Free Cisco 200-201 CCNACBR Practice Questions

Shared by Montoya on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

Options:

A- NetScout
B- tcpdump
C- SolarWinds
D- netsh

Answer:

B

Explanation:

tcpdump is an open-source packet capture tool that uses the libpcap library to capture network traffic on Linux and Mac OS X operating systems. It can display the contents of packets in various formats, filter packets based on criteria, and save packets to a file.tcpdump is a command-line tool that can be run on a terminal or a remote shell1Reference:Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 2: Security Monitoring

Question 2

Question Type: MultipleChoice

A network engineer noticed in the NetFlow report that internal hosts are sending many DNS requests to external DNS servers A SOC analyst checked the endpoints and discovered that they are infected and became part of the botnet Endpoints are sending multiple DNS requests but with spoofed IP addresses of valid external sources What kind of attack are infected endpoints involved in1?

Options:

A- DNS hijacking
B- DNS tunneling
C- DNS flooding

D- DNS amplification

Answer:

D

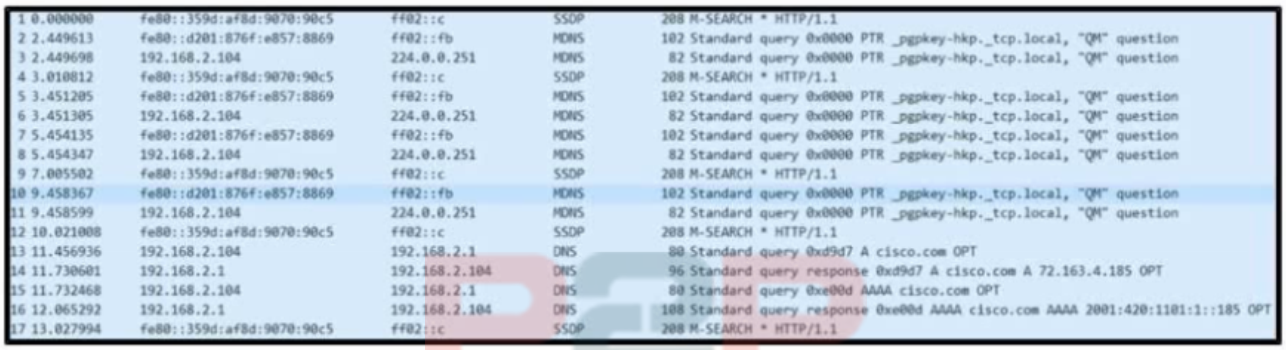
Explanation:

The attack described is a DNS amplification attack. It involves infected endpoints sending DNS requests with spoofed IP addresses to external DNS servers. The DNS servers then send large responses to the spoofed addresses, which are actually the targets of the attack. This can result in a significant amount of traffic being directed at the target, overwhelming their network resources. DNS amplification is a type of Distributed Denial of Service (DDoS) attack that leverages the DNS protocol to amplify the attack traffic.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



1	0.000000	fe80::359d:af8d:9070:90c5	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
2	2.449613	fe80::d201:876f:e857:8869	ff02::fb	MDNS	102 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
3	2.449698	192.168.2.104	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
4	3.010812	fe80::359d:af8d:9070:90c5	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
5	3.451205	fe80::d201:876f:e857:8869	ff02::fb	MDNS	102 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
6	3.451305	192.168.2.104	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
7	5.454135	fe80::d201:876f:e857:8869	ff02::fb	MDNS	102 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
8	5.454347	192.168.2.104	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
9	7.005502	fe80::359d:af8d:9070:90c5	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
10	9.458367	fe80::d201:876f:e857:8869	ff02::fb	MDNS	102 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
11	9.458599	192.168.2.104	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
12	10.021008	fe80::359d:af8d:9070:90c5	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
13	11.456936	192.168.2.104	192.168.2.1	DNS	80 Standard query 0xd9d7 A cisco.com OPT
14	11.730601	192.168.2.1	192.168.2.104	DNS	96 Standard query response 0xd9d7 A cisco.com A 72.163.4.185 OPT
15	11.732468	192.168.2.104	192.168.2.1	DNS	80 Standard query 0xe00d AAAA cisco.com OPT
16	12.065292	192.168.2.1	192.168.2.104	DNS	108 Standard query response 0xe00d AAAA cisco.com AAAA 2001:420:1101:1::185 OPT
17	13.027994	fe80::359d:af8d:9070:90c5	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1

Refer to the exhibit. Based on the .pcap file, which DNS server is used to resolve cisco.com?

Options:

A- 224.0.0.251
B- 192.168.2.1
C- 72.163.4.185
D- 192.168.2.104

Answer:

B

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

Options:

A- The file will appear legitimate by evading signature-based detection.
B- The file will not execute its behavior in a sandbox environment to avoid detection.
C- The file will insert itself into an application and execute when the application is run.
D- The file will monitor user activity and send the information to an outside source.

Answer:

B

Explanation:

The Cuckoo report indicates that the file has been identified by Yara rules as being capable of detecting a sandbox environment, which is a security mechanism for isolating and analyzing suspicious code. The presence of the ''vmdetect'' and ''anti_dog'' Yara rules suggests that the file may have mechanisms to avoid executing its malicious behavior when it detects that it is being analyzed in a sandbox. This is a common evasion technique used by malware to prevent detection and analysis by security researchers or automated systems.

Question 5

Question Type: MultipleChoice

A suspicious user opened a connection from a compromised host inside an organization. Traffic was going through a router and the network administrator was able to identify this flow. The admin was following 5-tuple to collect needed dat

a. Which information was gathered based on this approach?

Options:

A- direct path
B- user name
C- protocol
D- NAT

Answer:

D

Question 6

Question Type: MultipleChoice

What is a difference between SIEM and SOAR?

Options:

A- SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.
B- SlEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
C- SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
D- SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

Answer:

B

Explanation:

SIEM (Security Information and Event Management) systems are solutions that provide real-time analysis of security alerts generated by applications and network hardware. They collect, store, analyze, and report on log data for incident response, forensics, and regulatory compliance. On the other hand, SOAR (Security Orchestration Automation and Response) platforms allow organizations to collect data about security threats from multiple sources and respond to low-level security events without human assistance.Reference:Cisco Cybersecurity Operations Fundamentals

Question 7

Question Type: MultipleChoice

Which CVSS metric group identifies other components that are affected by a successful security attack?

Options:

A- scope
B- attack vector
C- integrity
D- privileges required

Answer:

A

Question 8

Question Type: MultipleChoice

An engineer is sharing folders and files with different departments and got this error: "No such file or directory". What must the engineer verify next?

Options:

A- memory allocation
B- symlinks
C- permission
D- disk space

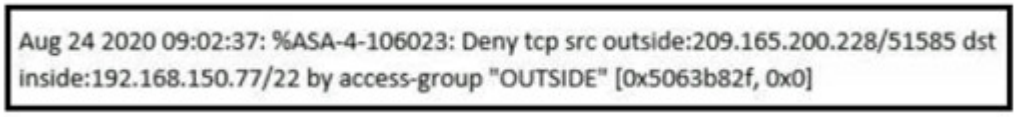
Answer:

C

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced. How should this type of evidence be categorized?

Options:

A- indirect
B- circumstantial
C- corroborative
D- best

Answer:

B

Explanation:

The alert from the Cisco ASA device and the numerous activity logs are examples of circumstantial evidence. Circumstantial evidence is evidence that relies on an inference or deduction to connect it to a conclusion of fact, such as a security incident or an attack. Circumstantial evidence does not directly prove the fact in question, but rather suggests or implies it. In this case, the alert and the logs indicate that a TCP connection attempt was denied by an access group, but they do not directly prove that an attack occurred or who was behind it. There could be other explanations for the denied connection, such as a misconfiguration, a network error, or a legitimate request. Therefore, this type of evidence is circumstantial and

requires further investigation and analysis to confirm or rule out the possibility of an attack.Reference:=Circumstantial evidence - Wikipedia;Circumstantial Evidence - Definition, Examples, Cases, Processes;Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 92.

Question 10

Question Type: MultipleChoice

An engineer must verify vulnerabilities found in the scanning process The engineer checks the impact of those findings to the organization and compares the results with known threats inside organization What is the benefit of knowing this information?

Options:

A- A pcap file can be prepared
B- An exploit can be built.
C- Risk can be calculated
D- Logs can be gathered

Answer:

C

Question 11

Question Type: MultipleChoice

An automotive company provides new types of engines and special brakes for rally sports cars. The company has a database of inventions and patents for their engines and technical information Customers can access the database through the company's website after they register and identify themselves. Which type of protected data is accessed by customers?

Options:

A- IP data
B- PII data
C- PSI data
D- PHI data

Answer:

A

Explanation:

IP data stands for Intellectual Property data, which is any data that represents the creations of the mind, such as inventions, patents, designs, or artistic works. IP data is protected by law and has commercial value for its owners. In this case, the automotive company has a database of IP data for their engines and technical information, which customers can access after they register and identify themselves.Reference:= Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.2: Data Protection, Topic 1.2.1: Data Types

P2P exams