

[February-2023Exam Pass 100% !Brindump2go 200-201 Dumps PDF 200-201 278Q Instant Download[Q77-Q122

February/2023 Latest Brindump2go 200-201 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Brindump2go 200-201 Real Exam Questions!

QUESTION 77 Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies? A. CSIRT B. PSIRT C. public affairs D. management Answer: D

QUESTION 78 An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic? A. ransomware communicating after infection B. users downloading copyrighted content C. data exfiltration D. user circumvention of the firewall Answer: D

QUESTION 79 Which of the following access control models use security labels to make access decisions? A. Mandatory access control (MAC) B. Role-based access control (RBAC) C. Identity-based access control (IBAC) D. Discretionary access control (DAC) Answer: A

QUESTION 80 What is the main advantage of using a mandatory access control (MAC) model instead of a discretionary access control (DAC) model? A. MAC is more secure because the operating system ensures security policy compliance. B. MAC is more secure because the data owner can decide which user can get access, thus providing more granular access. C. MAC is more secure because permissions are assigned based on roles. D. MAC is better because it is easier to implement. Answer: A

QUESTION 81 How is attacking a vulnerability categorized? A. action on objectives B. delivery C. exploitation D. installation Answer: C

QUESTION 82 A system administrator is ensuring that specific registry information is accurate. Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain? A. file extension associations B. hardware, software, and security settings for the system C. currently logged in users, including folders and control panel settings D. all users on the system, including visual settings Answer: B

QUESTION 83 What is the difference between statistical detection and rule-based detection models? A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time. B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis. C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior. D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis Answer: B

QUESTION 84 Which step in the incident response process researches an attacking host through logs in a SIEM? A. detection and analysis B. preparation C. eradication D. containment Answer: A

QUESTION 85 What is the difference between a threat and a risk? A. Threat represents a potential danger that could take advantage of a weakness in a system. B. Risk represents the known and identified loss or danger in the system. C. Risk represents the nonintentional interaction with uncertainty in the system. D. Threat represents a state of being exposed to an attack or a compromise either physically or logically Answer: A

QUESTION 86 Which signature impacts network traffic by causing legitimate traffic to be blocked? A. false negative B. true positive C. true negative D. false positive Answer: D

QUESTION 87 Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key? A. forgery attack B. plaintext-only attack C. ciphertext-only attack D. meet-in-the-middle attack Answer: C

QUESTION 88 What is ransomware? A. A type of malware that compromises a system and then often demands a ransom from the victim to pay the attacker in order for the malicious activity to cease or for the malware to be removed from the affected system. B. A set of tools used by an attacker to elevate his privilege to obtain root-level access in order to completely take control of the affected system. C. A type of intrusion prevention system. D. A type of malware that doesn't affect mobile devices Answer: A

QUESTION 89 What two are examples of UDP-based attacks? (Choose two.) A. SYN flood B. SQL slammer C. UDP flooding D. MAC address flooding Answer: BC

QUESTION 90 What causes events on a Windows system to show Event Code 4625 in the log messages? A. The system detected an XSS attack. B. Someone is trying a brute force attack on the network. C. Another device is gaining root access to the system. D. A privileged user successfully logged into the system Answer: B

QUESTION 91 Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources? A. resource exhaustion B. tunneling C. traffic fragmentation D. timing attack Answer: A

QUESTION 92 Refer to the exhibit. What does the message indicate?

10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1" 200 5000
www.Braindump2go.com
Gecko/20100101 Firefox/54.0"

A. an access attempt was made from the Mosaic web browser B. a successful access attempt was made to retrieve the password file C. a successful access attempt was made to retrieve the root of the website D. a denied access attempt was made to retrieve the password file Answer: C

QUESTION 93 What are two social engineering techniques? (Choose two.) A. privilege escalation B.

DDoS attackC. phishingD. man-in-the-middleE. pharmingAnswer: CEQUESTION 94Refer to the exhibit. What does the output indicate about the server with the IP address 172.18.104.139?

```
# nmap -sV 172.18.104.139
Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 65535 closed ports
PORT      State Service
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp      Postfix smtpd
110/tcp   open  pop3      Dovecot pop3d
143/tcp   open  imap      Dovecot imapd
Service Info: Host: 172.18.104.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

A. open ports of a web serverB. open port of an FTP serverC. open ports of an email serverD. running processes of the serverAnswer: CQUESTION 95Refer to the exhibit. This request was sent to a web application server driven by a database.

Which type of web server attack is represented?A. parameter manipulationB. heap memory corruptionC. command injection

D. blind SQL injectionAnswer: DQUESTION 96What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?A. MAC is controlled by the discretion of the owner and DAC is controlled by an administratorB. MAC is the strictest of all levels of control and DAC is object-based accessC. DAC is controlled by the operating system and MAC is controlled by an administratorD. DAC is the strictest of all levels of control and MAC is object-based accessAnswer: BQUESTION 97A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions.

Which identifier tracks an active program?A. application identification numberB. active process identification numberC. runtime identification numberD. process identification numberAnswer: DQUESTION 98A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?A. file typeB. file sizeC. file nameD. file hash valueAnswer: DQUESTION 99Which attack method intercepts traffic on a switched network?A. denial of serviceB. ARP cache poisoningC. DHCP snoopingD. command and controlAnswer: BExplanation: In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

QUESTION 100Which two elements are used for profiling a network? (Choose two.)A. session durationB. total throughputC. running processesD. listening portsE. OS fingerprintAnswer: ABExplanation: A network profile should include some important elements, such as the following: Total throughput - the amount of data passing from a given source to a given destination in a given period of time Session duration - the time between the establishment of a data flow and its termination Ports used - a list of TCP or UDP processes that are available to accept data Critical asset address space - the IP addresses or the logical location of essential systems or data

QUESTION 101What does an attacker use to determine which network ports are listening on a potential target device?A. man-in-the-middleB. port scanningC. SQL injectionD. ping sweepAnswer: BQUESTION 102What type of spoofing attack uses fake source IP addresses that are different than their real IP addresses?A. MAC spoofingB. IP spoofingC. application spoofingD. name spoofingAnswer: BQUESTION 103What is a purpose of a vulnerability management framework?A. identifies, removes, and mitigates system vulnerabilitiesB. detects and removes vulnerabilities in source codeC. conducts vulnerability scans on the networkD. manages a list of reported vulnerabilitiesAnswer: AQUESTION 104Refer to the exhibit. Which kind of attack method is depicted in this string?

A. cross-site scriptingB. man-in-the-middleC. SQL injectionD. denial of serviceAnswer: AQUESTION 105Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.472353	173.37.145.94	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.94	10.0.2.15	HTTP	249	HTTP/1.1 204 Not Modified
1987	6.736873	10.0.2.15	173.37.145.94	TCP	56	49522->80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
217	7.011111	10.0.2.15	173.37.145.94	TCP	62	80->49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
2222	7.244640	173.37.145.94	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
2322	7.244642	173.37.145.94	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
2542	7.512750	173.37.145.94	10.0.2.15	HTTP	642	HTTP/1.1 200 OK (GZIP) ...
2643	7.512793	10.0.2.15	173.37.145.94	TCP	56	49522->80 [ACK] Seq=6873 Ack=14979 Win=62480 Len=0

A. 2317B. 1986C. 2318D. 2542Answer: DQUESTION 106How does certificate authority impact a security system?A. It authenticates client identity when requesting SSL certificateB. It validates domain identity of a SSL certificateC. It authenticates domain identity when requesting SSL certificateD. It validates client identity when communicating with the serverAnswer:

QUESTION 107How is NetFlow different than traffic mirroring?
A. NetFlow collects metadata and traffic mirroring clones data
B. Traffic mirroring impacts switch performance and NetFlow does not
C. Traffic mirroring costs less to operate than NetFlow
D. NetFlow generates more data than traffic mirroring

Answer: A
QUESTION 108What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?
A. least privilege
B. need to know
C. integrity validation
D. due diligence

Answer: A
QUESTION 109Which type of data collection requires the largest amount of storage space?
A. alert data
B. transaction data
C. session data
D. full packet capture

Answer: D
QUESTION 110Which HTTP header field is used in forensics to identify the type of browser used?
A. referrer
B. host
C. user-agent
D. accept-language

Answer: C
QUESTION 111Refer to the exhibit. What is the potential threat identified in this Stealthwatch dashboard?



A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.
Answer: D
QUESTION 112A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs. Which technology should be used to accomplish this task?
A. application whitelisting/blacklisting
B. network NGFW
C. host-based IDS
D. antivirus/antispysware software

Answer: A
QUESTION 113What is the virtual address space for a Windows process?
A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used

10.44.101.23 - - [20/Nov/2017:10:54:15] "GET / HTTP/1.1" 200 5000
Gecko/20100101 Firefox/54.0"

A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file

Answer: C
QUESTION 115Which access control model does SELinux use?
A. RBAC
B. DACC
C. MAC
D. ABAC

Answer: C
QUESTION 116Which two compliance frameworks require that data be encrypted when it is transmitted over a public network? (Choose two.)
A. PCIB
B. GLBAC
C. HIPAA
D. SOXE
E. COBIT

Answer: AC
QUESTION 117Which IETF standard technology is useful to detect and analyze a potential security incident by recording session flows that occurs between hosts?
A. SFlow
B. NetFlow
C. NFlow
D. IPFIX

Answer: D
QUESTION 118What do the Security Intelligence Events within the FMC allow an administrator to do?
A. See if a host is connecting to a known-bad domain.
B. Check for host-to-server traffic within your network.
C. View any malicious files that a host has downloaded.
D. Verify host-to-host traffic within your network.

Answer: A
QUESTION 119The target web application server is running as the root user and is vulnerable to command injection. Which result of a successful attack is true?
A. cross-site scripting
B. cross-site scripting request forgery
C. privilege escalation
D. buffer overflow

Answer: B
QUESTION 120A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?
A. the intellectual property that was stolen
B. the defense contractor who stored the intellectual property
C. the method used to conduct the attack
D. the foreign government that conducted the attack

Answer: D
QUESTION 121What is the practice of giving an employee access to only the resources needed to accomplish their job?
A. principle of least privilege
B. organizational separation
C. separation of duties
D. need to know principle

Answer: A
QUESTION 122Which metric is used to capture the level of access

needed to launch a successful attack?A. privileges requiredB. user interactionC. attack complexityD. attack vectorAnswer:
AResources From:1.2023 Latest Braindump2go 200-201 Exam Dumps (PDF & VCE) Free Share:
<https://www.braindump2go.com/200-201.html>2.2023 Latest Braindump2go 200-201 PDF and 200-201 VCE Dumps Free Share:
<https://drive.google.com/drive/folders/1fTPALtM-eluHFw8sUjNGF7Y-ofOP3s-M?usp=sharing>Free Resources from
Braindump2go, We Devoted to Helping You 100% Pass All Exams!