PASSAIC COUNTY TECHNICAL INSTITUTE
45 Reinhardt Rd.
Wayne, NJ

Information Technology & Network Security III
(ITNS III)
Course # 1025
Developed 2018

I. Course Description:

This course builds on the experience students have gained in the first two years of Information Technology and Network Security, on how to maintain PCs and setup a corporate network. Now you will learn how to protect that network from a myriad of threats. Presenting the evolution of computer security, the main threats, attacks & mechanisms, security protocols, storage protection methods, cryptography, ways of identifying, understanding & recovery from attacks against computer systems. Additionally, various methods of security breach prevention, network systems availability, recovery procedures and counter systems penetrations techniques will be discussed.

II. Units:

Content Area:	**Informational Technology & Network Security III**	**Grade(s)**	**11**
Unit Plan Title:	**Unit 1 – Security Introduction** *Unit 1 will introduce the essential concepts of Security including the ability to implement processes to protect an organization's assets against danger, damage, loss, and criminal activity.* I. Intro to Security (2 days) a. The security landscapes b. Security Concepts II. Installing a security appliance (2 days) a. Configuring a Security Appliance b. Installing a Security Appliance 4 days are required for Unit 1.		
NJSLS/CCTC Standard(s) Addressed			
CRP4. Communicate clearly and effectively and with reason. CRP5. Consider the environmental, social and economic impacts of decisions.			

CRP8. Utilize critical thinking to make sense of problems and persevere in solving them.
CRP11. Use technology to enhance productivity.
CRP12. Work productively in teams while using cultural global competence.
9.3. IT.12 Demonstrate knowledge of the hardware components associated with information systems.
9.3. IT- NET.4 Perform network system installation and configuration.

Essential Questions (3-5)

1. What challenges does a security professional face?
2. What is the difference between integrity and non-repudiation?
3. What are the three main goals of the CIA of Security?
4. What are the key components of risk management?
5. What are three types of threat agents?

Anchor Text(s)

CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition Author: Mark Ciampa ISBN#: 978-1-337-28878-1
Hands-On Ethical Hacking and Network Defense, 3rd edition ISBN# 978-1285454610

Short & Informational Texts (3-5)

ARTICLES
"The Top Cyber Security Challenges Experts Are Facing Today"
https://www.forbes.com/sites/quora/2017/05/31/the-top-cyber-security-challenges-experts-are-facing-today/#65bd3a122238
"The 3 Most Frustrating Challenges IT Security Teams Face"
https://securityintelligence.com/three-most-frustrating-challenges-it-security-teams-face
"Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving"
https://www.sciencedirect.com/science/article/pii/S0167404814001849

Expected Proficiencies/Career and Life Skills

• Configure a security appliance
• Install a security appliance

Formative & Summative Assessments

- TestOut Module quizzes (Formative)

- TestOut lab simulations (Formative)
- Section assignments/activities (Formative)
- Module review packets (Summative)
- Comprehensive module tests (Summative)
- Practical scenario assessments (Real world labs) (Summative)
- Trimester projects (Summative)
- Trimester exam (Summative)

Resources (Websites, LMS, Google Classroom, documents, etc.)

- Testout's LabSim
- Canvas LMS
- Microsoft PowerPoint
- Microsoft Word
- Instructional Videos
- Wikis
- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Google Drive/Docs/Slides
- Career search engines (i.e. Careerbuilder, Indeed)
- Knowledgebase
- Technical forums
- Microsoft Visio
- YouTube videos

Content Area:	**Informational Technology & Network Security III**	**Grade(s)**	**11**
Unit Plan Title:	**Unit 2 – Security Basics** *Unit 2 will cover the importance of a basic attack and defense plan. It will address network monitoring and response to an incident related to a cyber-attack*		

	I. Understanding Attacks (2 days) II. Defense Planning (2 days) III. Access Control (3 days) IV. Cryptography (2 days) V. Network Monitoring (2day) VI. Incident Response (3 days) 14 days are required for Unit 2.

NJSLS/CCTC Standard(s) Addressed

CRP1. Act as a responsible and contributing citizen and employee.
CRP2. Apply appropriate academic and technical skills.
CRP4. Communicate clearly and effectively and with reason.
CRP6. Demonstrate creativity and innovation.
CRP8. Utilize critical thinking to make sense of problems and persevere in solving them.
9.3. IT.6 Describe trends in emerging and evolving computer technologies and their influence on IT practices.
9.3. IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3. IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.

Essential Questions (3-5)

1. How do persistent and non-persistent threats differ?
2. What is layered security?
3. Why is defense-in-depth important?
4. What is a legitimate use for cryptanalysis?
5. Why is network monitoring important?

Anchor Text(s)

CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition Author: Mark Ciampa ISBN#: 978-1-337-28878-1
Hands-On Ethical Hacking and Network Defense, 3rd edition ISBN# 978-1285454610

Short & Informational Texts (3-5)

ARTICLES

Understanding layered security and defense in depth
https://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/
How to Protect Your PC with Multiple Layers of Security
https://heimdalsecurity.com/blog/protect-your-pc-multiple-layers-security/
Cryptanalysis
http://www.tech-faq.com/cryptanalysis.html

Expected Proficiencies/Career and Life Skills

- Explain penetration testing concepts
- Explain use cases and purpose for frameworks, best practices and secure configuration guides
- Compare identity and access management concepts
- Given a scenario, differentiate common account management practices
- Explain the importance of policies, plans and procedures related to organizational security
- Compare basic concepts of cryptography
- Analyze and record forensic evidence.

Formative & Summative Assessments

- TestOut Module quizzes (Formative)
- TestOut lab simulations (Formative)
- Section assignments/activities (Formative)
- Module review packets (Summative)
- Comprehensive module tests (Summative)
- Practical scenario assessments (Real world labs) (Summative)
- Trimester projects (Summative)
- Trimester exam (Summative)

Resources (Websites, LMS, Google Classroom, documents, etc.)

- Testout's LabSim
- Canvas LMS
- Microsoft PowerPoint

- Microsoft Word
- Instructional Videos
- Wikis
- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Google Drive/Docs/Slides
- Knowledgebase
- Technical forums
- Microsoft Visio
- YouTube videos

Content Area:	**Informational Technology & Network Security III**	**Grade(s)**	**11**
Unit Plan Title:	**Unit 3 – Policy, Procedures and Awareness** *Unit 3 will delve in security policies, risk management and creating a manageable employee awareness procedure.* I. Security Policies (5 days) II. Risk Management (3 days) III. Business Continuity (1 day) IV. Manageable Network Plan (2 day) V. Social Engineering (5 days) VI. App Development and Deployment (1 day) VII. Employee Management (1 day) VIII. Mobile Devices (1 day) *IX.* Third-Party Integration (1 day)		

	20 days are required for Unit 3.

NJSLS/CCTC Standard(s) Addressed

CRP2. Apply appropriate academic and technical skills.
CRP4. Communicate clearly and effectively and with reason.
CRP5. Consider the environmental, social and economic impacts of decisions.
CRP7. Employ valid and reliable research strategies.
9.3.IT.6 Describe trends in emerging and evolving computer technologies and their influence on IT practices.
9.3. IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3. IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.

Essential Questions (3-5)

1. What is the difference between a regulation and a guideline?
2. What kinds of components are *tangible* assets?
3. When you develop a manageable network plan, what should you keep in mind as you prepare to document your network?
4. How is passive social engineering different from active social engineering?
5. What methods do attackers use to make an interaction appear legitimate?

Anchor Text(s)

CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition Author: Mark Ciampa ISBN#: 978-1-337-28878-1
Hands-On Ethical Hacking and Network Defense, 3rd edition ISBN# 978-1285454610

Short & Informational Texts (3-5)

ARTICLES
Security laws, regulations and guidelines directory
https://www.computerworld.com/article/2514027/security0/security-laws--regulations-and-guidelines-directory.html
What is social engineering? How criminals take advantage of human behavior
https://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html
Don't Take the Bait
https://www.irs.gov/newsroom/dont-take-the-bait-step-1-avoid-spear-phishing-emails

Expected Proficiencies/Career and Life Skills

- Explain risk management processes and concepts
- Explain disaster recovery and continuity of operation concepts.
- Identify and ignore email hoaxes
- Explain the importance of policies, plans and procedures related to organizational security.

Formative & Summative Assessments

- TestOut Module quizzes (Formative)
- TestOut lab simulations (Formative)
- Section assignments/activities (Formative)
- Module review packets (Summative)
- Comprehensive module tests (Summative)
- Practical scenario assessments (Real world labs) (Summative)
- Trimester projects (Summative)
- Trimester exam (Summative)

Resources (Websites, LMS, Google Classroom, documents, etc.)

- Testout's LabSim (Modules 3, 5, and 10)
- Canvas LMS
- Microsoft PowerPoint
- Microsoft Word
- Instructional Videos
- Wikis
- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Google Drive/Docs/Slides
- Knowledgebase
- Technical forums

- Microsoft Visio
- YouTube videos

Content Area:	ITNS IV Informational Technology & Network Security III	Grade(s)	11
Unit Plan Title:	**Unit 4 – Physical Threats and Perimeter Defense** *Unit 4 will compare physical security and environmental controls and explain the importance of physical security. Unit 4 will also introduce perimeter defenses as methods to enhance physical security.* I. Physical Threats (1 day) II. Device Protection (1 day) III. Network Infrastructure Protection (1 day) IV. Environmental Controls (2 Days) V. Recon and Denial (5 days) VI. Spoofing and Poisoning (2 days) VII. Security Appliances (3 days) VIII. Demilitarized Zones (DMZ) (2 days) IX. Firewalls (2 days) X. Network Address Translation (NAT) (3 Days) XI. Virtual Private Networks (VPN) (2 days) XII. Web Threat Protection (1 day) XIII. Network Access Protection (1 day) XIV. Wireless Overview (3 days) XV. Wireless Attacks (3 days) XVI. Wireless Defenses (3 days) 35 days are required for Unit 4.		

NJSLS/CCTC Standard(s) Addressed

CRP2. Apply appropriate academic and technical skills.
CRP4. Communicate clearly and effectively and with reason.
CRP5. Consider the environmental, social and economic impacts of decisions.
CRP8. Utilize critical thinking to make sense of problems and persevere in solving them.
9.3. IT- NET.2 Analyze wired and wireless network systems to determine if they meet specifications (e.g.,IEEE, power and security).
9.3. IT- NET.3 Design a network system using technologies, tools and standards.
9.3. IT- NET.4 Perform network system installation and configuration.
9.3. IT- NET.5 Perform network administration, monitoring and support to maintain a network system.

Essential Questions (3-5)

1. What types of physical controls can be implemented to protect the perimeter of a building?
2. What are the security guidelines you should implement to protect servers in your organization?
3. What countermeasures help mitigate DoS and DDoS attacks?
4. What are the uses of a DMZ?
5. What methods can you use to secure a wireless network from data emanation?

Anchor Text(s)

CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition Author: Mark Ciampa ISBN#: 978-1-337-28878-1
Hands-On Ethical Hacking and Network Defense, 3rd edition ISBN# 978-1285454610

Short & Informational Texts (3-5)

ARTICLES
What is a wireless network**?**
https://www.cisco.com/c/en/us/solutions/small-business/resource-center/work-anywhere/wireless-network.html
Using a DMZ in a computer network
https://www.lifewire.com/demilitarized-zone-computer-networking-816407
Hackers infiltrate free PC cleaning software
http://money.cnn.com/2017/09/18/technology/business/windows-ccleaner-hack/index.html

Expected Proficiencies/Career and Life Skills

- Implement physical security
- Explain the importance of physical security controls.

- Explain penetration testing concepts
- Configure Network Security Appliance access
- Configure a DMZ
- Install and configure the Network Address Translation (NAT) IP routing protocol on a router
- Configure the NAT router to act as a DHCP server
- Configure the NAT router to act as a DNS proxy
- Configure NAT from the CLI
- Configure NAT on an NSA
- Configure a remote access VPN
- Configure a VPN connection iPad
- Implement NAC with DHCP enforcement
- Configure a wireless network

Formative & Summative Assessments

- TestOut Module quizzes (Formative)
- TestOut lab simulations (Formative)
- Section assignments/activities (Formative)
- Module review packets (Summative)
- Comprehensive module tests (Summative)
- Practical scenario assessments (Real world labs) (Summative)
- Trimester projects (Summative)
- Trimester exam (Summative)

Resources (Websites, LMS, Google Classroom, documents, etc.)

- Testout's LabSim
- Canvas LMS
- Microsoft PowerPoint
- Microsoft Word
- Instructional Videos
- Google Drive/Docs/Slides
- Wikis

- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Knowledgebase
- Technical forums
- Microsoft Visio
- YouTube videos

Content Area:	**Informational Technology & Network Security III**	**Grade(s)**	**11**
Unit Plan Title:	Unit 5 – Network *Unit 5 will cover the basics network threats and attacks on switches and routers. It will also cover hardening security on these network devices by using tools to analyze and assess the best course of action to prevent future attacks* I. Network Threats – 1 days II. Network Device Vulnerabilities – 1 day III. Network Applications – 1 day IV. Switch Attacks – 1 day V. Switch Security – 3 days VI. Using VLANs – 3 days VII. Router Security – 3 days VIII. Intrusion Detection and Prevention – 1 day IX. Vulnerability Assessment – 2 days X. Protocol Analyzers – 1 day XI. Remote Access – 2 days XII. Network Authentication – 3 days XIII. Penetration Testing – 1 days XIV. Virtual Networking – 2 days		

	XV. Software-Defined Networking (SDN) – 1 day XVI. XVII. Cloud Services – 1 day 28 days are required for Unit 5.
NJSLS/CCTC Standard(s) Addressed	
CRP1. Act as a responsible and contributing citizen and employee. CRP2. Apply appropriate academic and technical skills. CRP4. Communicate clearly and effectively and with reason. CRP6. Demonstrate creativity and innovation. CRP7. Employ valid and reliable research strategies. CRP8. Utilize critical thinking to make sense of problems and persevere in solving them. 9.3. IT- NET.2 Analyze wired and wireless network systems to determine if they meet specifications (e.g. IEEE, power and security). 9.3. IT- NET.3 Design a network system using technologies, tools and standards. 9.3. IT- NET.4 Perform network system installation and configuration. 9.3. IT- NET.5 Perform network administration, monitoring and support to maintain a network system.	
Essential Questions (3-5)	
1. Which areas of your network should you focus on to best understand it? 2. What is the difference between a hybrid cloud and a community cloud? 3. Which technology allows network and security professionals to manage, control, and make changes to a network?	
Anchor Text(s)	
CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition Author: Mark Ciampa ISBN#: 978-1-337-28878-1 Hands-On Ethical Hacking and Network Defense, 3rd edition ISBN# 978-1285454610	
Short & Informational Texts (3-5)	
ARTICLES The Future of Cloud Computing https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/ Network Authentication, Authorization, and Accounting https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-35/101-aaa-part1.html What is Penetration Testing?	

https://www.coresecurity.com/content/penetration-testing

Expected Proficiencies/Career and Life Skills

- Configure Network Security Appliance access
- Install and configure the Network Address Translation (NAT) IP routing protocol on a router
- Configure the NAT router to act as a DHCP server
- Configure the NAT router to act as a DNS proxy
- Configure NAT from the CLI
- Configure NAT on an NSA
- Configure a remote access VPN
- Configure a VPN connection iPad
- Configure a wireless network

Formative & Summative Assessments

- TestOut Module quizzes (Formative)
- TestOut lab simulations (Formative)
- Section assignments/activities (Formative)
- Module review packets (Summative)
- Comprehensive module tests (Summative)
- Practical scenario assessments (Real world labs) (Summative)
- Trimester projects (Summative)
- Trimester exam (Summative)

Resources (Websites, LMS, Google Classroom, documents, etc.)

- Testout's LabSim
- Canvas LMS
- Cisco Packet Tracer
- Microsoft PowerPoint
- Microsoft Word
- Instructional Videos
- Wikis

- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Google Drive/Docs/Slides
- Knowledgebase
- Technical forums
- Microsoft Visio
- YouTube videos

Content Area:	**Informational Technology & Network Security III**	**Grade(s)**	**11**
Unit Plan Title:	**Unit 6 – Host** *Unit 6 will cover the various security threats that users and devices face and how to protect against those threats.* I. Malware – 2 days II. Password Attacks – 2 days III. Windows System Hardening – 2 days IV. Hardening Enforcement – 2 days V. File Server Security – 1 day VI. Linux Host Security – 1 day VII. Embedded Systems – 1 day VIII. Log Management – 1 day IX. Audits – 1 day X. BYOD Security – 1 day XI. Mobile Device Management – 1 day XII. Host Virtualization – 1 day		

	16 days are required for Unit 6.

NJSLS/CCTC Standard(s) Addressed

CRP1. Act as a responsible and contributing citizen and employee.
CRP2. Apply appropriate academic and technical skills.
CRP4. Communicate clearly and effectively and with reason.
CRP6. Demonstrate creativity and innovation.
CRP7. Employ valid and reliable research strategies.
CRP8. Utilize critical thinking to make sense of problems and persevere in solving them.
9.3. IT- NET.4 Perform network system installation and configuration.
9.3.IT.8 -Recognize and analyze potential IT security threats to develop and maintain security requirements
9.3. IT.13 - Compare key functions and applications of software and determine maintenance strategies for computer systems.

Essential Questions (3-5)

1. What is hardening? How does it benefit security?
2. What is a socket?
3. What is a SoC?
4. What does a mobile device management (MDM) solution allow you to do?

Anchor Text(s)

CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition Author: Mark Ciampa ISBN#: 978-1-337-28878-1
Hands-On Ethical Hacking and Network Defense, 3rd edition ISBN# 978-1285454610

Short & Informational Texts (3-5)

ARTICLES
What is mobile device management**?** **https://www.webopedia.com/TERM/M/mobile_device_management.html**
What is malware? Everything you need to know
https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/
Seven measures to protect your servers
https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers

Expected Proficiencies/Career and Life Skills

- Configure Windows Defender protections to secure a network from malware
- Configure windows firewall
- Configure GPO's to enforce security
- Configure NTFS permissions
- Configure advanced audit policies
- Secure emails and email servers
- Secure an IPAD

Formative & Summative Assessments

- TestOut Module quizzes (Formative)
- TestOut lab simulations (Formative)
- Section assignments/activities (Formative)
- Module review packets (Summative)
- Comprehensive module tests (Summative)
- Practical scenario assessments (Real world labs) (Summative)
- Trimester projects (Summative)
- Trimester exam (Summative)

Resources (Websites, LMS, Google Classroom, documents, etc.)

- Testout's LabSim
- Canvas LMS
- Google Drive/Docs/Slides
- Microsoft PowerPoint
- Microsoft Word
- Instructional Videos
- Wikis
- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Knowledgebase
- Technical forums

- Microsoft Visio
- YouTube videos

Content Area:	Informational Technology & Network Security III	Grade(s)	11
Unit Plan Title:	**Unit 7 – Application** *Unit 7 will utilize capstone lab simulations and hands-on assessments to prepare the student for the certification exam.* I. Access Control Models – 1 day II. Authentication – 1 day III. Authorization – 1 day IV. Web Application Attacks– 1 day V. Internet Browsers – 3 days VI. Application Development– 1 day VII. Active Directory Overview – 3 days VIII. Windows Domain Users and Groups – 1 day IX. Linux Users – 2 days X. Linux Groups – 2 days XI. Linux User Security – 3 days XII. Group Policy Overview – 3 days XIII. 23 days are required for Unit 7.		
NJSLS/CCTC Standard(s) Addressed			

CRP1. Act as a responsible and contributing citizen and employee.
CRP2. Apply appropriate academic and technical skills.
CRP4. Communicate clearly and effectively and with reason.
CRP8. Utilize critical thinking to make sense of problems and persevere in solving them.
9.3. IT- NET.5 Perform network administration, monitoring and support to maintain a network system.
9.3. IT- PRG.10 Design, create and maintain a database.

Essential Questions (3-5)

1. What is access control? Why is it important?
2. What is the difference between authentication and identification?
3. What three types of information make up an access token?
4. What is the purpose of a domain?
5. What is the order in which GPOs are applied?

Anchor Text(s)

CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition Author: Mark Ciampa ISBN#: 978-1-337-28878-1
Hands-On Ethical Hacking and Network Defense, 3rd edition ISBN# 978-1285454610

Short & Informational Texts (3-5)

ARTICLES
Overview of Linux
https://opensource.com/resources/linux
What is Active Directory?
https://aws.amazon.com/directoryservice/active-directory/
What is a windows domain and how does it affect my pc?
https://www.howtogeek.com/194069/what-is-a-windows-domain-and-how-does-it-affect-my-pc/

Expected Proficiencies/Career and Life Skills

- Configure IE preferences in a GPO
- Implement Data Execution Prevention
- Create, rename, delete, and manage user accounts in Linux
- Configure Linux user security and restrictions

- Create and link GPO's

Formative & Summative Assessments

- TestOut Module quizzes (Formative)
- TestOut lab simulations (Formative)
- Section assignments/activities (Formative)
- Module review packets (Summative)
- Comprehensive module tests (Summative)
- Practical scenario assessments (Real world labs) (Summative)
- Trimester projects (Summative)
- Trimester exam (Summative)

Resources (Websites, LMS, Google Classroom, documents, etc.)

- Testout's LabSim
- Canvas LMS
- Google Drive/Docs/Slides
- Microsoft PowerPoint
- Microsoft Word
- Instructional Videos
- Wikis
- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Knowledgebase
- Technical forums
- Microsoft Visio
- YouTube videos

Content Area:	**Informational Technology & Network Security III**	**Grade(s)**	**11**

Unit Plan Title:	**Unit 8 – Python - Programming Essentials in Python** *Unit 7 will utilize capstone lab simulations and hands-on assessments to prepare the student for the certification exam.* I. Introduction – 5 days II. Basics – 10 days III. Making decisions in Python - 5 days IV. Logic and operations in Python – 5 days V. Writing functions in Python – 5 days 30 days are required for Unit 7.

NJSLS/CCTC Standard(s) Addressed

CRP2. Apply appropriate academic and technical skills.
CRP5. Consider the environmental, social and economic impacts of decisions.
CRP6. Demonstrate creativity and innovation.
CRP7. Employ valid and reliable research strategies.
CRP8. Utilize critical thinking to make sense of problems and persevere in solving them.
9.3. IT- PRG.1 Analyze customer software needs and requirements.
9.3. IT- PRG.2 Demonstrate the use of industry standard strategies and project planning to meet customer specifications.
9.3.IT- PRG.3 Analyze system and software requirements to ensure maximum operating efficiency.
9.3. IT- PRG.4 Demonstrate the effective use of software development tools to develop software applications.
9.3. IT- PRG.5 Apply an appropriate software development process to design a software application.
9.3. IT- PRG.6 Program a computer application using the appropriate programming language.
9.3. IT- PRG.7 Demonstrate software testing procedures to ensure quality products.

Essential Questions (3-5)

1) What is Python program language?
2) How is Python used for automation?
3) Why is Python programming needed in the Cisco environment?

Anchor Text(s)
Cisco Network Academy PCAP – Programming Essentials in Python
Short & Informational Texts (3-5)
ARTICLES Introduction to network programming in Python https://code.tutsplus.com/tutorials/introduction-to-network-programming-in-python--cms-30459 Networks and Python https://www.pythonforbeginners.com/network/ Python for Network Administrators https://pynet.twb-tech.com/
Expected Proficiencies/Career and Life Skills
• Create basic programs in Python • Use iterative programming code • Solve and troubleshoot coding error problems • Create a program using turtle
Formative & Summative Assessments
• TestOut Module quizzes (Formative) • TestOut lab simulations (Formative) • Section assignments/activities (Formative) • Module review packets (Summative) • Comprehensive module tests (Summative) • Practical scenario assessments (Real world labs) (Summative) • Trimester projects (Summative) • Trimester exam (Summative)
Resources (Websites, LMS, Google Classroom, documents, etc.)
• Testout's LabSim • Canvas LMS • Google Drive/Docs/Slides

- Microsoft PowerPoint
- Microsoft Word
- Instructional Videos
- Wikis
- Infographics (www.piktochart.com)
- Review Game websites (i.e. www.classtools.net)
- Knowledgebase
- Technical forums
- Microsoft Visio
- YouTube videos
- Raspberry Pi

III. Instructional Strategies:

- Lecture
- Instructional videos (YouTube, TestOut's LabSim)
- Instructional demos (LabSim)
- Lab simulations (LabSim)
- Class discussions
- Slide shows and other visual data
- Strategy games to enhance critical thinking
- Collaborative hands-on projects
- Researching information
- Technical writing
- Debating
- Role-playing scenarios
- Answering questions
- Extrapolating data

- Differentiated instruction
    - Students will be placed into lab groups based on a pre-assessment. Each group will be a mix of students with some/little experience to students with more experience.
    - At times, students will collaborate to solve real-world scenarios. Each student will bring his/her own strength to the group and assist others who are not as strong in a particular area. This balance will help them solve real-world problems in the IT world.
    - Through lectures, hands-on scenarios, simulations, video demos, and SMART Board interactions, the students will be exposed to a variety of teaching methods that appeal to auditory, visual, and kinesthetic learners.

IV. Methods of Student Evaluation:

Assessment in a vocational area can be divided into four general categories—formal (graded), informal (ungraded), certification, and practical application.

Formal Assessments:

- Module quizzes
- Do-Now quizzes
- Section assignments or activities
- Lab Reports
- Oral presentations
- Lab simulations
- Tests

Some of the informal assessments include, but are not limited to:

- Daily closure discussion – At the end of each day, the instructor and students discuss the day's topic and provide insight and ask questions
- Canvas Collaborations – Students are always working in groups. At the end of lab time, students are to exchange information, project data, lab reports, et al with their group members via Canvas or Google.

Certification (Summative, counts as Exam grade) –

Practical application is the most important component to any vocational area. It demonstrates that a student can put the learned information into action by applying it in a real-world scenario. Some practical application assessments include, but are not limited to:

- Real world labs – Students will perform hands-on activities with the equipment based on a given set of instructions. Upon completion, they must develop a lab report summarizing their findings.
- Professional performance – While academics and discipline are separate entities, they are conjunctive in this shop because acting in a professional manner during lab is of paramount importance. Therefore, students will be assessed on their behavior in the lab.
- Projects – There will be a project each trimester. Successful completion of the project demonstrates that the students can practically apply most (or all) of the unit's concepts.

VI. Scope and Sequence

I = Introduce **D = Develop** **R = Reinforce** **M = Master**	
Act as a responsible and contributing citizen and employee.	D, R
Apply appropriate academic and technical skills.	D, R
Communicate clearly and effectively and with reason.	D, R
Utilize critical thinking to make sense of problems and persevere in solving them.	D, R

Use technology to enhance productivity.	D, R
Work productively in teams while using cultural global competence.	D, R
Demonstrate effective professional communication skills and practices that enable positive customer relationships.	D, R
Demonstrate positive cyber citizenry by applying industry accepted ethical practices and behaviors.	D. R
Describe trends in emerging and evolving computer technologies and their influence on IT practices.	D, R
Perform standard computer backup and restore procedures to protect IT information.	D, R
Recognize and analyze potential IT security threats to develop and maintain security requirements.	D, R
Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.	D, R
Compare key functions and applications of software and determine maintenance strategies for computer systems.	R, M

Analyze customer software needs and requirements.	R
Program a computer application using the appropriate programming language.	D, R
Analyze customer or organizational network system needs and requirements.	R
Analyze wired and wireless network systems to determine if they meet specifications (e.g., IEEE, power and security).	D, R
Design a network system using technologies, tools and standards.	D, R
Perform network system installation and configuration.	D, R
Perform network administration, monitoring and support to maintain a network system.	D, R
Analyze customer software needs and requirements	I , R
Demonstrate the use of industry standard strategies and project planning to meet customer specifications.	I, R
Analyze system and software requirements to ensure maximum operating efficiency	I , R
Demonstrate the effective use of software development tools to develop software applications.	I, R

Apply an appropriate software development process to design a software application.	I, R
Program a computer application using the appropriate programming language.	I, R
Demonstrate software testing procedures to ensure quality products.	I, R
Design, create and maintain a database.	I, R, D, M

VII. Course Textbooks, Instructional Resources & Software Student Resources

TestOut's LabSim Security Pro: http://www.testout.com/

- Fact sheets (notes)
- Video lessons
- Video demonstrations
- Lab simulations
- Formative assessments
- Practice exams
- Simulated sandbox environment
- Certification program

Microsoft Visio

- Industry standard software for IT blueprints

Cisco Packet Tracer

- Industry standard software for designing mock networks
- Simulates real world packet transmissions and routing
- Simulates real world TCP/IP configuration and network management

Cisco Networking Academy

- PCAP – Programming Essentials in Python
- CCNA Routing and Switching Essentials
- CCNA Routing and Switching “Intro to networks”
- Cybersecurity Essentials
- Mobility Fundamentals
- Entrepreneurship

VIII. Student Handout

This course builds on the experience students have gained in the first two years of Information Technology and Network Security, on how to maintain PCs and setup a corporate network. Now you will learn how to protect that network from a myriad of threats. Presenting the evolution of computer security, the main threats, attacks & mechanisms, security protocols, storage protection methods, cryptography, ways of identifying, understanding & recovery from attacks against computer systems. Additionally, various methods of security breach prevention, network systems availability, recovery procedures and counter systems penetrations techniques will be discussed.

PROFICIENCIES

A. Configure a security appliance
B. Install a security appliance
C. Explain penetration testing concepts
D. Explain use cases and purpose for frameworks, best practices and secure configuration guides
E. Compare identity and access management concepts
F. Analyze and record forensic evidence.
G. Explain risk management processes and concepts
H. Explain disaster recovery and continuity of operation concepts.
I. Configure Network Security Appliance access
J. Configure a remote access VPN
K. Configure a wireless network
L. Configure Windows Defender protections to secure a network from malware
M. Configure windows firewall
N. Configure GPO's to enforce security
O. Configure NTFS permissions
P. Secure an IPAD
Q. Create and link GPO's
R. Create basic programs in Python
S. Use iterative programming code
T. Solve and troubleshoot coding error problems
U. Create a program using turtle