# CCNA Cyber Ops (Version 1.1) – Chapter 7 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-7-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 technology is a proprietary SIEM system?**

- SNMP agent
- **Splunk** *
- Stealthwatch
- NetFlow collector

B. Security information event management (SIEM) is a technology that is used in enterprise organizations to provide real-time reporting and long-term analysis of security events. Splunk is a proprietary SIEM system.

**2. Which term is used to describe legitimate traffic that is mistaken for unauthorized traffic by firewalls and IPSs?**

- True positive
- True negative
- **False positive** *
- False negative

C. Network security devices such as firewalls and intrusion prevention systems (IPSs) use preconfigured rules to identify malicious traffic on the network. Sometimes legitimate traffic is mistakenly identified as unauthorized or malicious. When legitimate traffic is incorrectly identified as unauthorized, it is known as a false positive.

**3. Which monitoring technology mirrors traffic flowing through a switch to an analysis device connected to another switch port?**

- SNMP
- SIEM

- **SPAN ***
- NetFlow

C. When enabled on a switch, SPAN, or port mirroring, copies frames sent and received by the switch and forwards them to another port, known as a Switch Port Analyzer port, which has an analysis device attached.

### 4. Which network monitoring tool saves captured network frames in PCAP files?

- NetFlow
- **Wireshark ***
- SNMP
- SIEM

B. Wireshark is a network protocol analyzer used to capture network traffic. The traffic captured by Wireshark is saved in PCAP files and includes interface information and timestamps.

### 5. Which language is used to query a relational database?

- **SQL ***
- C++
- Python
- Java

A. Cybercriminals use SQL injections to breach a relational database, create malicious SQL queries, and obtain sensitive data.

### 6. Which network monitoring tool is in the category of network protocol analyzers?

- SNMP
- SPAN
- **Wireshark ***
- SIEM

C. Wireshark is a network protocol analyzer used to capture network traffic. The traffic captured by Wireshark is saved in PCAP files and includes interface information and timestamps.

### 7. Which SIEM function is associated with examining the logs and events of multiple systems to reduce the amount of time of detecting and reacting to security events?

- Retention
- Aggregation
- **Correlation ***
- Forensic analysis

C. SIEM provides administrators with details on sources of suspicious activity such as user information, device location, and compliance with security policies. One of the essential functions of SIEM is correlation of logs and events from different systems in order to speed the detection and reaction to security events.

**8. Which network technology uses a passive splitting device that forwards all traffic, including Layer 1 errors, to an analysis device?**

- IDS
- SNMP
- NetFlow
- **Network TAP ***

D. A network TAP is a common technology that is used to capture traffic for monitoring the network. The TAP is typically a passive splitting device implemented inline on the network and that forwards all traffic, including physical layer errors, to an analysis device.

**9. What technique is a security attack that depletes the pool of IP addresses available for legitimate hosts?**

- DHCP spoofing
- DHCP snooping
- **DHCP starvation ***
- Reconnaissance attack

C. DHCP starvation attacks create a denial of service for network clients. Theattacker sends DHCP discovery messages that contain fake MAC addresses in an attempt to lease all of the IP addresses. In contrast, DHCP spoofing occurs when a cybercriminal configures a rogue DHCP server to provide network clients with incorrect IP configuration information.

**10. In what type of attack is a cybercriminal attempting to prevent legitimate users from accessing network services?**

- **DoS ***
- MITM
- Session hijacking
- Address spoofing

A. In a DoS, or denial-of-service, attack, the goal of the attacker is to prevent legitimate users from accessing network services.

**11. Which network monitoring technology collects IP operational data on packets flowing through Cisco routers and multilayer switches?**

- SNMP
- SIEM
- **NetFlow ***
- Wireshark

C. NetFlow is a Cisco technology that runs on Cisco routers and multilayer switches and that gathers statistics on forwarded packets.

**12. What are two monitoring tools that capture network traffic and forward it to network monitoring devices? (Choose two.)**

- **SPAN**
- **network tap**
- SNMP
- SIEM
- Wireshark

A network tap is used to capture traffic for monitoring the network. The tap is typically a passive splitting device implemented inline on the network and forwards all traffic including physical layer errors to an analysis device. SPAN is a port mirroring technology supported on Cisco switches that enables the switch to copy frames and forward them to an analysis device.

**13. Which technology is an open source SIEM system?**

- Wireshark
- StealWatch
- Splunk
- **ELK**

There are many SIEM systems available to network administrators. The ELK suite is an open source option.

**14. What network attack seeks to create a DoS for clients by preventing them from being able to obtain a DHCP lease?**

- IP address spoofing
- **DHCP starvation**
- CAM table attack
- DHCP spoofing

DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages in order to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

**15. Which protocol would be the target of a cushioning attack?**

- DHCP
- **HTTP**
- ARP
- DNS

The HTTP 302 cushioning attack is used by cybercriminals to take advantage of the 302 Found HTTP response status code to redirect the browser of the user to a new location, usually a malicious site.

**16. Which network monitoring capability is provided by using SPAN?**

- Network analysts are able to access network device log files and to monitor network behavior.
- Statistics on packets flowing through Cisco routers and multilayer switches can be captured.
- **Traffic exiting and entering a switch is copied to a network monitoring device.**
- Real-time reporting and long-term analysis of security events are enabled.

When enabled on a switch, SPAN or port mirroring, copies frames that are sent and received by the switch and forwards them to another port, known as a Switch Port Analyzer port, which has a analysis device attached.

**17. Which type of DNS attack involves the cybercriminal compromising a parent domain and creating multiple subdomains to be used during the attacks?**

- **shadowing**
- amplification and reflection
- tunneling
- cache poisoning

Two threats to DNS are DNS shadowing and DNS tunneling attacks. DNS shadowing attacks compromise a parent domain and then the cybercriminal creates subdomains to be used in attacks. DNS tunneling attacks build botnets to bypass traditional security solutions. Three threats to DNS open resolvers are cache poisoning, amplification and reflection, and resource utilization attacks.

**18. Refer to the exhibit. What protocol would be used by the syslog server service to create this type of output for security purposes?**

- NTP
- AAA
- ICMP
- **SNMP**

The Simple Network Management Protocol is used by network devices to send and log messages to a syslog server in order to monitor traffic and network device events.

**19. What is the result of a passive ARP poisoning attack?**

- **Confidential information is stolen.**
- Network clients experience a denial of service
- Data is modified in transit or malicious data is inserted in transit.
- Multiple subdomains are created.

ARP poisoning attacks can be passive or active. The result of a passive attack is that cybercriminals steal confidential information. With an active attack, cybercriminals modify data in transit or they inject malicious data.

**20. Which term is used for bulk advertising emails flooded to as many end users as possible?**

- **spam**
- adware
- brute force
- phishing

Spam is annoying and unwanted bulk email that is sent to as many end users as possible.

**21. Which capability is provided by the aggregation function in SIEM?**

- **reducing the volume of event data by consolidating duplicate event records**
- searching logs and event records of multiple sources for more complete forensic analysis
- presenting correlated and aggregated event data in real-time monitoring
- increasing speed of detection and reaction to security threats by examining logs from many systems and applications

The aggregation function of SIEM reduces the volume of event data by consolidating duplicate event records.

**22. Which protocol is attacked when a cybercriminal provides an invalid gateway in order to create a man-in-the-middle attack?**

- HTTP or HTTPS
- ICMP
- DNS
- **DHCP**

A cybercriminal could set up a rogue DHCP server that provides one or more of the following:Wrong default gateway that is used to create a man-in-the-middle attack and allow the attacker to intercept data
Wrong DNS server that results in the user being sent to a malicious website
Invalid default gateway IP address that results in a denial of service attack on the DHCP client

**23. Which network monitoring tool can provide a complete audit trail of basic information of all IP flows on a Cisco router and forward the data to a device?**

- SPAN
- Wireshark
- **NetFlow**
- SIEM

NetFlow is a Cisco technology that provides statistics on packets flowing through a Cisco router or multilayer switch.

**24. What are two methods used by cybercriminals to mask DNS attacks? (Choose two.)**

- **domain generation algorithms**
- shadowing
- **fast flux**
- reflection
- tunneling

Fast flux, double IP flux, and domain generation algorithms are used by cybercrimals to attack DNS servers and affect DNS services. Fast flux is a technique used to hide phishing and malware delivery sites behind a quickly-changing network of compromised DNS hosts (bots within botnets). The double IP flux technique rapidly changes the hostname to IP address mappings and the authoritative name server. Domain generation algorithms randomly generate domain names to be used as rendezvous points.

**25. Which protocol is exploited by cybercriminals who create malicious iFrames?**

- **HTTP**
- ARP
- DNS
- DHCP

An HTML element known as an inline frame or iFrame allows the browser to load a different web page from another source.

### 26. Which SIEM function is associated with speeding up detection of security threats by examining logs and events from different systems?

- forensic analysis
- retention
- **correlation**
- aggregation

The correlation function of SIEM speeds the detection and reaction to security threats by examining logs and events from different systems.

### 27. In which TCP attack is the cybercriminal attempting to overwhelm a target host with half-open TCP connections?

- reset attack
- session hijacking attack
- port scan attack
- **SYN flood attack**

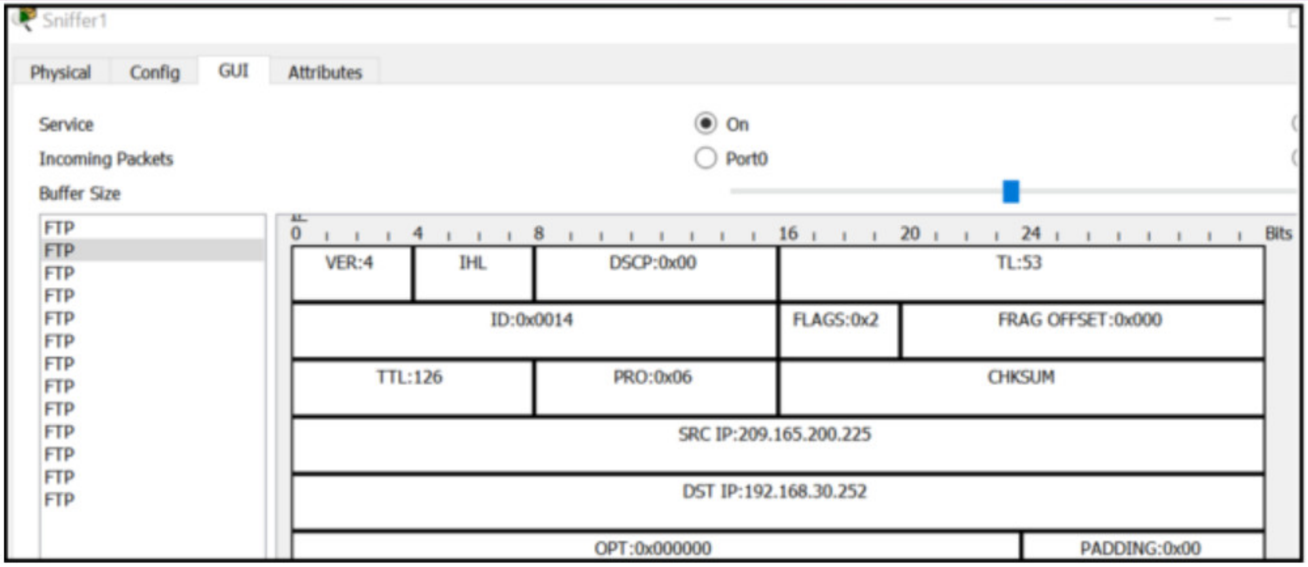
In a TCP SYN flood attack, the attacker sends to the target host a continuous flood of TCP SYN session requests with a spoofed source IP address. The target host responds with a TCP-SYN-ACK to each of the SYN session requests and waits for a TCP ACK that will never arrive. Eventually the target is overwhelmed with half-open TCP connections.

### 28. In which type of attack is falsified information used to redirect users to malicious Internet sites?

- ARP cache poisoning
- DNS amplification and reflection
- **DNS cache poisoning**
- domain generation

In a DNS cache poisoning attack, falsified information is used to redirect users from legitimate to malicious internet sites.

**29. Refer to the exhibit. A junior network administrator is inspecting the traffic flow of a particular server in order to make security recommendations to the departmental supervisor. Which recommendation should be made?**



Service ● On

Incoming Packets ○ Port0

Buffer Size

FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP

VER:4 | IHL | DSCP:0x00 | TL:53

ID:0x0014 | FLAGS:0x2 | FRAG OFFSET:0x000

TTL:126 | PRO:0x06 | CHKSUM

SRC IP:209.165.200.225

DST IP:192.168.30.252

OPT:0x000000 | PADDING:0x00

- **A more secure protocol should be used.**
- The total length (TL) field indicates an unsecure Layer 4 protocol is being used.
- The person accessing the server should never access it from a device using a private IP address.
- The person accessing the server should use the private IP address of the server.

FTP is an unsecure network protocol. Anyone capturing packets can obtain the username and password from the capture. A more secure protocol such as SFTP should be used.

**30. Which network monitoring tool saves captured packets in a PCAP file?**

- **Wireshark**
- SIEM
- SNMP
- NetFlow

Wireshark captures are saved as PCAP files, which contain frame, interface, and packet information, and also time stamps.

**31. Which cyber attack involves a coordinated attack from a botnet of zombie computers?**

- ICMP redirect
- MITM
- **DDoS**
- address spoofing

DDoS is a distributed denial-of-services attack. A DDoS attack is launched from multiple coordinated sources. The sources of the attack are zombie hosts that the cybercriminal has built into a botnet. When ready, the cybercriminal instructs the botnet of zombies to attack the chosen target.

**32. How is optional network layer information carried by IPv6 packets?**

- inside an options field that is part of the IPv6 packet header
- inside the Flow Label field
- inside the payload carried by the IPv6 packet
- **inside an extension header attached to the main IPv6 packet header**

IPv6 uses extension headers to carry optional network layer information. Extension headers are not part of the main IPv6 header but are separate headers placed between the IPv6 header and the payload.

**33. What type of attack targets an SQL database using the input field of a user?**

- Cross-site scripting
- **SQL injection**
- buffer overflow
- XML injection

A criminal can insert a malicious SQL statement in an entry field on a website where the system does not filter the user input correctly.

**34. What network monitoring technology enables a switch to copy and forward traffic sent and received on multiple interfaces out another interface toward a network analysis device?**

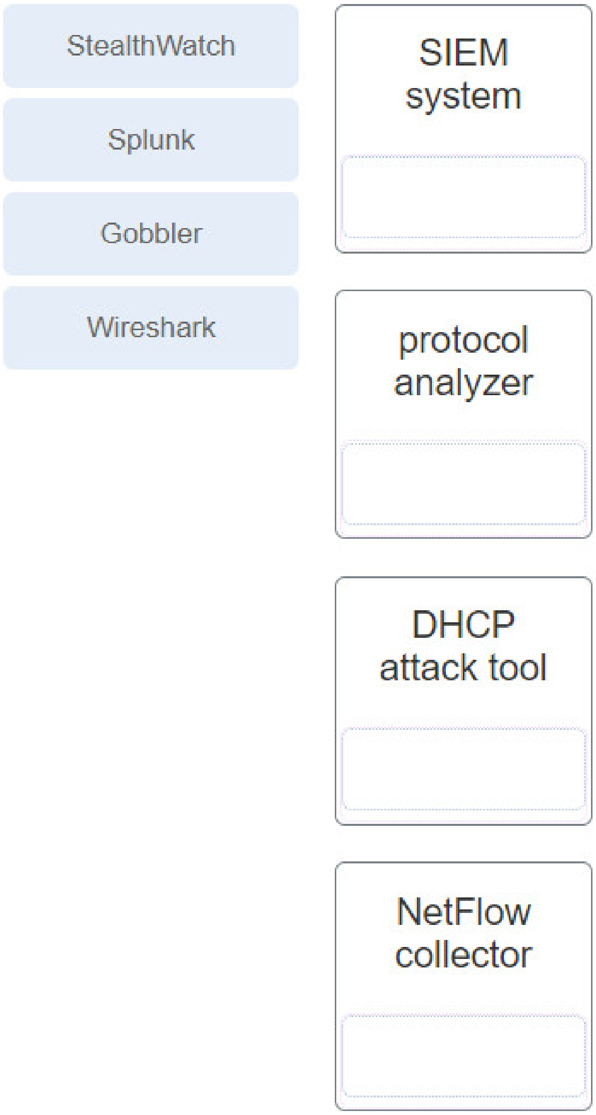
- **port mirroring**
- NetFlow
- SNMP
- network tap

When enabled on a switch, port mirroring copies frames sent and recieved by the switch and forwards them to another port, which has a analysis device attached.

**35. Match the monitoring tool to the description.**

Answer

**36. Match the attack to the definition. (Not all options are used.)**



StealthWatch

Splunk

Gobbler

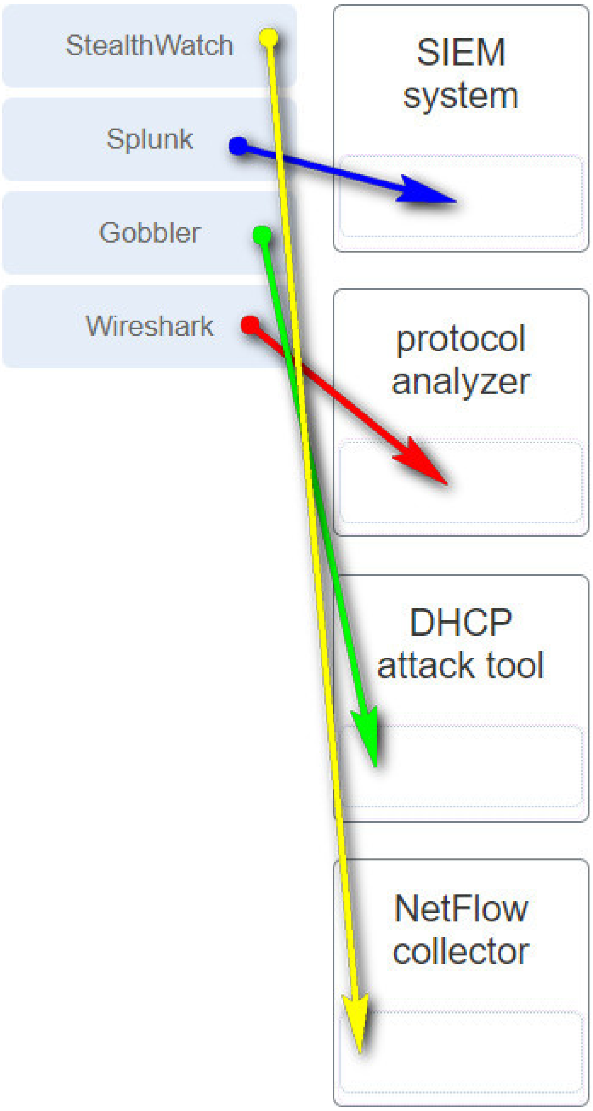
Wireshark

SIEM system

protocol analyzer

DHCP attack tool

NetFlow collector



StealthWatch

Splunk

Gobbler

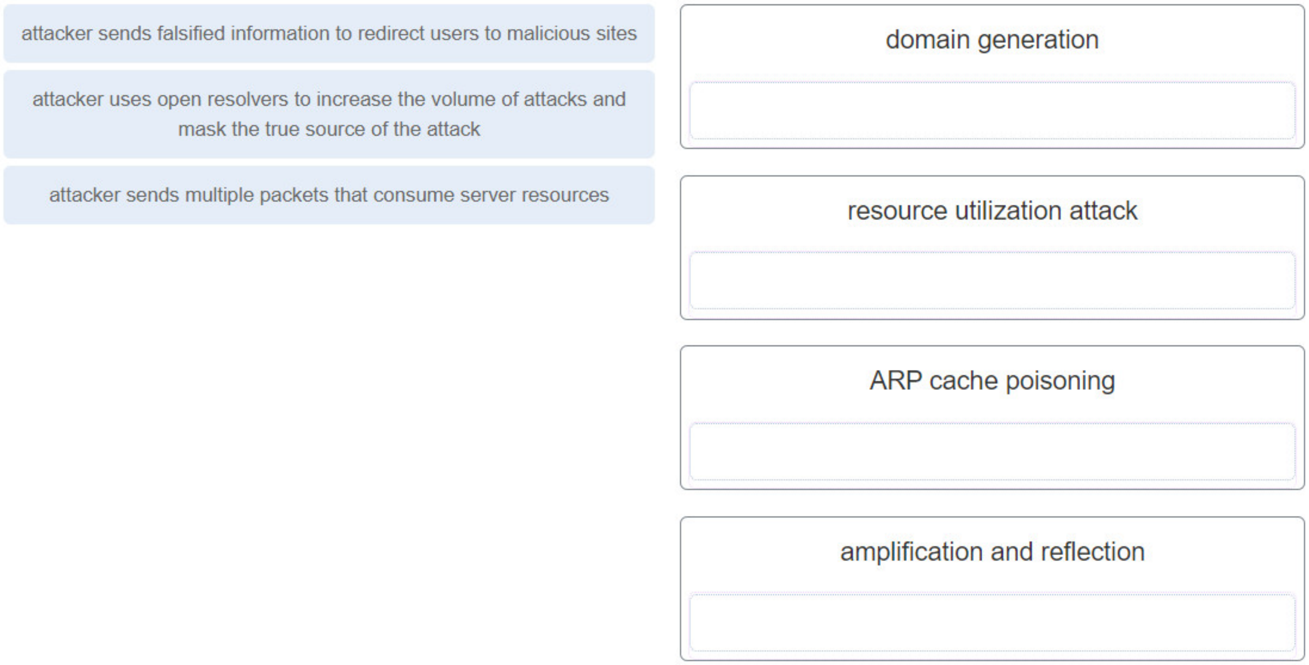
Wireshark

SIEM system

protocol analyzer

DHCP attack tool

NetFlow collector



attacker sends falsified information to redirect users to malicious sites

attacker uses open resolvers to increase the volume of attacks and mask the true source of the attack

attacker sends multiple packets that consume server resources

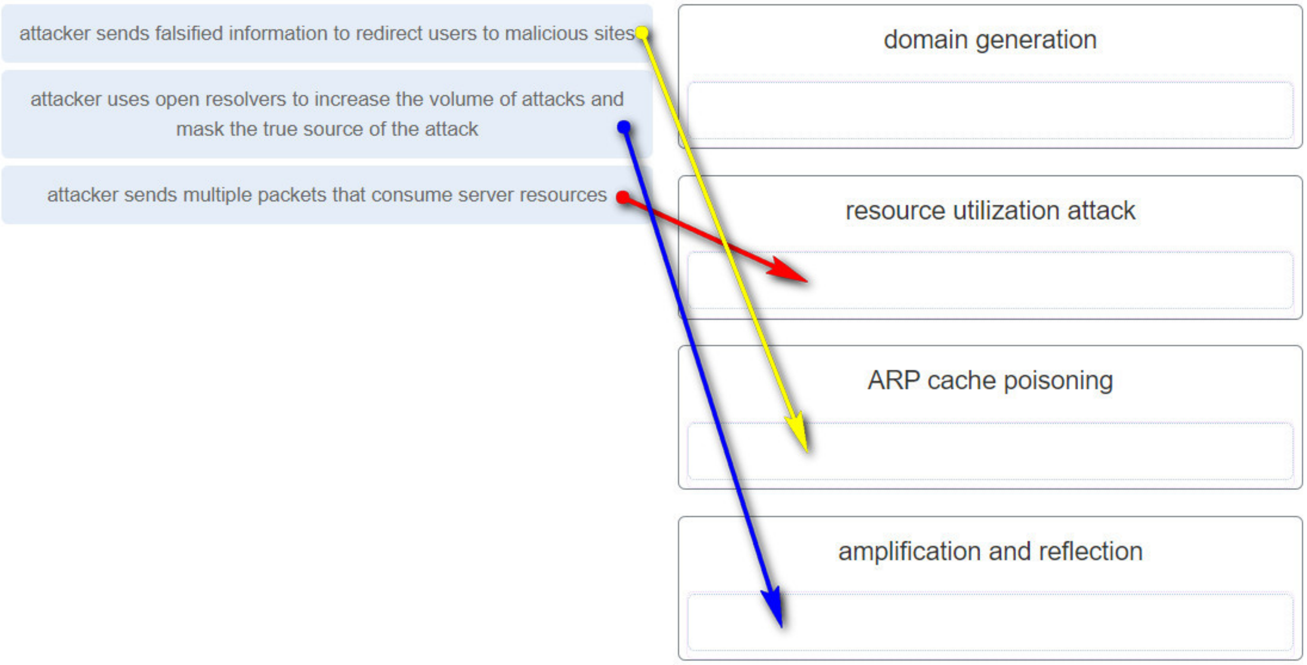
domain generation

resource utilization attack

ARP cache poisoning

amplification and reflection

Answer



attacker sends falsified information to redirect users to malicious sites

attacker uses open resolvers to increase the volume of attacks and mask the true source of the attack

attacker sends multiple packets that consume server resources

domain generation

resource utilization attack

ARP cache poisoning

amplification and reflection

## Download PDF File below:

[sociallocker id="54558″]

**CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 7 Exam Answers.pdf** 365.40 KB 1238 downloads

...

Download

[/sociallocker]