td>high</td>
<td>SNMP Agent Default Community Name (public)</td>
<td>SNMP</td>
<td>1</td>
</tr>
<tr>
<td>medium</td>
<td>Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Attack</td>
<td>Windows</td>
<td>5</td>
</tr>
<tr>
<td>medium</td>
<td>Terminal Services Encryption Level is Medium or Low</td>
<td>Misc.</td>
<td>5</td>
</tr>
<tr>
<td>medium</td>
<td>SMB Signing Disabled</td>
<td>Misc.</td>
<td>4</td>
</tr>
</tbody>
</table>
Potential Training to Train Cybersecurity Experts

Training next generation SOC Professional

• Job Role focused
• Hands-on Lab focused
• Skill development not tool focused
• Competency focused
• Real-world lab environment
Cyber Range Service Delivery Platform

Cyber Range is a Platform to Experience the Intelligent Cyber Security for the Real World

Customer Outcomes

- A Platform for Service Delivery and Learning
- Deeper understanding of leading security methodologies, operations, and procedures
- Empower customers with the architecture and capability to combat modern cyber threats

The Solution at a Glance

- Over 50 Attack Cases for 9 Technology Solutions
- 100+ applications simultaneously merged with 200-500 different Malware types
- Virtual environment accessible from any place in the world

PEOPLE
PROCESS
DATA
THINGS
Cyber Range Capabilities

… can improve cyber defence operational capabilities, by way of:

• **Architecture / Design** validation

• **Incident response playbook** creation / validation

• **War game** exercises

• **Hands-on training** for individual technologies

• **Threat mitigation** process verification

• **Simulating advanced threats** (zero day / APT)
What Should the Advanced Training Look Like?

Cisco is looking for your help. Please send me an email if you have ideas.

- Should Cisco focus on SOC job roles?
- What training in Cybersecurity threat detection and mitigation are needed?
- Would a Cyber Range Training lab and exam be of value?
- Should we build a training lab where the students are the Blue Team and Cisco is the Red Team?
Links to study information

- **Cisco Talos**
  - [www.talosintel.com](http://www.talosintel.com) (Great White Papers)
  - Free tools such as SNORT

- [http://www.sans.org/security-resources/policies/info_sys_audit.pdf](http://www.sans.org/security-resources/policies/info_sys_audit.pdf)

- Microsoft Malware Protection Center

- Full Disclosure mailing list
  - [seclists.org/fulldisclosure/](http://seclists.org/fulldisclosure/)
Links and must reads

• NetFlow


• Microsoft


• What is a baseline?


• SIEM tools – Do’s and Don’ts

http://www.csoonline.com/article/print/509553
My Promise to You

• Add Documents to the Cisco Learning Network Cyber Security Study Group
• Over the next Month go through the exam blueprint and cover all of the topics

Link to the study group:
https://learningnetwork.cisco.com/groups/cyber-security-study-group
Beer Brewing leads to this…
Participate in the “My Favorite Speaker” Contest
Promote Your Favorite Speaker and You Could Be a Winner

• Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)

• Send a tweet and include
  • Your favorite speaker’s Twitter handle @JimRisler
  • Two hashtags: #CLUS #MyFavoriteSpeaker

• You can submit an entry for more than one of your “favorite” speakers

• Don’t forget to follow @CiscoLive and @CiscoPress

• View the official rules at http://bit.ly/CLUSwin
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

• Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions
## Security Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing Cisco IOS Network Security (IINS)</td>
<td>Focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features</td>
<td>CCNA® Security</td>
</tr>
<tr>
<td>Implementing Cisco Edge Network Security Solutions (SENSS)</td>
<td>Configure Cisco perimeter edge security solutions utilizing Cisco Switches, Cisco Routers, and Cisco Adaptive Security Appliance (ASA) Firewalls</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Threat Control Solutions (SITCS)</td>
<td>Deploy Cisco's Next Generation Firewall (NGFW) as well as Web Security, Email Security and Cloud Web Security</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Secure Access Solutions (SISAS)</td>
<td>Deploy Cisco's Identity Services Engine and 802.1X secure network access</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Secure Mobility Solutions (SIMOS)</td>
<td>Protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions</td>
<td></td>
</tr>
<tr>
<td>Securing Cisco Networks with Threat Detection and Analysis (SCYBER)</td>
<td>Designed for professional security analysts, the course covers essential areas of competency including event monitoring, security event/alarm/traffic analysis, and incident response</td>
<td>Cisco Cybersecurity Specialist</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com
Thank you
TOMORROW starts here.