Network Security Course

40 Hours

Course Description

Towson University’s Network Security course is an entry-level program that provides two key certifications—Network+ and Security+—into one program. These certifications are recognized worldwide in all IT-related industries and form the foundation of hiring requirements necessary to pursue a career in IT. Completion of this course prepares you to take the CompTIA Network+, and the CompTIA Security+ certification exams.

This course applies principles of computer networking and security including the OSI model, topologies, network devices, routing protocols, virtualization and wireless networking, auditing, firewalls, malware, cryptography, encryption, wireless security, social engineering and disaster recovery. Tools such as network simulation, virtualization, public key infrastructure, and anti-malware programs are used.

Pre-requisites

You must already have both A+ certifications or a college degree in IT to be eligible to take this course. If you have work experience, you may demonstrate your knowledge by passing a short exam that we can administer to you.

Course Objectives

Upon completion of this course, students will be able to:

- Evaluate the data communication process in a computer network
- Implement a DHCP & DNS server
- Analyze network addresses and subnets using both IPv4 and IPv6
- Construct a LAN using simulation software
- Administer user accounts and firewall
- Use encryption and malware
- Assess cloud services and security
- Formulate a business security policy and disaster recovery plan
# Course Outline

<table>
<thead>
<tr>
<th>WEEK</th>
<th>SUBJECT</th>
<th>ASSIGNMENT</th>
</tr>
</thead>
</table>
| 1    | Chapter 1 – Course Introduction  
Chapter 2 – The Open Systems Interconnection Specifications | 1: Introduction to Network Simulation Software |
|      | Chapter 7 – IP Addressing  
Chapter 3 – Networking Topologies and Cabling | 2: Making a LAN using Network Simulation Software |
| 2    | Chapter 4 – Current Ethernet Specification  
Chapter 5 – Networking Devices  
Chapter 6 – Internet Protocols | 3: Configure a DHCP Server and a DNS Server |
|      | Chapter 8 – IP Subnetting | 4: Calculate and Configure Subnets using Network Simulation Software |
| 3    | Chapter 9 – IP Routing  
Chapter 10 – Routing Protocols | 5: Configure Routing Protocols part 1 using Network Simulation Software  
6: Configure Routing Protocols part 2 using Network Simulation Software |
| 4    | Chapter 11 – Switching and Virtual LANS  
Chapter 12 – Wireless Networking | 7: Configure a Network Switch create VLANs using Network Simulation Software  
8: Configure a Wireless Network Using Network Simulation Software |
| 5    | Chapter 13 – Authentication and Access Control Virtualization  
Chapter 14 – Network Threats and Mitigation | 9: Create a Virtual Machine  
10: Configure User Accounts in Windows |
| 6    | Chapter 15 – Physical Security and Risk  
Chapter 16 – Wide Area Networks  
Chapter 17 – Troubleshooting Tools | 11: Configure the Windows Firewall  
12: Using command line FTP |
| 7    | Chapter 18 – Software and Hardware tools  
Chapter 19 – Network Troubleshooting  
Chapter 20 – Management, Monitoring, and Optimization | 13: Design a Troubleshooting Scenario Using Network Simulation Software |
|      | Midterm Exam |  |
| 8    | Chapter 1 – Measuring and Weighing Risks  
Chapter 2 – Monitoring and Diagnosing Networks  
Chapter 3 – Understanding Devices and Infrastructure | 14: Using Wireshark |
|      | Chapter 4 – Access Control, Authentication, and Authorization  
Chapter 5 – Protecting Wireless Networks | 15: Securing a Wireless Network Using Simulation Software |
<p>| 9    | Chapter 6 – Securing the Cloud | 16: Analyzing Host Security |</p>
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Chapter 8 – Cryptography</td>
<td>17: File Carving</td>
</tr>
<tr>
<td>11</td>
<td>Chapter 9 – Malware, Vulnerabilities, and Threats</td>
<td>18: Analyzing Password</td>
</tr>
<tr>
<td></td>
<td>Chapter 10 – Social Engineering and Other Foes</td>
<td>19: Using Public Key Infrastructure</td>
</tr>
<tr>
<td>12</td>
<td>Chapter 11 – Security Administration</td>
<td>20: Research Major Malware Incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21: The Social Engineering Toolkit</td>
</tr>
<tr>
<td>13</td>
<td>Chapter 12 – Disaster Recovery</td>
<td>22: Creating a Business Security Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23: Using Steganography</td>
</tr>
<tr>
<td>14</td>
<td>Choice Labs</td>
<td>24: Creating a Disaster Recovery Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>25: Using nmap</td>
</tr>
<tr>
<td>15</td>
<td>Review</td>
<td>26: Installation and use of Linux</td>
</tr>
<tr>
<td></td>
<td>Final Exam</td>
<td></td>
</tr>
</tbody>
</table>