CCRI CCNA Network Security CNVT-2200 Fall 2022

Instructor	John Mowry
Telephone	401-825-2138
E-mail	jmowry@ccri.edu
Office Hours	See Office Door KN2126
Class Sections	102 Monday & Wednesday 6:00 PM-8:50 PM, starts 8/31, ends 12/21

Instructional Material and Web Sites

1	CCRI Lesson Web Site	www.netacad.com (Network Security 1.0)
3	Cisco Academy Assessment Web Site	https://www.netacad.com

Grading Policies

Skills:	
Journal-Entries	5% Due December 12, 2022 @ 6:00 PM
Labs and Class Participation	10%
Research Paper	10% Due December 7, 2022 @ 6:00 PM
Practical Final	40%
Academic:	
Quizzes	10%
Final	25%

Mission of the Computer Science Department:

The mission of the Computer Studies and Information Processing Department at the Community College of Rhode Island is to provide high quality education in the areas of computer science and information technology to a diverse student population. We offer programs of study that provide our students with the skills necessary for transfer, career success, and lifelong learning. With programs in: Cybersecurity, Computer Support Specialist, Networking Technology, Computer Programming, and Web Technologies we offer a variety of options in the fields of computer science and information technology.

Course Description:

The Security course provides a next step for individuals who want to enhance their networking skill set to help meet the growing demand for network security professionals. Course introduces the core security concepts and skills needed for the installation, troubleshooting, and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices.

Course Objectives:

As a result of this course, a student will be able to:

- Describe security threats facing modern network infrastructures, explain network mitigation techniques, and the basics of securing a network
- Secure administrative access to network devices and implement secure network management and reporting
- Implement Authentication, Authorization and Accounting (AAA) on network devices

- Mitigate threats to networks using ACLs and firewall technologies to secure the network perimeter
- Implement intrusion detection and prevention, configure Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) to mitigate attacks on the network
- Describe methods for implementing data confidentiality and integrity

Time Management

1. Course will meet for two (2) Lecture Hours and, two (2) laboratory hours per week of instruction. Based on a 15-week schedule. Shorter courses will meet respective to the number of class meetings
2. Course will meet for sixty (60) hours of combined instruction and laboratory exercises.
3. Students are expected to spend an equal amount of time (60 hours) in reading the curriculum, and studying related material in addition to the required lecture/laboratory.
4. All Packet Tracer lab activities are to be completed as homework assignments

Journal-Entries:

The Journal is your **Notebook.** The Notebook is to be Hand-Written and presented to your instructor on the date specified. The Notebook must have your name clearly printed on the front cover, either inside or outside, or if using a binder on the first page.

Practical Exam

1. The practical exam will encompass a majority of concepts and procedures developed during the laboratory experiments and required readings.
2. The practical exam will be totally "hands-on" including routing and switching equipment as well as security equipment and programs related to a secure network environment.
3. Absolutely no electronic devices are allowed during the exam, including USB's, mobile phones or any other media.
4. **Hand-Written** notes will be allowed for use during the Practical Exam only.

Examinations

1. All exams, excluding the practical exam, will be a combination of multiple choice, fill-in the blank, matching as well as simulations.

Other Policies

1. The student expected to complete the On-Line lessons outside of class time.
2. Late assignments, including labs, will be penalized 10%.
3. All assignments must be completed using a word processor.
4. Students are responsible to see the instructor about any work missed due to absence.
5. Students who miss a quiz must take the quiz within two classes of the original quiz date.
6. Students are expected to participate as a member of teams
7. Students must pass both the Skills based portion in addition to the Academic portion of the curriculum to pass the course.
8. Student's final grade can only raise one letter grade above the on-line final exam score based on other class assignments.
9. Students are allowed a **maximum** of three (3) re-takes of chapter quizzes per the semester.
10. All re-takes must be completed **prior** to the final exam, **without exception**.
11. Department policy is that if you miss the equivalent of two (2) weeks of classes your final grade will drop by one (1) letter grade.

Research Paper

You are the Emergency Management Director of a small island nation. Your nation has come under Cyber-attack and the attackers have made non-functional the Communications system (Phone, Internet, and Cellular), Water supply, Electrical, Natural Gas, and Waste Treatment. Your staff assures you that each system can be recovered but will take an undetermined time period. You must decide what system should be made operational first with the limited staff available to you.

In your paper, explain what system you would bring back first and your reasoning behind making your decision. Take into account possible outcomes from your choice.

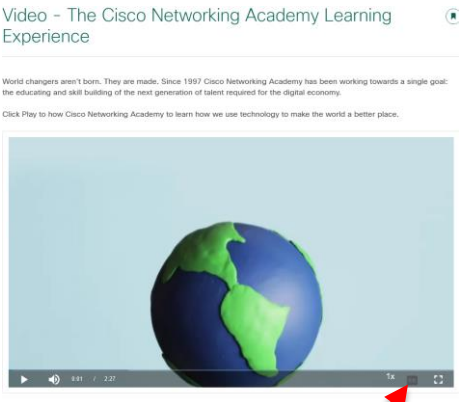
As a research paper, all sources of information must be properly footnoted and identified. The paper will be delivered as a Word document, single-sided, include a cover page, and using a 12pt font. Your findings will be presented during a class meeting and your justification for decisions will be questioned and discussed.

Services for Students with Disabilities:

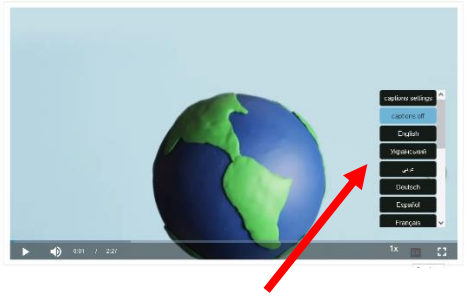
Any student with a documented disability may arrange reasonable accommodations. As part of this process, students are encouraged to contact the office of Disability Services for Students as early in the semester as possible (http://www.ccri.edu/dss/index.shtml).

Enabling Closed Caption:

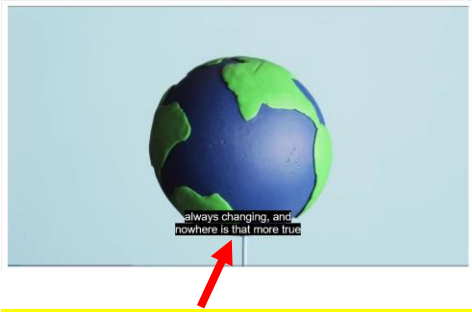
All embedded videos on the Cisco Academy website have the ability to display closed captioning in multiple languages. The procedure to enable this feature is as follows;



Closed Caption Option



When selected the user can choose what language they would like to see displayed from available languages.



After selecting "English" the appropriate text is now displayed. ***This needs to be done for each embedded video individually.***

Chapter Exam Topics:

LI	Chapter/Section/Topic Titles	Items
1	**Explain network security.**	**5**
1.1	Describe the current network security landscape.	
1.2	Describe how all types of networks need to be protected.	
2	**Explain the various types of threats and attacks.**	**6**
2.1	Explain how network threats have evolved.	
2.2	Describe the various types of attack tools used by threat actors.	
2.3	Describe types of malware.	
2.4	Explain reconnaissance, access, and social engineering network attacks.	
2.5	Explain Denial of Service, buffer overflow, and evasion attacks.	
3	**Explain tools and procedures to mitigate the effects of malware and common network attacks.**	**4**
3.1	Describe methods and resources to protect the network.	
3.2	Explain several types of network security policies.	
3.3	Explain the purpose of security platforms.	
3.4	Describe the techniques used to mitigate common network attacks.	
3.5	Explain how to secure the three functional areas of Cisco routers and switches.	
4	**Configure secure administrative access.**	**6**
4.1	Explain how to secure a network perimeter.	
4.2	Use the correct commands to configure passwords on a Cisco IOS device.	
4.3	Use the correct commands to configure enhanced security for virtual logins.	
4.4	Configure an SSH daemon for secure remote management.	
Modules 1-4: Securing Networks Group Exam		**21**
5	**Configure command authorization using privilege levels and role-based CLI.**	**7**
5.1	Use the correct commands to configure administrative privilege levels to control command availability.	
5.2	Use the correct commands to configure role-based CLI access to control command availability.	
6	**Implement the secure management and monitoring of network devices.**	**7**
6.1	Explain how the Cisco IOS resilient configuration feature and Secure Copy are used to secure the Cisco IOS image and configuration files.	
6.2	Use the correct commands for AutoSecure to enable security on IOS-based routers.	
6.3	Use the correct command to configure routing protocol authentication.	
6.4	Compare in-band and out-of-band management access.	
6.5	Explain how to configure syslog to log system events.	

6.6	Configure NTP to enable accurate timestamping between all devices.	
6.7	Configure SNMP to monitor system status.	
7	**Configure AAA to secure a network.**	**7**
7.1	Describe the characteristics of AAA	
7.2	Configure AAA authentication to validate users against a local database.	
7.3	Describe the server-based AAA protocols.	
7.4	Configure server-based AAA authentication on Cisco routers.	
7.5	Use the correct commands to configure server-based AAA authorization and accounting.	
Modules 5-7: Monitoring and Managing Devices Group Exam		**21**
8	**Implement access control lists (ACLs) to filter traffic and mitigate network attacks.**	**7**
8.1	Describe standard and extended IPv4 ACLs.	
8.2	Explain how ACLs use wildcard masks.	
8.3	Explain how to configure ACLs.	
8.4	Use sequence numbers to edit existing standard IPv4 ACLs.	
8.5	Implement ACLs.	
8.6	Use ACLs to mitigate common network attacks.	
8.7	Configure IPv6 ACLs using CLI.	
9	**Explain how firewalls are implemented to provide network security.**	**7**
9.1	Explain how firewalls are used to help secure networks.	
9.2	Explain design considerations for implementing firewall technologies	
10	**Implement Zone-Based Policy Firewall using CLI.**	**7**
10.1	Explain how Zone-Based Policy Firewalls are used to help secure a network.	
10.2	Explain the operation of a Zone-Based Policy Firewall.	
10.3	Configure a Zone-Based Policy Firewall with CLI.	
Modules 8-10: ACLs and Firewalls Group Exam		**21**
11	**Explain how network-based Intrusion Prevention Systems are used to help secure a network.**	**10**
11.1	Explain the functions and operations of IDS and IPS systems.	
11.2	Explain how network-based IPS is implemented.	
11.3	Describe the IPS technologies that are available on Cisco ISR routers.	
11.4	Configure Cisco SPAN.	
12	**Explain how signatures are used to detect malicious network traffic.**	**10**
12.1	Describe IPS signatures.	
12.2	Explain how the Cisco Snort IPS provides network security services.	

12.3	Explain how to configure Snort IPS on a Cisco ISR G2.	
Modules 11-12: Intrusion Prevention Group Exam		**20**
13	**Explain endpoint vulnerabilities and protection methods.**	**10**
13.1	Describe endpoint security and the enabling technologies.	
13.2	Explain the functions of 802.1x components.	
14	**Implement security measures to mitigate Layer 2 attacks.**	**10**
14.1	Describe Layer 2 vulnerabilities.	
14.2	Describe MAC address spoofing attacks.	
14.3	Configure port security.	
14.4	Explain how to mitigate VLAN attacks.	
14.5	Use correct command to implement DHCP Snooping for attack mitigation.	
14.6	Use correct command to mitigate ARP attacks.	
14.7	Use the correct command to mitigate address spoofing attacks.	
14.8	Explain the operation of Spanning Tree Protocol.	
14.9	Configure security measures to mitigate STP attacks.	
Modules 13-14: Layer 2 and Endpoint Security Group Exam		**20**
15	**Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.**	**7**
15.1	Explain the requirements of secure communications including integrity, authentication, and confidentiality.	
15.2	Describe cryptography.	
15.3	Describe cyrptoanalysis.	
15.4	Describe cyrptology.	
16	**Explain how cryptography is used to ensure data integrity and authenticity.**	**7**
16.1	Explain the role of cryptography in ensuring the integrity and authenticity of data.	
16.2	Describe the components of key management.	
16.3	Explain how cryptographic approaches enhance data confidentiality.	
17	**Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication.**	**7**
17.1	Explain public key cryptography.	
17.2	Explain how the public key infrastructure functions.	
17.3	Explain how the use of cryptography affects cybersecurity operations.	
Modules 15-17: Cryptography Group Exam		**21**
18	**Explain the purpose of VPNs.**	**10**
18.1	Describe VPNs and their benefits.	
18.2	Compare site-to-site and remote-access VPNs.	
18.3	Describe the IPsec protocol and its basic functions.	
18.4	Compare AH and ESP protocols.	

18.5	Describe the IKE protocol.	
19	**Configure a site-to-site IPsec VPN, with pre-shared key authentication, using CLI.**	**10**
19.1	Describe IPsec negotiation and the five steps of IPsec configuration.	
19.2	Use the correct commands to configure an ISAKMP policy.	
19.3	Use the correct commands to configure the IPsec policy.	
19.4	Use the correct commands to configure and apply a Cryptomap.	
19.5	Configure an Ipsec VPN.	
Modules 18-19: VPNs Group Exam		**20**
20	**Explain how the ASA operates as an advanced stateful firewall.**	**7**
20.1	Compare ASA solutions to other routing firewall technologies.	
20.2	Describe three ASA deployment scenarios.	
21	**Implement an ASA firewall configuration.**	**6**
21.1	Explain how to configure an ASA-5506-X with FirePOWER Services.	
21.2	Configure management settings and services on a ASA 5506-X firewall.	
21.3	Explain how to configure object groups on an ASA.	
21.4	Use the correct commands to configure access lists with object groups on an ASA.	
21.5	Use the correct commands to configure an ASA to provide NAT services.	
21.6	Use the correct commands to configure access control using the local database and AAA server.	
21.7	Configure service policies on an ASA.	
22	**Describe the various techniques and tools used for network security testing.**	**7**
22.1	Describe the techniques used in network security testing.	
22.2	Describe the tools used in network security testing	
Modules 20-22: ASA Group Exam		**20**

Final Exam Subjects:

Module	Chapter/Section/Topic Titles	Items
1	Explain network security.	2
2	Explain the various types of threats and attacks.	2
3	Explain tools and procedures to mitigate the effects of malware and common network attacks.	2
4	Configure secure administrative access.	2
5	Configure command authorization using privilege levels and role-based CLI.	2
6	Implement the secure management and monitoring of network devices.	3
7	Configure AAA to secure a network.	3

8	Implement access control lists (ACLs) to filter traffic and mitigate network attacks.	3
9	Explain how firewalls are implemented to provide network security.	3
10	Implement Zone-Based Policy Firewall using CLI.	3
11	Explain how network-based Intrusion Prevention Systems are used to help secure a network.	3
12	Explain how signatures are used to detect malicious network traffic.	3
13	Explain endpoint vulnerabilities and protection methods.	3
14	Implement security measures to mitigate Layer 2 attacks.	3
15	Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.	3
16	Explain how cryptography is used to ensure data integrity and authenticity.	3
17	Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication.	3
18	Explain the purpose of VPNs.	3
19	Configure a site-to-site IPsec VPN, with pre-shared key authentication, using CLI.	3
20	Explain how the ASA operates as an advanced stateful firewall.	2
21	Implement an ASA firewall configuration.	3
22	Describe the various techniques and tools used for network security testing.	3
Final Exam		**60**

Network Security 1.0

Class	Lesson	Module Group Exam	Subjects	Labs/Projects
Aug 31	1 & 2		**Module 1:** Securing Networks **Module 2:** Network Threats	**Video 1.1.5:** Anatomy of an Attack **Video 2.4.3:** Reconnaissance Attacks **Animation 2.3.6:** Worm Components **Animation 2.4.2:** Reconnaissance Attacks **Animation 2.4.4:** Access Attacks **Video 2.4.5:** Access and Social Engineering Attacks **Video 2.5.1:** Denial of Service Attacks **Video 2.5.4:** Mirai Botnet
Aug 31			**Laboratory Exercises**	**Lab 2.4.8:** Social Engineering
Sept 7	3 & 4		**Module 3:** Mitigating Threats **Module 4:** Secure Device Access	**Video 3.3.4:** Cisco SecureX Demonstration **Video 4.3.6:** Configure Passwords and Enhanced Login Security **Video 4.4.1:** The Need for SSH
Sept 12			**Laboratory Exercises**	**Lab 4.4.7:** Configure Network Devices with SSH **Lab 4.4.9:** Configure Network Devices
Sept 14		1 (1-4)	**Module 5:** Assigning Administrative Roles **Module 6:** Device Monitoring and Management Labs Due September 20, 2022 @ Midnight	**Animation 5.2.2:** Role-Based Views **Animation 6.3.2:** Routing Protocol Spoofing **Lab 6.6.4:** Packet Tracer - Configure and Verify NTP **Lab 6.7.12:** Packet Tracer - Configure Cisco Devices for Syslog, NTP, and SSH Operations
Sept 19			**Laboratory Exercises**	**Lab 5.2.5:** Configure Network Devices with SSH **Lab 6.2.7:** Configure Automated Security Features **Lab 6.3.6:** Basic Device Configuration and OSPF Authentication
Sept 21	7 & 8		**Module 7:** Authentication, Authorization, and Accounting (AAA) **Module 8:** Access Control Lists Labs Due September 27, 2022 @ Midnight	**Animation 7.3.4:** Process for TACACS+ Authentication **Animation 7.3.5:** Process for RADIUS Authentication **Video 7.4.6:** Configure a Cisco Router to Access a AAA RADIUS Server **Interactive Activity 8.5.9:** Configuring Standard ACLs **Interactive Activity 8.5.10:** Creating an Extended ACL Statement **Lab 7.2.6:** Packet Tracer - Configure Local AAA for Console and VTY Access **Lab 8.6.5:** Packet Tracer - Configure IP ACLs to Mitigate Attacks **Lab 8.7.4:** Packet Tracer - Configure IPv6 ACLs
Sept 26			**Laboratory Exercises**	**Lab 7.4.7:** Install the Virtual Machine **Lab 7.4.8:** Configure Server-Based Authentication with RADIUS

Class	Lesson	Module Group Exam	Subjects	Labs/Projects
Sept 28	9 & 10	2 (5-7)	**Module 9:** Firewall Technologies **Module 10:** Zone-Based Policy Firewalls Labs Due October 4, 2022 @ Midnight	**Animation 9.1.1:** Firewalls **Video 10.3.10:** Video Demonstration of ZPF **Lab 9.2.4:** Packet Tracer - Identify Packet Flow
Oct 3			**Laboratory Exercises**	**Lab 10.3.12:** Configure ZPFs
Oct 5	11 & 12	3 (8-10)	**Module 11:** IPS Technologies **Module 12:** IPS Operation and Implementation Labs Due October 11, 2022 @ Midnight	**Lab 11.4.6:** Packet Tracer - Implementing a Local SPAN
Oct 12	13 & 14	4 (11-12)	**Module 13:** Endpoint Security **Module 14:** Layer 2 Security Considerations Labs Due October 18, 2022 @ Midnight	**Video 14.4.8:** Private VLAN Tutorial and Demonstration **Video 14.6.2:** ARP Spoofing **Animation 14.8.1:** STP Normal Operation **Animation 14.8.2:** STP Recalculation **Animation 14.8.3:** Layer 2 Loops **Animation 14.8.9:** Observe STP Operation **Lab 14.3.11:** Packet Tracer - Implement Port Security **Lab 14.8.10:** Packet Tracer - Investigate STP Loop Prevention **Lab 14.9.11:** Packet Tracer - Layer 2 VLAN Security
Oct 17			**Laboratory Exercises**	**Lab 14.9.9:** Configure STP Security
Oct 19	15	5 (13-14)	**Module 15:** Cryptographic Services **Module 16:** Basic Integrity and Authenticity	**Video 16.3.8:** Cryptography
Oct 24			**Laboratory Exercises**	**Lab 15.0.3:** Creating Codes **Lab 15.4.5:** Exploring Encryption Methods
Oct 26			**Laboratory Exercises**	**Lab 16.1.6:** Hashing Things Out **Lab 16.3.10:** Encrypting and Decrypting Data Using OpenSSL
Oct 31			**Laboratory Exercises**	**Lab 16.3.11:** Encrypting and Decrypting Data Using a Hacker Tool **Lab 16.3.12:** Examining Telnet and SSH in Wireshark
Nov 2	17 & 18		**Module 17:** Public Key Cryptography **Module 18:** VPNs	**Video 18.3.1:** IPsec Concepts **Video 18.3.8:** IPsec Transport and Tunnel Modes **Video 18.5.4:** IKE Phase 1 and Phase 2
Nov 7			**Laboratory Exercises**	**Lab 17.2.7:** Certificate Authority Stores
Nov 14	19	6 (15-17)	**Module 19:** Implement Site-to-Site IPsec VPNs with CLI	**Video 19.5.4:** Site-to-Site IPsec VPN Configuration
Nov 16			**Laboratory Exercises**	**Lab 19.5.6:** Configure a Site-to-Site VPN
Nov 21	20	7 (18-19)	**Module 20:** Introduction to the ASA	**Video 20.1.2:** Cisco ASA Next-Generation Firewall Appliances **Video 20.1.5:** Collect Firepower Threat Defense (FTD) Packet captures with Firepower Management Center (FMC)

Class	Lesson	Module Group Exam	Subjects	Labs/Projects
Nov 23	21		**Module 21:** ASA Firewall Configuration	
Nov 28			**Laboratory Exercises**	**Lab 21.2.10:** Configure ASA Basic Settings Using the CLI **Lab 21.7.6:** Configure ASA Network Services, Routing, and DMZ with ACLs Using CLI
Nov 30	22		**Module 22:** Network Security Testing	
Dec 5			**Laboratory Exercises**	**Lab 21.9.5:** Configure ASA Basic Settings and Firewall Using ASDM
Dec 7		8 (20-22)	**Research Paper Presentation / Review**	
Dec 7 – Dec 12		**Additionally:** All Chapter Exams will be active until Monday December 12, 2022 @ 6:00 PM As a reminder, each student is allowed three (3) retakes total of all Chapter Exams.		
Dec 12	**On-Line Final Exam (3 Hours) Notebook is Due!**			
Dec 14	**Three (3) Hour Practical**			
Dec 19	**Three (3) Hour Practical**			
Dec 21	**Three (3) Hour Practical**			

All items in this document are subject to change!