Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

https://www.2passeasy.com/dumps/200-201/

NEW QUESTION 1
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

NEW QUESTION 2
An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

A. Recovery
B. Detection
C. Eradication
D. Analysis

Answer: B

NEW QUESTION 3
What is an advantage of symmetric over asymmetric encryption?

A. A key is generated on demand according to data type.
B. A one-time encryption key is generated for data transmission
C. It is suited for transmitting large amounts of data.
D. It is a faster encryption mechanism for sessions

Answer: D

NEW QUESTION 4
What makes HTTPS traffic difficult to monitor?

A. SSL interception
B. packet header size
C. signature detection time
D. encryption

Answer: D

NEW QUESTION 5
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

Explanation:
https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

NEW QUESTION 6
Drag and drop the type of evidence from the left onto the description of that evidence on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 7
What describes a buffer overflow attack?

A. injecting new commands into existing buffers
B. fetching data from memory buffer registers
C. overloading a predefined amount of memory
D. suppressing the buffers in a process

Answer: C

NEW QUESTION 8
An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, "File: Clean." Which regex must the analyst import?

A. File: Clean
B. ^Parent File Clean$
C. File: Clean (.*)
D. ^File: Clean$

Answer: A

NEW QUESTION 9
Refer to the exhibit.

An engineer received an event log file to review. Which technology generated the log?

A. NetFlow
B. proxy
C. firewall
D. IDS/IPS

Answer: C

NEW QUESTION 10
What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

A. DAC requires explicit authorization for a given user on a given object, and RBAC requires specific conditions.
B. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
D. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups

Answer: A

NEW QUESTION 10
Why is HTTPS traffic difficult to screen?

A. HTTPS is used internally and screening traffic (or external parties is hard due to isolation.
B. The communication is encrypted and the data in transit is secured.
C. Digital certificates secure the session, and the data is sent at random intervals.
D. Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

Answer: B

NEW QUESTION 15
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic
B. Tapping interrogations detect and block malicious traffic
C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A

Explanation:
A network TAP is a simple device that connects directly to the cabling infrastructure to split or copy packets for use in analysis, security, or general network management

NEW QUESTION 16
Refer 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

NEW QUESTION 21
What is the difference between deep packet inspection and stateful inspection?

A. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.
B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.
C. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.
D. Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

Answer: B

NEW QUESTION 23
What is a benefit of using asymmetric cryptography?

A. decrypts data with one key
B. fast data transfer
C. secure data transfer
D. encrypts data with one key

Answer: C

NEW QUESTION 25
Which piece of information is needed for attribution in an investigation?

A. proxy logs showing the source RFC 1918 IP addresses
B. RDP allowed from the Internet
C. known threat actor behavior
D. 802.1x RADIUS authentication pass arid fail logs

Answer: C

Explanation:
Actually this is the most important thing: know who, what, how, why, etc.. attack the network.

NEW QUESTION 27
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

A. total throughput on the interface of the router and NetFlow records
B. output of routing protocol authentication failures and ports used
C. running processes on the applications and their total network usage
D. deep packet captures of each application flow and duration

Answer: C

NEW QUESTION 31
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

NEW QUESTION 34
Refer to the exhibit.

Which field contains DNS header information if the payload is a query or a response?

A. Z
B. ID
C. TC
D. QR

Answer: B

NEW QUESTION 35
Refer to the exhibit.

Which two elements in the table are parts of the 5-tuple? (Choose two.)

A. First Packet
B. Initiator User
C. Ingress Security Zone
D. Source Port
E. Initiator IP

Answer: DE

NEW QUESTION 36
What 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 administrator
B. MAC is the strictest of all levels of control and DAC is object-based access
C. DAC is controlled by the operating system and MAC is controlled by an administrator
D. DAC is the strictest of all levels of control and MAC is object-based access

Answer: B

NEW QUESTION 37
What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

A. Untampered images are used in the security investigation process
B. Tampered images are used in the security investigation process
C. The image is tampered if the stored hash and the computed hash match

D. Tampered images are used in the incident recovery process
E. The image is untampered if the stored hash and the computed hash match

Answer: AE

Explanation:
Cert Guide by Omar Santos, Chapter 9 - Introduction to digital Forensics. "When you collect evidence, you must protect its integrity. This involves making sure that nothing is added to the evidence and that nothing is deleted or destroyed (this is known as evidence preservation)."

NEW QUESTION 38
Which artifact is used to uniquely identify a detected file?

A. file timestamp
B. file extension
C. file size
D. file hash

Answer: D

NEW QUESTION 40
Which event is user interaction?

A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file

Answer: D

NEW QUESTION 43
Which information must an organization use to understand the threats currently targeting the organization?

A. threat intelligence
B. risk scores
C. vendor suggestions
D. vulnerability exposure

Answer: A

NEW QUESTION 46
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: C

Explanation:
Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware’s vShield.

NEW QUESTION 50
The security team has detected an ongoing spam campaign targeting the organization. The team's approach is to push back the cyber kill chain and mitigate ongoing incidents. At which phase of the cyber kill chain should the security team mitigate this type of attack?

A. actions
B. delivery
C. reconnaissance
D. installation

Answer: B

NEW QUESTION 55
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

Explanation:
Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).
Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 57
Which evasion technique is a function of ransomware?

A. extended sleep calls
B. encryption
C. resource exhaustion
D. encoding

Answer: B

NEW QUESTION 58
What does cyber attribution identify in an investigation?

A. cause of an attack
B. exploit of an attack
C. vulnerabilities exploited
D. threat actors of an attack

Answer: D

Explanation:
https://www.techtarget.com/searchsecurity/definition/cyber-attribution

NEW QUESTION 61
Which process is used when IPS events are removed to improve data integrity?

A. data availability
B. data normalization
C. data signature
D. data protection

Answer: B

NEW QUESTION 65
Refer to the exhibit.

An attacker scanned the server using Nmap. What did the attacker obtain from this scan?

A. Identified a firewall device preventing the pert state from being returned.
B. Identified open SMB ports on the server
C. Gathered information on processes running on the server
D. Gathered a list of Active Directory users

Answer: C

NEW QUESTION 68
Which technology prevents end-device to end-device IP traceability?

A. encryption
B. load balancing
C. NAT/PAT
D. tunneling

Answer: C

NEW QUESTION 71
What describes the defense-m-depth principle?

A. defining precise guidelines for new workstation installations
B. categorizing critical assets within the organization
C. isolating guest Wi-Fi from the focal network
D. implementing alerts for unexpected asset malfunctions

Answer: B

NEW QUESTION 74

Refer to the exhibit.

A security analyst is investigating unusual activity from an unknown IP address Which type of evidence is this file1?

A. indirect evidence
B. best evidence
C. corroborative evidence
D. direct evidence

Answer: A

NEW QUESTION 78
An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

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

Answer: C

NEW QUESTION 83
Drag and drop the access control models from the left onto the correct descriptions on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 86
A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders After further investigation, the analyst learns that customers claim that they cannot access company servers According to NIST SP800-61, in which phase of the incident response process is the analyst?

A. post-incident activity
B. detection and analysis
C. preparation
D. containment, eradication, and recovery

Answer: B

NEW QUESTION 90
Refer to the exhibit.

What is occurring in this network?

A. ARP cache poisoning
B. DNS cache poisoning
C. MAC address table overflow
D. MAC flooding attack

Answer: A

NEW QUESTION 94
Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

A. The average time the SOC takes to register and assign the incident.
B. The total incident escalations per week.
C. The average time the SOC takes to detect and resolve the incident.
D. The total incident escalations per month.

Answer: C

NEW QUESTION 98
Which two elements of the incident response process are stated in NIST SP 800-61 r2? (Choose two.)

A. detection and analysis
B. post-incident activity
C. vulnerability scoring
D. vulnerability management
E. risk assessment

Answer: AB

NEW QUESTION 103
Which system monitors local system operation and local network access for violations of a security policy?

A. host-based intrusion detection
B. systems-based sandboxing
C. host-based firewall
D. antivirus

Answer: A

Explanation:
HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

NEW QUESTION 104
How does an attacker observe network traffic exchanged between two users?

A. port scanning
B. man-in-the-middle
C. command injection
D. denial of service

Answer: B

NEW QUESTION 105
Which 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

Explanation:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:12.0) Gecko/20100101 Firefox/12.0 In computing, a user agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with Web content".[1] A user agent is therefore a special kind of software agent.
https://en.wikipedia.org/wiki/User_agent#User_agent_identification
A user agent is a computer program representing a person, for example, a browser in a Web context. https://developer.mozilla.org/en-US/docs/Glossary/User_agent

NEW QUESTION 109
Which are two denial-of-service attacks? (Choose two.)

A. TCP connections
B. ping of death
C. man-in-the-middle
D. code-red
E. UDP flooding

Answer: BE

NEW QUESTION 111
What is a difference between SOAR and SIEM?

A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not
B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
C. SOAR receives information from a single platform and delivers it to a SIEM
D. SIEM receives information from a single platform and delivers it to a SOAR

Answer: A

NEW QUESTION 116
Syslog collecting software is installed on the server For the log containment, a disk with FAT type partition is used An engineer determined that log files are being corrupted when the 4 GB tile size is exceeded. Which action resolves the issue?

A. Add space to the existing partition and lower the retention penod.
B. Use FAT32 to exceed the limit of 4 GB.

C. Use the Ext4 partition because it can hold files up to 16 TB.
D. Use NTFS partition for log file containment

Answer: D

NEW QUESTION 121
According to the NIST SP 800-86. which two types of data are considered volatile? (Choose two.)

A. swap files
B. temporary files
C. login sessions
D. dump files
E. free space

Answer: CE

NEW QUESTION 124
Refer 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 manipulation
B. heap memory corruption
C. command injection
D. blind SQL injection

Answer: D

NEW QUESTION 125
A 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/antispyware software

Answer: A

NEW QUESTION 129
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

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

Answer: B

NEW QUESTION 134
What are two social engineering techniques? (Choose two.)

A. privilege escalation
B. DDoS attack
C. phishing
D. man-in-the-middle
E. pharming

Answer: CE

NEW QUESTION 136
An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?

A. social engineering
B. eavesdropping
C. piggybacking
D. tailgating

Answer: A

NEW QUESTION 138
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

NEW QUESTION 139
An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

A. nmap --top-ports 192.168.1.0/24
B. nmap –sP 192.168.1.0/24
C. nmap -sL 192.168.1.0/24
D. nmap -sV 192.168.1.0/24

Answer: B

Explanation:
https://explainshell.com/explain?cmd=nmap+-sP

NEW QUESTION 142
What is the difference between vulnerability and risk?

A. A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.
B. A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself
C. A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.
D. A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit

Answer: C

NEW QUESTION 144
Refer to the exhibit.

What does the message indicate?

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

NEW QUESTION 145
Which technology on a host is used to isolate a running application from other applications?

A. sandbox
B. application allow list
C. application block list
D. host-based firewall

Answer: A

NEW QUESTION 149
Refer to the exhibit.

In which Linux log file is this output found?

A. /var/log/authorization.log
B. /var/log/dmesg
C. var/log/var.log
D. /var/log/auth.log

Answer: D

NEW QUESTION 150
What 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

NEW QUESTION 152
Which utility blocks a host portscan?

A. HIDS
B. sandboxing
C. host-based firewall
D. antimalware

Answer: C

NEW QUESTION 155
Refer to the exhibit.

What does this output indicate?

A. HTTPS ports are open on the server.
B. SMB ports are closed on the server.
C. FTP ports are open on the server.
D. Email ports are closed on the server.

Answer: D

NEW QUESTION 157
Refer to the exhibit.

What is occurring in this network traffic?

A. High rate of SYN packets being sent from a multiple source towards a single destination IP.
B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.
C. Flood of ACK packets coming from a single source IP to multiple destination IPs.
D. Flood of SYN packets coming from a single source IP to a single destination IP.

Answer: D

NEW QUESTION 161
How does an SSL certificate impact security between the client and the server?

A. by enabling an authenticated channel between the client and the server
B. by creating an integrated channel between the client and the server
C. by enabling an authorized channel between the client and the server
D. by creating an encrypted channel between the client and the server

Answer: D

NEW QUESTION 162
Refer to the exhibit.

An employee received an email from an unknown sender with an attachment and reported it as a phishing attempt. An engineer uploaded the file to Cuckoo for further analysis. What should an engineer interpret from the provided Cuckoo report?

A. Win32.polip.a.exe is an executable file and should be flagged as malicious.

B. The file is clean and does not represent a risk.
C. Cuckoo cleaned the malicious file and prepared it for usage.
D. MD5 of the file was not identified as malicious.

Answer: C

NEW QUESTION 165
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity
B. confidentiality
C. availability
D. scope

Answer: A

NEW QUESTION 170
What is an attack surface as compared to a vulnerability?

A. any potential danger to an asset
B. the sum of all paths for data into and out of the environment
C. an exploitable weakness in a system or its design
D. the individuals who perform an attack

Answer: C

Explanation:
An attack surface is the total sum of vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. The term attack surface is often confused with the term attack vector, but they are not the same thing. The surface is what is being attacked; the vector is the means by which an intruder gains access.

NEW QUESTION 172
What are the two differences between stateful and deep packet inspection? (Choose two)

A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports
B. Deep packet inspection is capable of malware blocking, and stateful inspection is not
C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model
D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.
E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

Answer: AB

NEW QUESTION 177
How is NetFlow different from 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

NEW QUESTION 181
An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

A. management and reporting
B. traffic filtering
C. adaptive AVC
D. metrics collection and exporting
E. application recognition

Answer: AE

NEW QUESTION 184
Which type of evidence supports a theory or an assumption that results from initial evidence?

A. probabilistic
B. indirect
C. best
D. corroborative

Answer: D

Explanation:
Corroborating evidence (or corroboration) is evidence that tends to support a theory or an assumption deduced by some initial evidence. This corroborating

evidence confirms the proposition. Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

NEW QUESTION 188
A security incident occurred with the potential of impacting business services. Who performs the attack?

A. malware author
B. threat actor
C. bug bounty hunter
D. direct competitor

Answer: B

NEW QUESTION 190
How does an attack surface differ from an attack vector?

A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.
B. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.
C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.
D. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Answer: B

NEW QUESTION 191
Which security monitoring data type requires the largest storage space?

A. transaction data
B. statistical data
C. session data
D. full packet capture

Answer: D

NEW QUESTION 194
Which technology should be used to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier, and SSL session ID attributes?

A. AWS
B. IIS
C. Load balancer
D. Proxy server

Answer: C

Explanation:
Load Balancing: HTTP(S) load balancing is one of the oldest forms of load balancing. This form of load balancing relies on layer 7, which means it operates in the application layer. This allows routing decisions based on attributes like HTTP header, uniform resource identifier, SSL session ID, and HTML form data.
Load balancing applies to layers 4-7 in the seven-layer Open System Interconnection (OSI) model. Its capabilities are: L4. Directing traffic based on network data and transport layer protocols, e.g., IP address and TCP port. L7. Adds content switching to load balancing, allowing routing decisions depending on characteristics such as HTTP header, uniform resource identifier, SSL session ID, and HTML form data. GSLB. Global Server Load Balancing expands L4 and L7 capabilities to servers in different sites

NEW QUESTION 199
Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

A. src=10.11.0.0/16 and dst=10.11.0.0/16
B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
D. src==10.11.0.0/16 and dst==10.11.0.0/16

Answer: B

NEW QUESTION 204
An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.
What is the initial event called in the NIST SP800-61?

A. online assault
B. precursor
C. trigger
D. instigator

Answer: B

Explanation:
A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.

The following are common sources of precursor and indicator information:

Security Information and Event Management (SIEM)
Anti-virus and anti-spam software
File integrity checking applications/software
Logs from various sources (operating systems, devices, and applications)
People who report a security incident https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NEW QUESTION 205
Refer to the exhibit.

What is occurring?

A. ARP flood
B. DNS amplification
C. ARP poisoning
D. DNS tunneling

Answer: D

NEW QUESTION 209
An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture, the analyst cannot determine the technique and payload used for the communication.

Which obfuscation technique is the attacker using?

A. Base64 encoding
B. TLS encryption
C. SHA-256 hashing
D. ROT13 encryption

Answer: B

Explanation:
ROT13 is considered weak encryption and is not used with TLS (HTTPS:443). Source: https://en.wikipedia.org/wiki/ROT13

NEW QUESTION 212

What is an incident response plan?

A. an organizational approach to events that could lead to asset loss or disruption of operations
B. an organizational approach to security management to ensure a service lifecycle and continuous improvements
C. an organizational approach to disaster recovery and timely restoration of operational services
D. an organizational approach to system backup and data archiving aligned to regulations

Answer: C

NEW QUESTION 214
Refer to the exhibit.

What is shown in this PCAP file?

A. Timestamps are indicated with error.
B. The protocol is TCP.
C. The User-Agent is Mozilla/5.0.
D. The HTTP GET is encoded.

Answer: D

NEW QUESTION 216
What is a description of a social engineering attack?

A. fake offer for free music download to trick the user into providing sensitive data
B. package deliberately sent to the wrong receiver to advertise a new product
C. mistakenly received valuable order destined for another person and hidden on purpose
D. email offering last-minute deals on various vacations around the world with a due date and a counter

Answer: D

NEW QUESTION 217
Which action prevents buffer overflow attacks?

A. variable randomization
B. using web based applications
C. input sanitization
D. using a Linux operating system

Answer: C

NEW QUESTION 218
In a SOC environment, what is a vulnerability management metric?

A. code signing enforcement
B. full assets scan
C. internet exposed devices
D. single factor authentication

Answer: C

NEW QUESTION 219
Which tool provides a full packet capture from network traffic?

A. Nagios
B. CAINE
C. Hydra
D. Wireshark

Answer: D

NEW QUESTION 221
What is the impact of encryption?

A. Confidentiality of the data is kept secure and permissions are validated
B. Data is accessible and available to permitted individuals
C. Data is unaltered and its integrity is preserved
D. Data is secure and unreadable without decrypting it

Answer: A

NEW QUESTION 222
Which vulnerability type is used to read, write, or erase information from a database?

A. cross-site scripting
B. cross-site request forgery
C. buffer overflow
D. SQL injection

Answer: D

NEW QUESTION 223
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. known-plaintext
B. replay
C. dictionary
D. man-in-the-middle

Answer: D

NEW QUESTION 226
Which regular expression is needed to capture the IP address 192.168.20.232?

A. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}
B. ^ (?:[0-9]f1,3}\.){1,4}
C. ^ (?:[0-9]{1,3}\.)'
D. ^ ([0-9]-{3})

Answer: A

NEW QUESTION 231
A user received a malicious attachment but did not run it. Which category classifies the intrusion?

A. weaponization
B. reconnaissance
C. installation
D. delivery

Answer: D

NEW QUESTION 232
A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

A. event name, log source, time, source IP, and host name
B. protocol, source IP, source port, destination IP, and destination port
C. event name, log source, time, source IP, and username
D. protocol, log source, source IP, destination IP, and host name

Answer: B

NEW QUESTION 237
Refer to the exhibit.

A company employee is connecting to mail google.com from an endpoint device. The website is loaded but with an error. What is occurring?

A. DNS hijacking attack
B. Endpoint local time is invalid.
C. Certificate is not in trusted roots.
D. man-m-the-middle attack

Answer: C

NEW QUESTION 242
Which security model assumes an attacker within and outside of the network and enforces strict verification
before connecting to any system or resource within the organization?

A. Biba
B. Object-capability
C. Take-Grant
D. Zero Trust

Answer: D

Explanation:
Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

NEW QUESTION 245
What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

A. additional PPTP traffic due to Windows clients
B. unauthorized peer-to-peer traffic
C. deployment of a GRE network on top of an existing Layer 3 network
D. attempts to tunnel IPv6 traffic through an IPv4 network

Answer: D

NEW QUESTION 246
Refer to the exhibit.

Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

A. 7,14, and 21
B. 7 and 21
C. 14,16,18, and 19
D. 7 to 21

Answer: B

NEW QUESTION 247
Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

A. Hypertext Transfer Protocol
B. SSL Certificate
C. Tunneling
D. VPN

Answer: B

NEW QUESTION 249
Refer to the exhibit.

A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of
requests and data being transmitted What is occurring?

A. indicators of denial-of-service attack due to the frequency of requests
B. garbage flood attack attacker is sending garbage binary data to open ports
C. indicators of data exfiltration HTTP requests must be plain text
D. cache bypassing attack: attacker is sending requests for noncacheable content

Answer: D

NEW QUESTION 251
What are two denial-of-service (DoS) attacks? (Choose two)

A. port scan
B. SYN flood

C. man-in-the-middle
D. phishing
E. teardrop

Answer: BC

NEW QUESTION 255
A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

If the process is unsuccessful, a negative value is returned.
If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.
Which component results from this operation?

A. parent directory name of a file pathname
B. process spawn scheduled
C. macros for managing CPU sets
D. new process created by parent process

Answer: D

Explanation:
There are two tasks with specially distinguished process IDs: swapper or sched has process ID 0 and is responsible for paging, and is actually part of the kernel rather than a normal user-mode process. Process ID 1 is usually the init process primarily responsible for starting and shutting down the system. Originally, process ID 1 was not specifically reserved for init by any technical measures: it simply had this ID as a natural consequence of being the first process invoked by the kernel. More recent Unix systems typically have additional kernel components visible as 'processes', in which case PID 1 is actively reserved for the init process to maintain consistency with older systems

NEW QUESTION 257
What is the difference between the rule-based detection when compared to behavioral detection?

A. Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.
B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes.
C. Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.
D. Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

Answer: D

NEW QUESTION 260
......