Oklahoma State Regents for Higher Education

CONTRACTUAL ARRANGEMENTS AND/OR TECHNICAL PRIOR LEARNING ASSESSMENT PROGRAM REQUEST FORM

Rose State College
Institution Submitting Proposal

Networking/Cybersecurity Associate in Applied Science (111)
Program name and State Regents' three-digit program code

Eastern Oklahoma County Technology Center
Contractual Entity

Date of Governing Board Approval: 09/17/15
Signature of President: 9/27/15
Signature of Other Entity Signatory: 9/23/15

State Regents' Policy 3.6 and 3.15
http://www.okhighered.org/admin-ltc/academic-forms/
Thank you for your submission. Based on the information detailed below, the Commission has determined that it has sufficient information to constitute notification of the contractual relationship per policy and no further action is required. If you have any further questions, please send an email to changerequests@hlcommission.org.

Name: Dr. Frances M. Hendrix  
Institution: 1635 - Rose State College - OK  
City: Midwest City  
State: Oklahoma  
Email address: fhendrix@rose.edu  
Phone number: 405.733.7395

You confirm you are authorized to provide the Commission with information regarding your institution's contractual arrangements.

Academic program: Network and Systems Administration/Administrator  
CIP code: 11.1001  
Course catalog name: Networks  
Program or credential level: Associate  
Expected start date: 2015-08-18  
Contractual partner: Eastern Oklahoma County Technology Center

Total program credit hours: 62  
Credit hours taught by contractual partner: 15  
Calculated percentage: 24.19

The percentage taught by the contractual partner is less than 25%.  
Does the contractual partner provide oversight of the curriculum? Yes  
Does the contractual partner provide assurance of the consistency? Yes  
Does the contractual partner establish academic qualifications for instructional personnel? Yes

The percentage representing the aggregate of the contractual partner's total efforts: Less than 25%
Thank you for your submission. Based on the information detailed below, the Commission has determined that it has sufficient information to constitute notification of the contractual relationship per policy and no further action is required. If you have any further questions, please send an email to changerequests@hlcommission.org.

Name: Dr. Frances M. Hendrix  
Institution: 1635 - Rose State College - OK  
City: Midwest City  
State: Oklahoma  
Email address: fhendrix@rose.edu  
Phone number: 405.733.7395

You confirm you are authorized to provide the Commission with information regarding your institution's contractual arrangements.

Academic program: Network and Systems Administration/Administrator  
CIP code: 11.1001  
Course catalog name: Computer Hardware and Operating Systems  
Program or credential level: Associate  
Expected start date: 2015-08-18  
Contractual partner: Eastern Oklahoma County Technology Center

Total program credit hours: 62  
Credit hours taught by contractual partner: 15  
Calculated percentage: 24.19

The percentage taught by the contractual partner is less than 25%.  
Does the contractual partner provide oversight of the curriculum? Yes  
Does the contractual partner provide assurance of the consistency? Yes  
Does the contractual partner establish academic qualifications for instructional personnel? Yes

The percentage representing the aggregate of the contractual partner's total efforts: Less than 25%
Thank you for your submission. Based on the information detailed below, the Commission has determined that it has sufficient information to constitute notification of the contractual relationship per policy and no further action is required. If you have any further questions, please send an email to changerequests@hlcommission.org.

Name: Dr. Frances M. Hendrix
Institution: 1635 - Rose State College - OK
City: Midwest City
State: Oklahoma
Email address: fhendrix@rose.edu
Phone number: 405.733.7395

You confirm you are authorized to provide the Commission with information regarding your institution's contractual arrangements.

Academic program: Network and Systems Administration/Administrator
CIP code: 11.1001
Course catalog name: Network Administration
Program or credential level: Associate
Expected start date: 2015-08-18
Contractual partner: Eastern Oklahoma County Technology Center

Total program credit hours: 62
Credit hours taught by contractual partner: 15
Calculated percentage: 24.19

The percentage taught by the contractual partner is less than 25%. Does the contractual partner provide oversight of the curriculum? Yes
Does the contractual partner provide assurance of the consistency? Yes
Does the contractual partner establish academic qualifications for instructional personnel? Yes

The percentage representing the aggregate of the contractual partner's total efforts: Less than 25%
Thank you for your submission. Based on the information detailed below, the Commission has determined that it has sufficient information to constitute notification of the contractual relationship per policy and no further action is required. If you have any further questions, please send an email to changerequests@hlcommission.org.

Name: Dr. Frances M. Hendrix  
Institution: 1635 - Rose State College - OK  
City: Midwest City  
State: Oklahoma  
Email address: fhendrix@rose.edu  
Phone number: 405.733.7395

You confirm you are authorized to provide the Commission with information regarding your institution's contractual arrangements.

Academic program: Network and Systems Administration/Administrator  
CIP code: 11.1001  
Course catalog name: Network Troubleshooting and Management Design  
Program or credential level: Associate  
Expected start date: 2015-08-18  
Contractual partner: Eastern Oklahoma County Technology Center

Total program credit hours: 62  
Credit hours taught by contractual partner: 15  
Calculated percentage: 24.19

The percentage taught by the contractual partner is less than 25%.  
Does the contractual partner provide oversight of the curriculum? Yes  
Does the contractual partner provide assurance of the consistency? Yes  
Does the contractual partner establish academic qualifications for instructional personnel? Yes

The percentage representing the aggregate of the contractual partner's total efforts: Less than 25%
Thank you for your submission. Based on the information detailed below, the Commission has determined that it has sufficient information to constitute notification of the contractual relationship per policy and no further action is required. If you have any further questions, please send an email to changerequests@hlcommission.org.

Name: Dr. Frances M. Hendrix  
Institution: 1635 - Rose State College - OK  
City: Midwest City  
State: Oklahoma  
Email address: fhendrix@rose.edu  
Phone number: 405.733.7395

You confirm you are authorized to provide the Commission with information regarding your institution's contractual arrangements.

Academic program: Network and Systems Administration/Administrator  
CIP code: 11.1001  
Course catalog name: Network Security  
Program or credential level: Associate  
Expected start date: 2015-08-18  
Contractual partner: Eastern Oklahoma County Technology Center

Total program credit hours: 62  
Credit hours taught by contractual partner: 15  
Calculated percentage: 24.19

The percentage taught by the contractual partner is less than 25%.  
Does the contractual partner provide oversight of the curriculum? Yes  
Does the contractual partner provide assurance of the consistency? Yes  
Does the contractual partner establish academic qualifications for instructional personnel? Yes

The percentage representing the aggregate of the contractual partner's total efforts: Less than 25%
Contractual Arrangement and/or Technical Prior Learning Assessment Program Request Form

The proposal for a contractual arrangement or technical prior learning assessment (PLA) program should provide the following information.

NOTE: INFORMATION NOT INCLUDED IN THE PROPOSAL MAY CAUSE A DELAY IN PROCESSING.

1. A signature page (institutional president and entity’s signatory) that includes the names of the participating college and other entity.

2. Name of college-level certificate or degree program(s) toward which credit will be awarded, including the State Regents’ three-digit program code and any options.

(The size of the box is NOT an indicator of the amount of information required to address the request. Please include as much information as necessary [the boxes will expand].)

3. Will this arrangement include:
   - X contractual arrangement
   - technical assessments (PLA)
   - Combination of both

4. List a) technical courses on the Statewide Contractual Course Inventory/Technical Crosswalk, b) assessments on the Statewide Inventory of Industrial, Technical and Other Assessments, and/ or c) general education courses that will be included in the contractual or technical PLA program.

   a) Technical Courses in Contractual Arrangements:

<table>
<thead>
<tr>
<th>Higher Education Course:</th>
<th>Contractual Technical Course:</th>
<th>Approved for listing on Statewide Contractual Course Inventory/Technical Crosswalk?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIT 1523 Computer Hardware and Operating Systems</td>
<td>A+</td>
<td>Yes  No X Request Pending</td>
</tr>
<tr>
<td>Higher Education Course:</td>
<td>Contractual Technical Course:</td>
<td>Approved for listing on Statewide Contractual Course Inventory/Technical Crosswalk?</td>
</tr>
<tr>
<td>CIT 1503 Networks</td>
<td>Network +</td>
<td>Yes  No X Request Pending</td>
</tr>
<tr>
<td>Higher Education Course:</td>
<td>Contractual Technical Course:</td>
<td>Approved for listing on Statewide Contractual Course Inventory/Technical Crosswalk?</td>
</tr>
<tr>
<td>CIT 2053 Network Administration</td>
<td>INF 2253 Windows XP Pro INF 2213 Managing Server 2003</td>
<td>Yes  No X Request Pending</td>
</tr>
<tr>
<td>Higher Education Course:</td>
<td>Contractual Technical Course:</td>
<td>Approved for listing on Statewide Contractual Course Inventory/Technical Crosswalk?</td>
</tr>
<tr>
<td>CIT 2423 Network Troubleshooting and Management Design</td>
<td>INF 2233 Planning a Network Infrastructure</td>
<td>Yes  No X Request Pending</td>
</tr>
</tbody>
</table>

State Regents' Policy 3.6 and 3.15
http://www.okhighered.org/admin-fac/academic-forms/
| Higher Education Course: CIT 2323 Network Security | Contractual Technical Course: Security Fundamentals | Approved for listing on Statewide Contractual Course Inventory/Technical Crosswalk?  
Yes  No  X  Request Pending |
|--------------------------------------------------|--------------------------------------------------|--------------------------------------------------|

b) Technical Assessments (PLA):

| Higher Education Course: NONE | Technical Assessment: | Approved for listing on the Statewide Matrix of Industrial, Technical and Other Assessments?  
Yes  No  Request Pending |
|-------------------------------|---------------------|--------------------------------------------------|
| Higher Education Course:     | Technical Assessment: | Approved for listing on the Statewide Matrix of Industrial, Technical and Other Assessments?  
Yes  No  Request Pending |
| Higher Education Course:     | Technical Assessment: | Approved for listing on the Statewide Matrix of Industrial, Technical and Other Assessments?  
Yes  No  Request Pending |

(add rows as needed)

c) General Education Courses:

<table>
<thead>
<tr>
<th>Higher Education Course: NONE</th>
<th>Location?</th>
<th>Delivery Method?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher Education Course:</td>
<td>Location?</td>
<td>Delivery Method?</td>
</tr>
<tr>
<td>Higher Education Course:</td>
<td>Location?</td>
<td>Delivery Method?</td>
</tr>
</tbody>
</table>

(add rows as needed)
5. Detail the maximum number of college credit hours to be articulated through contractual technical courses or technical assessments and the maximum college credit awarded toward the degree for work completed outside the institution¹.

<table>
<thead>
<tr>
<th>Description</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total credit hours articulated through contractual technical courses:</td>
<td>15</td>
</tr>
<tr>
<td>Total credit hours articulated through technical assessments:</td>
<td>0</td>
</tr>
<tr>
<td>Total credit hours that can be applied to the degree through approved contractual technical courses and/or assessments:</td>
<td>15</td>
</tr>
<tr>
<td>Total credit hours in general education:</td>
<td>0</td>
</tr>
<tr>
<td>Total credit hours required for the degree:</td>
<td>62</td>
</tr>
</tbody>
</table>

¹ Note: the Higher Learning Commission requires that at least "15 of the 60 credits for the associate’s degree be credits earned at the institution itself, through arrangements with other accredited institutions, or through contractual relationships approved by the Commission." However, any time the credit from outside the institution surpasses 50%, a higher level of scrutiny/review from HLC should be expected.

6. Description of the contractual entity’s classroom and laboratory facilities and how they will be utilized.

Eastern Oklahoma County Technology Center offers facilities and equipment which allows students to learn in a computer-based, laboratory environment for students to apply what they have learned to their assignments. EOCTC also offers a lecture environment which allows faculty to demonstrate concepts to students from an instructional station.

7. Academic credentials of contractual entity’s faculty responsible for classroom and laboratory experiences. (Include a summary document here. Full vitae, resume and certifications must be included as attachments, as well as documentation of the institutional process for credential and/or experience evaluation for contractual entity’s faculty.)

College faculty supervising the contractual arrangement or application of PLA credit for the program: N/A
Contractual entity’s faculty teaching in the contractual arrangement:
Mr. Tom Buntin, M.Ed., Adult Education, University of Central Oklahoma; B.S., Educational Computer Science, University of Central Oklahoma; CompTIA, Network+, CCNA

8. Outline the process to assure quality academic programming and continuous improvement in the contractual arrangement or technical PLA program.

Rose State College faculty reviewed the Eastern Oklahoma County Technology Center curriculum and determined that the curriculum duplicated 9 credit hours of instruction that occurs through the Networking/CyberSecurity Associate in Applied Science degree program at Rose State College. Rose State College faculty reviewed the credentials of faculty from Eastern Oklahoma County Technology Center to ensure faculty hold credentials that meet the minimum requirements for adjunct and full-time faculty assignments at Rose State College. Rose State College faculty added the Eastern Oklahoma County Technology Center faculty to the Rose State College Family Networking/CyberSecurity program advisory committee. Rose State College faculty were added to the Eastern Oklahoma County Technology Center Computer Repair and Networking Program.

9. Describe the criteria for assessment of student outcomes in each contractual technical course and/or assessment.

See attached syllabus.

10. To maintain quality courses, the higher education institution will designate an appropriate individual to direct and oversee the contractual arrangement. Provide the name of the individual as well as the

In addition to the full-time Networking/CyberSecurity Program faculty member and director, Mr. Ken Dewey, Ms. Jerri Cachero, Coordinator for Technology Center Programs, Rose State College, oversees all contractual arrangements with technology centers to ensure that students are advised and enrolled appropriately, serves as the liaison between faculty representatives from the technology centers and the college. She holds meetings with faculty on campus, meets with faculty and staff at each technology center, and arranges and holds joint meetings. She also develops the annual Technology Center catalog, meets with admissions and enrollment staffs from the technology center and on campus, and hosts students from the technology centers on campus on enrollment/advisement days. In addition, she attends advisory committees, and other statewide meetings at the Oklahoma State Regents for Higher Education.

State Regents' Policy 3.6 and 3.15
http://www.okhlighered.org/admin-fac/academic-forms/
criteria and procedures that will be used for an annual evaluation of courses. (Note if same or different from #7)

11. Describe the academic and student support services available to students enrolled in the contractual arrangement.

Students from the technology center are hosted on campus. Students are enrolled on campus by Academic Advisors, tour the campus and receive financial aid/college life information from Prospective Student Services and are taken on a campus-wide tour. Students complete their admissions forms, take COMPASS exams, are enrolled and attend various related seminars on campus. Students have access to the College's website services such as those available in the Learning Resources Center and receive a Rose State College student I.D. card which grants students' rights and privileges of a Rose State College student.

A college liaison visits each campus on a weekly basis to assist with questions related to degree completion, financial aid deadlines, Ticket to Rose, etc., and serves as an advisor to these students at their technology center.

12. Outline the financial arrangements between the institution and the contractual entity if different from that specified in policy; this should include student tuition and other charges applicable to the contractual arrangement.

Students pay the state-adopted rate of $8.00 per credit hour since instruction takes place at the technology center under the technology center budget.

13. Indicate if high school students may be enrolled in this contractual arrangement and/or any restriction based on age of students due to the nature of the technical field, licensure requirements, etc.

High school students are eligible for enrollment provided that they meet the admission requirements under the cooperative agreement policy.
COOPERATIVE AGREEMENTS PROGRAM
ROSE STATE COLLEGE/EASTERN OKLAHOMA COUNTY TECHNOLOGY CENTER
Fall 2015 – Spring 2016

Rose State College – Business & Information Technology Division
Degree: A.A.S. - Networking/Cybersecurity (0111)
Contact: Professor Ken Dewey
Division Academic Advisor: Mr. Steve Johnson

EOC Technology Center Program: Computer Repair and Networking
Contact: Mr. Tom Buntin

Credit Total: 15 hours

<table>
<thead>
<tr>
<th>RSC Course Number and Title</th>
<th>EOC Tech Center Units Covered</th>
<th>Credit Hours</th>
<th>RSC Faculty Initials</th>
<th>Tech Center Faculty Initials</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIT 1523  Computer Hardware and Operating Systems</td>
<td>A+</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIT 1503  Network</td>
<td>Network+</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIT 2053  Network Administration</td>
<td>INF 2253 Windows XP Pro INF 2213 Managing Server 2003</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIT 2423  Network Troubleshooting and Management Design</td>
<td>INF 2223 Maintaining a Network INF 2233 Planning a Network Infrastructure</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(More on following page)
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Network Fundamentals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Number</td>
<td>8136  OHLAP Approved</td>
</tr>
<tr>
<td>Career cluster/Pathway</td>
<td>Information Technology/Information support &amp; Services/</td>
</tr>
<tr>
<td>Career Majors</td>
<td>Desktop support Technician</td>
</tr>
<tr>
<td>Pre-requisite</td>
<td>Fundamentals of Technology</td>
</tr>
<tr>
<td>Location</td>
<td>EOC Technology Center</td>
</tr>
<tr>
<td>Length</td>
<td>120 hrs</td>
</tr>
</tbody>
</table>

**Course Description:** This course is designed to be a study of local area networks, their topologies and their functions and provides a general understanding of the basic LAN protocols. Topics covered include: fundamental concepts and terminology, the IEEE/ISO Logical Link control standard, construction of a LAN, and LAN data links.

Methods of Instruction
Instruction will be Testout Labsim which includes lectures, Labs, and tests. In addition there will be class discussions, Hands on training, demonstrations, projects, and webinars.

**GRADING**

<table>
<thead>
<tr>
<th>Daily Grade/Attendance</th>
<th>15 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>LabSim Tests and Scenarios</td>
<td>60%</td>
</tr>
<tr>
<td>Technician Project(s)</td>
<td>25%</td>
</tr>
</tbody>
</table>

**Grading Scale**

- 100 - 90% = A Superior Achievement
- 89 - 80% = B Above-Average
- 79 - 70% = C Average Achievement
- 69 - 60% = D Below-Average
- 0 - 59% = F Falling Work

Certifications (Select from the following options)

- ODCTE - Microcomputer Networkr Technician OD41001
- Comptia - Network+
- Microsoft - MTA Networking Fundamentals
Credit Toward Certification

When you pass Exam 98-366: you complete the requirements for the following certification(s):

- Microsoft Technology Associate Infrastructure Track

MAJOR COURSE LEARNING OBJECTIVES: Upon successful completion of this course you will be expected to:

1. Recognize logical or physical network topology given a diagram or description.
2. Specify the main features of 802.3 (Ethernet), 802.5 (token ring), 802.11b,g (wireless), and FDDI networking technologies.
3. Specify the characteristics (e.g., speed, link, topology, cable time, etc.) of various networking media types.
4. Recognize media connectors and describe their uses.
5. Choose the appropriate media type and connectors to add a client to an existing network.
6. Identify the purpose, features and functions of network components.
7. Given an example identify a MAC address.
8. Identify the seven layers of the OSI model and their functions.
9. Differentiate between network protocols in terms of routing, addressing schemes, interoperability, and naming conventions.
10. Identify the OSI layers at which networking components operate.
11. Define the purpose, function and use of all the protocols within the TCP/IP suite.
12. Define the function of TCP/UDP ports. Identify well-known ports.
13. Identify the purpose of network services such as DHCP, DNS, NAT, WINS.
14. Identify IP addresses (IPv4, IPv6) and their default subnet masks.
15. Identify the purpose of subnetting and default gateways.
16. Identify the differences between public versus private networks.
17. Identify the basic characteristics of WAN technologies.
18. Define the function of remote access protocols and services.
19. Identify security protocols and describe their purpose and function.
20. Identify the basic capabilities (i.e., client support, interoperability, authentication, file and print services, application support, and security) of server operating systems such as Unix/Linux, Netware, Windows, and Macintosh.
21. Identify the basic capabilities of client workstations (i.e., client connectivity, local security mechanisms, and authentication).
22. Identify the main characteristics of VLANs.
23 Identify the main characteristics of network attached storage.
24 Identify the purpose and characteristics of fault tolerance.
25 Identify the purpose and characteristics of disaster recovery.
26 Given a remote connectivity scenario e.g. IP, IPX, dial-up, PPPoE, authentication, physical connectivity, etc.) configure the connection.
27 Identify the purpose, benefits and characteristics of using a firewall.
28 Identify that purpose, benefits and characteristics are using a proxy.
29 Given a scenario, predict the impact of a particular security implementation on network functionality (e.g., locking port numbers, encryption, etc.).
30 Given a network configuration, select the appropriate NIC and network configuration settings (DHCP, DNS, WINS, protocols, NETBIOS, host name, etc.).
31 Given a trouble shooting scenario, select the appropriate TCP/IP utility.
32 Given a troubleshooting scenario involving a small office/home office network failure (e.g. xDSL, cable, home satellite, wireless, POTS), identify the cause of the failure.
33 Given a troubleshooting scenario involving a remote connectivity problem (e.g., authentication failure, protocol configuration, physical connectivity) identify the cause of the problem.
34 Given specific parameters, configure a client to connect to a server running an identified NOS.
35 Given a wiring task, select the appropriate tool (wire crimper, media tester/certifier, punch-down tool, tone generator, optical tester, etc.).
36 Given a network scenario interpret the visual indicators (link the lights, collision lights, etc.), to determine the nature of the problem.
37 Given a scenario, predict the impact of modifying, adding, or removing network services on network resources and users.
38 Given a network problem scenario, select an appropriate course of action based on a general troubleshooting strategy.
39 Given a troubleshooting scenario involving a network with a particular physical topology (bus, star, hierarchical, mesh, ring, or wireless) and including a network diagram, identify the network area affected and the cause of the problem.
40 Given a network troubleshooting scenario involving a client connectivity problem (incorrect protocols/client software/authentication configuration, or insufficient rights/permissions), identify the cause of the problem.
41 Given a network troubleshooting scenario involving a wiring/infrastructure problem, identify the cause of the problem.
Security Pro Outline

- Videos: 139 (19:42:27)  
  Demonstrations: 117 (16:26:01)  
  Simulations: 74  
  Written Lessons: 122  
- Section Quizzes: 82  
  Practice Exams: 25  
  Exam Questions: 1037

CONTENTS:

1. 1.0 Introduction
   - 1.1 Security Overview
     - 1.1.1 Security Challenges (8:22)
     - 1.1.2 Security Roles and Concepts (5:36)
     - 1.1.3 Threat Agent Types (8:20)
     - 1.1.4 Security Introduction
     - 1.1.5 General Attack Strategy (8:51)
     - 1.1.6 General Defense Strategy (18:25)
     - 1.1.7 Attack and Defense Strategy Overview
     - 1.1.8 Practice Questions - Section 1.1 (12 questions)
   - 1.2 Using the Simulator
     - 1.2.1 Using the Simulator (13:19)
     - 1.2.2 Configure a Security Appliance
     - 1.2.3 Install a Security Appliance

2. 2.0 Access Control and Identity Management
   - 2.1 Access Control Models
     - 2.1.1 Access Control Models (3:38)
     - 2.1.2 Access Control Facts
     - 2.1.3 Access Control Model Facts
     - 2.1.4 Access Control Model Examples
     - 2.1.5 Implementing Discretionary Access Control (6:09)
     - 2.1.6 Practice Questions - Section 2.1 (15 questions)
   - 2.2 Authentication
     - 2.2.1 Authentication Part 1 (11:26)
     - 2.2.2 Authentication Part 2 (8:53)
     - 2.2.3 Authentication Facts
     - 2.2.4 Using a Biometric Scanner (3:49)
     - 2.2.5 Using Single Sign-on (12:20)
     - 2.2.6 Single Sign-on Facts
     - 2.2.7 Practice Questions - Section 2.2 (15 questions)
   - 2.3 Authorization
     - 2.3.1 Authorization (5:15)
     - 2.3.2 Cumulative Access (9:37)
     - 2.3.3 Authorization Facts
     - 2.3.4 Examining the Access Token (9:08)
     - 2.3.5 Practice Questions - Section 2.3 (4 questions)
   - 2.4 Access Control Best Practices
     - 2.4.1 Access Control Best Practices (3:12)
     - 2.4.2 Viewing Implicit Deny (10:13)
     - 2.4.3 Best Practices Facts
     - 2.4.4 Practice Questions - Section 2.4 (12 questions)
   - 2.5 Active Directory Overview
     - 2.5.1 Active Directory Introduction (9:04)
     - 2.5.2 Active Directory Structure (9:24)
     - 2.5.3 Viewing Active Directory (8:05)
     - 2.5.4 Active Directory Facts
2.5.5 Practice Questions - Section 2.5 (3 questions)

2.6 Windows Domain Users and Groups
- 2.6.1 Creating User Accounts (4:50)
- 2.6.2 Managing User Account Properties (7:45)
- 2.6.3 Create User Accounts
- 2.6.4 Manage User Accounts
- 2.6.5 Managing Groups (5:05)
- 2.6.6 Create a Group
- 2.6.7 Create Global Groups
- 2.6.8 User Account Management Facts
- 2.6.9 Practice Questions - Section 2.6 (5 questions)

2.7 Linux Users
- 2.7.1 Linux User and Group Overview (19:14)
- 2.7.2 Managing Linux Users (9:28)
- 2.7.3 Linux User Commands and Files
- 2.7.4 Create a User Account
- 2.7.5 Rename a User Account
- 2.7.6 Delete a User
- 2.7.7 Change Your Password
- 2.7.8 Change a User's Password
- 2.7.9 Lock and Unlock User Accounts
- 2.7.10 Practice Questions - Section 2.7 (7 questions)

2.8 Linux Groups
- 2.8.1 Managing Linux Groups (3:15)
- 2.8.2 Linux Group Commands
- 2.8.3 Rename and Create Groups
- 2.8.4 Add Users to a Group
- 2.8.5 Remove a User from a Group
- 2.8.6 Practice Questions - Section 2.8 (3 questions)

2.9 Linux User Security
- 2.9.1 Linux User Security and Restrictions (9:53)
- 2.9.2 Configuring Linux User Security and Restrictions (6:40)
- 2.9.3 Linux User Security and Restriction Facts
- 2.9.4 Practice Questions - Section 2.9 (5 questions)

2.10 Group Policy Overview
- 2.10.1 Group Policy Overview (8:41)
- 2.10.2 Viewing Group Policy (14:31)
- 2.10.3 Group Policy Facts
- 2.10.4 Create and Link a GPO
- 2.10.5 Practice Questions - Section 2.10 (3 questions)

2.11 Hardening Authentication
- 2.11.1 Hardening Authentication (19:31)
- 2.11.2 Configuring User Account Restrictions (9:30)
- 2.11.3 Configure User Account Restrictions
- 2.11.4 Configuring Account Policies and UAC Settings (14:18)
- 2.11.5 Configure Account Policies
- 2.11.6 Hardening User Accounts (10:20)
- 2.11.7 Restrict Local Accounts
- 2.11.8 Secure Default Accounts
- 2.11.9 Enforce User Account Control
- 2.11.10 Hardening Authentication Facts
- 2.11.11 Practice Questions - Section 2.11 (11 questions)
• 2.12 Hardening Authentication 2
  • 2.12.1 Configuring Smart Card Authentication (6:20)
  • 2.12.2 Configure Smart Card Authentication
  • 2.12.3 Smart Card Authentication Facts
  • 2.12.4 Using Fine-Grained Password Policies (7:00)
  • 2.12.5 Fine-Grained Password Policy Facts
  • 2.12.6 Create a Fine-Grained Password Policy
  • 2.12.7 Practice Questions - Section 2.12 (5 questions)

• 2.13 Remote Access
  • 2.13.1 Remote Access (8:43)
  • 2.13.2 Remote Access Facts
  • 2.13.3 RADIUS and TACACS+ (6:51)
  • 2.13.4 RADIUS and TACACS+ Facts
  • 2.13.5 Practice Questions - Section 2.13 (15 questions)

• 2.14 Network Authentication
  • 2.14.1 Network Authentication Protocols (14:09)
  • 2.14.2 Network Authentication via LDAP (10:30)
  • 2.14.3 Network Authentication Facts
  • 2.14.4 Controlling the Authentication Method (6:39)
  • 2.14.5 Configure Kerberos Policy Settings
  • 2.14.6 Browsing a Directory Tree via LDAP (6:38)
  • 2.14.7 Trusts and Transitive Access (5:33)
  • 2.14.8 Trusts and Transitive Access Facts
  • 2.14.9 Credential Management (10:06)
  • 2.14.10 Credential Management Facts
  • 2.14.11 Practice Questions - Section 2.14 (14 questions)

• 2.15 Identity Management
  • 2.15.1 Identity Management (16:31)
  • 2.15.2 Identity Management Facts
  • 2.15.3 Practice Questions - Section 2.15 (4 questions)

3. 3.0 Cryptography

• 3.1 Cryptography
  • 3.1.1 Cryptography Concepts (4:29)
  • 3.1.2 Cryptography Facts
  • 3.1.3 Cryptographic Attacks (17:47)
  • 3.1.4 Cryptographic Attack Facts
  • 3.1.5 Practice Questions - Section 3.1 (15 questions)

• 3.2 Hashing
  • 3.2.1 Hashing (11:31)
  • 3.2.2 Hashing Facts
  • 3.2.3 Using Hashes (7:43)
  • 3.2.4 Practice Questions - Section 3.2 (12 questions)

• 3.3 Symmetric Encryption
  • 3.3.1 Symmetric Encryption (5:27)
  • 3.3.2 HMAC (6:13)
  • 3.3.3 Symmetric Encryption Facts
  • 3.3.4 Cracking a Symmetric Encryption Key (4:11)
  • 3.3.5 Practice Questions - Section 3.3 (15 questions)

• 3.4 Asymmetric Encryption
  • 3.4.1 Asymmetric Encryption (8:66)
  • 3.4.2 Asymmetric Encryption Facts
  • 3.4.3 Practice Questions - Section 3.4 (12 questions)
• 3.5 Public Key Infrastructure (PKI)
  • 3.5.1 Certificates (11:02)
  • 3.5.2 Managing Certificates (14:45)
  • 3.5.3 Manage Certificates
  • 3.5.4 Certificate Lifecycle Facts
  • 3.5.5 CA Implementation (5:17)
  • 3.5.6 Configuring a Subordinate CA (14:13)
  • 3.5.7 PKI Management Facts
  • 3.5.8 Practice Questions - Section 3.5 (15 questions)

• 3.6 Cryptography Implementations
  • 3.6.1 Combining Cryptographic Methods (10:30)
  • 3.6.2 Hardware Based Encryption Devices (7:12)
  • 3.6.3 Cryptographic Implementation Facts
  • 3.6.4 Practice Questions - Section 3.6 (15 questions)

4. 4.0 Policies, Procedures, and Awareness

• 4.1 Security Policies
  • 4.1.1 Security Policies (7:23)
  • 4.1.2 Data Privacy Laws (9:42)
  • 4.1.3 Security Policy Facts
  • 4.1.4 Security Documentation Facts
  • 4.1.5 Security Management Facts
  • 4.1.6 Information Classification (5:40)
  • 4.1.7 Information Classification Facts
  • 4.1.8 Data Retention Policies (11:54)
  • 4.1.9 Wiping a Hard Drive (12:58)
  • 4.1.10 Data Retention Facts
  • 4.1.11 Practice Questions - Section 4.1 (15 questions)

• 4.2 Manageable Network Plan
  • 4.2.1 Manageable Network Plan (16:49)
  • 4.2.2 Manageable Network Plan 2 (14:05)
  • 4.2.3 Manageable Network Plan Facts
  • 4.2.4 Practice Questions - Section 4.2 (3 questions)

• 4.3 Business Continuity
  • 4.3.1 Business Continuity (2:39)
  • 4.3.2 Succession Planning (5:23)
  • 4.3.3 Business Continuity Facts
  • 4.3.4 Practice Questions - Section 4.3 (7 questions)

• 4.4 Risk Management
  • 4.4.1 Risk Management (4:04)
  • 4.4.2 Security Controls (3:21)
  • 4.4.3 Data Loss Prevention (DLP) (4:57)
  • 4.4.4 Risk Management Facts
  • 4.4.5 Practice Questions - Section 4.4 (15 questions)

• 4.5 Incident Response
  • 4.5.1 First Responder (7:17)
  • 4.5.2 Basic Forensic Procedures (18:31)
  • 4.5.3 Using Forensic Tools (6:17)
  • 4.5.4 Creating a Forensic Drive Image (10:00)
  • 4.5.5 Incident Response Facts
  • 4.5.6 Forensic Investigation Facts
  • 4.5.7 Practice Questions - Section 4.5 (15 questions)
• 4.6 Social Engineering
  • 4.6.1 Social Engineering (4:39)
  • 4.6.2 Phishing Variations (13:04)
  • 4.6.3 Social Engineering Facts
  • 4.6.4 Investigating a Social Engineering Attack (9:45)
  • 4.6.5 Respond to Social Engineering
  • 4.6.6 Practice Questions - Section 4.6 (15 questions)

• 4.7 Certification and Accreditation
  • 4.7.1 Trusted Computing (10:01)
  • 4.7.2 Certification and Accreditation (4:46)
  • 4.7.3 Certification and Accreditation Facts
  • 4.7.4 Practice Questions - Section 4.7 (12 questions)

• 4.8 Development
  • 4.8.1 System Development Life Cycle (8:40)
  • 4.8.2 System Development Life Cycle 2 (7:49)
  • 4.8.3 SDLC Facts
  • 4.8.4 Software Development Models
  • 4.8.5 Practice Questions - Section 4.8 (7 questions)

• 4.9 Employee Management
  • 4.9.1 Employment Practices (13:45)
  • 4.9.2 Employee Management Facts
  • 4.9.3 Employee Documents Facts
  • 4.9.4 Ethics Facts
  • 4.9.5 Practice Questions - Section 4.9 (15 questions)

• 4.10 Third-Party Integration
  • 4.10.1 Third-Party Integration Security Issues (11:24)
  • 4.10.2 Third-Party Integration Security Facts
  • 4.10.3 Practice Questions - Section 4.10 (4 questions)

5. 6.0 Physical Security
• 5.1 Physical Security
  • 5.1.1 Physical Security (18:39)
  • 5.1.2 Tailgating and Piggybacking (3:28)
  • 5.1.3 Physical Security Facts
  • 5.1.4 Implement Physical Security
  • 5.1.5 Practice Questions - Section 5.1 (15 questions)

• 5.2 Hardware Security
  • 5.2.1 Hardware Security Guidelines (7:50)
  • 5.2.2 Breaking into a System (7:30)
  • 5.2.3 Hardware Security Facts
  • 5.2.4 Practice Questions - Section 5.2 (4 questions)

• 5.3 Environmental Controls
  • 5.3.1 Environmental Controls (6:00)
  • 5.3.2 Environmental Monitoring (11:33)
  • 5.3.3 Hot and Cold Aisles (5:17)
  • 5.3.4 Environmental Control Facts
  • 5.3.5 Fire Protection Facts
  • 5.3.6 Practice Questions - Section 5.3 (11 questions)

• 5.4 Mobile Devices
  • 5.4.1 Mobile Device Security (7:33)
  • 5.4.2 Mobile Device Security Facts
  • 5.4.3 BYOD Security Issues (9:33)
  • 5.4.4 BYOD Security Facts
5.4.5 Securing Mobile Devices (10:20)
5.4.6 Secure an iPad
5.4.7 Practice Questions - Section 5.4 (8 questions)

- **5.5 Mobile Device Security Enforcement**
  - 5.5.1 Enforcing Security Policies on Mobile Devices (7:57)
  - 5.5.2 Enrolling Devices and Performing a Remote Wipe (8:49)
  - 5.5.3 Mobile Device Security Enforcement Facts
  - 5.5.4 Mobile Application Security (9:00)
  - 5.5.5 Mobile Application Security Facts
  - 5.5.6 Practice Questions - Section 5.5 (8 questions)

- **5.6 Telephony**
  - 5.6.1 Telephony (15:00)
  - 5.6.2 Telephony Security Facts
  - 5.6.3 Practice Questions - Section 5.6 (4 questions)

6. **6.0 Perimeter Defenses**

- **6.1 Network Layer Protocol Review**
  - 6.1.1 OSI Model (4:08)
  - 6.1.2 OSI Model Facts
  - 6.1.3 IP Addressing (17:22)
  - 6.1.4 IP Address Facts
  - 6.1.5 Configuring IPv6 (5:28)
  - 6.1.6 IP Subnetting (12:35)
  - 6.1.7 Configuring Subnetting (8:07)
  - 6.1.8 Subnetting Facts
  - 6.1.9 Practice Questions - Section 6.1 (9 questions)

- **6.2 Transport Layer Protocol Review**
  - 6.2.1 Network Protocols (4:45)
  - 6.2.2 Network Protocol Facts
  - 6.2.3 Analyzing a TCP Three-way Handshake (2:14)
  - 6.2.4 TCP and UDP Ports (9:02)
  - 6.2.5 Common Ports
  - 6.2.6 Practice Questions - Section 6.2 (15 questions)

- **6.3 Perimeter Attacks 1**
  - 6.3.1 Reconnaissance (2:40)
  - 6.3.2 Performing Reconnaissance (9:01)
  - 6.3.3 Reconnaissance Facts
  - 6.3.4 Denial of Service (DoS) (7:49)
  - 6.3.5 Xmas Tree Attacks (3:23)
  - 6.3.6 DoS Attack Facts
  - 6.3.7 Performing a UDP Flood Attack (3:54)
  - 6.3.8 Practice Questions - Section 6.3 (15 questions)

- **6.4 Perimeter Attacks 2**
  - 6.4.1 Session and Spoofing Attacks (6:41)
  - 6.4.2 Session Based Attack Facts
  - 6.4.3 Performing ARP Poisoning (4:24)
  - 6.4.4 Spoofing Facts
  - 6.4.5 DNS Attacks (4:30)
  - 6.4.6 DNS Attack Facts
  - 6.4.7 Examining DNS Attacks (13:29)
  - 6.4.8 Prevent Zone Transfers
  - 6.4.9 Practice Questions - Section 6.4 (15 questions)
6.5 Security Appliances
- 6.5.1 Security Solutions (4:02)
- 6.5.2 Security Zones (5:31)
- 6.5.3 Security Zone Facts
- 6.5.4 All-In-One Security Appliances (4:30)
- 6.5.5 Security Solution Facts
- 6.5.6 Configuring Network Security Appliance Access (6:55)
- 6.5.7 Configure Network Security Appliance Access
- 6.5.8 Practice Questions - Section 6.5 (4 questions)

6.6 Demilitarized Zones (DMZ)
- 6.6.1 Demilitarized Zones (9:49)
- 6.6.2 Configuring a DMZ (5:42)
- 6.6.3 Configure a DMZ
- 6.6.4 DMZ Facts
- 6.6.5 Practice Questions - Section 6.6 (8 questions)

6.7 Firewalls
- 6.7.1 Firewalls (5:33)
- 6.7.2 Firewall Facts
- 6.7.3 Configuring a Perimeter Firewall (9:47)
- 6.7.4 Configure a Perimeter Firewall
- 6.7.5 Practice Questions - Section 6.7 (15 questions)

6.8 Network Address Translation (NAT)
- 6.8.1 Network Address Translation (15:57)
- 6.8.2 Configuring NAT (5:11)
- 6.8.3 NAT Facts
- 6.8.4 Practice Questions - Section 6.8 (6 questions)

6.9 Virtual Private Networks (VPN)
- 6.9.1 Virtual Private Networks (VPNs) (10:16)
- 6.9.2 Configuring a VPN (4:25)
- 6.9.3 Configure a Remote Access VPN
- 6.9.4 Configure a VPN Connection iPad
- 6.9.5 VPN Facts
- 6.9.6 VPN Protocol Facts
- 6.9.7 Practice Questions - Section 6.9 (11 questions)

6.10 Web Threat Protection
- 6.10.1 Web Threat Protection (9:29)
- 6.10.2 Configuring Web Threat Protection (4:26)
- 6.10.3 Configure Web Threat Protection
- 6.10.4 Web Threat Protection Facts
- 6.10.5 Practice Questions - Section 6.10 (4 questions)

6.11 Network Access Control (NAC)
- 6.11.1 Network Access Protection (19:57)
- 6.11.2 Implementing NAP with DHCP Enforcement (15:56)
- 6.11.3 NAP Facts
- 6.11.4 Practice Questions - Section 6.11 (4 questions)

6.12 Wireless Overview
- 6.12.1 Wireless Networking Overview (5:35)
- 6.12.2 Wireless Antenna Types (8:03)
- 6.12.3 Wireless Networking Facts
- 6.12.4 Wireless Encryption (6:46)
- 6.12.5 Wireless Encryption Facts
- 6.12.6 Configuring a Wireless Connection (12:22)
6.12.7 Secure a Wireless Network
6.12.8 Practice Questions - Section 6.12 (15 questions)

6.13 Wireless Attacks
6.13.1 Wireless Attacks (13:28)
6.13.2 Wireless Attack Facts
6.13.3 Using Wireless Attack Tools (9:06)
6.13.4 Detecting Rogue Hosts (7:37)
6.13.5 Practice Questions - Section 6.13 (15 questions)

6.14 Wireless Defenses
6.14.2 Wireless Authentication (4:40)
6.14.3 Wireless Authentication Facts
6.14.4 Configuring a Wireless Access Point (19:54)
6.14.5 Obscure a Wireless Network
6.14.6 Configure a Wireless Profile
6.14.7 Configuring a Captive Portal (12:02)
6.14.9 Practice Questions - Section 6.14 (15 questions)

7. 7.0 Network Defenses
7.1 Network Devices
7.1.1 Network Devices (5:51)
7.1.2 Network Device Facts
7.1.3 Practice Questions - Section 7.1 (7 questions)

7.2 Network Device Vulnerabilities
7.2.1 Device Vulnerabilities (1:47)
7.2.2 Device Vulnerability Facts
7.2.3 Searching Defaultpasswords.com (1:23)
7.2.4 Securing a Switch (3:21)
7.2.5 Secure a Switch
7.2.6 Practice Questions - Section 7.2 (4 questions)

7.3 Switch Attacks
7.3.1 Switch Attacks (5:04)
7.3.2 Switch Attack Facts
7.3.3 Practice Questions - Section 7.3 (4 questions)

7.4 Router Security
7.4.1 Router Security (8:56)
7.4.2 Router Security Facts
7.4.3 Practice Questions - Section 7.4 (4 questions)

7.5 Switch Security
7.5.1 Switch Security (13:01)
7.5.2 Switch Loop Protection (10:46)
7.5.3 Switch Security Facts
7.5.4 Configuring VLANs from the CLI (4:32)
7.5.5 Explore VLANs from the CLI
7.5.6 Configuring VLANs (3:32)
7.5.7 Explore VLANs
7.5.8 Hardening a Switch (14:10)
7.5.9 Harden a Switch
7.5.10 Secure Access to a Switch
7.5.11 Secure Access to a Switch 2
7.5.12 Practice Questions - Section 7.5 (15 questions)
• 7.6 Intrusion Detection and Prevention
  • 7.6.1 Intrusion Detection (7:13)
  • 7.6.2 Detection vs. Prevention Controls (7:50)
  • 7.6.3 IDS Facts
  • 7.6.4 Implementing Intrusion Monitoring (3:33)
  • 7.6.5 Implementing Intrusion Prevention (7:51)
  • 7.6.6 Implement Intrusion Prevention
  • 7.6.7 Practice Questions - Section 7.6 (15 questions)

• 7.7 SAN Security
  • 7.7.1 SAN Security Issues (14:32)
  • 7.7.2 Configuring an iSCSI SAN (9:57)
  • 7.7.3 SAN Security Facts
  • 7.7.4 Practice Questions - Section 7.7 (5 questions)

8. 8.0 Host Defenses

• 8.1 Malware
  • 8.1.1 Malware (9:28)
  • 8.1.2 Malware Facts
  • 8.1.3 Malware Protection Facts
  • 8.1.4 Implementing Malware Protections (23:43)
  • 8.1.5 Using Windows Defender (14:22)
  • 8.1.6 Configure Windows Defender
  • 8.1.7 Practice Questions - Section 8.1 (15 questions)

• 8.2 Password Attacks
  • 8.2.1 Password Attacks (2:04)
  • 8.2.2 Password Attack Facts
  • 8.2.3 Using Rainbow Tables (4:48)
  • 8.2.4 Capturing Passwords (5:40)
  • 8.2.5 Practice Questions - Section 8.2 (4 questions)

• 8.3 Windows System Hardening
  • 8.3.1 Operating System Hardening (5:13)
  • 8.3.2 Hardening Facts
  • 8.3.3 Hardening an Operating System (6:41)
  • 8.3.4 Managing Automatic Updates (18:31)
  • 8.3.5 Configure Automatic Updates
  • 8.3.6 Configuring Windows Firewall (10:11)
  • 8.3.7 Configure Windows Firewall
  • 8.3.8 Configuring Windows Firewall Advanced Features (16:59)
  • 8.3.9 Configuring Parental Controls (18:21)
  • 8.3.10 Configure Parental Controls
  • 8.3.11 Practice Questions - Section 8.3 (10 questions)

• 8.4 Hardening Enforcement
  • 8.4.1 Hardening Enforcement with GPOs (1:50)
  • 8.4.2 Using Security Templates and Group Policy (6:53)
  • 8.4.3 Configuring GPOs to Enforce Security (15:24)
  • 8.4.4 Hardening Enforcement Facts
  • 8.4.5 Manage Services with Group Policy
  • 8.4.6 Practice Questions - Section 8.4 (4 questions)

• 8.5 File Server Security
  • 8.5.1 File Server Security (7:58)
  • 8.5.2 Scanning for Open Ports (3:52)
  • 8.5.3 File System Security Facts
  • 8.5.4 File Permission Facts
8.6 Linux Host Security
- 8.6.1 Linux Host Security (7:10)
- 8.6.2 Removing Unneeded Services and Scanning Ports (6:30)
- 8.6.3 Network Security Facts
- 8.6.4 Practice Questions - Section 8.6 (4 questions)

8.7 Static Environment Security
- 8.7.1 Security Risks in Static Environments (4:26)
- 8.7.2 Static Environment Security Facts
- 8.7.3 Practice Questions - Section 8.7 (3 questions)

9. 9.0 Application Defenses

9.1 Web Application Attacks
- 9.1.1 Web Application Attacks (2:49)
- 9.1.2 Cross-site Request Forgery (XSRF) Attack (10:51)
- 9.1.3 Injection Attacks (14:30)
- 9.1.4 Header Manipulation (9:01)
- 9.1.5 Zero Day Application Attacks (6:59)
- 9.1.6 Client Side Attacks (6:22)
- 9.1.7 Web Application Attack Facts
- 9.1.8 Preventing Cross-site Scripting (4:05)
- 9.1.9 Practice Questions - Section 9.1 (15 questions)

9.2 Internet Browsers
- 9.2.1 Managing Security Zones and Add-ons (20:26)
- 9.2.2 Configuring IE Enhanced Security (9:11)
- 9.2.3 Managing Cookies (12:38)
- 9.2.4 Configure Cookie Handling
- 9.2.5 Clearing the Browser Cache (9:28)
- 9.2.6 Clear the Browser Cache
- 9.2.7 Implementing Popup Blockers (7:26)
- 9.2.8 Configure IE Popup Blocker
- 9.2.9 Internet Explorer Security Facts
- 9.2.10 Enforcing IE Settings through GPO (12:47)
- 9.2.11 Enforce IE Settings through GPO
- 9.2.12 Configure IE Preferences in a GPO
- 9.2.13 Practice Questions - Section 9.2 (8 questions)

9.3 E-mail
- 9.3.1 E-mail Security (4:43)
- 9.3.2 E-mail Security Facts
- 9.3.3 Protecting a Client from Spam (10:29)
- 9.3.4 Securing an E-mail Server (2:45)
- 9.3.5 Configure E-mail Filters
- 9.3.6 Securing E-mail on iPad (5:52)
- 9.3.7 Secure E-mail on iPad
- 9.3.8 Practice Questions - Section 9.3 (8 questions)

9.4 Network Applications
- 9.4.1 Network Application Security (2:19)
- 9.4.2 Spim (3:43)
- 9.4.3 Using Peer-to-peer Software (3:04)
- 9.4.4 Securing Windows Messenger (2:48)
9.4.5 Configuring Application Control Software (9.05)
9.4.6 Network Application Facts
9.4.7 Practice Questions - Section 9.4 (5 questions)

9.5 Virtualization
9.5.1 Virtualization Introduction (4:01)
9.5.2 Virtualization Benefits (3:08)
9.5.3 Load Balancing with Virtualization (10:39)
9.5.4 Creating Virtual Machines (4.22)
9.5.5 Managing Virtual Machines (5.09)
9.5.6 Create Virtual Machines
9.5.7 Adding Virtual Network Adapters (1:30)
9.5.8 Creating Virtual Switches (3:26)
9.5.9 Create Virtual Switches
9.5.10 Virtualization Facts
9.5.11 Practice Questions - Section 9.5 (8 questions)

9.6 Application Development
9.6.1 Secure Coding Concepts (16:18)
9.6.2 Application Hardening (11:02)
9.6.3 Application Development Security Facts
9.6.4 Hardening Applications on Linux (4:26)
9.6.5 Implementing Application Whitelisting with AppLocker (13:03)
9.6.6 Implement Application Whitelisting with AppLocker
9.6.7 Implementing Data Execution Preventions (DEP) (4:01)
9.6.8 Implement Data Execution Preventions (DEP)
9.6.9 Hardening Applications Facts
9.6.10 NoSQL Security (5:18)
9.6.11 NoSQL Security Facts
9.6.12 Practice Questions - Section 9.6 (6 questions)

10.0 Data Defenses
10.1 Redundancy
10.1.1 Redundancy (4:55)
10.1.2 Redundancy Measurement Parameters (5:12)
10.1.3 Redundancy Facts
10.1.4 RAID (7:27)
10.1.5 Implementing RAID (6:16)
10.1.6 RAID Facts
10.1.7 Configure Fault Tolerant Volumes
10.1.8 Clustering (9:06)
10.1.9 Clustering Facts
10.1.10 Practice Questions - Section 10.1 (15 questions)

10.2 Backup and Restore
10.2.1 Backup and Restore (13:27)
10.2.2 Backup and Restore Facts
10.2.3 Backup Management Facts
10.2.4 Backing Up Workstations (6:18)
10.2.5 Back Up a Workstation
10.2.6 Restoring Workstation Data from Backup (2:19)
10.2.7 Backing Up a Domain Controller (2:33)
10.2.8 Back Up a Domain Controller
10.2.9 Restoring Server Data from Backup (2:12)
10.2.10 Practice Questions - Section 10.2 (15 questions)
10.3 File Encryption
- 10.3.1 Encrypting File System (EFS) (11:47)
- 10.3.2 Securing Files using EFS (11:45)
- 10.3.3 Encrypt Files with EFS
- 10.3.4 PGP and GPG (4:34)
- 10.3.5 Encrypting Files with GPG (4:58)
- 10.3.6 BitLocker and Database Encryption (13:02)
- 10.3.7 Configuring BitLocker (6:17)
- 10.3.8 Configure BitLocker with a TPM
- 10.3.9 File Encryption Facts
- 10.3.10 Practice Questions - Section 10.3 (8 questions)

10.4 Secure Protocols
- 10.4.1 Secure Protocols (8:44)
- 10.4.2 Secure Protocols 2 (15:26)
- 10.4.3 Secure Protocols Facts
- 10.4.4 Adding SSL to a Web Site (5:23)
- 10.4.5 Allow SSL Connections
- 10.4.6 IPSec (5:14)
- 10.4.7 IPSec Facts
- 10.4.8 Requiring IPSec for Communications (14:22)
- 10.4.9 Practice Questions - Section 10.4 (15 questions)

10.5 Cloud Computing
- 10.5.1 Cloud Computing Introduction (15:59)
- 10.5.2 Cloud Computing Security Issues (6:32)
- 10.5.3 Cloud Computing Facts
- 10.5.4 Practice Questions - Section 10.5 (5 questions)

11. 11.0 Assessments and Audits

11.1 Vulnerability Assessment
- 11.1.1 Vulnerability Assessment (4:54)
- 11.1.2 Vulnerability Assessment Facts
- 11.1.3 Scanning a Network with Nessus (18:26)
- 11.1.4 Scanning a Network with Retina (12:12)
- 11.1.5 Scanning for Vulnerabilities Using MBSA (6:02)
- 11.1.6 Review a Vulnerability Scan 1
- 11.1.7 Review a Vulnerability Scan 2
- 11.1.8 Review a Vulnerability Scan 3
- 11.1.9 Performing Port and Ping Scans (2:36)
- 11.1.10 Checking for Weak Passwords (9:21)
- 11.1.11 Practice Questions - Section 11.1 (14 questions)

11.2 Penetration Testing
- 11.2.1 Penetration Testing (2:32)
- 11.2.2 Penetration Testing Facts
- 11.2.3 Exploring Penetration Testing Tools (11:22)
- 11.2.4 Practice Questions - Section 11.2 (12 questions)

11.3 Protocol Analyzers
- 11.3.1 Protocol Analyzers (3:07)
- 11.3.2 Protocol Analyzer Facts
- 11.3.3 Analyzing Network Traffic (6:50)
- 11.3.4 Practice Questions - Section 11.3 (8 questions)

11.4 Log Management
- 11.4.1 Logs (3:24)
- 11.4.2 Log Facts
11.4.3 Logging Events with Event Viewer (3:52)
11.4.4 Windows Event Subscriptions (10:36)
11.4.5 Configuring Source-initiated Subscriptions (4:50)
11.4.6 Configuring Remote Logging on Linux (8:23)
11.4.7 Remote Logging Facts
11.4.8 Practice Questions - Section 11.4 (15 questions)

11.5 Audits
11.5.1 Audits (3:13)
11.5.2 Audit Facts
11.5.3 Auditing the Windows Security Log (11:41)
11.5.4 Configure Advanced Audit Policy
11.5.5 Auditing Device Logs (6:57)
11.5.6 Enable Device Logs
11.5.7 Practice Questions - Section 11.5 (7 questions)

12. Security Pro Practice Exams

• Preparing for Certification
  • Security Pro Exam Objectives
  • How to take the Certification Exam
  • Certification FAQs
  • Security Pro Domain 1: Access Control and Identity Management (22 simulation questions)
  • Security Pro Domain 2: Policies, Procedures, Awareness (1 simulation question)
  • Security Pro Domain 3: Physical Security (3 simulation questions)
  • Security Pro Domain 4: Perimeter Defenses (10 simulation questions)
  • Security Pro Domain 5: Network Defenses (7 simulation questions)
  • Security Pro Domain 6: Host Defenses (8 simulation questions)
  • Security Pro Domain 7: Application Defenses (10 simulation questions)
  • Security Pro Domain 8: Data Defenses (5 simulation questions)
  • Security Pro Domain 9: Audits and Assessments (5 simulation questions)
  • Security Pro Certification Practice Exam (15 simulation questions)

13. Security+ Practice Exams

• Preparing for Certification
  • Exam Objectives   Exam FAQs
  • How to Register for an Exam   Exam-taking Hints and Tips
  • Security+ Domain 1: Network Security, All Questions (172 questions)
  • Security+ Domain 2: Compliance and Operational Security, All Questions (128 questions)
  • Security+ Domain 3: Threats and Vulnerabilities, All Questions (178 questions)
  • Security+ Domain 4: Application, Data and Host Security, All Questions (70 questions)
  • Security+ Domain 5: Access Control and Identity Management, All Questions (98 questions)
  • Security+ Domain 6: Cryptography, All Questions (92 questions)
  • Security+ Certification Practice Exam (100 questions)

14. SSCP Practice Exams

• Preparing for Certification
  • Exam Objectives   Exam FAQs
  • SSCP Domain 1: Access Control, All Questions (60 questions)
  • SSCP Domain 2: Security Operations & Administration, All Questions (64 questions)
  • SSCP Domain 3: Monitoring and Analysis, All Questions (21 questions)
  • SSCP Domain 4: Risk, Response, and Recovery, All Questions (38 questions)
  • SSCP Domain 5: Cryptography, All Questions (90 questions)
  • SSCP Domain 6: Networks and Communications, All Questions (68 questions)
  • SSCP Domain 7: Malicious Code and Attacks, All Questions (85 questions)
  • SSCP Certification Practice Exam (125 questions)