Free Questions for 200-201 by braindumpscollection

Shared by Gray on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

```
alert tcp !$HOME_NET any -> $HOME_NET 80 (flags: s; msg:"Attempt to access server is
made with TCP packets"; classtype:attempted-dos; sid:1000990; rev:1;)
```

What is the outcome of the command?

Options:

A- TCP rule that detects TCP packets with the SYN flag in an external FTP server

B- TCP rule that detects TCP packets with a SYN flag in the internal network

C- TCP rule that detects TCP packets with a ACK flag in the internal network

D- TCP rule that detects TCP packets with the ACK flag in an external FTP server

Answer:

B

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any ( msg:"BROWSER-
CHROME Google Chrome XSSAuditor filter security policy bypass attempt";
flow:to_client,established; file_data; content:"<iframe",nocase; content:"srcdoc",within
20,nocase; content:"<script>",within 10,nocase;
pcre:"/<iframe[^>]*?srcdoc\s?=\s?[\x22\x27]<script>/smi"; metadata:policy max-detect-
ips drop; service:http; reference:bugtraq,65066;
reference:url,googlechromereleases.blogspot.ca/2014/01/stable-channel-update.html;
classtype:attempted-user; sid:30252; rev:3; )
```

A company's user HTTP connection to a malicious site was blocked according to configured policy What is the source technology used for this measure'?

Options:

A- network application control

B- firewall

C- IPS

D- web proxy

Answer:

B

Question 4

Question Type: MultipleChoice

An engineer must configure network systems to detect command-and-control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology must be used to accomplish this task?

Options:

A- static IP addresses

B- signatures

C- digital certificates

D- cipher suite

Answer:

C

Question 5

Question Type: MultipleChoice

Which action matches the weaponization step of the Cyber Kill Chain model?

Options:

A- Scan a host to find open ports and vulnerabilities

B- Construct the appropriate malware and deliver it to the victim.

C- Test and construct the appropriate malware to launch the attack

D- Research data on a specific vulnerability

Answer:

B

Question 6

Question Type: MultipleChoice

Which technique is a low-bandwidth attack?

Options:

A- social engineering

B- session hijacking

C- evasion

D- phishing

Answer:

C

Question 7

Question Type: MultipleChoice

What does the Zero Trust security model signify?

Options:

A- Zero Trust security means that no one is trusted by default from inside or outside the network

B- Zero Trust states that no users should be given enough privileges to misuse the system on their own

C- Zero Trust addresses access control and states that an individual should have only the minimum access privileges necessary to perform specific tasks

D- Zero Trust states that unless a subject is given explicit access to an object, it should be denied access to that object

Answer:

A

Question 8

Question Type: MultipleChoice

Which element is included in an incident response plan as stated m NIST SP800-617

Options:

A- security of sensitive information

B- individual approach to incident response

C- approval of senior management

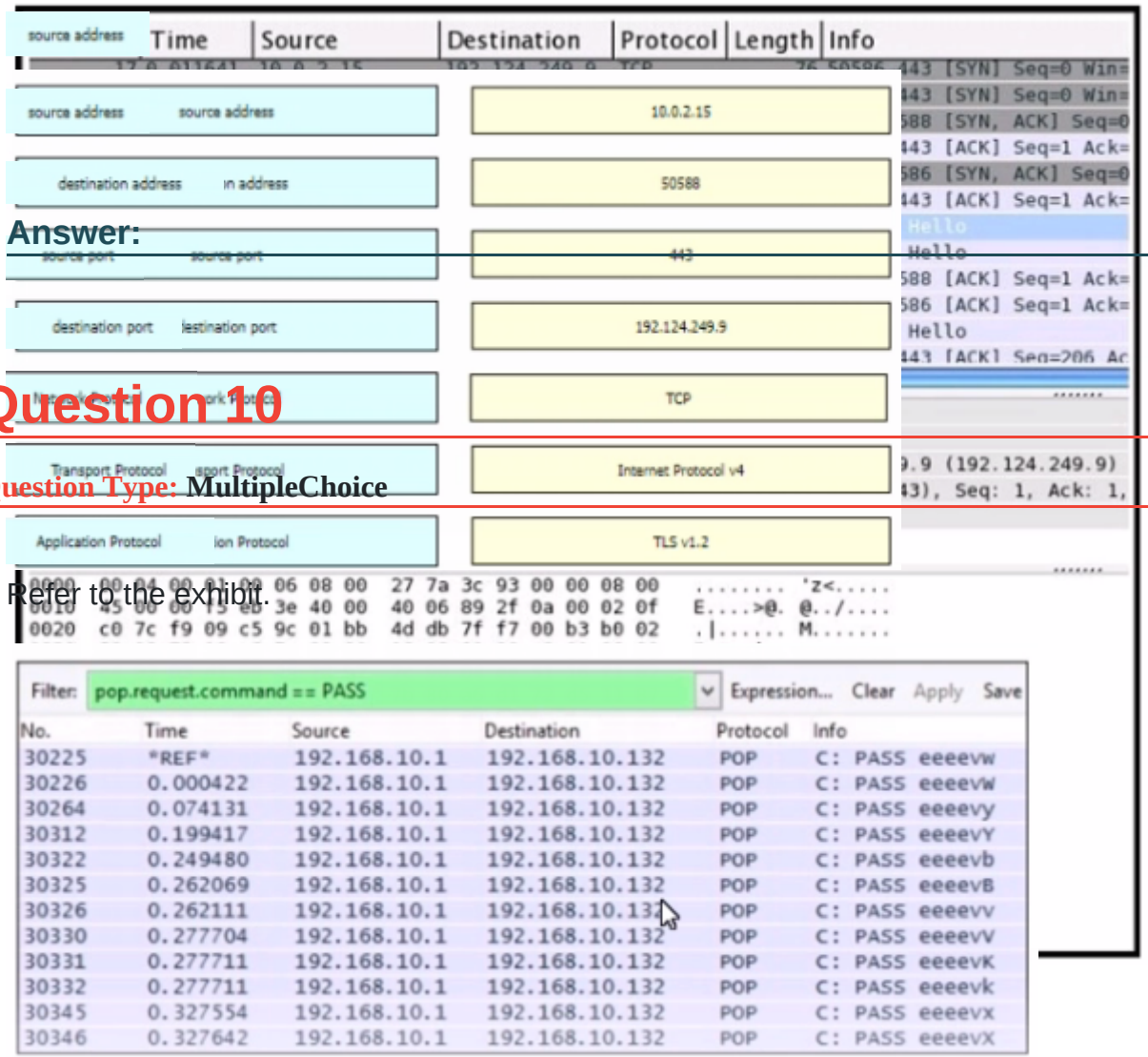
D- consistent threat identification

Answer:

D

Question 9

Question Type: **DragDrop**



nding pieces of the PCAP file on the right.

Answer:

Question 10

Question Type: MultipleChoice

Refer to the exhibit.

Which alert is identified from this packet capture?

Options:

A- man-in-the-middle attack

B- ARP poisoning

C- brute-force attack

D- SQL injection

Answer:

C

Question 11

Question Type: **MultipleChoice**

What is the dataflow set in the NetFlow flow-record format?

Options:

A- Dataflow set is a collection of HEX records.

B- Dataflow set provides basic information about the packet such as the NetFlow version

C- Dataflow set is a collection of binary patterns

D- Dataflow set is a collection of data records.

Answer:

D