

Exam Questions 210-250

Understanding Cisco Cybersecurity Fundamentals

<https://www.2passeasy.com/dumps/210-250/>



NEW QUESTION 1

which purpose of command and control for network aware malware is true?

- A. It helps the malware to profile the host
- B. It takes over the user account
- C. It contacts a remote server for command and updates
- D. It controls and down services on the infected host

Answer: C

NEW QUESTION 2

you get an alert on your desktop computer showing that an attack was successful on the host but up on investigation you see that occurred duration the attack. Which reason is true?

- A. The computer has HIDS installed on it
- B. The computer has NIDS installed on it
- C. The computer has HIPS installed on it
- D. The computer has NIPS installed on it

Answer: A

NEW QUESTION 3

According to the common vulnerability scoring system, which term is associated with scoring multiple vulnerabilities that are exploit in the course of a single attack?

- A. chained score
- B. risk analysis
- C. Vulnerability chaining
- D. Confidentiality

Answer: C

NEW QUESTION 4

Based on which statement does the discretionary access control security model grant or restrict access?

- A. discretion of the system administrator
- B. security policy defined by the owner of an object
- C. security policy defined by the system administrator
- D. role of a user within an organization

Answer: B

NEW QUESTION 5

For which kind of attack does an attacker use known information in encrypted files to break the encryption scheme for the rest of the file

- A. known-plaintext
- B. known-ciphertext
- C. unknown key
- D. man in the middle

Answer: A

NEW QUESTION 6

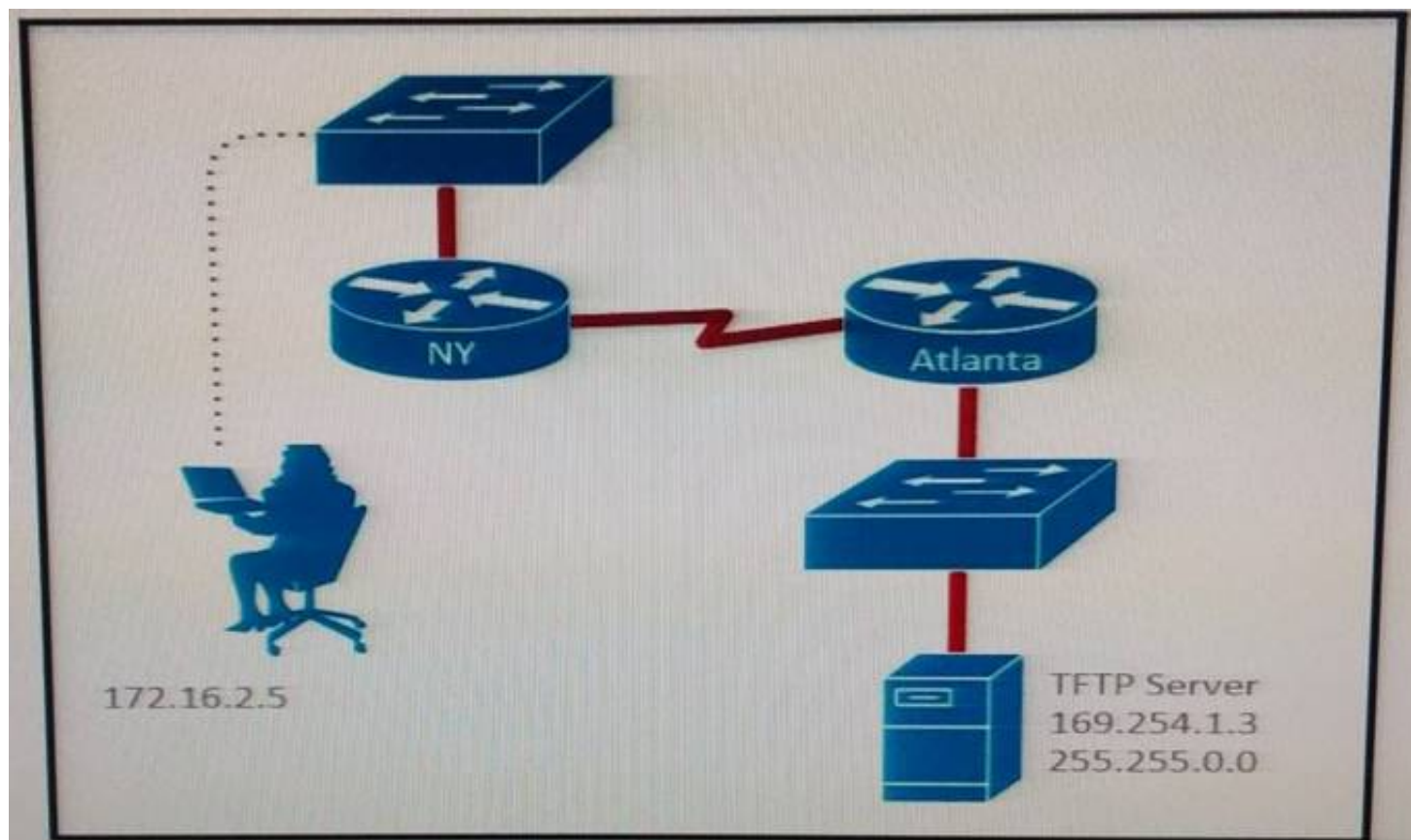
Which protocol maps IP network addresses to MAC hardware addresses so that IP packets can be sent across networks?

- A. Internet Control Message Protocol
- B. Address Resolution Protocol
- C. Session Initiation Protocol
- D. Transmission Control Protocol/Internet Protocol

Answer: B

NEW QUESTION 7

Refer to the exhibit.



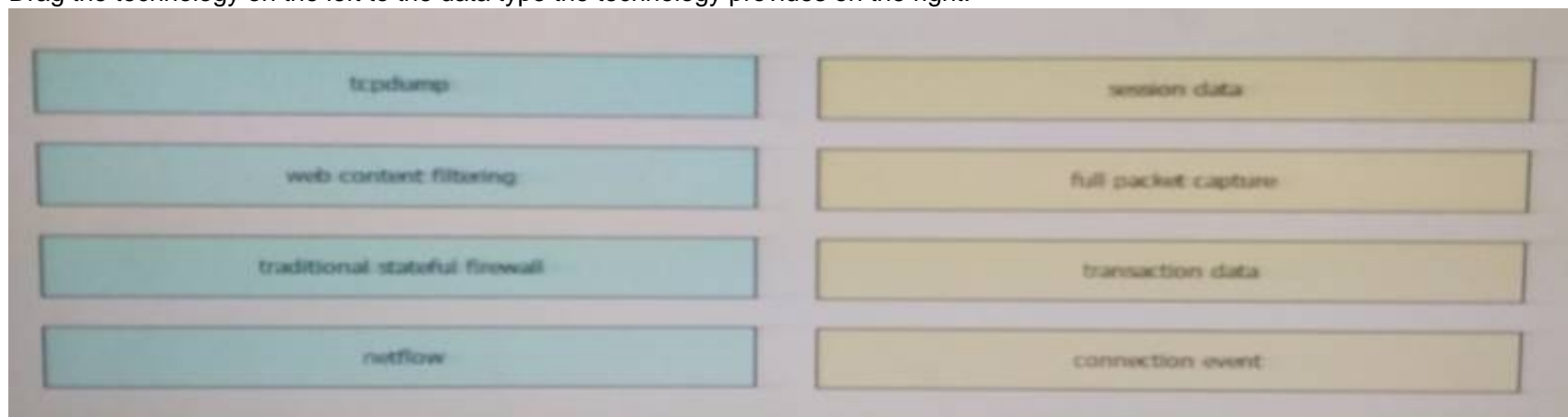
A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has attempted to make a connection to the TFTP server. They are unable to back up the configuration file and Cisco IOS of the NY router to the TFTP server Which cause of this problem is true?

- A. The TFTP server cannot obtain an address from a DHCP Server.
- B. The TFTP server has an incorrect IP address.
- C. The network administrator computer has an incorrect IP address
- D. The TFTP server has an incorrect subnet mask.

Answer: A

NEW QUESTION 8

Drag the technology on the left to the data type the technology provides on the right.



Answer:

Explanation: TCPDump = Full packet capture Netflow =Session Data
 Traditional stateful firewall = Connection Event Web content filtering = Transaction Data

NEW QUESTION 9

Which of the following are Cisco cloud security solutions?

- A. CloudDLP
- B. OpenDNS
- C. CloudLock
- D. CloudSLS

Answer: BC

NEW QUESTION 10

Which evasion method servers as an important functionality of ransomware?

- A. Encoding
- B. Encryption
- C. Resource exhaustion
- D. Extended sleep calls

Answer: B

NEW QUESTION 10

Which NTP command configures the local device as an NTP reference clock source?

- A. ntp peer
- B. ntp broadcast
- C. ntp master
- D. ntp server

Answer: C

NEW QUESTION 13

DNS query uses which protocol

- A. TCP
- B. UDP
- C. HTTP
- D. ICMP

Answer: B

NEW QUESTION 18

Endpoint logs indicate that a machine has obtained an unusual gateway address and unusual DNS servers via DHCP. Which option is this situation most likely an example of?

- A. Command injection
- B. Phishing
- C. Man in the middle attack
- D. Evasion methods

Answer: C

NEW QUESTION 19

An intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources. Which evasion technique does this attempt indicate?

- A. traffic fragmentation
- B. resource exhaustion
- C. timing attack
- D. tunneling

Answer: B

NEW QUESTION 24

What Does the sum of the risk presented by an application represent for that application ?

- A. Security violation
- B. Application Attack Surface
- C. HIPPA violation
- D. Vulnerability

Answer: B

NEW QUESTION 28

Which protocols is primarily supported by the 3rd layer of the OSI ref models ?

- A. HTTP/TLS
- B. ATM/MPLS
- C. Ipv4/IPv6
- D. TCP/UDP

Answer: C

NEW QUESTION 29

For which purpose can Windows management instrumentation be used?

- A. Remote viewing of a computer
- B. Remote blocking of malware on a computer
- C. Remote reboot of a computer
- D. Remote start of a computer

Answer: A

NEW QUESTION 31

Which term represents a weakness in a system that could lead to the system being compromised?

- A. vulnerability
- B. threat
- C. exploit
- D. risk

Answer: A

NEW QUESTION 34

Which term represents the likely hood of potential danger that could take advantage of a weakness in a system?

- A. vulnerability
- B. risk
- C. threat
- D. exploit

Answer: B

NEW QUESTION 37

If a router has four interfaces and each interface is connected to four switches, how many broadcast domains are present on the router?

- A. 1
- B. 2
- C. 4
- D. 8

Answer: C

NEW QUESTION 41

What does the sum of the risks presented by an application represent for that application?

- A. Application attack surface
- B. Security violation
- C. Vulnerability
- D. HIPPA violation

Answer: A

NEW QUESTION 46

You must create a vulnerability management framework. Which main purpose of this framework is true?

- A. Conduct vulnerability scans on the network.
- B. Manage a list of reported vulnerabilities.
- C. Identify, remove and mitigate system vulnerabilities.
- D. Detect and remove vulnerabilities in source code.

Answer: C

NEW QUESTION 50

What are the advantages of a full-duplex transmission mode compared to half-duplex mode? (Select all that apply.)

- A. Each station can transmit and receive at the same time.
- B. It avoids collisions.
- C. It makes use of back off time.
- D. It uses a collision avoidance algorithm to transmit.

Answer: AB

NEW QUESTION 55

Which event occurs when a signature-based IDS encounters network traffic that triggers an alert?

- A. connection event
- B. endpoint event
- C. NetFlow event
- D. intrusion event

Answer: D

NEW QUESTION 58

How many broadcast domains are created if three hosts are connected to a Layer 2 switch in full-duplex mode?

- A. 4
- B. 3
- C. None
- D. 1

Answer: D

NEW QUESTION 62

Which of the following are some useful reports you can collect from Cisco ISE related to endpoints? (Select all that apply.)

- A. Web Server Log reports
- B. Top Application reports
- C. RADIUS Authentication reports
- D. Administrator Login reports

Answer: ABD

NEW QUESTION 67

How does NTP help with monitoring?

- A. Using TCP allows you to view HTTP connections between servers and clients.
- B. By synchronizing the time of day allows correlation of events from different system logs.
- C. To receive system generated emails
- D. To look up IP addresses in the system using the FQDN.

Answer: B

NEW QUESTION 68

Which actions can a promiscuous IPS take to mitigate an attack? Choose three

- A. Denying Frames
- B. Resetting the TCP Connection
- C. Requesting host blocking
- D. Modifying packets
- E. Denying packets
- F. Requesting connection blocking

Answer: BCF

NEW QUESTION 70

Which Linux terminal command can be used to display all the processes?

- A. ps -ef
- B. ps -u
- C. ps -d
- D. ps -m

Answer: A

NEW QUESTION 75

Which option is a purpose of port scanning?

- A. Identify the Internet Protocol of the target system.
- B. Determine if the network is up or down
- C. Identify which ports and services are open on the target host.
- D. Identify legitimate users of a system.

Answer: C

NEW QUESTION 78

Which type of attack occurs when an attacker utilizes ABotnet to reflect requests off an NTP server to overwhelm their target?

- A. man in the middle
- B. denial of service
- C. distributed denial of service
- D. replay

Answer: C

NEW QUESTION 83

You have deployed an enterprise-wide-host/endpoint technology for all of the company corporate PCs Management asks you to block a selected set application on all corporate PCs. Which technology is the option?

- A. Application whitelisting/blacklisting
- B. Antivirus/antispysware software.
- C. Network NGFW
- D. Host-based IDS

Answer: A

NEW QUESTION 88

Which of the following are metrics that can measure the effectiveness of a runbook?

- A. Mean time to repair (MTTR)
- B. Mean time between failures (MTBF)
- C. Mean time to discover a security incident
- D. All of the above

Answer: D

NEW QUESTION 93

A zombie process occurs when which of the following happens?

- A. A process holds its associated memory and resources but is released from the entry table.
- B. A process continues to run on its own.
- C. A process holds on to associate memory but releases resources.
- D. A process releases the associated memory and resources but remains in the entry table.

Answer: D

NEW QUESTION 97

A child process that's permitted to continue on its own after its parent process is terminated. What is that child process called?

- A. Leaf.
- B. Child tab.
- C. Orphan
- D. Zombie.

Answer: C

NEW QUESTION 98

Which vulnerability is an example of Heartbleed?

- A. Buffer overflow
- B. Denial of service
- C. Command injection
- D. Information disclosure

Answer: D

NEW QUESTION 99

Which of the following are public key standards?

- A. IPSEC
- B. PKCS #10
- C. PKCS #12
- D. ISO33012
- E. AES

Answer: BC

NEW QUESTION 104

What is one of the advantages of the mandatory access control (MAC) model?

- A. Easy and scalable.
- B. Stricter control over the information access.
- C. The owner can decide whom to grant access to.

Answer: B

NEW QUESTION 106

The other one was, something similar to, what cryptography is used on Digital Certificates? The answers included:

- A. SHA-256
- B. SHA-512
- C. RSA 4096

Answer: A

NEW QUESTION 107

Which protocol is expected to have NTP a user agent, host, and referrer headers in a packet capture?

- A. NTP
- B. HTTP
- C. DNS

D. SSH

Answer: B

NEW QUESTION 108

Which data can be obtained using NetFlow?

- A. session data
- B. application logs
- C. network downtime
- D. report full packet capture

Answer: A

NEW QUESTION 109

Which term describes reasonable effort that must be made to obtain relevant information to facilitate appropriate courses of action?

- A. Due diligence
- B. ethical behavior
- C. decision making
- D. data mining.

Answer: A

NEW QUESTION 114

Which two features must a next generation firewall include? (Choose two.)

- A. data mining
- B. host-based antivirus
- C. application visibility and control
- D. Security Information and Event Management
- E. intrusion detection system

Answer: CE

NEW QUESTION 115

In which technology is network level encrypted not natively incorporated?

- A. Kerberos
- B. ssl
- C. tls
- D. IPsec

Answer: A

NEW QUESTION 116

Which technology allows a large number of private IP addresses to be represented by a smaller number of public IP addresses?

- A. NAT
- B. NTP
- C. RFC 1631
- D. RFC 1918

Answer: A

NEW QUESTION 119

What Linux commands show the process for all users?

- A. ps -a
- B. ps -u
- C. ps -d
- D. ps -m

Answer: A

NEW QUESTION 123

Stateful and traditional firewalls can analyze packets and judge them against a set of predetermined rules called access control lists (ACLs). They inspect which of the following elements within a packet? (Choose Two)

- A. Session headers
- B. NetFlow flow information
- C. Source and destination ports and source and destination IP addresses
- D. Protocol information

Answer: CD

NEW QUESTION 124

Which statement about digitally signing a document is true?

- A. The document is hashed and then the document is encrypted with the private key.
- B. The document is hashed and then the hash is encrypted with the private key.
- C. The document is encrypted and then the document is hashed with the public key
- D. The document is hashed and then the document is encrypted with the public key.

Answer: B

NEW QUESTION 126

Which vulnerability is an example of Shellshock?

- A. SQL injection
- B. heap Overflow
- C. cross site scripting
- D. command injection

Answer: D

NEW QUESTION 127

According to RFC 1035 which transport protocol is recommended for use with DNS queries?

- A. Transmission Control Protocol
- B. Reliable Data Protocol
- C. Hypertext Transfer Protocol
- D. User Datagram Protocol

Answer: D

NEW QUESTION 131

For which reason can HTTPS traffic make security monitoring difficult?

- A. encryption
- B. large packet headers
- C. Signature detection takes longer.
- D. SSL interception

Answer: A

NEW QUESTION 136

Which term represents the practice of giving employees only those permissions necessary to perform their specific role within an organization?

- A. integrity validation
- B. due diligence
- C. need to know
- D. least privilege

Answer: D

NEW QUESTION 140

Which term represents a potential danger that could take advantage of a weakness in a system?

- A. vulnerability
- B. risk
- C. threat
- D. exploit

Answer: D

NEW QUESTION 142

Which term represents the chronological record of how evidence was collected- analyzed, preserved, and transferred?

- A. chain of evidence
- B. evidence chronology
- C. chain of custody
- D. record of safekeeping

Answer: C

NEW QUESTION 146

Which three statements about host-based IPS are true? (Choose three.)

- A. It can view encrypted files.
- B. It can have more restrictive policies than network-based IPS.
- C. It can generate alerts based on behavior at the desktop level.
- D. It can be deployed at the perimeter.
- E. It uses signature-based policies.
- F. It works with deployed firewalls.

Answer: ABC

NEW QUESTION 150

Which definition of an antivirus program is true?

- A. program used to detect and remove unwanted malicious software from the system
- B. program that provides real time analysis of security alerts generated by network hardware and application
- C. program that scans a running application for vulnerabilities
- D. rules that allow network traffic to go in and out

Answer: A

NEW QUESTION 151

According to the attribute-based access control (ABAC) model, what is the subject location considered?

- A. Part of the environmental attributes
- B. Part of the object attributes
- C. Part of the access control attributes
- D. None of the above

Answer: A

NEW QUESTION 154

What event types does FMC record?

- A. standard common event logs types
- B. successful login event logs
- C. N/A

Answer: C

NEW QUESTION 155

Which definition of vulnerability is true?

- A. an exploitable unpatched and unmitigated weakness in software
- B. an incompatible piece of software
- C. software that does not have the most current patch applied
- D. software that was not approved for installation

Answer: A

NEW QUESTION 159

Which tool provides universal query access to text-based data such as event logs and file system?

- A. Service viewer
- B. Log parser
- C. Windows management instrumentation
- D. Handles

Answer: B

NEW QUESTION 161

Which definition of Windows Registry is true?

- A. set of pages that are currently resident in physical memory
- B. basic unit to which the operating system allocates processor time
- C. set of virtual memory addresses
- D. database that stores low-level settings for the operating system

Answer: D

NEW QUESTION 164

Which three options are types of Layer 2 network attack? (Choose three.)

- A. ARP attacks
- B. brute force attacks
- C. spoofing attacks
- D. DDOS attacks

- E. VLAN hopping
- F. botnet attacks

Answer: ACE

NEW QUESTION 168

Where does routing occur within the DoD TCP/IP reference model?

- A. application
- B. internet
- C. network
- D. transport

Answer: B

NEW QUESTION 173

Which two terms are types of cross site scripting attacks? (Choose two)

- A. directed
- B. encoded
- C. stored
- D. reflected
- E. cascaded

Answer: CD

NEW QUESTION 178

The FMC can share HTML, Pdf and csv data type that relate to a specific event type which event type:

- A. Connection
- B. Host
- C. Netflow
- D. Intrusion

Answer: D

NEW QUESTION 179

Which definition of permissions in Linux is true?

- A. rules that allow network traffic to go in and out
- B. table maintenance program
- C. written affidavit that you have to sign before using the system
- D. attributes of ownership and control of an object

Answer: D

NEW QUESTION 180

An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

- A. The switch could offer fake DHCP addresses.
- B. The switch could become the root bridge.
- C. The switch could be allowed to join the VTP domain
- D. The switch could become a transparent bridge.

Answer: B

NEW QUESTION 182

Which two actions are valid uses of public key infrastructure? (Choose two)

- A. ensuring the privacy of a certificate
- B. revoking the validation of a certificate
- C. validating the authenticity of a certificate
- D. creating duplicate copies of a certificate
- E. changing ownership of a certificate

Answer: AC

NEW QUESTION 187

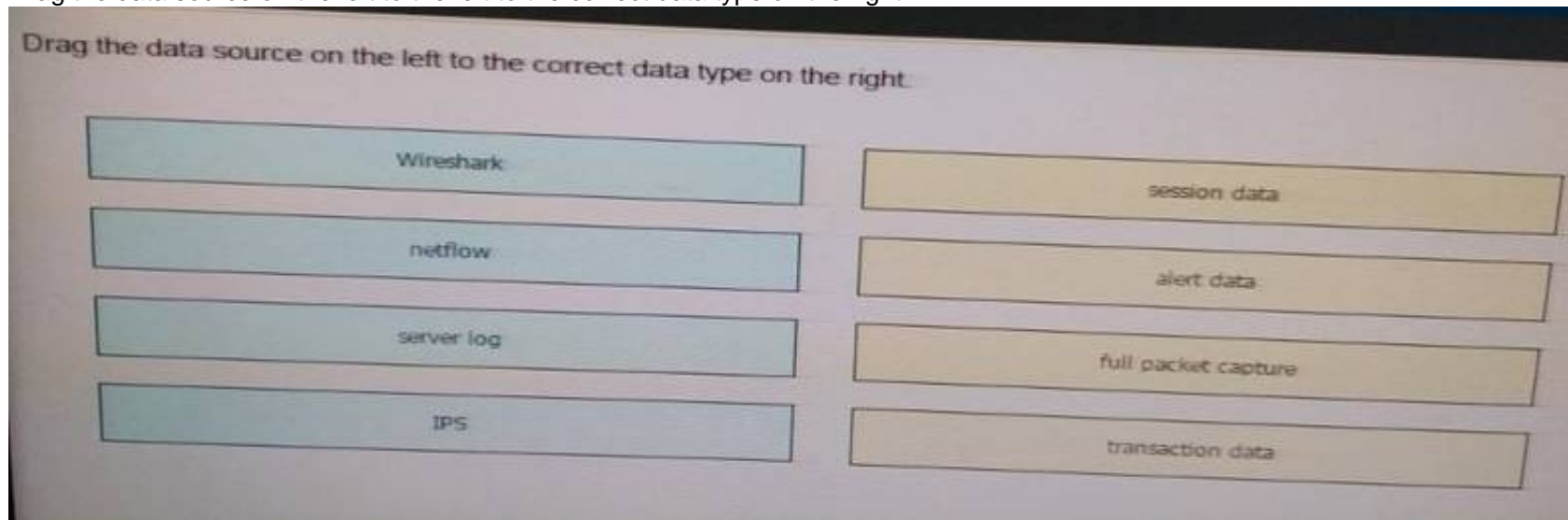
Which action is an attacker taking when they attempt to gain root access on the victim's system?

- A. privilege escalation
- B. command injections
- C. root kit
- D. command and control

Answer: A

NEW QUESTION 190

Drag the data source on the left to the left to the correct data type on the right.



Answer:

Explanation: Wireshark = Full packet capture
 Netflow = Session Data
 Server log = Transaction Data
 IPS = Alert data

NEW QUESTION 195

Which two protocols are often used for DDoS amplification attacks (choose two)

- A. HTTP
- B. TCP
- C. DNS
- D. ICMPv6
- E. NTP

Answer: CE

NEW QUESTION 200

Which hash algorithm is the weakest?

- A. SHA-512
- B. RSA 4096
- C. SHA-1
- D. SHA-256

Answer: C

NEW QUESTION 202

After a large influx of network traffic to externally facing devices, you begin investigating what appear to be a denial of service attack. When you review packets capture data, you notice that the traffic is a single SYN packet to each port. Which kind of attack is this?

- A. SYN flood.
- B. Host porfiling.
- C. Traffic fragmentation.
- D. Port scanning.

Answer: D

NEW QUESTION 207

Which type of exploit normally requires the culprit to have prior access to the target system?

- A. local exploit
- B. denial of service
- C. system vulnerability
- D. remote exploit

Answer: A

NEW QUESTION 211

A firewall requires deep packet inspection to evaluate which layer?

- A. application
- B. Internet
- C. link

D. transport

Answer: A

NEW QUESTION 212

In which case should an employee return his laptop to the organization?

- A. When moving to a different role
- B. Upon termination of the employment
- C. As described in the asset return policy
- D. When the laptop is end of lease

Answer: C

NEW QUESTION 215

which security principle is violated by running all processes as root/admin

- A. RBAC
- B. Principle of least privilege
- C. Segregation of duty

Answer: B

NEW QUESTION 216

What is a trunk link used for?

- A. To pass multiple virtual LANs
- B. To connect more than two switches
- C. To enable Spanning Tree Protocol
- D. To encapsulate Layer 2 frames

Answer: A

NEW QUESTION 217

Which of the following is true about heuristic-based algorithms?

- A. Heuristic-based algorithms may require fine tuning to adapt to network traffic and minimize the possibility of false positives.
- B. Heuristic-based algorithms do not require fine tuning.
- C. Heuristic-based algorithms support advanced malware protection.
- D. Heuristic-based algorithms provide capabilities for the automation of IPS signature creation and tuning.

Answer: A

NEW QUESTION 221

Which protocol is primarily supported by the Fourth layer of the Open Systems Interconnection reference model?

- A. HTTP/TLS
- B. IPv4/IPv6
- C. TCP/UDP
- D. ATM/ MPLS

Answer: C

NEW QUESTION 226

In which context is it inappropriate to use a hash algorithm?

- A. Telnet logins
- B. Verifying file integrity
- C. SSH logins
- D. Digital signature verification

Answer: A

NEW QUESTION 231

Which of the following access control models use security labels to make access decisions?

- A. Role-based access control (RBAC)
- B. Mandatory access control (MAC)
- C. Identity-based access control (IBAC)

Answer: B

NEW QUESTION 234

Cisco pxGrid has a unified framework with an open API designed in a hub-and-spoke architecture. pxGrid is used to enable the sharing of contextual-based

information from which devices?

- A. From a Cisco ASA to the Cisco OpenDNS service
- B. From a Cisco ASA to the Cisco WSA
- C. From a Cisco ASA to the Cisco FMC
- D. From a Cisco ISE session directory to other policy network systems, such as Cisco IOS devices and the Cisco ASA

Answer: D

NEW QUESTION 239

Which of the following are examples of system-based sandboxing implementations? (Select all that apply.)

- A. Google Project Zero
- B. Google Chromium sandboxing
- C. Java JVM sandboxing
- D. Threat Grid
- E. HTML5 “sandbox” attribute for use with iframes.

Answer: BCE

NEW QUESTION 243

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 210-250 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 210-250 Product From:

<https://www.2passeasy.com/dumps/210-250/>

Money Back Guarantee

210-250 Practice Exam Features:

- * 210-250 Questions and Answers Updated Frequently
- * 210-250 Practice Questions Verified by Expert Senior Certified Staff
- * 210-250 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 210-250 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year