# COMMUNITY COLLEGE OF RHODE ISLAND

## Network Security CNVT 2200 Section 102 Spring 2023

| | | |
|---|---|---|
| **Instructor** | John Mowry | |
| **Telephone** | 401-825-2138 | |
| **E-mail** | jmowry@ccri.edu | If you put @my.ccri.edu, you will be sending an email to a student at CCRI and not to me. Any time you want to email me for this class, you **must** have **CNVT-2200-102** in the subject. If you do not do this, I may not give you a response within 24 hours. I do not answer emails between 9 pm and 8 am on Monday to Saturday; or on weekends at any time. |
| **Office Hours** | See Office Door (Knight Campus Office 2126) | |
| **Class Sections** | 102 Monday and Wednesday 6:00 PM-8:50 PM, starts 1/23 ends 5/10 | |
| **Credit Hours** | 4 Credit Hours, 3 Lecture Hours & 3 Laboratory Hours per week, based on a fifteen-week schedule. | |
| **Administrative Assistant** | Donna Scattone (825-2155) | |

**Instructional Material and Web Sites**

| | | |
|---|---|---|
| 1 | CCRI Lesson Web Site | www.netacad.com (Network Security 1.0) |
| 2 | Cisco Academy Assessment Web Site | http://netacad.com |
| 3 | J Mowry CCRI Website | https://www.ccri.edu/faculty_staff/comp/jmowry |
| 4 | Blackboard | www.blackboard.ccri.edu Material including PowerPoint slides and Grading will be also available here. Detailed material as well as full-instructional material will be available on the Cisco Netacad website listed above. All exams will be administered through the Netacad website. |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**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.

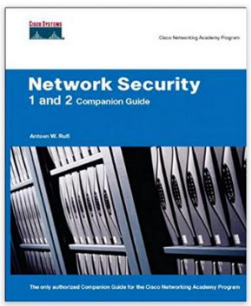
**Course Description:**

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 Delivery Mode:** The course is comprised of both Lecture and Laboratory. There will be both an on-line final as well as a Practical, Hands-On final. All exams will be taken In-Person.

**Course Expectations:** Students are to follow the rules and regulations as outlined in the Student Handbook, available on-line at:
http://www.ccri.edu/advising/student_services/handbook.html

**Additional Learning Material:**
Textbook, (Not Required) (All reading material is available on the Netacad website.)




Network Security 1 And 2 Companion Guide: Cisco Networking Academy Program
by Antoon W. Rufi (Author)

- ISBN-10: 1587131625
- ISBN-13: 978-1587131622

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**Grading Policies**

| | | |
|---|---|---|
| **Skills:** | | |
| Journal-Entries | 5% | Due: Day of assigned Final Exam |
| Labs and Class Participation | 10% | |
| Practical Final | 40% | |
| Research Paper | 10% | Due: May 1, 2023 @ 6:00 PM |
| **Academic:** | | |
| Quizzes | 10% | |
| Final | 25% | |

**Final Grades:** Final grades will be calculated using a mathematical scale utilizing statistical Standard-Deviation methods. The following chart is for reference purposes only! Your instructor reserves the right to evaluate and adjust final grades.

**Grading Scale**:

| Percentage | Letter Grade |
|---|---|
| 94% - 100% | A |
| 90% - less than 94% | A- |
| 87% - less than 90% | B+ |
| 84% - less than 87% | B |
| 80% - less than 84% | B- |
| 77% - less than 80% | C+ |
| 70% - less than 77% | C |
| 67% - less than 70% | D+ |
| 60% - less than 67% | D |
| Below 60% | F |

**Verification of Enrollment:** Per federal financial aid regulations, CCRI is required to verify student enrollment. All faculty members are required to complete a verification of enrollment per the dates in the College Calendar. Students can confirm enrollment through attendance at any academically related activity, a sign-in sheet will be available each class, or by emailing me explaining why you have not attended class or completed the labs in the first week.

**Incomplete Grade:**
This temporary grade designation is awarded at the end of a course. It is awarded only when a student is PASSING, has completed at least 75 percent of the course and is unable to complete the course due to extenuating circumstances (e.g., illness, death, unforeseeable accident, unavoidable circumstance).

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**Late Assignments:**
Since this course would meet 4-hours in person and have 8-hours of reading or homework per-week, you are expected to be putting in 12-hours on this course per college policy. All assignments to be turned in to the instructor will have a due-date prescribed and late assignments will be graded at 75% accordingly at the discretion of your instructor.

**Course Outcomes:**

**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

**Practical Exam**

- The practical exam will encompass a majority of concepts and procedures developed during the laboratory experiments and required readings.
- 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.
- Absolutely no electronic devices are allowed during the exam, including USB's, mobile phones or any other media.
- **Hand-Written** notes will be allowed for use during the Practical Exam only.

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**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.

**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.

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**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. All quizzes must be taken in class and will not be available from the student web site
3. After the listed due date, late submissions (up to one week) will be graded at 75%
4. All assignments must be completed using a word processor.
5. Students are responsible to see the instructor about any work missed due to absence.
6. Students who miss a quiz must take the quiz within two classes of the original quiz date.
7. Students are expected to participate as a member of teams
8. Students must pass both the Skills based portion in addition to the Academic portion of the curriculum to pass the course.
9. Student's final grade can only raise one letter grade above the on-line final exam score based on other class assignments.
10. Students are allowed a **maximum** of three (3) re-takes of chapter quizzes per the semester.
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.

**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).

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**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.***

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**Netiquette Policy**:

- Respect others and their opinions. In online learning, students from various backgrounds come together to learn. It is important to respect their feelings and opinions though they may differ from your own.
- Tone down your language. Given the absence of face-to-face clues, written text can easily be misinterpreted. Avoid the use of strong or offensive language and the excessive use of exclamation points. Review before posting to remove any strong language.
- Keep personal discussions off the class discussion board.
- Do not type all capitals, which is difficult to read, and has come to be considered the electronic version of "shouting."
- Do be courteous, even when you disagree, with your instructors as well as your classmates, and always provide clear, logical support for your views.
- Avoid inappropriate material.
- Be forgiving. If someone states something that you find offensive, mention this directly to the instructor. Remember that the person contributing to the discussion might be new to this form of communication. What you find offensive may quite possibly have been unintended and can best be cleared up by the instructor.
- Think before you hit the send button. Think carefully about the content of your message before contributing it. Once sent to the group there is no taking it back. Grammar and spelling errors reflect on you and your audience might not be able to decode misspelled words or poorly constructed sentences. It can also adversely affect your grade.
- Escalate your issues privately via email versus discussion forums. Should you have a disagreement with an instructor or classmate it is best to send an individual email to that individual. Do not argue your case in the discussion forum.
- Brevity is best. Be as concise as possible when contributing to a discussion. Your points might be missed if hidden in a flood of text.

Avoid disciplinary action. Any type of online behavior that is perceived as disrespectful to a fellow student or instructor, or anything that has the potential to be perceived as less than courteous is unacceptable and can be subject to disciplinary action by the Chair of the department. Repetition of such behavior can result in expulsion from the class.

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**Technical Requirements:**

Learning requires certain technical requirements to participate actively and be successful. At the minimum, students must have access to a computer and stable Internet connection. Many courses at CCRI require certain technical requirements to participate actively and be successful. View Set Up Your Tech to learn more about technical requirements.

**CISCO Netacad**:

Students need a stable Internet connection. Chrome, Firefox, or Edge web browsers can be used. You should clear your web browser cache, which is found in the settings of the web browser. If you do not do this, some of your labs will not work correctly. Chromebooks will not work for your labs. You must have a computer/laptop running Windows 10 or better or MAC.

**CCRI Computer Labs**:

The academic computer lab is available for CCRI students and allows access to computers with required software. Information regarding CCRI's academic computer labs is available at the following link: Academic Computer Labs.

**MS Office 365**:

Microsoft Office 365 is available for all CCRI students to download. This version of Office will be accessible as long as you are actively enrolled at CCRI. It is recommended that students download MS 365 to their computers for access to MS Word, PowerPoint, and Excel offline. If you use other programs, I may not be able to open the files.

**MS OneDrive**:

OneDrive is a clouded-based storage system that lets CCRI students store, share and organize files, photos and favorites on Windows servers, and access them from any computer with an Internet connection. You will need and know how to use a computer or mobile device with Internet access. You will also need one of the following web browsers: Edge, Firefox, Chrome, or Safari (Mac only). However, if you put something into OneDrive, you must give me permission to access the file. Once I click on allow, you will get an email that you give permission again before I can view the data.

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**Academic Integrity**:

Academic integrity is vital to an institution of higher education. The integrity of your work – that it represents your independent thought and effort and that it properly acknowledges the work of others – is essential to the awarding of credit and to the development of your academic potential. As such, instances of academic dishonesty – cheating, plagiarism, etc., – are extremely serious academic offenses that should not be overlooked. Students should be aware and regularly cautioned that violations of academic integrity may result in suspension or expulsion from the college. For more information, go to the CCRI's Policy on Academic Integrity.

**Managing Life Crisis and Finding Support**:

Should you encounter an unexpected crisis during the semester (i.e., securing food or housing, addressing mental health concerns, personal safety, managing a financial crisis, and/or dealing with a family emergency, etc.), please reach out to the office of Community and Social Resources. If you are uncomfortable doing so on your own, please know that I can submit a referral on your behalf—just email me or schedule a meeting with me during my office hours.

**Veteran Services**:

CCRI Veteran Services Office is committed to being a resource to all VA education beneficiaries. Our mission is to assist veterans, service members, and dependents in the pursuit of their educational goals by maintaining up-to-date information on current programs and resources. Through a combination of experience with the educational system and contacts within the VA, we can help you with any aspect of your higher education.

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**Mental Health Services**:

CCRI is committed to advancing the mental health and wellbeing of its students. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available.

CCRI has partnered with MySSP (My Student Support Service) to provide 24/7 mental health and well-being support to students, including real-time and scheduled access to professional counselors. All services are confidential and 100% FREE to CCRI students!

In addition to MySSP, the Advising and Counseling Center provides one-on-one and group counseling for a variety of problems ranging from typical difficulties students experience (e.g., adjustment to the college setting) to problems associated with acute or long-standing psychological disturbances. For a listing of mental health services on and off campus, visit Mental Health Services.

**Student Success Center**:

The Student Success Center provides academic assistance through tutoring services; coordinate information and referrals to college resources; seek ways to improve student satisfaction and retention; and help students achieve their goals. Student Success Center staff members help students understand their individual learning needs, develop better study habits and behaviors, and create plans to achieve their goals. For more information about our services, email successcenter@ccri.edu or visit the website. Watch this video, to learn how to book Free CCRI tutoring appointments through Starfish.

**Writing Center**:

The Writing Center offers a variety of free services, including online and in-person help with prewriting, organization, thesis statements, topic sentences, research papers, revision/editing, and answers to questions. Online help at Writing Center includes:

- Zoom links for Writing Center Virtual Drop-in Tutoring Sessions
- Virtual Zoom appointments
- Email responses to questions and help with papers
- Website content, such as handouts, practice quizzes, literature analysis, PowerPoint presentations, reading resources, and information about research papers (MLA, APA, and Chicago systems)

In-person appointments can be made by contacting writingcenter@ccri.edu. The Writing Center is available at three of our four campuses to assist CCRI students, faculty, and staff members with different kinds of writing and revision tasks.

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

**Religious & Cultural Observance**:

Persons who have religious or cultural observances that coincide with this class should let me know in an email during the first two weeks of the semester. However, if I do not hear from you by the end of the second week of school, I will assume you plan on doing the work for the week.

**Explicit Content**:

If you are aware of cognitive or emotional triggers that could disrupt your intellectual or mental health, please let me know so that I can be aware in terms of course content.

**Title IX and Gender Pronouns**:

This course affirms equality and respect for all gendered identities and expressions. Please don't hesitate to correct me regarding your preferred gender pronoun and/or name if different from what is indicated on the official class roster. Likewise, I am committed to nurturing an environment free from discrimination and harassment. Consistent with Title IX policy, please be aware that I, as a responsible employee, am obligated to report information that you provide to me about a situation involving sexual harassment or assault.

**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. | |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

| | | |
|---|---|---|
| 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** |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

| | | |
|---|---|---|
| 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. | |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

| | | |
|---|---|---|
| 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. | |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

| | | |
|---|---|---|
| **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** |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

## 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** |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

# Network Security 1.0

| Class | Lesson | Module Group Exam | Subjects | Labs/Projects |
|---|---|---|---|---|
| Jan 23 | 1 & 2 | | **Module 1:** Securing Networks<br>**Module 2:** Network Threats | **Video 1.1.5:** Anatomy of an Attack<br>**Video 2.4.3:** Reconnaissance Attacks<br>**Animation 2.3.6:** Worm Components<br>**Animation 2.4.2:** Reconnaissance Attacks<br>**Animation 2.4.4:** Access Attacks<br>**Video 2.4.5:** Access and Social Engineering Attacks<br>**Video 2.5.1:** Denial of Service Attacks<br>**Video 2.5.4:** Mirai Botnet |
| Jan 25 | | | **Laboratory Exercises** | **Lab 2.4.8:** Social Engineering |
| Jan 30 | 3 & 4 | | **Module 3:** Mitigating Threats<br>**Module 4:** Secure Device Access | **Video 3.3.4:** Cisco SecureX Demonstration<br>**Video 4.3.6:** Configure Passwords and Enhanced Login Security<br>**Video 4.4.1:** The Need for SSH |
| Feb 1 | | | **Laboratory Exercises** | **Lab 4.4.7:** Configure Network Devices with SSH<br>**Lab 4.4.9:** Configure Network Devices |
| Feb 6 | | 1 (1-4) | **Module 5:** Assigning Administrative Roles<br>**Module 6:** Device Monitoring and Management<br>Labs Due February 12, 2023 @ Midnight | **Animation 5.2.2:** Role-Based Views<br>**Animation 6.3.2:** Routing Protocol Spoofing<br>**Lab 6.6.4:** Packet Tracer - Configure and Verify NTP<br>**Lab 6.7.12:** Packet Tracer - Configure Cisco Devices for Syslog, NTP, and SSH Operations |
| Feb 8 | | | **Laboratory Exercises** | **Lab 5.2.5:** Configure Network Devices with SSH<br>**Lab 6.2.7:** Configure Automated Security Features<br>**Lab 6.3.6:** Basic Device Configuration and OSPF Authentication |
| Feb 13 | 7 & 8 | | **Module 7:** Authentication, Authorization, and Accounting (AAA)<br>**Module 8:** Access Control Lists<br>Labs Due February 19, 2023 @ Midnight | **Animation 7.3.4:** Process for TACACS+ Authentication<br>**Animation 7.3.5:** Process for RADIUS Authentication<br>**Video 7.4.6:** Configure a Cisco Router to Access a AAA RADIUS Server<br>**Interactive Activity 8.5.9:** Configuring Standard ACLs<br>**Interactive Activity 8.5.10:** Creating an Extended ACL Statement<br>**Lab 7.2.6:** Packet Tracer - Configure Local AAA for Console and VTY Access<br>**Lab 8.6.5:** Packet Tracer - Configure IP ACLs to Mitigate Attacks<br>**Lab 8.7.4:** Packet Tracer - Configure IPv6 ACLs |
| Feb 15 | | | **Laboratory Exercises** | **Lab 7.4.7:** Install the Virtual Machine<br>**Lab 7.4.8:** Configure Server-Based Authentication with RADIUS |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

| Class | Lesson | Module Group Exam | Subjects | Labs/Projects |
|---|---|---|---|---|
| Feb 20 | 9 & 10 | 2 (5-7) | **Module 9:** Firewall Technologies<br>**Module 10:** Zone-Based Policy Firewalls<br>Labs Due February 26, 2023 @ Midnight | **Animation 9.1.1:** Firewalls<br>**Video 10.3.10:** Video Demonstration of ZPF<br>**Lab 9.2.4:** Packet Tracer - Identify Packet Flow |
| Feb 22 | | | **Laboratory Exercises** | **Lab 10.3.12:** Configure ZPFs |
| Feb 27 | 11 & 12 | 3 (8-10) | **Module 11:** IPS Technologies<br>**Module 12:** IPS Operation and Implementation<br>Labs Due March 5, 2023 @ Midnight | **Lab 11.4.6:** Packet Tracer - Implementing a Local SPAN |
| March 1 | 13 & 14 | 4 (11-12) | **Module 13:** Endpoint Security<br>**Module 14:** Layer 2 Security Considerations<br>Labs Due March 7, 2023 @ Midnight | **Video 14.4.8:** Private VLAN Tutorial and Demonstration<br>**Video 14.6.2:** ARP Spoofing<br>**Animation 14.8.1:** STP Normal Operation<br>**Animation 14.8.2:** STP Recalculation<br>**Animation 14.8.3:** Layer 2 Loops<br>**Animation 14.8.9:** Observe STP Operation<br>**Lab 14.3.11:** Packet Tracer - Implement Port Security<br>**Lab 14.8.10:** Packet Tracer - Investigate STP Loop Prevention<br>**Lab 14.9.11:** Packet Tracer - Layer 2 VLAN Security |
| March 6 | | | **Laboratory Exercises** | **Lab 14.9.9:** Configure STP Security |
| March 8 | 15 | 5 (13-14) | **Module 15:** Cryptographic Services<br>**Module 16:** Basic Integrity and Authenticity | **Video 16.3.8:** Cryptography |
| March 20 | | | **Laboratory Exercises** | **Lab 15.0.3:** Creating Codes<br>**Lab 15.4.5:** Exploring Encryption Methods |
| March 22 | | | **Laboratory Exercises** | **Lab 16.1.6:** Hashing Things Out<br>**Lab 16.3.10:** Encrypting and Decrypting Data Using OpenSSL |
| March 27 | | | **Laboratory Exercises** | **Lab 16.3.11:** Encrypting and Decrypting Data Using a Hacker Tool<br>**Lab 16.3.12:** Examining Telnet and SSH in Wireshark |
| March 29 | 17 & 18 | | **Module 17:** Public Key Cryptography<br>**Module 18:** VPNs | **Video 18.3.1:** IPsec Concepts<br>**Video 18.3.8:** IPsec Transport and Tunnel Modes<br>**Video 18.5.4:** IKE Phase 1 and Phase 2 |
| April 3 | | | **Laboratory Exercises** | **Lab 17.2.7:** Certificate Authority Stores |
| April 5 | 19 | 6 (15-17) | **Module 19:** Implement Site-to-Site IPsec VPNs with CLI | **Video 19.5.4:** Site-to-Site IPsec VPN Configuration |
| April 10 | | | **Laboratory Exercises** | **Lab 19.5.6:** Configure a Site-to-Site VPN |
| April 12 | 20 | 7 (18-19) | **Module 20:** Introduction to the ASA | **Video 20.1.2:** Cisco ASA Next-Generation Firewall Appliances<br>**Video 20.1.5:** Collect Firepower Threat Defense (FTD) Packet captures with Firepower Management Center (FMC) |

© CNVT 2200 Spring 2023 John Mowry / All rights reserved

| Class | Lesson | Module Group Exam | Subjects | Labs/Projects |
|---|---|---|---|---|
| April 17 | 21 | | **Module 21:** ASA Firewall Configuration | |
| April 19 | | | **Laboratory Exercises** | **Lab 21.2.10:** Configure ASA Basic Settings Using the CLI<br>**Lab 21.7.6:** Configure ASA Network Services, Routing, and DMZ with ACLs Using CLI |
| April 24 | 22 | | **Module 22:** Network Security Testing | |
| April 26 | | | **Laboratory Exercises** | **Lab 21.9.5:** Configure ASA Basic Settings and Firewall Using ASDM<br>**Lab 21.9.6** Configure Clientless Remote Access SSL VPNs Using ASA 5506-X ASDM |
| May 1 | | 8 (20-22) | **Research Paper Presentation / Review** | |
| May 1 – May 10 | | **Additionally:**<br>All Chapter Exams will be active from May 1, 2023 @ 9:00 PM until May 10, 2023 @ 5:00 PM<br>As a reminder, each student is allowed three (3) retakes total of all Chapter Exams. | | |
| May 3 | **Three (3) Hour Practical / Final Exam / Notebook** | | | |
| May 8 | **Three (3) Hour Practical / Final Exam / Notebook** | | | |
| May 10 | **Three (3) Hour Practical / Final Exam / Notebook** | | | |

**All items in this document are subject to change!**

© CNVT 2200 Spring 2023 John Mowry / All rights reserved