**1. Which of the following firewalls hides or masquerades the private addresses of network hosts?**

* Reverse proxy firewall
* Host-based firewall
* Proxy server
* **Network address translation firewall**
* Network layer firewall

**2. Carrying out a multi-phase, long-term, stealthy and advanced operation against a specific target is often referred to as what?**

* **Advanced persistent threat**
* Network sniffing
* Social engineering
* Script kiddies
* Rainbow tables

**3. You are configuring access settings to require employees in your organization to authenticate first before accessing certain web pages. Which requirement of information security is addressed through this configuration?**

* Scalability
* Availability
* Integrity
* **Confidentiality**

**Explanation:** Confidentiality is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes. Methods to ensure confidentiality include data encryption, identity proofing and two factor authentication.

**4. What are the objectives of ensuring data integrity? (Choose two correct answers)**

* **Data is unaltered during transit**
* **Data is not changed by unauthorized entities**
* Data is encrypted while in transit and when stored on disks
* Access to the data is authenticated
* Data is available all the time

**Explanation:** The objectives for data integrity include data not being altered during transit and not being changed by unauthorized entities. Authentication and encryption are methods to ensure confidentiality. Data being available all the time is the goal of availability.

**5. An organization is experiencing overwhelming visits to a main web server. You are developing a plan to add a couple of more web servers for load balancing and redundancy. Which requirement of information security is addressed by implementing the plan?**

* Scalability
* Integrity
* Confidentiality
* **Availability**

**6. What of the following are examples of cracking an encrypted password? (Choose four correct answers)**

* Intimidation
* **Brute force attack**
* Network sniffing
* **Rainbow tables**
* Social engineering
* **Spraying**
* **Dictionary attack**

**7. Improper management of physical access to a resource, such as a file, can lead to what type of security vulnerability?**

* Weaknesses in security practices
* Race conditions
* **Access control problems**
* Buffer overflow
* Non-validated input

**8. A medical office employee sends emails to patients about their recent visits to the facility. What information would put the privacy of the patients at risk if it was included in the email?**

* Contact information
* Next appointment
* **Patient records**
* First and last name

**9. What is the best way to avoid getting spyware on a machine?**

* Install the latest antivirus updates
* Install the latest web browser updates
* **Install software only from trusted websites**
* Install the latest operating system updates

**10. You are surfing the Internet using a laptop at a public Wi-Fi cafe. What should you check first before you connect to the public network?**

* That the Bluetooth adapter is disabled
* **If the laptop requires user authentication for file and media sharing**
* That the laptop web browser is operating in private mode
* If the laptop has a master password set to secure the passwords stored in the password manager

**Explanation:** You should always verify that your device isn’t configured with file and media sharing and that it requires user authentication with encryption.

**11. What is the main function of the Cisco Security Incident Response Team?**

* To design next generation routers and switches that are less prone to cyber attacks
* To design polymorphic malware
* **To ensure company, system and data preservation**
* To provide standards for new encryption techniques

**12. Which of the following firewalls are placed in front of web services to protect, hide, offload and distribute access to web servers?**

* Application layer firewall
* Proxy server
* Transport layer firewall
* Network layer firewall
* **Reverse proxy server**

**Explanation:** Placed in front of web servers, reverse proxy servers protect, hide, offload and distribute access to web servers.

**13. Which of the following certifications meets the U.S. Department of Defense Directive 8570.01-M requirements, which is important for anyone looking to work in IT security for the federal government?**

* EC Council Certified Ethical Hacker
* Microsoft Technology Associate Security Fundamentals
* ISACA CSX Cybersecurity Fundamentals
* **CompTIA Security+**
* ISC2 Certified Information Systems Security Professional
* Palo Alto Networks Certified Cybersecurity Associate

**Explanation:** This is an entry-level security certification that meets the U.S. Department of Defense Directive 8570.01-M requirements, which is an important item for anyone looking to work in IT security for the federal government.

**14. One of your colleagues has lost her identification badge. She is in a hurry to get to a meeting and does not have time to visit Human Resources to get a temporary badge. You lend her your identification badge until she can obtain a replacement.**  
**Is this behavior ethical or unethical?**

* Ethical
* **Unethical**

**15. Which of the following certifications tests your understanding and knowledge in how to look for weaknesses and vulnerabilities in target systems using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner?**

* Palo Alto Networks Certified Cybersecurity Associate
* ISC2 Certified Information Systems Security Professional
* Microsoft Technology Associate Security Fundamentals
* CompTIA Security+
* ISACA CSX Cybersecurity Fundamentals
* **EC Council Certified Ethical Hacker**

**Explanation:** This certification tests your understanding and knowledge of how to look for weaknesses and vulnerabilities in target systems using the same knowledge and tools as a malicious hacker but in a lawful and legitimate manner.

**16. What is the main purpose of cyberwarfare?**

* To develop advanced network devices
* **To gain advantage over adversaries**
* To protect cloud-based data centers
* To simulate possible war scenarios among nations

**Explanation:** The main reason for resorting to cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

**17. What vulnerability occurs when the output of an event depends on ordered or timed outputs?**

* Weaknesses in security practices
* Non-validated input
* **Race conditions**
* Buffer overflow
* Access control problems

**18. What do you call the vulnerabilities discovered by Google security researchers that affect almost all CPUs released since 1995? (Select two correct answers)**

* Shell shock
* WannaCry
* NotPetva
* **Spectre**
* **Meltdown**

**19. If developers attempt to create their own security algorithms, it will likely introduce what type of vulnerabilities?**

* Buffer overflow
* Race conditions
* **Weaknesses in security practices**
* Non-validated input
* Access control problems

**Explanation:** Systems and sensitive data can be protected through techniques such as authentication, authorization and encryption. Developers should stick to using security techniques and libraries that have already been created, tested and verified and should not attempt to create their own security algorithms. These will only likely introduce new vulnerabilities.

**20. Which technology creates a security token that allows a user to log in to a desired web application using credentials from a social media website?**

* **Open authorization**
* VPN service
* Password manager
* In-private browsing mode3

**Explanation:** Open Authorization is an open standard protocol that allows end users to access third party applications without exposing their user passwords.

**21. Which of the following security implementations use biometrics? (Choose two correct answers)**

* **Fingerprint**
* Phone
* Credit card
* **Voice recognition**
* Fob

**22. Which of the following firewalls filters traffic based on source and destination IP addresses?**

* **Network layer firewall**
* Proxy server
* Application layer firewall
* Transport layer firewall
* Network address translation firewall

**23. Which of the following firewalls filters web content requests such as URLs and domain names?**

* Application layer firewall
* **Proxy server**
* Reverse proxy server
* Network layer firewall
* Network address translation firewall

**24. A port scan returns a ‘dropped’ response. What does this mean?**

* A service is listening on the port
* Connections to the port will be denied
* **There was no reply from the host**

**25. During a meeting with the Marketing department, a representative from IT discusses features of an upcoming product that will be released next year. Is this employee’s behavior ethical or unethical?**

* **Ethical**
* Unethical

**26. Which of the following is an entry-level certification for newcomers who are preparing to start their career in cybersecurity?**

* CompTIA Security+
* Microsoft Technology Associate Security Fundamentals
* ISC2 Certified Information Systems Security Professional
* ISACA CSX Cybersecurity Fundamentals
* EC Council Certified Ethical Hacker
* **Palo Alto Networks Certified Cybersecurity Associate**

**Explanation:** This is an entry-level certification for newcomers who are preparing to start their career in the cybersecurity field.

**27. ‘Cybersecurity certifications are a way for you to verify your skills and knowledge and can also boost your career.’ Is this statement true or false?**

* **True**
* False

**28. When describing malware, what is a difference between a virus and a worm?**

* A virus focuses on gaining privileged access to a device, whereas a worm does not.
* **A virus replicates itself by attaching to another file, whereas a worm can replicate itself independently.**
* A virus can be used to launch a DoS attack (but not a DDoS), but a worm can be used to launch both DoS and DDoS attacks.
* A virus can be used to deliver advertisements without user consent, whereas a worm cannot.

**Explanation:** Malware can be classified as follows:  
Virus (self-replicates by attaching to another program or file)  
Worm (replicates independently of another program)  
Trojan horse (masquerades as a legitimate file or program)  
Rootkit (gains privileged access to a machine while concealing itself)  
Spyware (collects information from a target system)  
Adware (delivers advertisements with or without consent)  
Bot (waits for commands from the hacker)  
Ransomware (holds a computer system or data captive until payment isreceived)

**29. An employee is laid off after fifteen years with the same organization. The employee is then hired by another organization within a week. In the new organization, the employee shares documents and ideas for products that the employee proposed at the original organization. Is the employee’s behavior ethical or unethical?**

* Ethical
* **Unethical**

**30. Which of the following firewalls filters traffic based on the user, device, role, application type and threat profile?**

* **Context aware application firewall**
* Host-based firewall
* Network address translation firewall
* Network layer firewall
* Application layer firewall

**31. What names are given to a database where all cryptocurrency transactions are recorded? (Select two correct answers)**

* **Blockchain**
* Table
* **Ledger﻿**
* Spreadsheet

**Explanation:** Cryptocurrency owners keep their money in encrypted, virtual ‘wallets.’ When a transaction takes place between the owners of two digital wallets, the details are recorded in a decentralized, electronic ledger or blockchain system. This means it is carried out with a degree of anonymity and is self-managed, with no interference from third parties such as central banks or government entities.

**32. Which of the following items are states of data? (Choose three correct answers)**

* **Storage**
* Text
* ASCII
* **Transmission**
* Binary
* **Processing**

**Explanation:** **Processing** refers to data that is being used to perform an operation such as updating a database record (data in process).  
**Storage** refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive or USB drive (data at rest).  
**Transmission** refers to data traveling between information systems (data in transit).

**33. ‘Internet-based cameras and gaming gear are not subject to security breaches.’**  
**Is this statement true or false?**

* True
* **False**

**34. What vulnerability occurs when data is written beyond the memory areas allocated to an application?**

* **Buffer overflow**
* Access control problems
* Race conditions
* Weaknesses in security practices
* Non-validated input

**35. An organization’s IT department reports that their web server is receiving an abnormally high number of web page requests from different locations simultaneously. What type of security attack is occurring?**

* Phishing
* Adware
* Social engineering
* **DDoS**
* Spyware

**36. Which of the following are commonly used port scanning applications? (Select two correct answers)**

* **Zenmap**
* Port number
* Sequence number
* **Nmap**

**37. What action will an IDS take upon detection of malicious traffic?**

* Block or deny all traffic
* **Create a network alert and log the detection**
* Drop only packets identified as malicious
* Reroute malicious traffic to a honeypot

**Explanation:** An IDS, or intrusion detection system, is a device that can scan packets and compare them to a set of rules or attack signatures. If the packets match attack signatures, then the IDS can create an alert and log the detection.

**38. Which of the following statements best describes cybersecurity?**

* It is the name of a comprehensive security application for end users to protect workstations from being attacked
* It is a standard-based model for developing firewall technologies to fight against cybercrime
* It is a framework for security policy development
* **It is an ongoing effort to protect Internet-connected systems and the data associated with those systems from unauthorized use or harm**

**39. ‘After a data breach, it’s important to educate employees, partners and customers on how to prevent future breaches.’ Is this statement true or false?**

* **True**
* False

**40. An employee points out a design flaw in a new product to the department manager. Is this employee’s behavior ethical or unethical?**

* **Ethical**
* Unethical

**41. ‘Data coming into a program should be sanitized, as it could have malicious content, designed to force the program to behave in an unintended way.’ This statement describes what security vulnerability?**

* Weaknesses in security practices
* Access control problems
* Buffer overflow
* **Non-validated input**
* Race conditions

**42. Which of the following are examples of on-path attacks? (Choose two correct answers)**

* SEO poisoning
* **Man-in-the-Mobile**
* Ransomware
* DDoS
* **Man-in-the-Middle**
* Worms

**43. Which of the following firewalls filters traffic based on application, program or service?**

* Context aware application firewall
* Proxy server
* **Application layer firewall**
* Host-based firewall
* Network layer firewall

**44. A port scan returns a ‘closed’ response. What does this mean?**

* There was no reply from the host
* A service is listening on the port
* **Connections to the port will be denied**

**45. ‘Cryptocurrency transactions are digital.’ Is this statement true or false?**

* **True**
* False

**46. What do you call a digital asset designed to work as a medium of exchange that uses strong encryption to secure a financial transaction?**

* Apple Pay
* Google Pay
* Near Field Communications
* **Cryptocurrency**

**47. Which of the following tools used for incident detection can be used to detect anomalous behavior, command and control traffic, and detect infected hosts? (Choose two correct answers)**

* **Intrusion detection system**
* Reverse proxy server
* **NetFlow**
* Nmap
* Honeypot

**48. What name is given to a group of bots, connected through the Internet, with the ability to be controlled by a malicious individual or group?**

* Hacker network
* Crime syndicate
* Zombie
* **Botnet**

**49. What is the best approach for preventing a compromised IoT device from maliciously accessing data and devices on a local network?**

* Install a software firewall on every network device
* **Place all IoT devices that have access to the Internet on an isolated network**
* Disconnect all IoT devices from the Internet
* Set the security settings of workstation web browsers to a higher level

**50. What name is given to the emerging threat that hides on a computer or mobile device and uses that machine’s resources to mine cryptocurrencies?**

* Phishing
* Bluejacking
* Cryptoransomware
* **Cryptojacking**

**51. A port scan returns an ‘open’ response. What does this mean?**

* **A service is listening on the port**
* Connections to the port will be denied
* There was no reply from the host

**52. An employee is at a restaurant with friends and tells them about an exciting new video game that is under development at the organization they work for. Is this employee’s behavior ethical or unethical?**

* Ethical
* **Unethical**

**53. ‘An advanced persistent threat (APT) is usually well funded.’ Is this statement true or false?**

* **True**
* False

**54. In networking, what name is given to the identifier at both ends of a transmission to ensure that the right data is passed to the correct application?**

* IP address
* **Port number**
* MAC address
* Sequence number

**55. ‘An employee does something as an organization representative with the knowledge of that organization and this action is deemed illegal. The organization is legally responsible for this action.’ Is this statement true or false?**

* **True**
* False

**56. What tool is used to lure an attacker so that an administrator can capture, log and analyze the behavior of the attack?**

* NetFlow
* **Honeypot**
* IDS
* Nmap

**57. ‘A data breach does not impact the reputation of an organization.’ Is this statement true or false?**

* True
* **False**

**58. Which of the following certifications is aimed at high school and early college students, as well as anyone interested in a career change?**

* CompTIA Security+
* **Microsoft Technology Associate Security Fundamentals**
* ISACA CSX Cybersecurity Fundamentals
* ISC2 Certified Information Systems Security Professional
* EC Council Certified Ethical Hacker
* Palo Alto Networks Certified Cybersecurity Associate

**59. Which of the following firewalls filters traffic based on source and destination data ports and filtering based on connection states?**

* Network address translation firewall
* Network layer firewall
* **Transport layer firewall**
* Application layer firewall
* Host-based firewall

**60. Which of the following are categories of security measures or controls? (Choose three correct answers)**

* Firewalls
* Guards
* Camera
* **Policy and procedure**
* **Technology**
* **Awareness, training and education**

**61. ‘A botnet can have tens of thousands of bots, or even hundreds of thousands.’ Is this statement true or false?**

* **True**
* False

**62. For what purpose would a network administrator use the Nmap tool?**

* To protect the private IP addresses of internal hosts
* To identify specific network anomalies
* **To detect and identify open ports**
* To collect and analyze security alerts and logs

**63. Which of the following certifications does not expire or require periodic recertification and is geared towards post-secondary graduates and those interested in a career change?**

* EC Council Certified Ethical Hacker
* **ISACA CSX Cybersecurity Fundamentals**
* CompTIA Security+
* Palo Alto Networks Certified Cybersecurity Associate
* ISC2 Certified Information Systems Security Professional
* Microsoft Technology Associate Security Fundamentals

**64. What type of attack uses zombies?**

* Spear phishing
* Trojan horse
* **DDoS**
* SEO poisoning

**Explanation:** A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources. For example:

* An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
* The zombie computers will constantly scan and infect more hosts, creating more and more zombies.
* When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

**65. What is the purpose of a backdoor?**

* To enable software vendors to update software
* For government access
* **To gain unauthorized access to a system without normal authentication procedures**
* To allow developers to debug software

**66. Which of the following firewalls filters ports and system service calls on a single computer operating system?**

* Network address translation firewall
* Transport layer firewall
* **Host-based firewall**
* Network layer firewall
* Application layer firewall

**67. What type of attack disrupts services by overwhelming network devices with bogus traffic?**

* **DDoS**
* Zero-day
* Brute force
* Port scans

**Explanation:** DDoS, or distributed denial of service, attacks are used to disrupt service by overwhelming network devices with bogus traffic.

**68. ‘Cryptocurrencies are handled on a centralized exchange.’ Is this statement true or false?**

* True
* **False**