[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Practice Final Exam Answers

1. A person coming to a cafe for the first time wants to gain wireless access to the Internet using a laptop. What is the first step the wireless client will do in order to communicate over the network using a wireless management frame?

- associate with the AP
- authenticate to the AP
- **discover the AP**
- agree with the AP on the payload

2. Refer to the exhibit. What is a valid address on the PC for the default gateway?

- 192.168.255.1
- 192.168.2.1
- **192.168.1.1**
- 192.168.0.1

3. A cybersecurity analyst believes that an attacker is announcing a forged MAC address to network hosts in an attempt to spoof the default gateway. Which command could the analyst use on the network hosts to see what MAC address the hosts are using to reach the default gateway?

- **arp -a**
- ipconfig /all
- netsat -r
- route print

4. Which management system implements systems that track the location and configuration of networked devices and software across an enterprise?

- risk management
- vulnerability management
- configuration management
- **asset management**

5. Refer to the exhibit. A cybersecurity analyst is viewing packets forwarded by switch S2. What addresses will identify frames containing data sent from PCA to PCB?

- Src IP: 192.168.2.1
  Src MAC: 00-60-0F-B1-33-33
  Dst IP: 192.168.2.101
  Dst MAC: 08-CB-8A-5C-BB-BB
- Src IP: 192.168.1.212
  Src MAC: 00-60-0F-B1-33-33
  Dst IP: 192.168.2.101
  Dst MAC: 00-D0-D3-BE-00-00
- **Src IP: 192.168.1.212**
  Src MAC: 00-60-0F-B1-33-33

Dst IP: 192.168.2.101
Dst MAC: 08-CB-8A-5C-BB-BB

- Src IP: 192.168.1.212
  Src MAC: 01-90-C0-E4-AA-AA
  Dst IP: 192.168.2.101
  Dst MAC: 08-CB-8A-5C-BB-BB

6. Which tool can be used in a Cisco AVC system to analyze and present the application analysis data into dashboard reports?

- NetFlow
- NBAR2
- **Prime**
- IPFIX

7. Which host-based firewall uses a three-profile approach to configure the firewall functionality?

- TCP Wrapper
- **Windows Firewall**
- nftables
- iptables

8. What are three functions provided by the syslog service? (Choose three.)

- to provide statistics on packets that are flowing through a Cisco device
- **to select the type of logging information that is captured**
- **to specify the destinations of captured messages**
- to periodically poll agents for data
- **to gather logging information for monitoring and troubleshooting**
- to provide traffic analysis

9. Which method can be used to harden a device?

- Allow users to re-use old passwords.
- **Force periodic password changes.**
- Allow USB auto-detection.
- Allow default services to remain enabled.

10. Refer to the exhibit. Which field in the Sguil event window indicates the number of times an event is detected for the same source and destination IP address?

- Pr
- **CNT**
- AlertID
- ST

11. A user successfully logs in to a corporate network via a VPN connection. Which part of the AAA process records that a certain user performed a specific operation at a particular date and time?

- access
- **accounting**
- authorization
- authentication

12. What is the responsibility of the IT support group when handling a security incident?

- Coordinate the incident response with other stakeholders and minimize the damage of the incident.
- Review the incident policies, plans, and procedures for local or federal guideline violations.
- **Perform actions to minimize the effectiveness of the attack and preserve evidence.**
- Perform disciplinary measures if an incident is caused by an employee.

13. Which Linux program is going to be used when installing an application?

- X Window System
- launcher
- **package manager**
- penetration tool

14. Refer to the exhibit. Which security issue would a cybersecurity analyst use the displayed tool?

- ARP cache poisoning
- DNS attack
- TCP attack
- **malware**

15. Which approach is intended to prevent exploits that target syslog?

- Use a VPN between a syslog client and the syslog server.
- **Use syslog-ng.**
- Use a Linux-based server.
- Create an ACL that permits only TCP traffic to the syslog server.

16. What would be the target of an SQL injection attack?

- **database**
- DHCP
- email
- DNS

18. Users report to the helpdesk that icons usually seen on the menu bar are randomly appearing on their computer screens. What could be a reason that computers are displaying these random graphics?

- A DoS attack has been launched against the network.
- The computers are subject to a reconnaissance attack.
- **A virus has infected the computers.**
- An access attack has occurred.

19. A disgruntled employee is using Wireshark to discover administrative Telnet usernames and passwords. What type of network attack does this describe?

- trust exploitation
- port redirection
- **reconnaissance**
- denial of service

20. Which two technologies are primarily used on peer-to-peer networks? (Choose two.)

- Darknet
- Snort
- **Bitcoin**
- **BitTorrent**
- Wireshark

21. Which value, that is contained in an IPv4 header field, is decremented by each router that receives a packet?

- Header Length
- Differentiated Services
- **Time-to-Live**
- Fragment Offset

22. What are two elements that form the PRI value in a syslog message? (Choose two.)

- **facility**
- **severity**
- header
- hostname
- timestamp

24. Refer to the exhibit. Which IPv4 address does the PC use for sending traffic to remote networks?

- 127.0.0.1
- 192.168.1.2
- **192.168.1.1**
- 192.168.1.255

25. Which two options are security best practices that help mitigate BYOD risks? (Choose two.)

- Decrease the wireless antenna gain level.
- **Only turn on Wi-Fi when using the wireless network.**
- Use wireless MAC address filtering.
- Only allow devices that have been approved by the corporate IT team.
- **Keep the device OS and software updated.**
- Use paint that reflects wireless signals and glass that prevents the signals from going outside the building.

26. What is an essential function of SIEM?

- forwarding traffic and physical layer errors to an analysis device
- providing 24×7 statistics on packets flowing through a Cisco router or multilayer switch
- monitoring traffic and comparing it against the configured rules
- **providing reporting and analysis of security events**

27. Which two statements describe the use of asymmetric algorithms? (Choose two.)

- If a public key is used to encrypt the data, a public key must be used to decrypt the data.
- If a private key is used to encrypt the data, a private key must be used to decrypt the data.
- Public and private keys may be used interchangeably.
- **If a private key is used to encrypt the data, a public key must be used to decrypt the data.**
- **If a public key is used to encrypt the data, a private key must be used to decrypt the data.**

28. Which statement describes the Cyber Kill Chain?

- **It identifies the steps that adversaries must complete to accomplish their goals.**
- It specifies common TCP/IP protocols used to fight against cyberattacks.
- It is a set of metrics designed to create a way to describe security incidents in a structured and repeatable way.
- It uses the OSI model to describe cyberattacks at each of the seven layers.

29. Why does a worm pose a greater threat than a virus poses?

- **Worms are more network-based than viruses are.**

- Worms are not detected by antivirus programs.
- Worms run within a host program.
- Worms directly attack the network devices.

30. Refer to the exhibit. Approximately what percentage of the physical memory is in use on this Windows system?

- **33%**
- 53%
- 67%
- 90%

31. Refer to the exhibit. A network security specialist is issuing the tail command to monitor the Snort alert in real time. Which option should be used in the command line to watch the file for changes?

- -c
- -q
- **-f**
- -n

32. A customer purchases an item from an e-commerce site. The e-commerce site must maintain proof that the data exchange took place between the site and the customer. Which feature of digital signatures is required?

- **nonrepudiation of the transaction**
- confidentiality of the public key
- integrity of digitally signed data
- authenticity of digitally signed data

33. A network security specialist is tasked to implement a security measure that monitors the status of critical files in the data center and sends an immediate alert if any file is modified. Which aspect of secure communications is addressed by this security measure?

- origin authentication
- **data integrity**
- nonrepudiation
- data confidentiality

34. What is the most common use of the Diffie-Helman algorithm in communications security?

- **to secure the exchange of keys used to encrypt data**
- to create password hashes for secure authentication
- to encrypt data for secure e-commerce communications
- to provide routing protocol authentication between routers

36. Which schema or model allows security professionals to enter data about a particular incident, such as victim demographics, incident description, discovery method and response, and impact assessment, and share that data with the security community anonymously?

- Diamond
- Cyber Kill Chain
- CSIRT
- **VERIS**

37. Which component in Linux is responsible for interacting directly with the device hardware?

- shell
- command interpreter
- **kernel**

- command line interface

38. A client device has initiated a secure HTTP request to a web browser. Which well-known port address number is associated with the destination address?

- 404
- **443**
- 110
- 80

39. A PC user issues the *netstat* command without any options. What is displayed as the result of this command?

- a historical list of successful pings that have been sent
- a local routing table
- a network connection and usage report
- **a list of all established active TCP connections**

40. How can statistical data be used to describe or predict network behavior?

- by listing results of user web surfing activities
- by displaying alert messages that are generated by Snort
- **by comparing normal network behavior to current network behavior**
- by recording conversations between network endpoints

41. A law office uses a Linux host as the firewall device for the network. The IT administrator is configuring the firewall iptables to block pings from Internet devices to the Linux host. Which iptables chain should be modified to achieve the task?

- INTERNET
- **INPUT**
- OUTPUT
- FORWARD

42. What is the main purpose of cyberwarfare?

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

43. Which statement describes the state of the administrator and guest accounts after a user installs Windows desktop version to a new computer?

- By default, both the administrator and guest accounts are enabled.
- **By default, both the administrator and guest accounts are disabled.**
- By default, the administrator account is enabled but the guest account is disabled.
- By default, the guest account is enabled but the administrator account is disabled.

45. Which two characteristics describe a virus? (Choose two.)

- Malware that executes arbitrary code and installs copies of itself in memory.
- A self-replicating attack that is independently launched.
- **Malware that relies on the action of a user or a program to activate.**
- Program code specifically designed to corrupt memory in network devices.
- **Malicious code that can remain dormant before executing an unwanted action.**

46. A technician has installed a third party utility that is used to manage a Windows 7 computer. However, the utility does not automatically start whenever the computer is started. What can the technician do to resolve this problem?

- Use the Add or Remove Programs utility to set program access and defaults.

- Uninstall the program and then choose Add New Programs in the Add or Remove Programs utility to install the application.
- Set the application registry key value to one.
- **Change the startup type for the utility to Automatic in Services.**

47. A security incident has been filed and an employee believes that someone has been on the computer since the employee left last night. The employee states that the computer was turned off before the employee left for the evening. The computer is running slowly and applications are acting strangely. Which Microsoft Windows tool would be used by the security analyst to determine if and when someone logged on to the computer after working hours?

- Task Manager
- **Event Viewer**
- PowerShell
- Performance Monitor

48. Which type of events should be assigned to categories in Sguil?

- **true positive**
- false positive
- true negative
- false negative

49. What information does an Ethernet switch examine and use to forward a frame?

- **destination MAC address**
- destination IP address
- source MAC address
- source IP address

51. Refer to the exhibit. A network security analyst is examining captured data using Wireshark. What is represented by the first three frames?

- request of a file from the client
- **TCP three-way handshake**
- UDP DNS request
- connectivity test between two hosts

52. The IT department is reporting that a company web server is receiving an abnormally high number of web page requests from different locations simultaneously. Which type of security attack is occurring?

- social engineering
- adware
- phishing
- **DDoS**
- spyware

53. How many host addresses are available on the 192.168.10.128/26 network?

- 30
- 32
- 60
- **62**
- 64

54. What are two types of attacks used on DNS open resolvers? (Choose two.)

- fast flux
- ARP poisoning

- **resource utilization**
- cushioning
- **amplification and reflection**

55. What are three access control security services? (Choose three.)

- **authentication**
- repudiation
- availability
- **accounting**
- **authorization**
- access

56. When dealing with security threats and using the Cyber Kill Chain model, which two approaches can an organization use to block a potential back door creation? (Choose two.)

- **Audit endpoints to discover abnormal file creations.**
- Establish an incident response playbook.
- **Use HIPS to alert or place a block on common installation paths.**
- Consolidate the number of Internet points of presence.
- Conduct damage assessment.

57. When a user visits an online store website that uses HTTPS, the user browser queries the CA for a CRL. What is the purpose of this query?

- to check the length of key used for the digital certificate
- to negotiate the best encryption to use
- **to verify the validity of the digital certificate**
- to request the CA self-signed digital certificate

58. Which term is used for describing automated queries that are useful for adding efficiency to the cyberoperations workflow?

- cyber kill chain
- **playbook**
- rootkit
- chain of custody

59. What is the result of a DHCP starvation attack?

- Clients receive IP address assignments from a rogue DHCP server.
- **Legitimate clients are unable to lease IP addresses.**
- The IP addresses assigned to legitimate clients are hijacked.
- The attacker provides incorrect DNS and default gateway information to clients.

60. In threat intelligence communications, which sharing standard is a specification for an application layer protocol that allows communication of cyberthreat intelligence over HTTPS?

- **Trusted automated exchange of indicator information (TAXII)**
- Structured threat information expression (STIX)
- Common vulnerabilities and exposures (CVE)
- Automated indicator sharing (AIS)