WHAT’S NEW IN SECURITY+ SY0-401?

PRESENTED BY NETCOM LEARNING

PRESENTER BRAD PARKER, MCT

www.NetComLearning.com
WHY SHOULD I TAKE SYO-401?

• CompTIA has increased the coverage of the Security+ exam
• Demonstrates a better understanding of mobile and cloud computing
• D.O.D. recognizes the changes and requires many positions to hold this certification
• Updates all CE requirements for Security+ and below certifications
• SY0-301 is available until Jan. 1, 2015 but SY0-401 carries more weight.
DEMAND FOR SECURITY IS UP!

- Mobile computing has increased dramatically
- BYOD is part of the network now
- Increased integration with third parties
- Data is escaping the enterprise more often
- Data breaches are occurring as often as ever and are publicized better
How to Prepare for the SYO-401

- The CompTIA Security+ Certification is aimed at an IT security professional who has:
  - A minimum of 2 years experience in IT administration with a focus on security
  - Day to day technical information security experience
  - Broad knowledge of security concerns and implementation including the topics in the domain list below
- Preferably already Network+ certified
- Sit the NetCom Learning Security+ Boot Camp
- Know the book information
- Memorize acronyms and glossary of terms
- Practice exam software

www.NetComLearning.com
### CompTIA Security+ Exam SY0-401

<table>
<thead>
<tr>
<th>Number of questions</th>
<th>Maximum of 100 questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of questions</td>
<td>Multiple choice and performance-based</td>
</tr>
<tr>
<td>Length of test</td>
<td>90 minutes</td>
</tr>
<tr>
<td>Passing score</td>
<td>750 (on a scale of 100-900)</td>
</tr>
</tbody>
</table>
The majority of questions will be multiple choice answers.

4-10 questions will be performance based.

Depending on the nature of the exam and the exam question, the simulated environments may include different aspects of IT infrastructure, such as command prompts, Windows or networking environments.

We’ll take a look at some examples later in this webinar.
# OBJECTIVES/TOPICS COVERED

<table>
<thead>
<tr>
<th>Domain</th>
<th>% of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Network Security</td>
<td>20%</td>
</tr>
<tr>
<td>2.0 Compliance and Operational Security</td>
<td>18%</td>
</tr>
<tr>
<td>3.0 Threats and Vulnerabilities</td>
<td>20%</td>
</tr>
<tr>
<td>4.0 Application, Data and Host Security</td>
<td>15%</td>
</tr>
<tr>
<td>5.0 Access Control and Identity Management</td>
<td>15%</td>
</tr>
<tr>
<td>6.0 Cryptography</td>
<td>12%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
1.0 NETWORK SECURITY

• 1.1 Implement security configuration parameters on network devices and other technologies.

• 1.2 Given a scenario, use secure network administration principles.

• 1.3 Explain network design elements and components.

• 1.4 Given a scenario, implement common protocols and services.

• 1.5 Given a scenario, troubleshoot security issues related to wireless networking.
2.0 COMPLIANCE AND OPERATIONAL SECURITY

• 2.1 Explain the importance of risk related concepts.
• 2.2 Summarize the security implications of integrating systems and data with third parties.
• 2.3 Given a scenario, implement appropriate risk mitigation strategies.
• 2.4 Given a scenario, implement basic forensic procedures.
• 2.5 Summarize common incident response procedures.
• 2.6 Explain the importance of security related awareness and training.
• 2.7 Compare and contrast physical security and environmental controls.
• 2.8 Summarize risk management best practices.
• 2.9 Given a scenario, select the appropriate control to meet the goals of security.
3.0 THREATS AND VULNERABILITIES

• 3.1 Explain types of malware.
• 3.2 Summarize various types of attacks.
• 3.3 Summarize social engineering attacks and the associated effectiveness with each attack.
• 3.4 Explain types of wireless attacks.
• 3.5 Explain types of application attacks.
• 3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
• 3.7 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
• 3.8 Explain the proper use of penetration testing versus vulnerability scanning.
4.0 APPLICATION, DATA AND HOST SECURITY

• 4.1 Explain the importance of application security controls and techniques.
• 4.2 Summarize mobile security concepts and technologies.
• 4.3 Given a scenario, select the appropriate solution to establish host security.
• 4.4 Implement the appropriate controls to ensure data security.
• 4.5 Compare and contrast alternative methods to mitigate security risks in static environments.
5.0 ACCESS CONTROL AND IDENTITY MANAGEMENT

• 5.1 Compare and contrast the function and purpose of authentication services.

• 5.2 Given a scenario, select the appropriate authentication, authorization or access control.

• 5.3 Install and configure security controls when performing account management, based on best practices.
6.0 CRYPTOGRAPHY

• 6.1 Given a scenario, utilize general cryptography concepts.

• 6.2 Given a scenario, use appropriate cryptographic methods.

• 6.3 Given a scenario, use appropriate PKI, certificate management and associated components.
EXAMPLES OF QUESTION FORMATS

• Majority will be multiple choice
• A few will be interactive
• Don’t be intimidated by the interactive

Typical Multiple Choice

What port is used by the DNS protocol?

- 21
- 53
- 389
- 22

Typical Interactive

Click and drag to place the sequence of data lost based on time factor.
<table>
<thead>
<tr>
<th>Definition</th>
<th>Security Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>only made possible by requiring validation of the receiver</td>
<td>ensuring confidentiality</td>
</tr>
<tr>
<td>only the intended recipients can access and read the data</td>
<td>maintaining integrity</td>
</tr>
<tr>
<td>only encrypted connections (VPNs) are allowed to transfer data</td>
<td>ensuring availability</td>
</tr>
<tr>
<td>the assurance that the information has not been altered during transmission</td>
<td></td>
</tr>
<tr>
<td>the assurance of timely and reliable access to data</td>
<td></td>
</tr>
</tbody>
</table>

**Types of Interactive Questions - 1**
## Ports to Memorize

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>20, 21</td>
<td>NNTP</td>
<td>119</td>
</tr>
<tr>
<td>SSH, SFTP, SCP</td>
<td>22</td>
<td>IMAP</td>
<td>143</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
<td>SNMP</td>
<td>161</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>LDAP</td>
<td>389</td>
</tr>
<tr>
<td>TACACS</td>
<td>49</td>
<td>ISAMP (VPN)</td>
<td>500</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>Syslog</td>
<td>514</td>
</tr>
<tr>
<td>TFTP</td>
<td>69</td>
<td>LDAP/TLS</td>
<td>636</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>L2TP</td>
<td>1701</td>
</tr>
<tr>
<td>Kerberos</td>
<td>88</td>
<td>PPTP</td>
<td>1723</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td>Remote access</td>
<td>3389</td>
</tr>
</tbody>
</table>

## Match Items

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>80</td>
</tr>
<tr>
<td>FTP</td>
<td>69</td>
</tr>
<tr>
<td>HTTP</td>
<td>21</td>
</tr>
<tr>
<td>LDAP</td>
<td>143</td>
</tr>
<tr>
<td>RDP</td>
<td>23</td>
</tr>
<tr>
<td>SCP</td>
<td>22</td>
</tr>
<tr>
<td>SFTP</td>
<td>25</td>
</tr>
<tr>
<td>SMTP</td>
<td>161</td>
</tr>
<tr>
<td>Telnet</td>
<td>53</td>
</tr>
<tr>
<td>TFTP</td>
<td>189</td>
</tr>
</tbody>
</table>

Match Protocols With Correct Ports
TYPES OF INTERACTIVE QUESTIONS - 3

Security Techniques

<table>
<thead>
<tr>
<th>Devices</th>
<th>Security Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Cable Locks</td>
</tr>
<tr>
<td></td>
<td>Proximity Lock</td>
</tr>
<tr>
<td>Desktop</td>
<td>Strong Password</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
</tr>
<tr>
<td>Secure Entry</td>
<td>Least Privilege</td>
</tr>
<tr>
<td></td>
<td>TPM</td>
</tr>
<tr>
<td>Key Storage</td>
<td>Screen Lock</td>
</tr>
<tr>
<td></td>
<td>HSM</td>
</tr>
<tr>
<td>Hardware Encryption</td>
<td>Mantrap</td>
</tr>
<tr>
<td></td>
<td>Remote Wipe</td>
</tr>
<tr>
<td>Smart Phone</td>
<td>Cipher Lock</td>
</tr>
<tr>
<td></td>
<td>Locked Cabinet or Safe</td>
</tr>
<tr>
<td>Tablet</td>
<td>GPS Tracking</td>
</tr>
<tr>
<td></td>
<td>Data encryption</td>
</tr>
</tbody>
</table>
Types of Interactive Questions - 4

Order of volatility of digital evidence
1. CPU, cache and register content, routing table, ARP cache, process table, kernel statistics
2. RAM – Main Memory
3. Paging File, temporary file system / swap space
4. HDD - Data on hard disk
5. Remotely logged data – remote systems
6. Data contained on archival media – Backups on remote or offsite locations

Order of Volatility

1.
2.
3.
4.
5.
6.
HOW TO BEST USE RESOURCES FOUND ONLINE TO PREPARE

• eBooks
• Brain Dumps
• Illicit exam prep material
• Google/Wikipedia
• Download software referenced in official training materials
SOFTWARE TO PRACTICE WITH - FREE

- Wireshark
- Microsoft Network Monitor
- Cain & Abel
- Snort
- NMAP
- Superscan
- Microsoft Server 2008 R2 with Active Directory
- Many others
RECOMMENDATIONS WHILE TESTING

- Write down lists or items you’ve memorized
- If a question takes longer than 15 seconds to answer – Mark if for Review
  - Gets the clock off your mind
- Read the question slowly and carefully
- Don’t read anything into the question
- When you decide on the correct answer, tell yourself why the others are wrong
- Look for Key Words – First, Last, Least administrative effort, least cost, etc.
- Look for “SELECT TWO”
- If you have no idea – use process of elimination
- Don’t second guess yourself
- Never leave an answer blank
WHAT DOES NETCOM LEARNING OFFER?

• Selective certified and experienced trainers
• Standard Security+ Course
• Security+ Boot Camp Course – brace yourself
  • Exam vouchers included!
• Excellent hands on and reference materials
• Live environment for practice
• Courses that qualify for CEUs (Continuing Educations Units)

www.NetComLearning.com
WHAT’S NEW IN SECURITY+ SY0-401?

PRESENTED BY NETCOM LEARNING

PRESENTER BRAD PARKER, MCT

www.NetComLearning.com