Cybersecurity & Networking Competency Profile

Computer Hardware

Introduction to Personal Computer Hardware

1.1 Utilize personal computer safety procedures.
1.2 Install and configure the features and functions of computer components.
1.3 Disassemble a PC.

PC Assembly

2.1 Build a computer.

Advanced Computer Hardware

3.1 Configure BIOS and UEFI settings.
3.2 Explain electrical power.
3.3 Explain advanced computer functionality.
3.4 Select components to upgrade a computer to meet requirements.
3.5 Explain safe disposal methods to protect the environment.

Preventive Maintenance and Troubleshooting

4.1 Explain why preventive maintenance must be performed on personal computers.
4.2 Troubleshoot problems with PC and peripheral devices.

Networking Concepts

5.1 Analyze components and types of computer networks.
5.2 Analyze networking protocols, standards and services.
5.3 Analyze the purpose of devices on a network.
5.4 Explain the characteristics of network cables.

Applied Networking

6.1 Configure devices for wired and wireless networks.
6.2 Troubleshoot a network.

Laptops and Other Mobile Devices

7.1 Explain the features and functions of laptops and other mobile devices.
7.2 Explain how to configure laptop power settings and wireless settings.
7.3 Explain how to remove and install laptop components.
7.4 Describe the purpose and characteristics of other mobile devices.
7.5 Explain how to configure network connectivity and email on mobile devices.
7.6 Explain common preventive maintenance techniques for laptops and other mobile devices.
7.7 Explain how to troubleshoot laptops and other mobile devices.

Printers

8.1 Explain the purpose and characteristics of different types of printers.
8.2 Compare different types of printers.
8.3 Install a printer.
8.4 Configure printer sharing.
8.5 Implement preventive maintenance and troubleshooting techniques on printers.

Virtualization and Cloud Computing

9.1 Install a virtual machine on a computer.
9.2 Compare cloud computing concepts.

Computer Software

Windows Installation

10.1 Explain operating system requirements.
10.2 Create a partition in Windows using the Disk Management Utility.
10.3 Install a Windows operating system.

Windows Configuration

11.1 Configure the Windows Desktop and File Explorer.
11.2 Configure Windows using Control Panels.
11.3 Use Windows tools and utilities to manage Windows systems.
11.4 Use Microsoft Windows command line tools.
11.5 Configure a Windows computer to work on a network.
11.6 Use common preventive maintenance techniques for Microsoft Windows operating systems.
11.7 Troubleshoot Microsoft Windows operating systems.

Mobile, Linux, and macOS Operating Systems

12.1 Explain the purpose and characteristics of mobile operating systems.
12.2 Explain methods for securing mobile devices.
12.3 Explain the purpose and characteristics of Mac and Linux operating systems.
12.4 Explain how to troubleshoot other operating systems.

Security

13.1 Explain security threats.
13.2 Explain security procedures.
13.3 Configure basic security settings and policies for end devices.
13.4 Configure wireless security.
13.5 Explain how to troubleshoot basic security problems.

The IT Professional

14.1 Use good communication skills as a part of IT work.
14.2 Explain how to manage change and unplanned disruptions in a business environment.
14.3 Explain appropriate behavior when faced with the legal and ethical issues that arise in the IT industry.
14.4 Explain the call center environment and technician responsibilities.

Cybersecurity & Networking Competency Profile

Networking

Networking Today

1.1 Explain how networks affect our daily lives.
1.2 Explain how host and network devices are used.
1.3 Explain network representations and how they are used in network topologies.
1.4 Compare the characteristics of common types of networks.
1.5 Explain how LANs and WANs interconnect to the internet.
1.6 Describe the four basic requirements of a reliable network.
1.7 Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.
1.8 Identify some basic security threats and solutions for all networks.
1.9 Explain employment opportunities in the networking field.

Basic Switch and End Device Configuration

2.1 Explain how to access a Cisco IOS device for configuration purposes.
2.2 Explain how to navigate Cisco IOS to configure network devices.
2.3 Describe the command structure of Cisco IOS software.
2.4 Configure a Cisco IOS device using CLI.
2.5 Use IOS commands to save the running configuration.
2.6 Explain how devices communicate across network media.
2.7 Configure a host device with an IP address.
2.8 Verify connectivity between two end devices.

Protocols and Models

3.1 Describe the types of rules that are necessary to successfully communicate.
3.2 Explain why protocols are necessary in network communication.
3.3 Explain the purpose of adhering to a protocol suite.
3.4 Explain the role of standards organizations in establishing protocols for network interoperability.
3.5 Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
3.6 Explain how data encapsulation allows data to be transported across the network.
3.7 Explain how local hosts access local resources on a network.

Physical Layer

4.1 Describe the purpose and functions of the physical layer in the network.
4.2 Describe characteristics of the physical layer.
4.3 Identify the basic characteristics of copper cabling.
4.4 Explain how UTP cable is used in Ethernet networks.
4.5 Describe fiber-optic cabling and its main advantages over other media.
4.6 Connect devices using wired and wireless media.

Number Systems

5.1 Calculate numbers between decimal and binary systems.

5.2 Calculate numbers between decimal and hexadecimal systems.

Data Link Layer

6.1 Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.

6.2 Compare the characteristics of media access control methods on WAN and LAN topologies.

6.3 Describe the characteristics and functions of the data link frame.

Ethernet Switching

7.1 Explain how the Ethernet sublayers are related to the frame fields.

7.2 Describe the Ethernet MAC address.

7.3 Explain how a switch builds its MAC address table and forwards frames.

7.4 Describe switch forwarding methods and port settings available on Layer 2 switch ports.

Network Layer

8.1 Explain how the network layer uses IP protocols for reliable communications.

8.2 Explain the role of the major header fields in the IPv4 packet.

8.3 Explain the role of the major header fields in the IPv6 packet.

8.4 Explain how network devices use routing tables to direct packets to a destination network.

8.5 Explain the function of fields in the routing table of a router.

Address Resolution

9.1 Compare the roles of the MAC address and the IP address.

9.2 Describe the purpose of ARP.

9.3 Describe the operation of IPv6 neighbor discovery.

Basic Router Configuration

10.1 Configure initial settings on a Cisco IOS router.

10.2 Configure two active interfaces on a Cisco IOS router.

10.3 Configure devices to use the default gateway.

IPv4 Addressing

11.1 Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.

11.2 Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.

11.3 Explain public, private, and reserved IPv4 addresses.

11.4 Explain how subnetting segments a network to enable better communication.

11.5 Calculate IPv4 subnets for a /24 prefix.

11.6 Calculate IPv4 subnets for a /16 and /8 prefix.

11.7 Given a set of requirements for subnetting, implement an IPv4 addressing scheme.

11.8 Explain how to create a flexible addressing scheme using variable length subnet masking (VLSM).

11.9 Implement a VLSM addressing scheme.

IPv6 Addressing

12.1 Explain the need for IPv6 addressing.
12.2 Explain how IPv6 addresses are represented.
12.3 Compare types of IPv6 network addresses.
12.4 Explain how to configure static global unicast and link- local IPv6 network addresses.
12.5 Explain how to configure global unicast addresses dynamically.
12.6 Configure link-local addresses dynamically.
12.7 Identify IPv6 addresses.
12.8 Implement a subnetted IPv6 addressing scheme.

ICMP

13.1 Explain how ICMP is used to test network connectivity.
13.2 Use ping and traceroute utilities to test network connectivity.

Transport Layer

14.1 Explain the purpose of the transport layer in managing the transportation of data in end-to-end communication.
14.2 Explain characteristics of the TCP.
14.3 Explain characteristics of the UDP.
14.4 Explain how TCP and UDP use port numbers.
14.5 Explain how TCP session establishment and termination processes facilitate reliable communication.
14.6 Explain how TCP protocol data units are transmitted and acknowledged to guarantee delivery.
14.7 Describe the UDP client processes to establish communication with a server.

Application Layer

15.1 Explain how the functions of the application layer, session layer, and presentation layer work together to provide network services to end user applications.
15.2 Explain how end user applications operate in a peer-to- peer network.
15.3 Explain how web and email protocols operate.
15.4 Explain how DNS and DHCP operate.
15.5 Explain how file transfer protocols operate.

Network Security Fundamentals

16.1 Explain why basic security measures are necessary on network devices.
16.2 Identify security vulnerabilities.
16.3 Identify general mitigation techniques.
16.4 Configure network devices with device hardening features to mitigate security threats.

Build a Small Network

17.1 Identify the devices used in a small network.
17.2 Identify the protocols and applications used in a small network.
17.3 Explain how a small network serves as the basis of larger networks.
17.4 Use the output of the ping and tracert commands to verify connectivity and establish relative network performance.
17.5 Use host and IOS commands to acquire information about the devices in a network.
17.6 Describe common network troubleshooting methodologies.
17.7 Troubleshoot issues with devices in the network.

Cybersecurity & Networking Competency Profile

Cybersecurity

Cybersecurity: A World of Experts and Criminals

1.1 Describe the common characteristics comprising the cybersecurity world.
1.2 Differentiate the characteristics of cyber criminals and cybersecurity specialists.
1.3 Compare how cybersecurity threats affect individuals, businesses, and organizations.
1.4 Describe the factors that lead to the spread and growth of cybercrime.
1.5 Describe the organizations and efforts committed to expanding the cybersecurity workforce.

The Cybersecurity Cube

2.1 Describe the three dimensions of the Cybersecurity Cube (McCumber Cube).
2.2 Describe the principles of confidentiality, integrity, and availability.
2.3 Differentiate the three states of data.
2.4 Compare the types of cybersecurity countermeasures.
2.5 Describe the ISO Cybersecurity Model.

Cybersecurity Threats, Vulnerabilities and Attacks

3.1 Differentiate the types of malware and malicious code.
3.2 Compare the different methods used in social engineering.
3.3 Compare different types of cyberattacks.

The Art of Protecting Secrets

4.1 Explain how encryption techniques protect confidentiality.
4.2 Describe how access control techniques protect confidentiality.
4.3 Describe the concept of obscuring data.

The Art of Ensuring Integrity

5.1 Explain processes used to ensure integrity.
5.2 Explain the purpose of digital signatures.
5.3 Explain the purpose of digital certificates.
5.4 Explain the need for database integrity enforcement.

The Five Nines Concept

6.1 Explain the concept of high availability.
6.2 Explain how high availability measures are used to improve availability.
6.3 Describe how an incident response plan improves high availability.
6.4 Describe how disaster recovery planning plays an important role in implementing high availability.

Protecting a Cybersecurity Domain

7.1 Explain how processes and procedures protect systems.
7.2 Explain how to protect servers on a network.
7.3 Explain how to implement security measures to protect network devices.
7.4 Explain how physical security measures are implemented to protect network equipment.

Becoming a Cybersecurity Specialist

8.1 Describe how cybersecurity domains are used within the CIA triad.
8.2 Explain how ethics provide guidance.
8.3 Explain how to take the next step to become a cybersecurity professional

Introduction to Ethical Hacking and Penetration Testing

9.1 Explain the importance of ethical hacking and penetration testing.
9.2 Explain different penetration testing methodologies and frameworks.
9.3 Configure a virtual machine for your penetration testing learning experience.

Planning and Scoping a Penetration Testing Assessment

10.1 Explain the role of governance, risk, compliance, and environmental factors in planning penetration testing.
10.2 Create a penetration test scope and plan document that addresses organizational requirements for penetration testing services.
10.3 Create your personal code of conduct to provide professionalism and integrity in your ethical hacking practice.

Information Gathering and Vulnerability Scanning

11.1 Perform passive reconnaissance activities.
11.2 Perform active reconnaissance activities.
11.3 Perform vulnerability scans.
11.4 Analyze the results of reconnaissance exercises.

Social Engineering Attacks

12.1 Explain how pretexting is used in social engineering attacks.
12.2 Explain different types of social engineering attacks.
12.3 Explain different types of physical attacks.
12.4 Explain how social engineering attack tools facilitate attacks.
12.5 Explain how social engineering attacks enlist user participation.

Exploiting Wired and Wireless Networks

13.1 Explain how to exploit network-based vulnerabilities.
13.2 Explain how to exploit wireless vulnerabilities.

Exploiting Application-Based Vulnerabilities

14.1 Explain common web application attacks.
14.2 Describe common web application testing tools.
14.3 Explain how business logic flows enable attackers to exploit web applications.
14.4 Use tools to conduct injection attacks.
14.5 Use tools to exploit authentication-based vulnerabilities.
14.6 Explain how authorization-based vulnerabilities are exploited.
14.7 Explain cross-site scripting vulnerabilities.
14.8 Explain cross-site request forgery (CSRF/XSRF) and server-side request forgery attacks.
14.9 Explain clickjacking.
14.11 Explain how file inclusion vulnerabilities are exploited.
14.12 Explain how to exploit insecure code.

Cloud, Mobile, and IoT Security

15.1 Explain how to attack cloud technologies.

15.2 Explain common attacks against specialized systems.

Performing Post-Exploitation Techniques

16.1 Explain how to create a foothold and maintain persistence after compromising a system.

16.2 Explain how to perform lateral movement, detection avoidance, and enumeration.

Reporting and Communication

17.1 Describe the major components of a written pentest report.

17.2 Recommend appropriate remediation based on the findings of a pentesting campaign.

17.3 Explain the components necessary for communications during the pentest process.

17.4 Explain necessary processes to complete the pentesting engagement.

Tools and Code Analysis

18.1 Analyze code for pentesting use.

18.2 Classify pentesting tools by their primary use cases.