Computer Networking Virtual Learning

ITE - 13.5 - BIOS/UEFI Security

May 1, 2020

Lesson: 5/1/2020

Objective/Learning Target:

- Configure BIOS/UEFI security

Focus Questions

- What is the difference between a user password and an administrator password in the BIOS/UEFI configuration?
- How can BIOS/UEFI passwords be circumvented on some systems?
- How does chassis intrusion detection help to secure the BIOS?
- How does a hard disk password differ from a BIOS/UEFI password? What happens to the hard disk password if the disk is moved to another system?
- What is the function of the TPM? Where is the TPM chip located?
- Which UEFI security feature ensures that firmware updates for the motherboard do not contain malware?
- Which UEFI security feature prevents the system from booting an operating system without a valid digital signature?

Learning Tasks

- Navigate to TestOut.com & log on using your credentials
- Navigate to PC Pro Chapter 13 - Security, Section 5 - BIOS/UEFI Security
- Review Vocabulary words for 13.5 before starting into Section
- Read Fact Sheets located in sections 13.5.3
- Watch videos located in sections 13.5.1, 13.5.2
- Complete Lab Simulation located in sections 13.5.4
- Answer/Review Practice Questions located in section 13.5.5

Time Breakdown

Videos = 17 Minutes
Fact Sheets = 5 minutes
Lab Sim = 5 minutes
Practice Questions = 5minutes
Total Time = 32 minutes

Reference: TestOut PC Pro Lesson Plan Document