

# **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**

Refer to the exhibit.

alert tcp !SHOME\_NET any -> SHOME\_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:

В

### **Question 3**

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-detectips 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

### 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

С

### **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:

### **Question 6**

#### **Question Type:** MultipleChoice

Which technique is a low-bandwidth attack?

<ul> <li>A- social engineering</li> <li>B- session hijacking</li> <li>C- evasion</li> </ul>	Options:			
	4- social engineering			
C- evasion	<ul> <li>B- session hijacking</li> </ul>			
	C- evasion			
D- phishing	D- phishing			

#### Answer:

С

### **Question 7**

**Question Type:** MultipleChoice

#### **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

nswer:			

A D

## **Question 9**

**Question Type:** DragDrop

rce addres	Time S	ource	Destination	Protoc	ol Lengt	hlinfo		0.0011056	nding pieces of the PCAP file on the right
_	17.0.011641 1		02 124 240 0	TCP	er lengt		443 [SYN]	Seq=0 Win=	
								Seq=0 Win=	
rce addres	ss source address			10.0.2.	15		588 [SYN,	ACK] Seq=0	
							443 [ACK]	Seq=1 Ack=	
destinatio	on address in addre	155		50588	8			ACK] Seq=0	
								Seq=1 Ack=	
swe	r:						Hello		
ource port	source port			443			Hello	Con-1 Ash	
								Seq=1 Ack= Seq=1 Ack=	
destinatio	n port destination por	:		192.124.2	249.9		Hello	Sed=1 WCK=	
								Seg=206 Ac	
es	tion 16			TCP					
Transport	Protocol sport Protoc	ol		Internet Prot	tocol v4		9.9 (192.	124.249.9)	
tion 1	ype: Multip	leChoice					43), Seq:	1, Ack: 1,	
							1		
plication P	Protocol ion Proto	col		TLS v1	2				
00-+00	the exhibit.	06 08 00 27 7a	3c 93 00 00	08 00		'z<			
E LO	SURP CATRICE.	3e 40 00 40 06	3c 93 00 00 89 2f 0a 00	02 Of 1	E>@.				
20 C	0 7c 19 09 c5	9c 01 bb 4d db	7f f7 00 b3	b0 02	· I · · · · · ·	м			
ter: po	p.request.commar	d == PASS			v Expressi	on Clea	r Apply Sa	ive	
_	Time	Source	Destination		Protocol	Info			
225	*REF*	192.168.10.1	192.168.1	0.132	POP		55 eeeevw		
	0.000422	192.168.10.1	192.168.1		POP		55 eeeevw		
226	0.000422				POP	C: PA	SS eeeevy		
226 264	0.074131	192.168.10.1	192.168.1	0.132					
	0.074131 0.199417	192.168.10.1 192.168.10.1	192.168.1		POP	C: PA	55 eeeevY		
264 312 322	0.074131 0.199417 0.249480	192.168.10.1 192.168.10.1	192.168.1 192.168.1	0.132	POP POP	C: PA	55 eeeevb		
264 312 322 325	0.074131 0.199417 0.249480 0.262069	192.168.10.1 192.168.10.1 192.168.10.1	192.168.1 192.168.1 192.168.1	0.132 0.132 0.132	POP POP	C: PA	SS eeeevb SS eeeevB		
264 312 322 325 326	0.074131 0.199417 0.249480 0.262069 0.262111	192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1	192.168.1 192.168.1 192.168.1 192.168.1	0.132 0.132 0.132 0.132	POP POP POP	C: PA C: PA C: PA	55 eeeevb 55 eeeevb 55 eeeevv		
264 312 322 325 326 330	0.074131 0.199417 0.249480 0.262069 0.262111 0.277704	192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1	192.168.1 192.168.1 192.168.1 192.168.1 192.168.1 192.168.1	0.132 0.132 0.132 0.133 0.133	POP POP POP POP	C: PA C: PA C: PA C: PA	55 eeeevb 55 eeeevb 55 eeeevv 55 eeeevv		
264 312 322 325 326 330 331	0.074131 0.199417 0.249480 0.262069 0.262111 0.277704 0.277711	192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1	192.168.1 192.168.1 192.168.1 192.168.1 192.168.1 192.168.1 192.168.1	0.132 0.132 0.132 0.132 0.132 0.132	POP POP POP POP POP	C: PA C: PA C: PA C: PA C: PA	55 eeeevb 55 eeeevb 55 eeeevv 55 eeeevv 55 eeeevk		
264 312 322 325 326 330 331 332	0.074131 0.199417 0.249480 0.262069 0.262111 0.277704 0.277711 0.277711	192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1	192.168.1 192.168.1 192.168.1 192.168.1 192.168.1 192.168.1 192.168.1	0.132 0.132 0.132 0.132 0.132 0.132 0.132 0.132	POP POP POP POP POP POP	C: PA C: PA C: PA C: PA C: PA C: PA	55 eeeevb 55 eeeevb 55 eeeevv 55 eeeevv 55 eeeevk 55 eeeevk		
264 312 322 325 326 330 331	0.074131 0.199417 0.249480 0.262069 0.262111 0.277704 0.277711	192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1 192.168.10.1	192.168.1 192.168.1 192.168.1 192.168.1 192.168.1 192.168.1 192.168.1	0.132 0.132 0.132 0.132 0.132 0.132 0.132 0.132 0.132	POP POP POP POP POP	C: PA C: PA C: PA C: PA C: PA C: PA C: PA	55 eeeevb 55 eeeevb 55 eeeevv 55 eeeevv 55 eeeevk		

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:

С

## **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:**

### **To Get Premium Files for 200-201 Visit**

https://www.p2pexams.com/products/200-201

For More Free Questions Visit

https://www.p2pexams.com/cisco/pdf/200-201

