CCNA Cyber Ops (Version 1.1) – Chapter 11 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-11-exam-answers-full.html

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Which statement describes the tcpdump tool?

- **It is a command line packet analyzer.**
- It is used to control multiple TCP-based applications.
- It accepts and analyzes data captured by Wireshark.
- It can be used to analyze network log data in order to describe and predict network behavior.

A. The tcpdump command line tool is a popular packet analyzer. It can display packet captures in real time or write packet captures to a file.

2. Which Windows host log event type describes the successful operation of an application, driver, or service?

- Error
- Warning
- **Information**
- Success Audit

C. Various Windows host logs can have different event types. The Information event type records an event that describes the successful operation of an application, driver, or service.

3. A NIDS/NIPS has identified a threat. Which type of security data will be generated and sent to a logging device?

- **Alert**
- Session
- Statistical
- Transaction

A. Alert data is generated by IPS or IDS devices in response to traffic that violates a rule or matches the signature of a known security threat.

4. What is the purpose of Tor?

- To donate processor cycles to distributed computational tasks in a processor-sharing P2P network
- **To allow users to browse the Internet anonymously**
- To securely connect to a remote network over an unsecure link such as an Internet connection
- To inspect incoming traffic and look for any that violates a rule or matches the signature of a known exploit

B. Tor is a software platform and network of peer-to-peer (P2P) hosts that function as routers. Users access the Tor network by using a special browserthat allows them to browse anonymously.

5. Which statement describes an operational characteristic of NetFlow?

- NetFlow captures the entire contents of a packet.
- NetFlow can provide services for user access control.
- NetFlow flow records can be viewed by the tcpdump tool.
- **NetFlow collects metadata about the packet flow, not the flow data itself.**

D. NetFlow does not capture the entire contents of a packet. Instead, NetFlow collects metadata, or data about the flow, not the flow data itself. NetFlow information can be viewed with tools such as nfdump and FlowViewer.

6. Which type of security data can be used to describe or predict network behavior?

- Alert
- Session
- **Statistical**
- Transaction

C. Statistical data is created through the analysis of other forms of network data. Conclusions from these analyses can be used to describe or predict network behavior.

7. What type of server can threat actors use DNS to communicate with?

- **CnC**
- Database
- NTP
- Web

A. Some malware uses DNS to communicate with command-and-control (CnC) servers to exfiltrate data in traffic that is disguised as normal DNS query traffic.

8. In a Cisco AVC system, in which module is NBAR2 deployed?

- Control
- Metrics Collection
- **Application Recognition**
- Management and Reporting

C. AVC uses Cisco Next-Generation Network-Based Application Recognition (NBAR2) to discover and classify the applications in use on the network.

9. A security analyst reviews network logs. The data shows user network activities such as username, IP addresses, web pages accessed, and timestamp. Which type of data is the analyst reviewing?

- Alert
- Session
- Application
- **Transaction**

D. Transaction data focuses on the results of network sessions as reflected by the device logs kept by server processes, such as the details of a user's visit to a website.

10. Which type of server daemon accepts messages sent by network devices to create a collection of log entries?

- SSH
- NTP
- **Syslog**
- AAA

C. Syslog is important to security monitoring because network devices send periodic messages to the syslog server. These logs can be examined to detect inconsistencies and issues within the network.

11. Which Windows tool can be used to review host logs?

- Services
- **Event Viewer**
- Task Manager
- Device Manager

B. Event Viewer in Windows can be used to review entries in various logs.

12. Which two protocols may devices use in the application process that sends email? (Choose two.)

- HTTP
- **SMTP**
- POP
- IMAP
- **DNS**
- POP3

B, E. POP, POP3, and IMAP are protocols that are used to retrieve email from servers. SMTP is the default protocol that is used to send email. DNS may be used by the sender email server to find the address of the destination email server. HTTP is a protocol for send and receiving web pages.

13. How does using HTTPS complicate network security monitoring?

- HTTPS cannot protect visitors to a company-provided web site.
- HTTPS can be used to infiltrate DNS queries.
- Web browser traffic is directed to infected servers.
- **HTTPS adds complexity to captured packets.**

HTTPS adds extra overhead to the HTTP-formed packet. HTTPS encrypts using secure socket layer (SSL). Even though some devices can perform SSL decryption and inspection, this can present processing and privacy issues. HTTPS adds complexity to packet captures due to the additional message involved in establishing an encrypted data connection.

14. Which protocol is used to send e-mail messages between two servers that are in different e-mail domains?

- POP3
- **SMTP**
- HTTP
- IMAP4

SMTP is used to send data between mail servers and to send data from a host to a mail server. The other two protocols that can be used for email are IMAP and POP3. IMAP and POP3 are used to download email messages from a mail server.

15. What are two ways that ICMP can be a security threat to a company? (Choose two.)

- **by collecting information about a network**
- by corrupting network IP data packets
- **by providing a conduit for DoS attacks**

- by corrupting data between email servers and email recipients
- by the infiltration of web pages

ICMP can be used as a conduit for DoS attacks. It can be used to collect information about a network such as the identification of hosts and network structure, and by determining the operating systems being used on the network.

16. Which function is provided by the Sguil application?

- **It makes Snort-generated alerts readable and searchable.**
- It detects potential network intrusions.
- It reports conversations between hosts on the network.
- It prevents malware from attacking a host.

Applications such as Snorby and Sguil can be used to read and search alert messages generated by NIDS/NIPS.

17. Which two options are network security monitoring approaches that use advanced analytic techniques to analyze network telemetry data? (Choose two.)

- NetFlow
- Snorby
- **NBAD**
- **NBA**
- IPFIX
- Sguil

Network behavior analysis (NBA) and network behavior anomaly detection (NBAD) are approaches to network security monitoring that use advanced analytical techniques to analyze NetFlow or IPFIX network telemetry data.

18. A system administrator has recommended to the CIO a move of some applications from a Windows server to a Linux server. The proposed server will use ext4 partitions and serve as a web server, file server, and print server. The CIO is considering the recommendation, but has some questions regarding security.

18.a. Which two methods does Linux use to log data in order to identify a security event? (Choose two.)

- **Apache access logs**
- Event Viewer
- NetFlow
- SPAN
- **syslog**

The syslog standard is used for logging event messages from network devices. Syslog messages are sent from the device to a logging server. Apache web server access logs are an important source of information for a cybersecurity analyst in order to see who accessed the server, the IP address used, date/time of access, and URL used.

18.b. What is a daemon?

- **a background process that runs without the need for user interaction**
- a record to keep track of important events
- a type of security attack
- an application that monitors and analyzes suspicious activity

A daemon in Linux is a background process that runs without the need for user interaction. A network administrator can view log files in order to see information about daemons running on the Linux server.

18.c. Because the company uses discretionary access control (DAC) for user file management, what feature would need to be supported on the server?

- access based on security clearance held
- principle of least privilege
- role-based access control
- **user-based data access control**

Discretionary access control allows users to control access to their data as owners of that data. ACLs may also be used in order to specify which users or groups have access to the data.

18.d. What are two benefits of using an ext4 partition instead of ext3? (Choose two.)

- compatibility with CDFS
- compatibility with NTFS
- decreased load time
- **improved performance**
- an increase in the number of supported devices
- **increase in the size of supported files**

Based on the ex3 file system, an ext4 partition includes extensions that improve performance and an increase in the of supported files. An ext4 partition also supports journaling, a file system feature that minimizes the risk of file system corruption if power is suddenly lost to the system.

19. How can IMAP be a security threat to a company?

- It can be used to encode stolen data and send to a threat actor.

- **An email can be used to bring malware to a host.**
- Encrypted data is decrypted.
- Someone inadvertently clicks on a hidden iFrame.

IMAP, SMTP, and POP3 are email protocols. SMTP is used to send data from a host to a server or to send data between servers. IMAP and POP3 are used to download email messages and can be responsible for bringing malware to the receiving host.

20. A system administrator runs a file scan utility on a Windows PC and notices a file lsass.exe in the Program Files directory. What should the administrator do?

- Open the Task Manager, right-click on the lsass process and choose End Task.
- Uninstall the lsass application because it is a legacy application and no longer required by Windows.
- Move it to Program Files (x86) because it is a 32bit application.
- **Delete the file because it is probably malware.**

On Windows computers, security logging and security policies enforcement are carried out by the Local Security Authority Subsystem Service (LSASS), running as lsass.exe. It should be running from the Windows\System32 directory. If a file with this name, or a camouflaged name, such as 1sass.exe, is running or running from another directory, it could be malware.

21. How does a web proxy device provide data loss prevention (DLP) for an enterprise?

- by checking the reputation of external web servers
- by functioning as a firewall
- by inspecting incoming traffic for potential exploits
- **by scanning and logging outgoing traffic**

A web proxy device can inspect outgoing traffic as means of data loss prevention (DLP). DLP involves scanning outgoing traffic to detect whether the data that is leaving the enterprise network contains sensitive, confidential, or secret information.

22. A system analyst is reviewing syslog messages and notices that the PRI value of a message is 26. What is the severity value of the message?

- 1
- **2**
- 3
- 6

The priority (PRI) value consists of two elements, the facility and severity of the message. It is calculated by multiplying the facility value by 8, and then adding the severity value, that is, priority = (facility * 8) + severity. To find the severity value from a given PRI, divide the PRI by 8 and the remainder is the severity value.

23. Which statement describes session data in security logs?

- **It is a record of a conversation between network hosts.**
- It can be used to describe or predict network behavior.
- It reports detailed network activities between network hosts.
- It shows the result of network sessions.

Session data is a record of a conversation between two network endpoints.

24. In a Cisco AVC system, in which module is NetFlow deployed?

- Management and Reporting
- **Metrics Collection**
- Control
- Application Recognition

NetFlow technology is deployed in the Metrics Collection module of a Cisco AVC system to collect network flow metrics and to export to management tools.

25. What port number would be used if a threat actor was using NTP to direct DDoS attacks?

- 443
- 25
- 69
- **123**

NTP uses UDP port number 123. Threat actors could use port 123 on NTP systems in order to direct DDoS attacks through vulnerabilities in client or server software.

26. Which information can be provided by the Cisco NetFlow utility?

- IDS and IPS capabilities
- security and user account restrictions
- **peak usage times and traffic routing**
- source and destination UDP port mapping

NetFlow efficiently provides an important set of services for IP applications including network traffic accounting, usage-based network billing, network planning, security, denial of service monitoring capabilities, and network monitoring. NetFlow provides valuable

information about network users and applications, peak usage times, and traffic routing.

27. What is Tor?

- a type of Instant Messaging (IM) software used on the darknet
- a way to share processors between network devices across the Internet
- a rule created in order to match a signature of a known exploit
- **a software platform and network of P2P hosts that function as Internet routers**

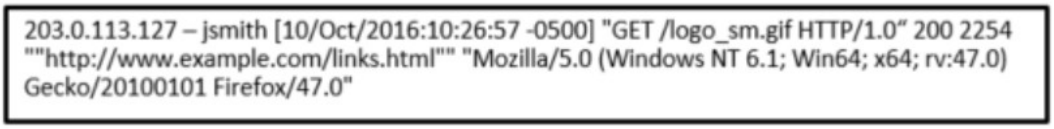
A special browser is used to access the Tor network. This browser allows a user to browse the Internet anonymously.

28. Which statement describes statistical data in network security monitoring processes?

- It shows the results of network activities between network hosts.
- It contains conversations between network hosts.
- **It is created through an analysis of other forms of network data.**
- It lists each alert message along with statistical information.

Like session data, statistical data is about network traffic. Statistical data is created through the analysis of other forms of network data.

29. Refer to the exhibit. A network administrator is reviewing an Apache access log message. What is the status of the access request by the client?



- The request was unsuccessful because of server errors.
- **The request was fulfilled successfully.**
- The request was redirected to another web server.
- The request was unsuccessful because of client errors.

The sixth field of the Apache access log message is the three-digital numeric status code. Codes that begin with a 2 represent success. Codes that begin with a 3 represent redirection. Codes that begin with a 4 represent client errors. Codes that begin with a 5 represent server errors.

30. How might corporate IT professionals deal with DNS-based cyber threats?

- **Monitor DNS proxy server logs and look for unusual DNS queries.**
- Use IPS/IDS devices to scan internal corporate traffic.

- Limit the number of simultaneously opened browsers or browser tabs.
- Limit the number of DNS queries permitted within the organization.

DNS queries for randomly generated domain names or extremely long random-appearing DNS subdomains should be considered suspicious. Cyberanalysts could do the following for DNS-based attacks:Analyze DNS logs.
Use a passive DNS service to block requests to suspected CnC and exploit domains.

31. Refer to the exhibit. A junior network engineer is handed a print-out of the network information shown. Which protocol or service originated the information shown in the graphic?

Service — On / Off

	Time	HostName	Message
1	03.01.1993 12:11:00.018 AM	192.168.1.1	%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/0 (171)
2	10.23.2017 10:40:30.364 AM	192.168.12.2	%SYS-5-CONFIG_I: Configured from console by console
3	10.23.2017 10:40:39.985 AM	192.168.12.2	%LINK-5-CHANGED: Interface Loopback100, changed state to up
4	10.23.2017 10:40:39.985 AM	192.168.12.2	%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback100, changed state to up

- NetFlow
- TACACS+
- RADIUS
- **Syslog**

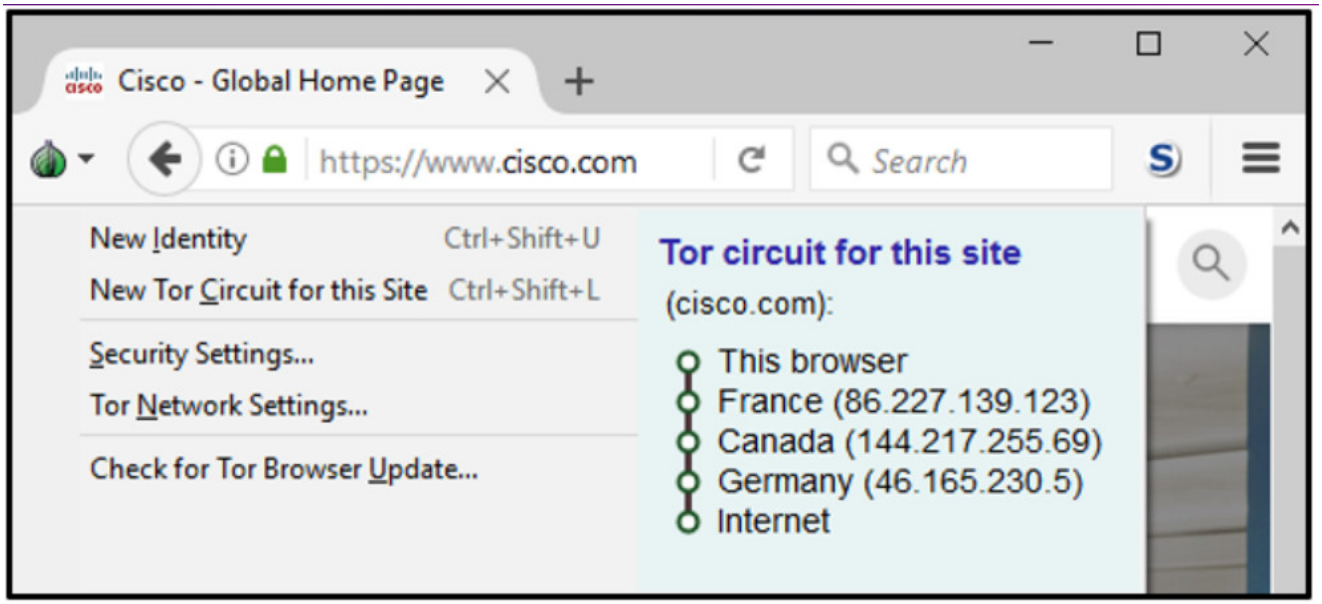
Syslog clients send log entries to a syslog server. The syslog server concentrates and stores log entries. Log entries are categorized by seven severity levels:
emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), and debugging (7).

32. Which technology is used in Cisco Next-Generation IPS devices to consolidate multiple security layers into a single platform?

- WinGate
- **FirePOWER**
- Apache Traffic Server
- Squid

Cisco Next-Generation IPS devices (NGIPS) use FirePOWER Services to consolidate multiple security layers into a single platform, which helps to contain costs and simplify management. Apache Traffic Server, Squid, and WinGate are examples of web proxies.

33. Refer to the exhibit. How is the traffic from the client web browser being altered when connected to the destination website of www.cisco.com?



- Traffic is sent in plain-text by the user machine and is encrypted by the TOR node in France and decrypted by the TOR node in Germany.
- Traffic is encrypted by the user machine and sent directly to the cisco.com server to be decrypted.
- Traffic is encrypted by the user machine, and the TOR network only routes the traffic through France, Canada, Germany, and delivers it to cisco.com.
- **Traffic is encrypted by the user machine, and the TOR network encrypts next-hop information on a hop-by-hop basis.**

When data is being sent into the TOR network, the data is only encrypted by the sending client itself. The next-hop information is encrypted and decrypted between the TOR relays on a hop-by-hop basis. In this way, no single device knows the entire path to the destination, and routing information is readable only by the device that requires it. Finally, at the end of the Tor path, the traffic reaches its Internet destination. The client data is not encrypted by the TOR network; that encryption is the responsibility of the user.

34. Which Windows log contains information about installations of software, including Windows updates?

- **setup logs**
- application logs
- system logs
- security logs

On a Windows host, setup logs record information about the installation of software, including Windows updates.

35. Which Windows log records events related to login attempts and operations related to file or object access?

- setup logs
- **security logs**
- application logs
- system logs

On a Windows host, security logs record events related to security, such as login attempts and operations related to file or object management and access.

36. What does it indicate if the timestamp in the HEADER section of a syslog message is preceded by a period or asterisk symbol?

- The timestamp represents the round trip duration value.
- The syslog message indicates the time an email is received.
- **There is a problem associated with NTP.**
- The syslog message should be treated with high priority.

The HEADER section of the message contains the timestamp. If the timestamp is preceded by the period (.) or asterisk (*) symbols, a problem is indicated with NTP.

37. Which two application layer protocols manage the exchange of messages between a client with a web browser and a remote web server? (Choose two.)

- **HTTPS**
- DHCP
- HTML
- DNS
- **HTTP**

Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) are two application layer protocols that manage the content requests from clients and the responses from the web server. HTML (Hypertext Mark-up Language) is the encoding language that describes the content and display features of a web page. DNS is for domain name to IP address resolution. DHCP manages and provides dynamic IP configurations to clients.

38. Which protocol is a name resolution protocol often used by malware to communicate with command-and-control (CnC) servers?

- IMAP
- HTTPS
- **DNS**
- ICMP

Domain Name Service (DNS) is used to convert domain names into IP addresses. Some organizations have less stringent policies in place to protect against DNS-based threats than they have in place for other exploits.

Download PDF File below:

[sociallocker id="54558"]

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 11 Exam Answers.pdf 427.19 KB 1107 downloads

---

...

Download

[/sociallocker]