CompTIA A+ 220-1101 (Core 1) & 220-1101 (Core 2) Exam Prep

A UWF Cybersecurity for All Course

Course Overview

Length of Completion: 40 contact hours

Prerequisites: None

Recommended Schedule: 8 Weeks + Exam Week

Learning Setting: Hybrid Asynchronous Online / Instructor-led Zoom sessions (weekly)

Target Audience: Entry-level IT practitioners (2+ year's experience recommended), college graduates, uniformed and civilian personnel subject to DoD Regulation 8570/8140.

Level of instruction: Undergraduate

Course Instructor:

Instructor	Email Address
Dr. Elizabeth Rasnick	erasnick@uwf.edu

Course Description

A+ certification is the vendor-neutral dominant entry-level IT certification – one million+ are already A+ certified. It is an ideal starting point for new career entrants, career changers but also existing PC Support technicians that want more credibility in order to achieve better employability and higher pay. Successful candidates will have the knowledge required to: Assemble components based on customer requirements, install, configure and maintain devices, PCs and software for end users, understand the basics of networking and security/forensics, properly and safely diagnose, resolve and document common hardware and software issues, apply troubleshooting skills, provide appropriate customer support, understand the basics of virtualization, desktop imaging, and deployment.

NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Cybersecurity Work Roles and Categories:

Operate and Maintain:
- Technical Support Specialist (OM-STS-001)
- Network Operations Specialist (OM-NET-001)
- System Administrator (OM-ADM-001)

Learning Outcomes mapped to the NICE Cybersecurity Workforce Framework Knowledge, Skills and Abilities (KSAs):

Upon completion of the course, students will be able to:
- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0004: Knowledge of cybersecurity and privacy principles.
- K0005: Knowledge of cyber threats and vulnerabilities.
- K0006: Knowledge of specific operational impacts of cybersecurity lapses.
- K0011: Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
- K0029: Knowledge of organization & Local and Wide Area Network connections.
- K0038: Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0088: Knowledge of systems administration concepts.
- K0100: Knowledge of the enterprise information technology (IT) architecture.
- K0104: Knowledge of Virtual Private Network (VPN) security.
- K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
- K0160: Knowledge of the common attack vectors on the network layer.
- K0167: Knowledge of system administration, network, and operating system hardening techniques.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0242: Knowledge of organizational security policies.
- K0260: Knowledge of Personally Identifiable Information (PII) data security standards.
- K0261: Knowledge of Payment Card Industry (PCI) data security standards.
- K0262: Knowledge of Personal Health Information (PHI) data security standards.
- K0287: Knowledge of an organization & information classification program and procedures for information compromise.
- K0292: Knowledge of the operations and processes for incident, problem, and event management.
- K0294: Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.
- K0317: Knowledge of procedures used for documenting and querying reported incidents, problems, and events.
- K0318: Knowledge of operating system command-line tools.

- S0040: Skill in implementing, maintaining, and improving established network security practices.
- S0076: Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
- S0077: Skill in securing network communications.
- S0079: Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
- S0084: Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
- S0158: Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).
- T0160: Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
- T0494: Administer accounts, network rights, and access to systems and equipment.

GRADING

The course is designed as examination preparation. Students should complete all assignments and take time to review any incorrect answers. Non-credit course students shall receive a grade of either complete or incomplete at the conclusion of the course. Participants must earn a total of 70% or higher on graded assessments to earn a course completion grade.

Students must register to take the certification exam during the first 10 days of the course and report their exam date(s) to their instructor. Students shall take the certification exam(s) within one week of course end date to receive a course completion certificate and digital badge. Each student will receive a voucher to take the exam and students who do not pass on the first attempt will be provided with additional resources and a second voucher.

Grading Scheme:

Assignment	Percentage of Grade
Exam Registration • Register for 220-1101 and 220-1102 Exams. • Submit Exam Date(s) to the Instructor. • Due no later than the 10th business day of the course.	10%
CompTIA Practice Assessments • Take 220-1001 and 220-1002 Practice Exams. • Submit a full Score Report pdf.	20%
Assignments • Quizzes • Practice Tests	20%
Online Labs • CompTia CertMaster Labs • CompTia PBQs • Test Out Labs • Test Out Practice Questions	30%
Final CompTIA Practice Assessment • Core 1 • Core 2	20%
Total	**100%**

Course Details

- Course includes online curriculum, instructor videos, online labs, quizzes, practice tests, and problem-based questions like those used on the A+ exam.
- Students receive a voucher for testing.
- If you have a disability that impacts your full participation in this course, please contact the Student Accessibility Resources at 850-474-2387 or by email, sar@uwf.edu

Course Outline

CompTIA A+ Certification Exam 220-1101 (Core 1)

Domain	Percentage of Examination
1.0 Mobile Devices	14%
2.0 Networking	20%
3.0 Hardware	27%
4.0 Virtualization and Cloud Computing	12%
5.0 Hardware & Network Troubleshooting	27%
Total	**100%**

CompTIA A+ Certification Exam 220-1102 (Core 2)

Domain	Percentage of Examination
1.0 Operating Systems	27%
2.0 Security	24%
3.0 Software Troubleshooting	26%
4.0 Operational Procedures	23%
Total	**100%**

Core 1

Week 1 (February 5 - 11) Mobile Devices Domain

1. Given a scenario, install and configure laptop hardware and components
2. Given a scenario, install components within the display of a laptop
3. Given a scenario, use appropriate laptop features
4. Compare and contrast accessories & ports of other mobile devices
5. Given a scenario, connect and configure accessories and ports of other mobile devices
6. Given a scenario, configure basic mobile device network connectivity and application support
7. Given a scenario, use methods to perform mobile device synchronization

Week 2 (February 12 - 18) Networking Domain

1. Compare and contrast TCP and UDP ports, protocols, and their purposes
2. Compare and contrast common networking hardware devices
3. Given a scenario, install and configure a basic wired/wireless SOHO network
4. Compare and contrast wireless networking protocols
5. Summarize the properties and purposes of services provided by networked hosts
6. Explain common network configuration concepts

7. Compare and contrast Internet connection types, network types, and their features
8. Given a scenario, use appropriate networking tools

Week 3 (February 19 - 25)

Hardware Domain

1. Explain basic cable types, features, and their purposes
2. Identify common connector types
3. Given a scenario, install RAM types
4. Given a scenario, select, install and configure storage devices
5. Given a scenario, install and configure motherboards, CPUs, and add-on cards
6. Explain the purposes and uses of various peripheral types
7. Summarize power supply types and features
8. Given a scenario, select and configure appropriate components for a custom PC configuration to meet customer specifications or needs
9. Given a scenario, install and configure common devices
10. Given a scenario, configure SOHO multifunction devices/printers and settings
11. Given a scenario, install and maintain various print technologies

Virtualization and Cloud Computing Domain

1. Compare and contrast cloud computing concepts
2. Given a scenario, set up and configure client-side virtualization

Week 4 (February 26 - March 3) Hardware and Network Troubleshooting Domain

1. Given a scenario, use the best practice methodology to resolve problems
2. Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools
3. Given a scenario, troubleshoot hard drives and RAID arrays
4. Given a scenario, troubleshoot video, projector and display issues
5. Given a scenario, troubleshoot and repair common mobile device issues while adhering to the appropriate procedures
6. Given a scenario, troubleshoot printers
7. Given a scenario, troubleshoot common wired and wireless network problems

Core 2

Week 5 (March 4 - 10) Operating Systems Domain

1. Compare and contrast common operating system types and their purposes
2. Compare and contrast features of Microsoft Windows versions
3. Summarize general OS installation considerations and upgrade methods
4. Given a scenario, use appropriate Microsoft command line tools
5. Given a scenario, use appropriate Microsoft operating system features and tools
6. Given a scenario, use Windows Control Panel utilities
7. Summarize application installation and configuration concepts
8. Given a scenario, configure Microsoft Windows networking on a client/desktop
9. Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems

Week 6 (March 11 - 17) Security Domain

1. Summarize the importance of physical security measures
2. Explain logical security concepts
3. Compare and contrast wireless security protocols and authentication methods
4. Given a scenario, detect, remove, and prevent malware using appropriate tools and methods
5. Compare and contrast social engineering, threats, and vulnerabilities
6. Compare and contrast the differences of basic Microsoft Windows OS security settings
7. Given a scenario, implement security best practices to secure a workstation
8. Given a scenario, implement methods for securing mobile devices
9. Given a scenario, implement appropriate data destruction and disposal methods
10. Given a scenario, configure security on SOHO wireless and wired networks

Week 7 (March 18 - 24) Software Troubleshooting Domain

1. Given a scenario, troubleshoot Microsoft Windows OS problems
2. Given a scenario, troubleshoot and resolve PC security issues
3. Given a scenario, use best practice procedures for malware removal
4. Given a scenario, troubleshoot mobile OS and application issues
5. Given a scenario, troubleshoot mobile OS and application security issues

Week 8 (March 25 - 31) Operational Procedures Domain

1. Compare and contrast best practices associated with types of documentation
2. Given a scenario, implement basic change management best practices
3. Given a scenario, implement basic disaster prevention and recovery methods
4. Explain common safety procedures
5. Explain environmental impacts and appropriate controls
6. Explain the processes for addressing prohibited content/ activity, and privacy, licensing, and policy concepts
7. Given a scenario, use proper communication techniques and professionalism
8. Identify the basics of scripting
9. Given a scenario, use remote access technologies.

Week 9 (April 1 - 5) Exam Week

1. Take the 220-1101 (Core 1) and 220-1102 (Core 2) exams.
2. Report scores to Instructor.