Security Pro (V8)
Competency Assessment Objectives

Identity Management and Authentication

Manage Identity

- Manage Windows Local and Domain Users and Groups

- Manage Linux Users and Groups

- Manage Active Directory OUs

Harden Authentication

- Configure Account Policies

- Manage account password

- Secure Default and local accounts

- Configure and Link Group Policy Objects (GPO)

Physical and Network Security

Harden Physical Access

- Implement Physical Security

- Install and Configure a Security Appliance

- Install and Configure a Firewall

- Create and Configure a Demilitarized Zone (DMZ)

- Configure Network Address Translation (NAT)

Harden Network Devices

- Configure and Access a Switch

- Configure and Access a Wireless Network

- Configure and Access a Virtual Private Network (VPN)

- Harden a Wireless Network

CompTIA.

- Configure Router Security

- Bring Your Own Device (BYOD) Security.

- Create and Connect to a Virtual Local Area Network (VLAN)

Host and Application Defenses

Harden Computer Systems

- Configure File system Inheritance

- Configure Anti-virus Protection

- Configure NTFS Permissions

- Configure Windows Update

Implement Application Defenses

- Implement Application Whitelisting

- Implement Data Execution Prevention (DEP)

- Configure Web Application Security

- Configure Email Filters and Settings

- Configure Browser Settings

Implement Virtualization

- Create Virtual Machines

- Create Virtual Switches

Data Security

Protect and Maintain Data files

- Perform data backups and recovery

- Implement redundancy

Implement Encryption Technologies

- Encrypt Data Communications

- Encrypt Files

- Manage Certificates

Audits and Security Assessments

Implement Logging and Auditing

- Configure Advanced Audit Policy

- Enable Device Logs

Assessment Techniques

- Implement Intrusion Detection

- Identify Social Engineering

- Scan for Vulnerabilities

- Analyze Network Attacks

- Analyze Password Attacks