D329 Network and Security – Applications

Assessments: CompTIA Security+ 3rd Party Objective Assessment
Average Completion Time: 8 weeks

Course Prerequisites

- D325 - Networks

Course Description

Network and Security – Applications: Prepares the learner for the CompTIA Security+ certification exam. The course introduces the learner to skills in identifying threats, attacks, and vulnerabilities to organizational security. The learner will also gain skills in designing security solutions for enterprise infrastructures and architectures, as well as in implementing security solutions across hardware, applications, and network services. The Learner will be able to execute operations and incident response with tools, policies, forensics, and mitigation techniques, and to analyze information security controls, governance, risk, and compliance.

Learning Objectives

- Identities, Threats, Attacks, and Vulnerabilities
- Designs Secure Architectures
- Implements Security Solutions
- Executes Operations and Incident Response
- Analyze Controls, Governance, Risk, and Compliance

Learning Resources

- CompTIA Learn
- CompTIA Labs
- CompTIA Practice
- Udemy
- Course Cohorts (review and register on the course page)

Student Course Page (WGU Portal)

- The WGU student portal course page has a lot of resources contained within it. Please review the following sections for more resources, information, and context related to the course.
    - ***Go to Course Materials:*** This button will take you to the course materials such as the e-textbook.
    - ***Explore Cohort Offerings:*** This button will allow the student to view the live cohort offerings and register for one or more cohorts that fit your schedule.

- ***Instructor information:*** This section will allow the student to review the assigned course instructor information, office hours, email, and appointment scheduling link. Each course has an instructor group mailbox this email box can be used to request assistance if the assigned instructor is out of the office: D329@wgu.edu
- ***Course Tips/Announcements:*** These buttons will allow the student to review any tips or announcements from the instructor team related to the course.
- ***Course Search:*** This button will allow the student to review all the articles and additional resources posted by the instructor team for the course (this includes recorded cohorts, study guides, and other long-term tips).
- ***Course Chatter:*** This section allows students to post tips and ask general questions. This is a forum and is moderated by the instructor team. Not all advice works for all students, so students should use caution if following advice from other students. Course instructors can answer questions in course chatter. However, some questions are better suited on a one-to-one basis with the student's instructor.

Course Schedule

Week	Theme/Topic	Learning Outcomes
1	Topic 1A: Compare and Contrast Information Security Roles Review Activity: Information Security Roles PBQ 1A: Compare and Contrast Security Control and Framework Types Topic 1B: Compare and Contrast Security Control and Framework Review Activity: Security Control and Framework PBQ 1B: Lesson 1: Practice Questions Assisted Lab: Exploring the lab environment. Topic 2A: Explain Threat Actor Types and Attack Vectors Review Activity: Threat Actor Types and Attack Vectors Topic 2B: Explain Threat Intelligence Sources Review Activity: Threat Intelligence Sources Lesson 2: Practice Questions Lesson 3A: Assess Organizational Security with Network Review Activity: Organizational Security with Network Reconnaissance Tools Assisted Lab: Exploring the Lab Environment Assisted Lab: Scanning and Identifying Network Nodes Assisted Lab: Scanning and Identifying Network Nodes Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools PBQ 3A: Assess Organizational Security with Network Reconnaissance Tools Topic 3B: Explain Security Concerns with General Vulnerability Types Review Activity: Security Concerns with General Vulnerability Types Topic 3C: Summarize Vulnerability Scanning Techniques Review Activity: Vulnerability Scanning Techniques Assisted Lab: analyzing the Results of a Credentialed Vulnerability Scan Topic 3D: Explain Penetration Testing Concepts Lesson 3: Practice Questions Assisted Lab: Scanning and Identifying Network Nodes Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan	Compare and Contrast Information Security Roles Explain Threat Actor Types and Attack Vectors Assess Organizational Security with Network Explain Security Concerns with General Vulnerability Types Summarize Vulnerability Scanning Techniques Explain Penetration Testing Concepts
2	Topic 4A: Compare and Contrast Social Engineering Techniques Review Activity: Social Engineering Techniques	Compare and Contrast Social Engineering Techniques

Week	Theme/Topic	Learning Outcomes
	PBQ 4A: Compare and Contrast Social Engineering Techniques Topic 4B: Analyze Indicators of Malware-Based Attacks Review Activity: Indicators of Malware-Based Attacks PBQ4B: Analyze Indicators of Malware-Based Attacks Assisted Lab: Installing, Using, and Blocking a Malware-Based Backdoor Applied Lab: Performing Network Reconnaissance and Vulnerability Scanning Lesson 4: Practice Questions Applied Lab: Performing Network Reconnaissance and Vulnerability Scanning Topic 5A: Compare and Contrast Cryptographic Ciphers Review Activity: Cryptographic Ciphers Topic 5B: Summarize Cryptographic Modes of Operation Review Activity: Cryptographic Modes of Operation PBQ 5B: Summarize Cryptographic Modes of Operation Topic 5C: Summarize Cryptographic Use Cases and Weaknesses Review Activity: Summarize Cryptographic Use Cases and Weaknesses Topic 5D: Summarize Other Cryptographic Technologies Review Activity: Other Cryptographic Technologies Lesson 5: Practice Questions Topic 6A: Implement Certificates and Certificate Authorities Review Activity: Certificates and Certificate Authorities PBQ 6A: Implement Certificates and Certificate Authorities Assisted Lab: Managing the Life Cycle of a Certificate Topic 6B: Implement PKI Management Review Activity: PKI Management Assisted Lab: Managing the Lifecycle of a Certificate Assisted Lab: Managing Certificates with OpenSSL Lesson 6: Practice Questions	Analyze Indicators of Malware-Based Attacks Compare and Contrast Cryptographic Ciphers Summarize Cryptographic Modes of Operation Summarize Cryptographic Use Cases and Weaknesses Summarize Other Cryptographic Technologies Implement Certificates and Certificate Authorities Implement PKI Management
3	Topic 7A: Summarize Authentication Design Concepts Review Activity: Authentication Design Concepts Topic 7B: Implement Knowledge-Based Authentication Review Activity: Knowledge-Based Authentication	Summarize Authentication Design Concepts Implement Knowledge-Based

Week	Theme/Topic	Learning Outcomes
	PBQ 7B: Implement Knowledge-Based Authentication Assisted Lab: Auditing Passwords with a Password Cracking Utility Topic 7C: implement Authentication Technologies Review Activity: Authentication Technologies Assisted Lab: Managing Centralized Authentication Topic 7D: Summarize Biometrics Authentication Concepts Review Activity: Biometrics Authentication Concepts Lesson 7 Practice Questions Assisted Lab: Auditing Passwords with a Password Cracking Utility Assisted Lab: Managing Centralized Authentication Topic 8A: Implement Identity and Account Types Review Activity: Identity and Account Types Topic 8B: Implement Account Policies Review Activity: Account Policies PBQ 8B: Implement Account Policies Assisted Lab: Configuring a System for Auditing Policies Topic 8C: Implement Authorization Solutions Review Activity: Authorization Solutions Assisted Lab: Managing Access Controls in Linux Topic 8D: Explain the Importance of Personnel Policies Review Activity: Importance of Personnel Policies Lesson 8: Practice Questions Lesson 8 PBQ: Implement Identity, Account Types, and Account Policies Assisted Lab: Managing Access Controls in Windows Server Assisted Lab: Configuring a System for Auditing Policies Assisted Lab: Managing Access Controls in Linux Applied Lab: Configuring Identity and Access Management Controls Topic 9A: Implement Secure Network Designs Review Activity: Secure Network Designs Topic 9B: Implement Secure Switching and Routing Review Activity: Secure Switching and Routing PBQ 9B: Implement Secure Switching and Routing	Authentication Implement Authentication Technologies Summarize Biometrics Authentication Concepts Implement Identity and Account Types Implement Account Policies Implement Authorization Solutions Explain the Importance of Personnel Policies Implement Secure Network Designs Implement Secure Switching and Routing Implement Secure Wireless Infrastructure Implement Load Balancers

Week	Theme/Topic	Learning Outcomes
	Review Activity: Secure Switching and Routing PBQ 9B: Implement Secure Switching and Routing Assisted Lab: Implementing a Secure Network Design Topic 9C: Implement Secure Wireless Infrastructure Review Activity: Secure Wireless Infrastructure PBQ 9C: Implement Secure Wireless Infrastructure Topic 9D: Implement Load Balancers Review Activity: Load Balancers Lesson 9: Practice Questions Assisted Lab: Implementing a Secure Network Design	
4	Topic 10A: Implement Firewalls and Proxy Servers Review Activity Firewalls and Proxy Servers PBQ 10A: Implement Firewalls and Proxy Servers Assisted Lab: Configuring a Firewall Topic 10B: Implement Network Security Monitoring Review Activity: Network Security Monitoring Assisted Lab: Configuring and Intrusion Detection System Topic 10C: Summarize the Use of SIEM Review Activity: Use of SIEM Lesson 10: Practice Questions Assisted Lab: Configuring a Firewall Assisted Lab: Configuring an Intrusion Detection System Topic 11A: Implement Secure Network Operations Protocols Review Activity: Secure Network Operations Protocols Assisted Lab: Implementing Secure Network Addressing Protocols Topic 11B: Implement Secure Application Protocols Review Activity: Secure Application Protocols PBQ 11B: Implement Secure Application Protocols Topic 11C: Implement Secure Remote Access Protocols Review Activity: Secure Remote Access Protocols PBQ 11C: Implement Secure Remote Access Protocols Assisted Lab: Implementing a Virtual Private Network	Implement Firewalls and Proxy Servers Implement Network Security Monitoring Summarize the Use of SIEM Implement Secure Network Operations Protocols Implement Secure Application Protocols Implement Secure Remote Access Protocols Implement Secure Firmware Implement Endpoint Security Explain Embedded System Security

Week	Theme/Topic	Learning Outcomes
	Assisted Lab: Implementing a secure SSH server Lesson 11: Practice Questions Assisted Lab: Implementing Secure Network Addressing Services Assisted Lab: Implementing a Virtual Private Network Assisted Lab: Implementing a Secure SSH Server Topic 12A: Implement Secure Firmware Review Activity: Secure Firmware Topic 12B: Implement Endpoint Security Review Activity: Endpoint Security Assisted Lab: Implementing Endpoint Protection Topic 12C: Explain Embedded System Security Implications Review Activity: Embedded System Security Implications Lesson 12: Practice Questions Assisted Lab: Implementing Endpoint Protection Applied Lab: Securing the Network Infrastructure	Implications
5	Topic 13A: Implement Mobile Device Management Review Activity: Mobile Device Management PBQ 13A: Implement Mobile Device Management Topic 13B: Implement Secure Mobile Device Connections Review Activity: secure Mobile Device Connections Lesson 13: Practice Questions Topic 14A: Analyze Indicators of Application Attacks Review Activity: Indicators of Application Attacks Assisted Lab: Identifying Application Attack Indicators Topic 14B: Analyze Indicators of Web Application Attacks Review Activity: Indicators of Web Application Attacks Assisted Lab: Identifying a Browser Attack Topic 14C: Summarize Secure Coding Practices Review Activity: Secure Coding Practices Topic 14D: Implement secure Script Environments Assisted Lab: Implementing PowerShell Security	Implement Mobile Device Management Implement Secure Mobile Device Connections Analyze Indicators of Application Attacks Analyze Indicators of Web Application Attacks Summarize Secure Coding Practices Implement secure Script

Week	Theme/Topic	Learning Outcomes
	Assisted Lab: Identifying Malicious Code Topic 14E: Summarize Deployment and Automation Concepts Review Activity: Deployment and Automation Concepts Lesson 14: Practice Questions Assisted Lab: Identifying Application Attack Indicators Assisted Lab: Identifying a Browser Attack Assisted Lab: Implementing PowerShell Security Assisted Lab: Identifying Malicious Code Applied Lab: Identifying Application Attacks Topic 15A: Summarize Secure Cloud and Virtualization Services Review Activity: Secure Cloud and Virtualization Services PBQ 15B Apply Cloud Security Solutions Topic 15B: Apply Cloud Security Solutions Review Activity: Cloud Security Solutions Topic 15C: Summarize Infrastructure as Code Concepts Review Activity: Infrastructure as a Code Lesson 15: Practice Questions	Environments Summarize Deployment and Automation Concepts Summarize Secure Cloud and Virtualization Services Apply Cloud Security Solutions Summarize Infrastructure as Code Concepts
6	Topic 16A: Explain Privacy and Data Sensitivity Concepts Review Activity: Privacy and Data Sensitivity Concepts PBQ 16A: Explain Privacy and Data Protection Controls Review Activity: Privacy and Data Protection Controls Lesson 16: Practice Questions Applied Lab: Identifying Application Attacks Topic 17A: Summarize Incident Response Procedures Review Activity: Incident Response Procedures PBQ 17A: Summarize Incident Response Procedures Topic 17B: Utilize Appropriate Data Sources for Incident Response Assisted Lab: Managing Data Sources for Incident Response Topic 17C: Apply Mitigation Controls Review Activity: Mitigation Controls Assisted Lab: Managing Data Sources for Incident Response Assisted Lab: Configuring Mitigation Controls	Explain Privacy and Data Sensitivity Concepts Summarize Incident Response Procedures Utilize Appropriate Data Sources for Incident Response Apply Mitigation Controls Explain Key Aspects of Digital Forensics Documentation

Week	Theme/Topic	Learning Outcomes
	Lesson 17: Practice Questions Topic 18A: Explain Key Aspects of Digital Forensics Documentation Review Activity: Explain Key Aspects of Digital Forensics Documentation Review Activity: Digital Forensics Documentation Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition Review Activity: Digital Forensics Evidence Acquisition Assisted Lab: Acquiring Digital Forensics Evidence Lesson 18: Practice Questions	Explain Key Aspects of Digital Forensics Evidence Acquisition
7	Topic 19A: Explain Risk Management Processes and Concepts Review Activity: Risk Management Processes and Concepts PBQ 19A: Explain Risk Management Processes and Concepts Topic 19B: Explain Business Impact Analysis Concepts Review Activity: Business Impact Analysis Concepts Lesson 19: Practice questions Topic 20A: Implement Redundancy Strategies Review Activity: Redundancy Strategies PBQ 20A: Implement Redundancy Strategies Topic 20B: Implement Backup Strategies Review Activity: Backup Strategies Topic 20C: Implement Cybersecurity Resiliency Strategies Review Activity: Cybersecurity Resiliency Strategies Assisted Lab: Backing Up and Restoring Data in Windows and Linux Applied Lab: Managing Incident Response, Mitigation, and Recovery Lesson 20: Practice Questions Topic 21A: Explain the Importance of Physical Site Security Controls Review Activity: Physical Site Security Controls Topic 21B: Explain the Importance of Physical Host Security Controls Review Activity: Physical Host Security Controls Lesson 21: Practice Question Applied Lab: Managing Incident Response, Mitigation, and Recover	Explain Risk Management Processes and Concepts Explain Business Impact Analysis Concepts Implement Redundancy Strategies Implement Backup Strategies Implement Cybersecurity Resiliency Strategies Explain the Importance of Physical Site Security Controls Explain the Importance of Physical Host Security Controls

Week	Theme/Topic	Learning Outcomes
8	Final Assessment: review gaps and take the Security + Exam	Final Assessment, Certification Exam