Cisco.300-215.v2026-01-19.q73

Exam Code:	300-215
Exam Name:	Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps
Certification Provider:	Cisco
Free Question Number:	73
Version:	v2026-01-19
# of views:	111
# of Questions views:	805
https://www.dumpsfiles.com/files/Cisco/300-215/Cisco.300-215.v2026-01-19.q73	

NEW QUESTION: 1
During a routine inspection of system logs, a security analyst notices an entry where Microsoft Word initiated a PowerShell command with encoded arguments. Given that the user's role does not involve scripting or advanced document processing, which action should the analyst take to analyze this output for potential indicators of compromise?
A. Monitor the Microsoft Word startup times to ensure they align with business hours.
B. Confirm that the Microsoft Word license is valid and the application is updated to the latest version.
C. Validate the frequency of PowerShell usage across all hosts to establish a baseline.
D. Review the encoded PowerShell arguments to decode and determine the intent of the script.
Answer: D (LEAVE A REPLY)
According to theCyberOps Technologies (CBRFIR) 300-215 study guidecurriculum, when analyzing suspicious behavior-especially when scripts or shell commands are executed from applications like Word (which is uncommon)-the encoded PowerShell payload must be decoded to determine if malicious intent is present. Deobfuscation is a critical step in identifying command-and-control behavior, persistence, or malware execution paths.
-

NEW QUESTION: 2
A threat actor has successfully attacked an organization and gained access to confidential files on a laptop.
What plan should the organization initiate to contain the attack and prevent it from spreading to other network devices?
A. root cause

B. intrusion prevention
C. incident response
D. attack surface
Answer: C (LEAVE A REPLY)
Once an incident has occurred, the appropriate course of action is to engage the organization's Incident Response (IR) plan. This is a structured approach to contain, analyze, and eradicate threats before they spread across the network.
The Cisco CyberOps Associate study guide emphasizes:
* "Incident response and handling are essential within an organization... The main objective of implementing an incident handling process is to reduce the impact of a cyber-attack, ensure the damages caused are assessed, and implement recovery procedures".
* In particular, the containment phase of IR is focused on isolating the threat and preventing lateral movement or further compromise.
Options such as "root cause" or "attack surface" are relevant at later stages of analysis and mitigation, not immediate containment. Therefore, the correct answer is C.

NEW QUESTION: 3
Which tool conducts memory analysis?
A. MemDump
B. Volatility
C. Sysinternals Autoruns
D. Memoryze
Answer: (SHOW ANSWER)

NEW QUESTION: 4

Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name:iraniansk.com

B. Content-Type: application/octet-stream

C. Hash value: 5f31ab113af08=1597090577

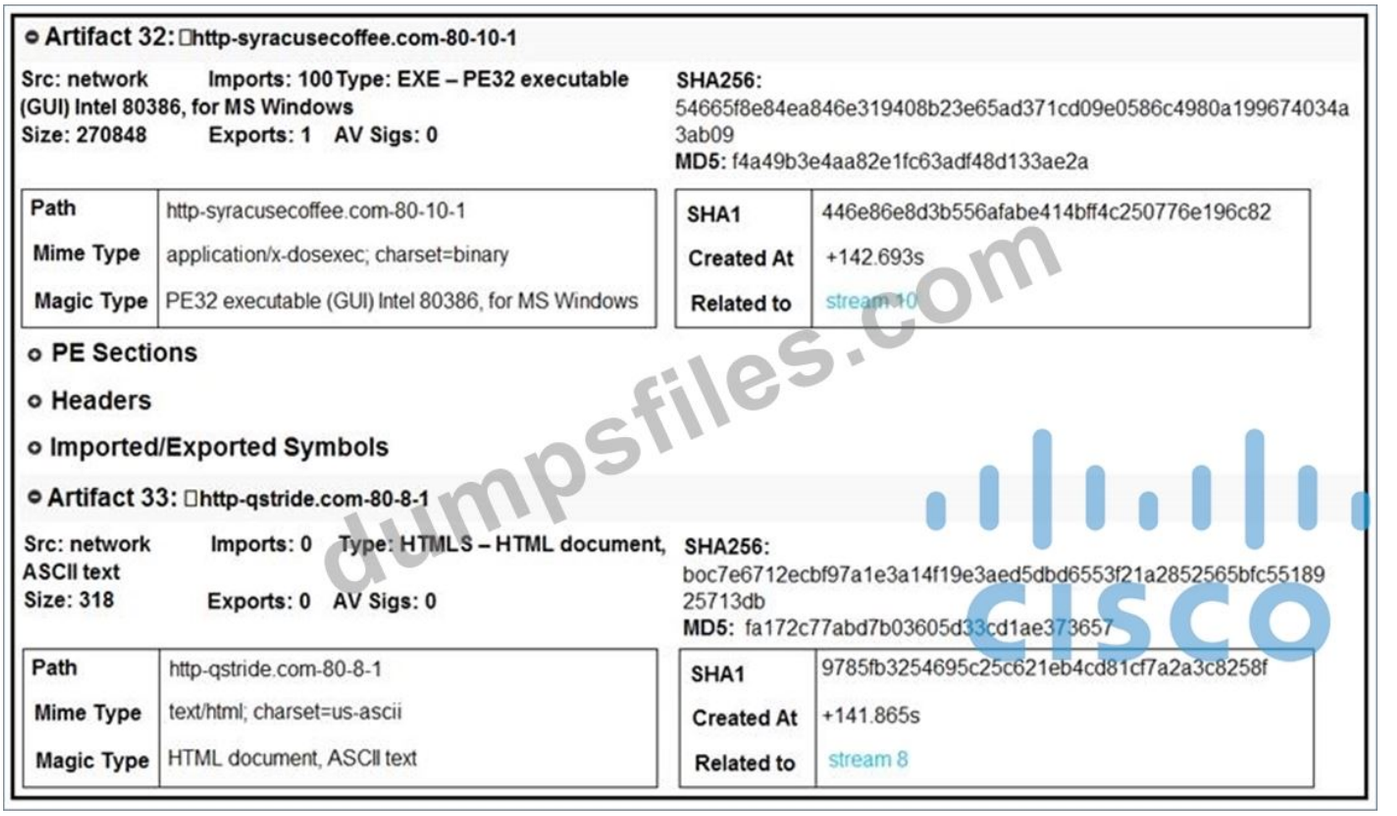
D. Server: nginx

E. filename= "Fy.exe"

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 5

Refer to the exhibit.



What do these artifacts indicate?

A. The MD5 of a file is identified as a virus and is being blocked.

B. A malicious file is redirecting users to different domains.

C. An executable file is requesting an application download.

D. A forged DNS request is forwarding users to malicious websites.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 6

A cybersecurity analyst must identify an unknown service causing high CPU on a Windows server. What tool should be used?

A. Volatility to analyze memory dumps for forensic investigation

B. Process Explorer from the Sysinternals Suite to monitor and examine active processes

C. TCPdump to capture and analyze network packets

D. SIFT (SANS Investigative Forensic Toolkit) for comprehensive digital forensics

Answer: B (LEAVE A REPLY)

Process Explorer is an advanced Windows-based utility that shows real-time data about running processes, CPU usage, services, DLLs, and handles. It is specifically designed for this kind of investigation and is part of the Sysinternals Suite.

NEW QUESTION: 7

An "unknown error code" is appearing on an ESXi host during authentication. An engineer checks the authentication logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

A. /var/log/syslog.log

B. /var/log/vmksummary.log

C. /var/log/shell.log

D. /var/log/general/log

Answer: B (LEAVE A REPLY)

In VMware ESXi systems, the vmksummary.log file is responsible for capturing general system events, including uptime, reboot statistics, and key service-related issues. It serves as a valuable source for troubleshooting persistent or unexplained system behaviors.

The Cisco CyberOps study guide references log file paths used in system diagnostics and incident response, and for authentication-related issues on ESXi where standard logs don't yield insights, vmksummary.log is the recommended next source for identifying systemic service faults or anomalies.

NEW QUESTION: 8

A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file's behavior. Which logs should be reviewed next to evaluate this file further?

A. DNS server

B. network device

C. Antivirus solution

D. email security appliance

Answer: A (LEAVE A REPLY)

NEW QUESTION: 9

A security team received an alert of suspicious activity on a user's Internet browser. The user's anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

A. Evaluate the process activity in Cisco Umbrella.

B. Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).

C. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).

D. Analyze the Magic File type in Cisco Umbrella.

E. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Answer: B,C (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 10

Refer to the exhibit.

After a cyber attack, an engineer is analyzing an alert that was missed on the intrusion detection system. The attack exploited a vulnerability in a business-critical, web-based application and violated its availability.

Which two mitigation techniques should the engineer recommend? (Choose two.)

A. encapsulation

B. NOP sled technique

C. address space randomization

D. heap-based security

E. data execution prevention

Answer: C,E (LEAVE A REPLY)

The alert indicates aWebDAV Stack Buffer Overflow, which is amemory corruptionattack targeting the stack, a common vector forremote code executionordenial-of-service (DoS).

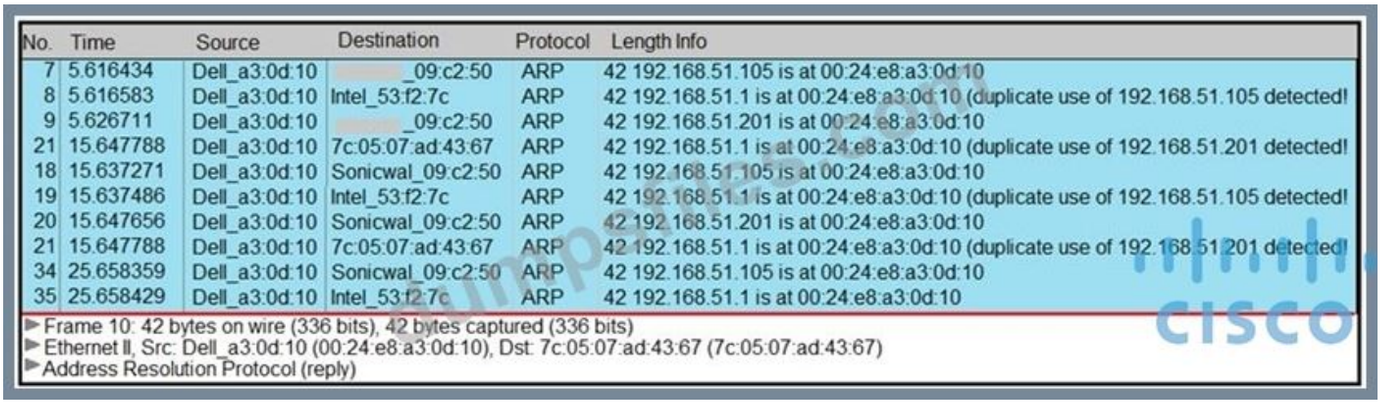
To mitigate such exploits, two effective system-hardening techniques are:

* C. Address Space Layout Randomization (ASLR):Randomizes memory addresses used by system and application processes, making it difficult for attackers to predict where their malicious code will be executed.

* E. Data Execution Prevention (DEP):Prevents execution of code from non-executable memory regions such as the stack, thus stopping buffer overflow attacks from successfully executing payloads.

Both are well-established protections against stack-based buffer overflow attacks and are strongly recommended in the Cisco CyberOps Associate guide and general security best practices.

NEW QUESTION: 11
Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length Info
7	5.616434	Dell_a3:0d:10	_09:c2:50	ARP	42 192.168.51.105 is at 00:24:e8:a3:0d:10
8	5.616583	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
9	5.626711	Dell_a3:0d:10	_09:c2:50	ARP	42 192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
18	15.637271	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42 192.168.51.105 is at 00:24:e8:a3:0d:10
19	15.637486	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
20	15.647656	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42 192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
34	25.658359	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42 192.168.51.105 is at 00:24:e8:a3:0d:10
35	25.658429	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42 192.168.51.1 is at 00:24:e8:a3:0d:10

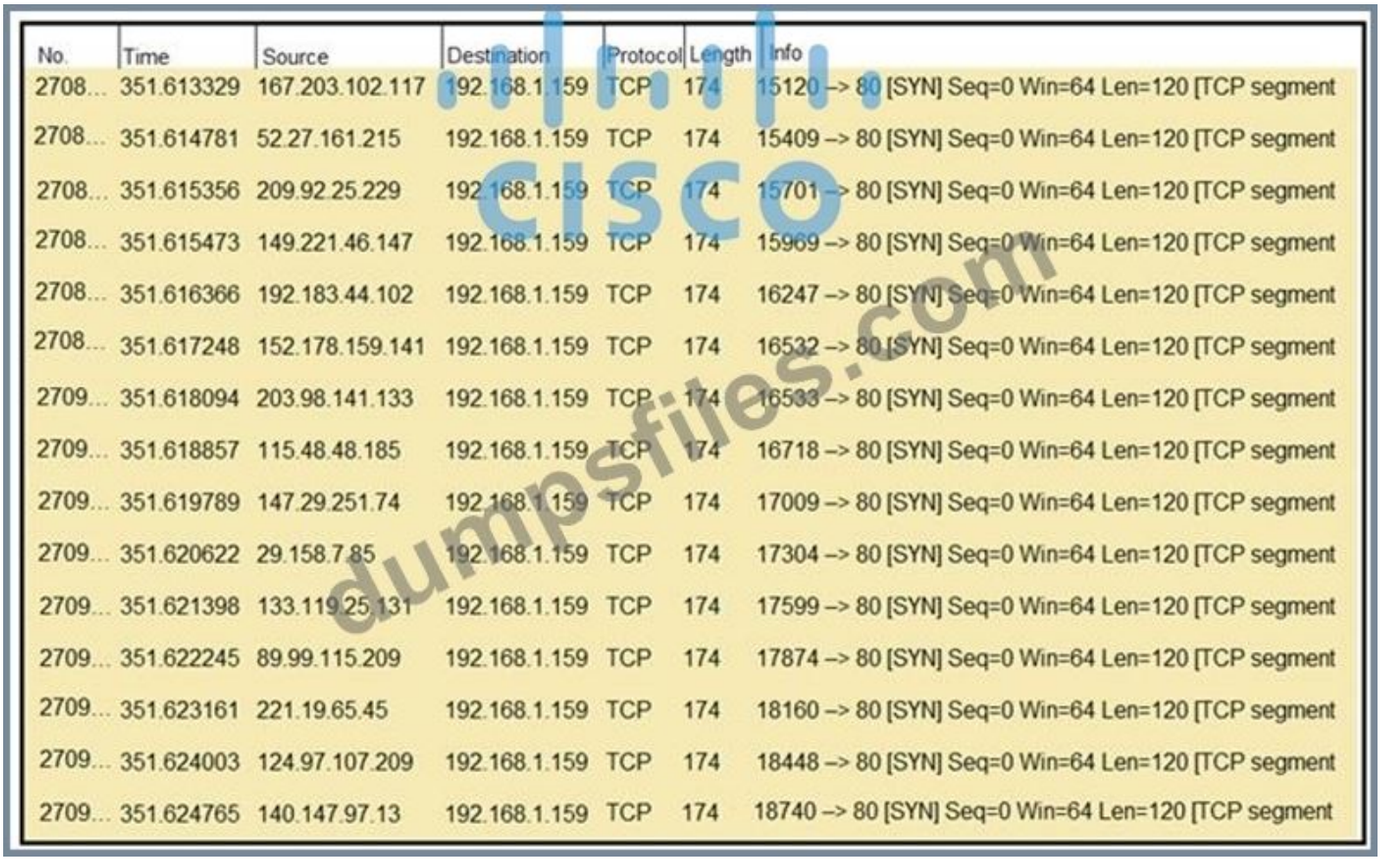
▶ Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▶ Ethernet II, Src: Dell_a3:0d:10 (00:24:e8:a3:0d:10), Dst: 7c:05:07:ad:43:67 (7c:05:07:ad:43:67)
▶ Address Resolution Protocol (reply)

A security analyst notices unusual connections while monitoring traffic. What is the attack vector, and which action should be taken to prevent this type of event?
A. MAC flooding; assign static entries
B. SYN flooding, block malicious packets
C. DNS spoofing; encrypt communication protocols
D. ARP spoofing; configure port security
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
An organization fell victim to a ransomware attack that successfully infected 256 hosts within its network. In the aftermath of this incident, the organization's cybersecurity team must prepare a thorough root cause analysis report. This report aims to identify the primary factor or factors that led to the successful ransomware attack and to develop strategies for preventing similar incidents in the future. In this context, what should the cybersecurity engineer include in the root cause analysis report to demonstrate the underlying cause of the incident?
A. log files from each of the 256 infected hosts
B. detailed information about the specific team members involved in the incident response effort
C. method of infection employed by the ransomware
D. complete threat intelligence report shared by the National CERT Association
Answer: C (LEAVE A REPLY)
According to the Cisco CyberOps Associate guide, the goal of a root cause analysis is to determine how an attacker successfully exploited a system so that similar vulnerabilities can be mitigated in the future. The
"method of infection" (e.g., phishing email with malicious attachment, drive-by download, credential compromise, etc.) is the most relevant factor in understanding the initial access vector and subsequent spread of ransomware across the network.
-

NEW QUESTION: 13

Refer to the exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
2708...	351.613329	167.203.102.117	192.168.1.159	TCP	174	15120 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.614781	52.27.161.215	192.168.1.159	TCP	174	15409 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615356	209.92.25.229	192.168.1.159	TCP	174	15701 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615473	149.221.46.147	192.168.1.159	TCP	174	15969 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.616366	192.183.44.102	192.168.1.159	TCP	174	16247 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.617248	152.178.159.141	192.168.1.159	TCP	174	16532 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618094	203.98.141.133	192.168.1.159	TCP	174	16533 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618857	115.48.48.185	192.168.1.159	TCP	174	16718 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.619789	147.29.251.74	192.168.1.159	TCP	174	17009 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.620622	29.158.7.85	192.168.1.159	TCP	174	17304 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.621398	133.119.25.131	192.168.1.159	TCP	174	17599 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.622245	89.99.115.209	192.168.1.159	TCP	174	17874 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.623161	221.19.65.45	192.168.1.159	TCP	174	18160 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624003	124.97.107.209	192.168.1.159	TCP	174	18448 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624765	140.147.97.13	192.168.1.159	TCP	174	18740 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment

What should an engineer determine from this Wireshark capture of suspicious network traffic?

A. There are signs of ARP spoofing, and the engineer should use Static ARP entries and IP address-to-MAC address mappings as a countermeasure.

B. There are signs of a malformed packet attack, and the engineer should limit the packet size and set a threshold of bytes as a countermeasure.

C. There are signs of SYN flood attack, and the engineer should increase the backlog and recycle the oldest half-open TCP connections.

D. There are signs of a DNS attack, and the engineer should hide the BIND version and restrict zone transfers as a countermeasure.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 14

An insider scattered multiple USB flash drives with zero-day malware in a company HQ building. Many employees connected the USB flash drives to their workstations. An attacker was able to get access to endpoints from outside, steal user credentials, and exfiltrate confidential information from internal web resources. Which two steps prevent these types of security incidents in the future? (Choose two.)

A. Automate security alerts on connected USB flash drives to workstations.

B. Provide security awareness training and block usage of external drives.

C. Deploy antivirus software on employee workstations to detect malicious software.

D. Encrypt traffic from employee workstations to internal web services.

E. Deploy MFA authentication to prevent unauthorized access to critical assets.

Answer: B,E (LEAVE A REPLY)
The scenario describes an attack vector where insiders or malicious actors useremovable media (USB drives) to introduce malware, which then connects to external sources to exfiltrate data and compromise systems.
* Option B addresses the human factor and technological prevention. The guide stresses the need for training to ensure users are aware of social engineering and removable media risks. Blocking the use of USB drives at a system level further minimizes attack vectors.
* Option E, usingMulti-Factor Authentication (MFA), provides an additional layer of defense. Even if credentials are stolen, MFA can prevent the attacker from accessing sensitive internal resources without the second authentication factor.
These controls align with defense-in-depth strategies recommended in the Cisco CyberOps Associate curriculum to combat insider threats and external unauthorized access.

NEW QUESTION: 15
What is a use of TCPdump?
A. to analyze IP and other packets
B. to view encrypted data fields
C. to decode user credentials
D. to change IP ports
Answer: A (LEAVE A REPLY)
TCPdump is a command-line packet analyzer used to capture and inspect network packets. As described in the study guide, "tcpdump is a command-line interface tool that is used to capture packets on a network. It is a very powerful and popular network protocol analyzer". The tool allows cybersecurity professionals to analyze headers and payloads of network traffic, making it valuable in forensic investigations and network diagnostics.

NEW QUESTION: 16
What is an issue with digital forensics in cloud environments, from a security point of view?
A. weak cloud computer specifications
B. lack of logs
C. no physical access to the hard drive
D. network access instability
Answer: C (LEAVE A REPLY)
One of the primary challenges of cloud forensics is the inability to physically access the underlying hardware (e.g., the hard drives storing VM or container data). This restricts investigators from performing traditional disk imaging and handling procedures, which are crucial for maintaining evidence integrity. This limitation is widely recognized in cloud forensics frameworks.
Correct answer: C. no physical access to the hard drive.

NEW QUESTION: 17
A security team received reports of users receiving emails linked to external or unknown URLs that are non-returnable and non-deliverable. The ISP also reported a 500% increase in the amount of ingress and egress email traffic received. After detecting the problem, the security team moves to the recovery phase in their incident response plan. Which two actions should be taken in the recovery phase of this incident?
(Choose two.)
A. request packet capture
B. remove vulnerabilities
C. verify the breadth of the attack
D. collect logs
E. scan hosts with updated signatures
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 18
Refer to the exhibit.

```
Dec 2811:27:10 CyberOps sshd[8423]: Failed password for invalid user admins from Cyber port 44216 ssh2
Dec 2811:27:13 CyberOps sshd[8425]: Failed password for invalid user phoenix from Cyber port 20532 ssh2
Dec 2811:27:17 CyberOps sshd[8428]: Failed password for invalid user test from Cyber port 24492 ssh2
Dec 2811:27:22 CyberOps sshd[8430]: Failed password for invalid user rainbow from Cyber port 46591 ssh2
Dec 2811:27:25 CyberOps sshd[8432]: Failed password for invalid user runner from Cyber port 57129 ssh2
Dec 2811:27:34 CyberOps sshd[8434]: Failed password for invalid user user from Cyber port 11960 ssh2
Dec 2811:27:37 CyberOps sshd[8437]: Failed password for invalid user abc123 from Cyber port 5921 ssh2
Dec 2811:27:48 CyberOps sshd[8439]: Failed password for invalid user passwd from Cyber port 21298 ssh2
```

A web hosting company analyst is analyzing the latest traffic because there was a 20% spike in server CPU usage recently. After correlating the logs, the problem seems to be related to the bad actor activities. Which attack vector is used and what mitigation can the analyst suggest?
A. SQL Injection; implement input validation and use parameterized queries.
B. Distributed denial of service; use rate limiting and DDoS protection services.
C. Phishing attack; conduct regular user training and use email filtering solutions.
D. Brute-force attack; implement account lockout policies and roll out MFA.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
The log entries show repeated SSH login attempts for various invalid usernames (e.g., admin, phoenix, rainbow, test, user, etc.) from different source ports. These are clear signs of a brute-

force attack-an automated process trying multiple usernames and passwords in hopes of gaining access.
Mitigating such attacks includes:
* Implementing account lockout policies (e.g., locking an account after several failed login attempts).
* Enabling Multi-Factor Authentication (MFA) to ensure that password guessing alone is insufficient for account access.
Therefore, the correct answer is:
D). Brute-force attack; implement account lockout policies and roll out MFA.

NEW QUESTION: 19
What is the goal of an incident response plan?
A. to determine security weaknesses and recommend solutions
B. to contain an attack and prevent it from spreading
C. to ensure systems are in place to prevent an attack
D. to identify critical systems and resources in an organization
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
Which tool is used for reverse engineering malware?
A. NMAP
B. SNORT
C. Ghidra
D. Wireshark
Answer: (SHOW ANSWER)

NEW QUESTION: 21
What can the blue team achieve by using Hex Fiend against a piece of malware?
A. Use the hex data to define patterns in VARA rules.
B. Read the hex data and transmognify into a readable ELF format
C. Use the hex data to modify BE header to read the file.
D. Read the hex data and decrypt payload via access key.
Answer: A (LEAVE A REPLY)
Hex Fiend is a hex editor that allows analysts to examine the raw byte content of files. One key use case is identifying and extracting byte-level patterns or signatures that can be translated into YARA rules for detecting malware. These hex patterns can be used to define precise signature-based detections.

NEW QUESTION: 22
An employee receives an email from a "trusted" person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an

alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance with the incident response plan. Which event detail should be included in this root cause analysis?

A. phishing email sent to the victim

B. alarm raised by the SIEM

C. information from the email header

D. alert identified by the cybersecurity team

Answer: (SHOW ANSWER)

Theroot cause analysisin incident response focuses on identifying theinitial trigger or root causeof the incident to understand how it started and how to prevent recurrence. In this scenario, thephishing email sent to the victim(A) is the initial trigger that led to the employee's action of clicking the malvertising link, resulting in the malware download.

The other options represent later stages in the incident response cycle, such as detection (SIEM alert, cybersecurity team's alert) or supporting evidence (email header information), but they do not address the root cause, which is thephishing email itself.

This aligns with theCyberOps Technologies (CBRFIR) 300-215 study guide, which states that identifying theinitial vector of compromiseis critical to theroot cause analysisphase of incident response (Chapter:

Incident Response Techniques, page 410-412).

Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Incident Response Techniques, Root Cause Analysis, page 410-412.

NEW QUESTION: 23

Refer to the exhibit.

```
        function decrypt(crypted, key)
On Error Resume Next

UUf  = crypted
sJs = "" '!!!
 wWLu = ""
 FETw = 1
        for i=1 to len(UUf)
 if ( asc(mid(UUF, i, 1)) > 47 and asc(mid(UUf, i, 1)) < 58) then
 sJs = sJs + mid(UUf, i, 1) '!!!
 FETw = 1
 else
 if FETw = 1 then
 NEL = CInt (sJs) '!!!
 VlxJ = XOR_Func(NEL, key) '!!!
 wWLu = wWLu + Chr(VlxJ) '!!!
 end if
  sJs = ""
 FETw = 0
 end if
 vkB = bEBk or CFc
next
  decrypt = wWLu
  end function
        function XOR_Func(qit, ANF)
 On Error Resume Next
 sCLx = qit xor ANF
 XOR_Func = sCLx

 end function
```


Which type of code created the snippet?

A. VB Script

B. Python

C. PowerShell

D. Bash Script

Answer: A (LEAVE A REPLY)

The syntax in the code snippet includes:

* On Error Resume Next- a classic VBScript error-handling directive.

* function ... end functionstructure.

* Use ofMid(),Chr(), andAsc()functions - all commonly used in VBScript for string manipulation.

* CInt()for conversion - typical in VBScript.

These characteristics alignexactly with VBScript, which is frequently used in malicious macros and obfuscated payloads for malware distribution, as covered in the Cisco CyberOps Associate curriculum when analyzing scripts and encoded threats.

NEW QUESTION: 24

What are two features of Cisco Secure Endpoint? (Choose two.)

A. file trajectory

B. rogue wireless detection

C. Orbital Advanced Search

D. web content filtering

E. full disk encryption

Answer: A,C (LEAVE A REPLY)

Cisco Secure Endpoint (formerly AMP for Endpoints) offers features like:

* File trajectory: to track file behavior and spread across endpoints.

* Orbital Advanced Search: for querying endpoint data to detect threats in real time.

NEW QUESTION: 25

Refer to the exhibit.

According to the SNORT alert, what is the attacker performing?

A. brute-force attack against the web application user accounts

B. brute-force attack against directories and files on the target webserver

C. SQL injection attack against the target webserver

D. XSS attack against the target webserver

Answer: B (LEAVE A REPLY)

NEW QUESTION: 26

What are YARA rules based upon?

A. binary patterns

B. IP addresses

C. HTML code

D. network artifacts

Answer: A (LEAVE A REPLY)

NEW QUESTION: 27

Refer to the exhibit.

```
<stix:Indicator id= "CISA:Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c" timestamp= "2020-04-
08T00:44:39.970278+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89">
<cybox:Object id= "CISA:Object-a2169ad2-5273-41cb-9491-48c69b22da74">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals" >Fightcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-2035a032-6b8d-4dd9-8752-7316af76e702" timestamp= "2020-04-
08T00:44:39.970417+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-463472d3-e45e-46c1-bf05-da7458cb943c">
<cybox:Object id= "CISA:Object-7728bd69-e724-4917-9550-9ae853becf28">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">nocovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-8b56999b-a015-4399-ab80-cca9bcaf7ebf" timestamp= "2020-04-
08T00:44:39.970554+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-0648e1db-aa4e-4aca-914e-ea0ccd445254">
<cybox:Object id= "CISA:Object-db21b6ca-0c1b-474d-8bf7-950ead2d9760">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">stopcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
```


Which two actions should be taken based on the intelligence information? (Choose two.)

A. Block network access to all .shop domains

B. Add a SIEM rule to alert on connections to identified domains.

C. Use the DNS server to block hole all .shop requests.

D. Block network access to identified domains.

E. Route traffic from identified domains to block hole.

Answer: B,D (LEAVE A REPLY)

The STIX intelligence feed in the exhibit identifies specific malicious domains, such as:

* fightcovid19.shop

* nocovid19.shop

* stopcovid19.shop

These are categorized as "Malicious FQDN Indicator." The recommended cybersecurity actions when such threat intelligence is received are:

* D. Block network access to identified domains: This directly prevents users or systems from communicating with known malicious infrastructure and is a critical first step in threat mitigation.
* B. Add a SIEM rule to alert on connections to identified domains: This ensures that any attempted communication with these domains is flagged for immediate review and action, enabling real-time threat detection and incident response.
Blocking all .shop domains (Option A or C) would be overbroad and potentially disruptive, as many legitimate websites also use that TLD. Option E (routing to block hole) could be valid as a DNS strategy, but B and D represent the most actionable and precise responses per standard incident response practices.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on "Threat Intelligence Platforms," covering how to operationalize STIX/TAXII indicators via blocking and SIEM integration.

NEW QUESTION: 28
Refer to the exhibit.

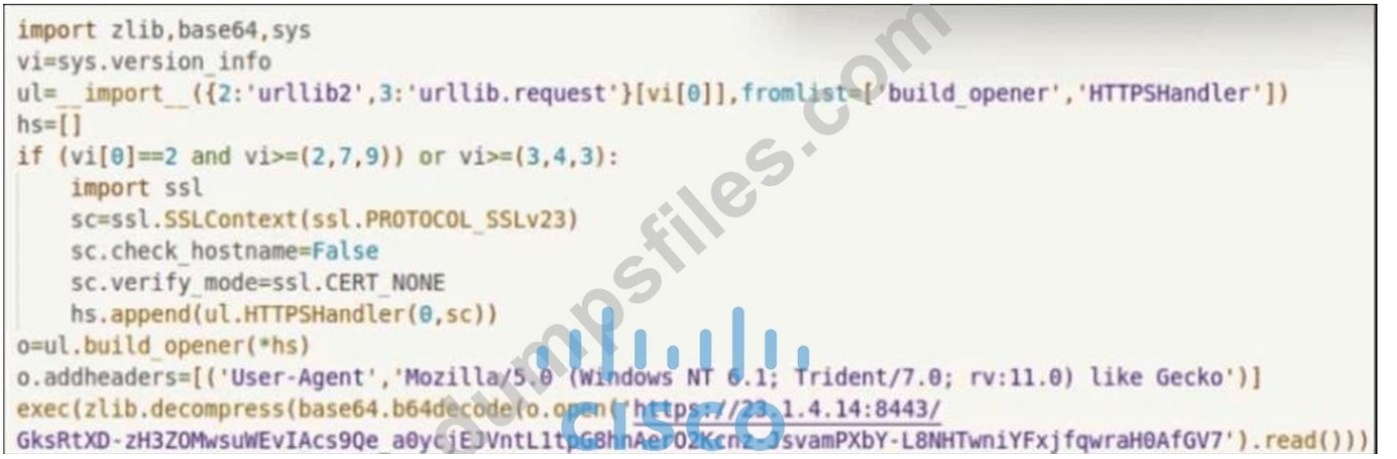
Time	TCP Data	Source	Destination	Protocol	Info
12 0.000000000	0.000230000	192.	192.	TCP	Microsoft-cis-sql-storman, ACK] Seq=0 Sck=1 Wind=8192 Len=0 WSS=3460 SACK_PER=1
15 0.000658000	0.000465000	192.	192.	SMB	Negotiate Protocol Response
21 0.004157000	0.000499000	192.	192.	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
23 0.001257000	0.000991000	192.	192.	TCP	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
25 0.000650000	0.000135000	192.	192.	TCP	microsoft-ds-sgf-storman [ACK] Seq=757 Ack=759 win=63620 Len=0
26 0.000049000	0.000049000	192.	192.	TCP	microsoft-ds-sgl-storman [RST, ACK] Seq=757 Ack=759 Win=0 Len=0
38 14.59967300	0.000232000	192.	192.	TCP	microsoft-ds+llsurfup-https [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 WSS=1460 SACK_PERM=1
41 0.000535000	0.000365000	192.	192.	SMB	Negotiate Protocol Response
58 0.005986000	0.000498000	192.	192.	TCP	microsoft-ds-llsurfup-https [ACK] Seq=198 Ack=3006 win=64240 Len=0
59 0.000854000	0.000854000	192.	192.	SMB	Session Setup AndX Response
61 0.000639000	0.000302000	192.	192.	SMB	Tree Connect AndX Response
63 0.002314000	0.000354000	192.	192.	SMB	MT Create AndX Response, FID: 0x4000
65 0.000440000	0.000249000	192.	192.	SMB	Write AndX Response, FID: 0x4000, 72 bytes
67 0.000336000	0.000232000	192.	192.		
69 0.000528000	0.000429000	192.	192.		
71 0.000417000	0.000317000	192.	192.		
73 0.000324000	0.000215000	192.	192.		
76 0.232074000	0.000322000	192.	192.	SMB	NT Create AndX Response, FID: 0x4001
78 0.000420000	0.000242000	192.	192.	SMB	Write AndX Response, FID: 0x4001, 72 bytes
80 0.000332000	0.000228000	192.	192.		
82 0.000472000	0.000372000	192.	192.		
84 0.000433000	0.000320000	192.	192.		
86 0.000416000	0.000310000	192.	192.		
88 0.000046500	0.000366000	192.	192.		
90 0.067630000	0.967518000	192.	192.		
92 0.000515000	0.000391000	192.	192.		
94 0.000477000	0.000368000	192.	192.		
96 0.090664000	0.090363000	192.	192.		
98 0.006860000	0.000280000	192.	192.		
100 0.000312000	0.000229000	192.	192.		
102 0.000329000	0.000217000	192.	192.		
104 0.000212900	0.000200000	192.	192.	SMB	Close Response, FID: 0x4001

An engineer is analyzing a TCP stream in Wireshark after a suspicious email with a URL. What should be determined about the SMB traffic from this stream?
A. It is redirecting to a malicious phishing website
B. It is exploiting redirect vulnerability
C. It is requesting authentication on the user site.
D. It is sharing access to files and printers.
Answer: D (LEAVE A REPLY)

The Wireshark output shows SMB protocol transactions, including NT Create AndX Response and Write AndX Response, indicating the transfer of files or objects. SMB (Server Message Block) is a protocol used for file sharing and printer access in Windows networks. The log does not indicate phishing or redirection behavior but rather normal SMB communication such as accessing files or shared resources.

-

NEW QUESTION: 29



A. Initiate a connection to 23.1.4.14 over port 8443.

B. Generate a Windows executable file.

C. Open the Mozilla Firefox browser.

D. Validate the SSL certificate for 23.1.4.14.

Answer: (SHOW ANSWER)

This Python script uses a combination of libraries (urllib,zlib,base64, andssl) to:

* Disable SSL certificate verification (ssl.CERT_NONEandcheck_hostname=False).

* Construct a custom HTTPS opener with the specified SSL context.

* Add a forgedUser-Agentheader to mimic Internet Explorer 11.

* Connect to the URLhttps://23.1.4.14:8443.

* Download and execute base64-encoded and zlib-compressed content from that URL using: exec(zlib.decompress(base64.b64decode(...).read()))

This shows a classic example of:

* Downloading payloads from a remote server (23.1.4.14:8443).

* Avoiding detection by disabling SSL verification.

* Executing the payload dynamically withexec()after decoding and decompressing.

The main goal is clearly to initiate a connection to a remote command-and-control (C2) server on port 8443 and download/execute additional code.

Hence, the correct answer is: A. Initiate a connection to 23.1.4.14 over port 8443.

NEW QUESTION: 30

A security team needs to prevent a remote code execution vulnerability. The vulnerability can be exploited only by sending '${ string in the HTTP request. WAF rule is blocking '${', but system

engineers detect that attackers are executing commands on the host anyway. Which action should the security team recommend?

A. Enable URL decoding on WAF.

B. Block incoming web traffic.

C. Add two WAF rules to block 'S' and '{' characters separately.

D. Deploy antimalware solution.

Answer: A (LEAVE A REPLY)

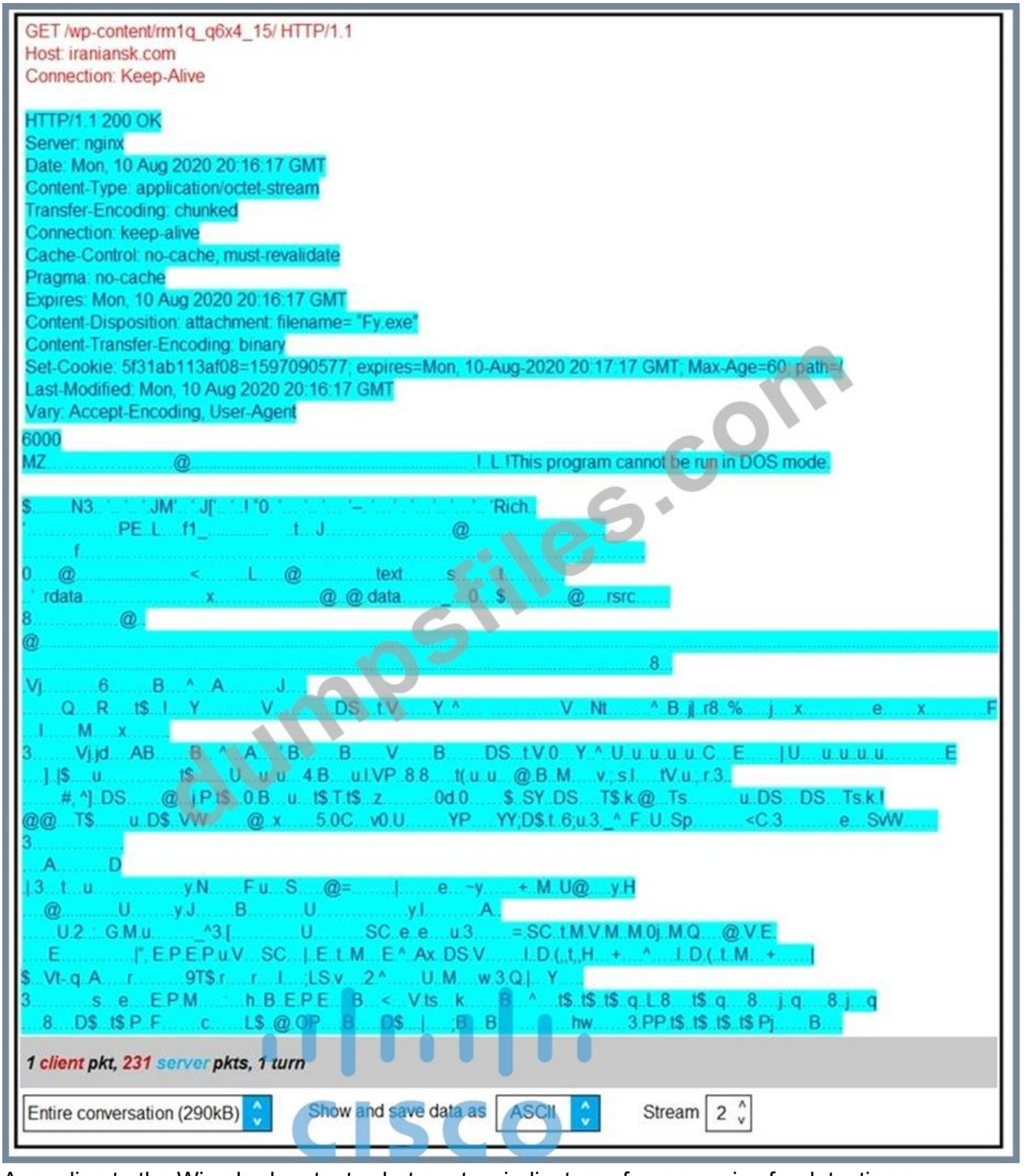
When Web Application Firewalls (WAFs) are configured to block specific patterns (like${), attackers may bypass this using URL encoding (e.g.,%24%7B). In such cases, the WAF must decode these patterns before applying matching rules. EnablingURL decodingensures the WAF recognizes encoded payloads and applies protections appropriately. This is a recommended hardening strategy against bypass techniques for command injection and remote code execution.

Reference: Cisco CyberOps v1.2 Guide, Chapter on WAFs and Input Validation Techniques.

-

NEW QUESTION: 31

Refer to the exhibit.



According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Content-Type: application/octet-stream

B. Server: nginx

C. Hash value: 5f31ab113af08=1597090577

D. filename= "Fy.exe"

E. Domain name:iraniansk.com

Answer: (SHOW ANSWER)

NEW QUESTION: 32

multiple machines behave abnormally. A sandbox analysis reveals malware. What must the administrator determine next?

A. if Patient 0 still demonstrates suspicious behavior

B. source code of the malicious attachment

C. if the file in Patient 0 is encrypted

D. if Patient 0 tried to connect to another workstation

Answer: D (LEAVE A REPLY)

The key goal during lateral movement analysis is to determine whether the malware spread or attempted to spread beyond the initially compromised system. This is crucial for containment and scoping of the incident.
Logs, sandbox behavior, or network activity may show if Patient 0 initiated outbound connections to other systems, potentially propagating malware across the environment.
Correct answer: D. if Patient 0 tried to connect to another workstation.

NEW QUESTION: 33
A workstation uploads encrypted traffic to a known clean domain over TCP port 80. What type of attack is occurring, according to the MITRE ATT&CK matrix?
A. Exfiltration Over Web Service
B. Exfiltration Over C2 Channel
C. Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
D. Command and Control Activity
Answer: C (LEAVE A REPLY)
According to the MITRE ATT&CK matrix, when encrypted traffic is tunneled through a legitimate protocol such as HTTP (port 80) to a non-malicious domain, this aligns with the tactic "Exfiltration Over Asymmetric Encrypted Non-C2 Protocol" (T1048.002). The attacker is trying to hide exfiltration in otherwise benign traffic.

NEW QUESTION: 34
An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?
A. Upload the file signature to threat intelligence tools to determine if the file is malicious.
B. Investigate the sender of the email and communicate with the employee to determine the motives.
C. Contain the threat for further analysis as this is an indication of suspicious activity.
D. Monitor processes as this a standard behavior of Word macro embedded documents.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
Refer to the exhibit.

What should be determined from this Apache log?

A. The SSL traffic setup is improper

B. The private key does not match with the SSL certificate.

C. A module named mod_ssl is needed to make SSL connections.

D. The certificate file has been maliciously modified

Answer: A (LEAVE A REPLY)

NEW QUESTION: 36

A cybersecurity analyst is examining a complex dataset of threat intelligence information from various sources. Among the data, they notice multiple instances of domain name resolution requests to suspicious domains known for hosting C2 servers. Simultaneously, the intrusion detection system logs indicate a series of network anomalies, including unusual port scans and attempts to exploit known vulnerabilities. The internal logs also reveal a sudden increase in outbound network traffic from a specific internal host to an external IP address located in a high-risk region. Which action should be prioritized by the organization?

A. Threat intelligence information should be marked as false positive because unnecessary alerts impact security key performance indicators.

B. Focus should be applied toward attempts of known vulnerability exploitation because the attacker might land and expand quickly.

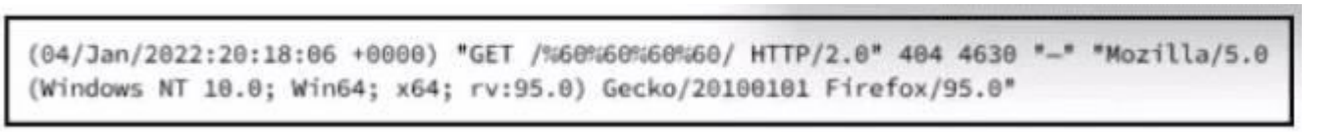
C. Organization should focus on C2 communication attempts and the sudden increase in outbound network traffic via a specific host.

D. Data on ports being scanned should be collected and SSL decryption on Firewall enabled to capture the potentially malicious traffic.

Answer: (SHOW ANSWER)

According to theCyberOps Technologies (CBRFIR) 300-215 study guidecurriculum, command-and-control (C2) communication is a strong indicator that a system has already been compromised and is actively under the control of an attacker. Sudden outbound traffic to high-risk regions and resolution of known malicious domains are high-confidence signs of an active threat. Therefore, prioritizing detection and disruption of this outbound traffic is critical to prevent further damage or data exfiltration.
While monitoring vulnerability exploitation (B) and gathering port scan data (D) are also valuable, they are more preventive or forensic in nature. The most immediate threat-and therefore the top priority-is stopping active C2 communications.

NEW QUESTION: 37
Refer to the exhibit.



What is occurring?
A. The request was redirected.
B. WAF detected code injection.
C. An attacker attempted SQL injection.
D. The requested page was not found.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The log entry contains the following key elements:
* The timestamp:(04/Jan/2022:20:18:06 +0000)
* HTTP method and URI:"GET /%60%60%60%60%60%60/ HTTP/2.0"
* HTTP status code:404
* User-Agent:Mozilla/5.0 ... Firefox/95.0
The status code404indicates that the requested resource was not found on the server. This is a standard HTTP response that signifies the server could not locate the requested URI (in this case, likely due to a malformed or invalid path/\`````/, where%60is the URL-encoded form of the backtick character "").
There is no clear evidence of SQL injection, WAF detection, or redirection in this log. The use of encoded backticks may suggest probing behavior, but the log does not show a definitive attack signature.
Therefore, the correct interpretation is:
D: The requested page was not found.

NEW QUESTION: 38

```
        function decrypt(crypted, key)
On Error Resume Next

UUf  = crypted
sJs = "" '!!!
 wWLu = ""
 FETw = 1
        for i=1 to len(UUf)
 if ( asc(mid(UUF, i, 1)) > 47 and asc(mid(UUf, i, 1)) < 58) then
 sJs = sJs + mid(UUf, i, 1) '!!!
 FETw = 1
 else
 if FETw = 1 then
 NEL = CInt (sJs) '!!!
 VlxJ = XOR_Func(NEL, key) '!!!
 wWLu = wWLu + Chr(VlxJ) '!!!
 end if
  sJs = ""
 FETw = 0
 end if
 vkB = bEBk or CFc
next
  decrypt = wWLu
  end function
        function XOR_Func(qit, ANF)
 On Error Resume Next
 sCLx = qit xor ANF
 XOR_Func = sCLx

 end function
```


Refer to the exhibit. Which type of code created the snippet?

A. VB Script

B. Python

C. PowerShell

D. Bash Script

Answer: A (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 39

What is the steganography anti-forensics technique?

A. hiding a section of a malicious file in unused areas of a file

B. changing the file header of a malicious file to another file type

C. sending malicious files over a public network by encapsulation

D. concealing malicious files in ordinary or unsuspecting places

Answer: A (LEAVE A REPLY)

Reference:

https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/

NEW QUESTION: 40

Refer to the exhibit.

```
<stix:Indicator id= "CISA:Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c" timestamp= "2020-04-
08T00:44:39.970278+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89">
<cybox:Object id= "CISA:Object-a2169ad2-5273-41cb-9491-48c69b22da74">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals" >Fightcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-2035a032-6b8d-4dd9-8752-7316af76e702" timestamp= "2020-04-
08T00:44:39.970417+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-463472d3-e45e-46c1-bf05-da7458cb943c">
<cybox:Object id= "CISA:Object-7728bd69-e724-4917-9550-9ae853becf28">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">nocovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-8b56999b-a015-4399-ab80-cca9bcaf7ebf" timestamp= "2020-04-
08T00:44:39.970554+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-0648e1db-aa4e-4aca-914e-ea0ccd445254">
<cybox:Object id= "CISA:Object-db21b6ca-0c1b-474d-8bf7-950ead2d9760">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">stopcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
```

Which two actions should be taken based on the intelligence information? (Choose two.)

A. Block network access to all .shop domains

B. Route traffic from identified domains to block hole.

C. Use the DNS server to block hole all .shop requests.

D. Block network access to identified domains.
E. Add a SIEM rule to alert on connections to identified domains.
Answer: D,E (LEAVE A REPLY)

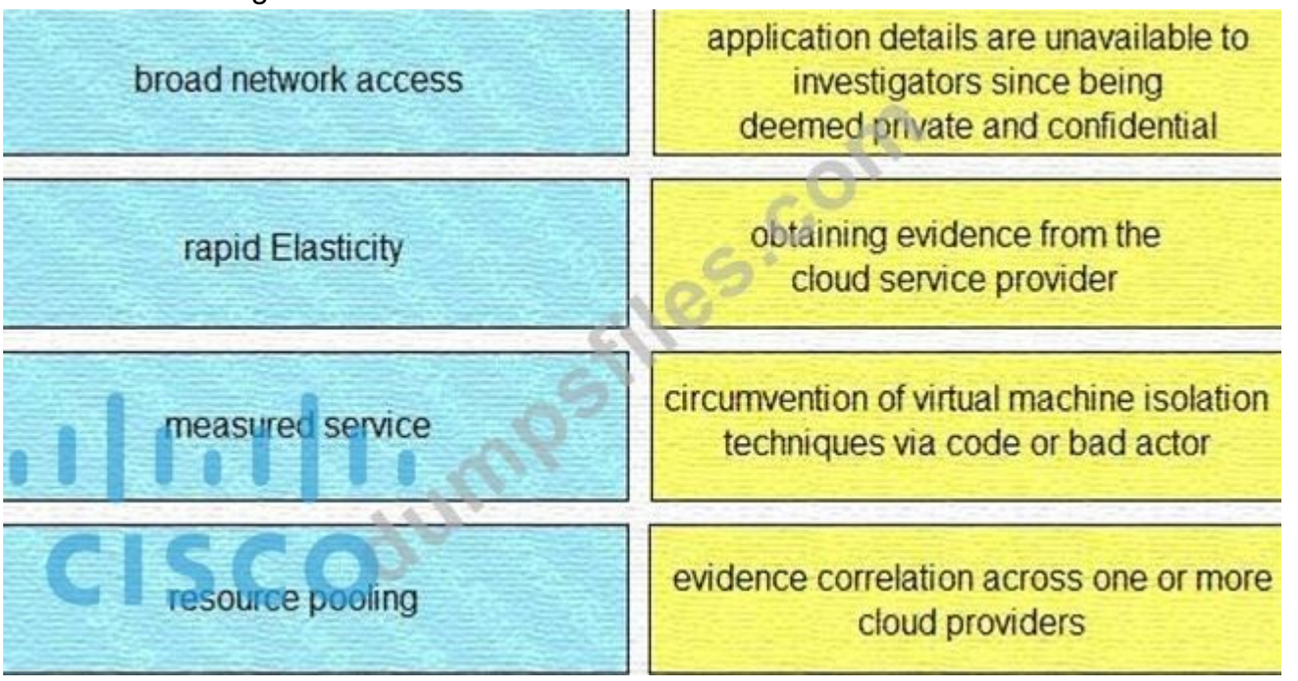
NEW QUESTION: 41
An analyst finds .xyz files of unknown origin that are large and undetected by antivirus. What action should be taken next?
A. Isolate the files and perform a deeper heuristic analysis to detect potential unknown malware or data exfiltration payloads.
B. Rename the file extensions to .txt to enable easier opening and review by team members.
C. Delete the files immediately to prevent potential risks.
D. Move the files to a less secure network segment for analysis.
Answer: (SHOW ANSWER)
The safest and most effective approach is to isolate the files and subject them to heuristic and behavioral analysis. This can reveal obfuscated malware or unauthorized data storage techniques, even if signature-based antivirus fails to flag them.

NEW QUESTION: 42
An organization recovered from a recent ransomware outbreak that resulted in significant business damage. Leadership requested a report that identifies the problems that triggered the incident and the security team's approach to address these problems to prevent a reoccurrence. Which components of the incident should an engineer analyze first for this report?
A. impact and flow
B. cause and effect
C. risk and RPN
D. motive and factors
Answer: D (LEAVE A REPLY)
Explanation/Reference:

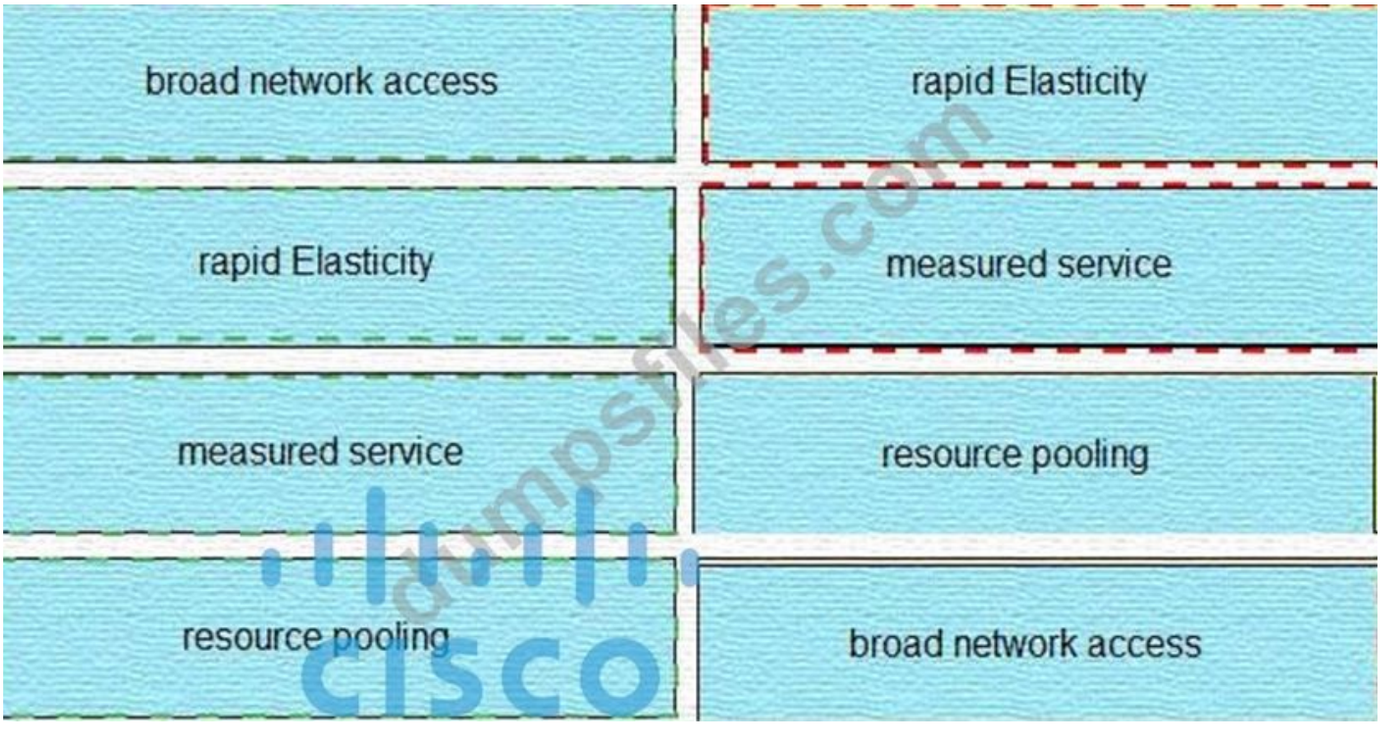
NEW QUESTION: 43
What is the transmogrify anti-forensics technique?
A. hiding a section of a malicious file in unused areas of a file
B. sending malicious files over a public network by encapsulation
C. concealing malicious files in ordinary or unsuspecting places
D. changing the file header of a malicious file to another file type
Answer: D (LEAVE A REPLY)
Reference:
https://www.csoonline.com/article/2122329/the-rise-of-anti-forensics.html#:~:text=Transmogrify%20is% 20similarly%20wise%20to,a%20file%20from%2C%20say%2C%20.

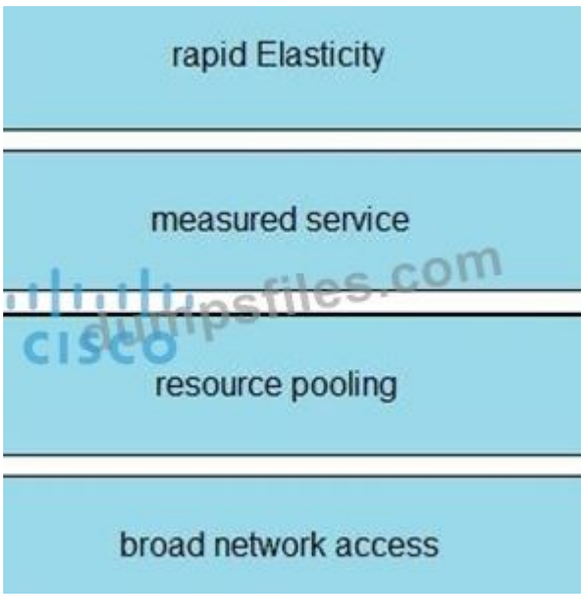
NEW QUESTION: 44

Drag and drop the cloud characteristic from the left onto the challenges presented for gathering evidence on the right.



Answer:





NEW QUESTION: 45
Over the last year, an organization's HR department has accessed data from its legal department on the last day of each month to create a monthly activity report. An engineer is analyzing suspicious activity alerted by a threat intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week. The engineer pulled the network data from the legal department's shared folders and discovered above average-size data dumps.
Which threat actor is implied from these artifacts?
A. internal user errors
B. privilege escalation
C. external exfiltration
D. malicious insider
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
Which magic byte indicates that an analyzed file is a pdf file?
A. cGRmZmlsZQ
B. 0a0ah4cg
C. 255044462d
D. 706466666
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
A malware outbreak revealed that a firewall was misconfigured, allowing external access to the SharePoint server. What should the security team do next?
A. Scan for and fix vulnerabilities on the firewall and server
B. Harden the SharePoint server
C. Disable external IP communications on all firewalls
D. Review and update all firewall rules and the network security policy
Answer: (SHOW ANSWER)
The incident stems from a policy-level issue rather than a technical vulnerability. According to incident response best practices, the priority should be to review and update firewall rules and ensure that the network security policy aligns with the principle of least privilege and correct access segmentation.

NEW QUESTION: 48
A security team receives reports of multiple files causing suspicious activity on users' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)
A. Inspect registry entries
B. Inspect processes.
C. Inspect file hash.
D. Inspect file type.
E. Inspect PE header.
Answer: B,C (LEAVE A REPLY)
Explanation/Reference: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually- d02744f7c43a

NEW QUESTION: 49
A network host is infected with malware by an attacker who uses the host to make calls for files and shuttle traffic to bots. This attack went undetected and resulted in a significant loss. The organization wants to ensure this does not happen in the future and needs a security solution that will generate alerts when command and control communication from an infected device is detected. Which network security solution should be recommended?
A. Cisco Secure Firewall ASA
B. Cisco Secure Firewall Threat Defense (Firepower)
C. Cisco Secure Email Gateway (ESA)
D. Cisco Secure Web Appliance (WSA)
Answer: B (LEAVE A REPLY)

TheCisco Secure Firewall Threat Defense (Firepower)includes advanced capabilities such as intrusion prevention, URL filtering, and deep packet inspection. According to the CyberOps guide, it can detect and block C2 communications by analyzing traffic patterns and comparing them to threat intelligence data. The guide specifically states: "Advanced solutions such as Firepower provide detection capabilities for command and control (C2) traffic by identifying unusual outbound connections and behavioral anomalies".

NEW QUESTION: 50
Refer to the exhibit.

```
        function decrypt(crypted, key)
On Error Resume Next

UUf  = crypted
sJs = "" '!!!
 wWLu = ""
 FETw = 1
        for i=1 to len(UUf)
 if ( asc(mid(UUF, i, 1)) > 47 and asc(mid(UUf, i, 1)) < 58) then
 sJs = sJs + mid(UUf, i, 1) '!!!
 FETw = 1
 else
 if FETw = 1 then
 NEL = Clnt (sJs) '!!!
 VlxJ = XOR_Func(NEL, key) '!!!
 wWLu = wWLu + Chr(VlxJ) '!!!
 end if
  sJs = ""
 FETw = 0
 end if
 vkB = bEBk or CFc
next
 decrypt = wWLu
 end function
         function XOR_Func(qit, ANF)
 On Error Resume Next
 sCLx = qit xor ANF
 XOR_Func = sCLx

 end function
```

Which type of code created the snippet?

A. PowerShell

B. VB Script

C. Bash Script

D. Python

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

An engineer is analyzing a ticket for an unexpected server shutdown and discovers that the web-server ran out of useable memory and crashed.

Which data is needed for further investigation?

A. /var/log/httpd/messages.log

B. /var/log/httpd/access.log

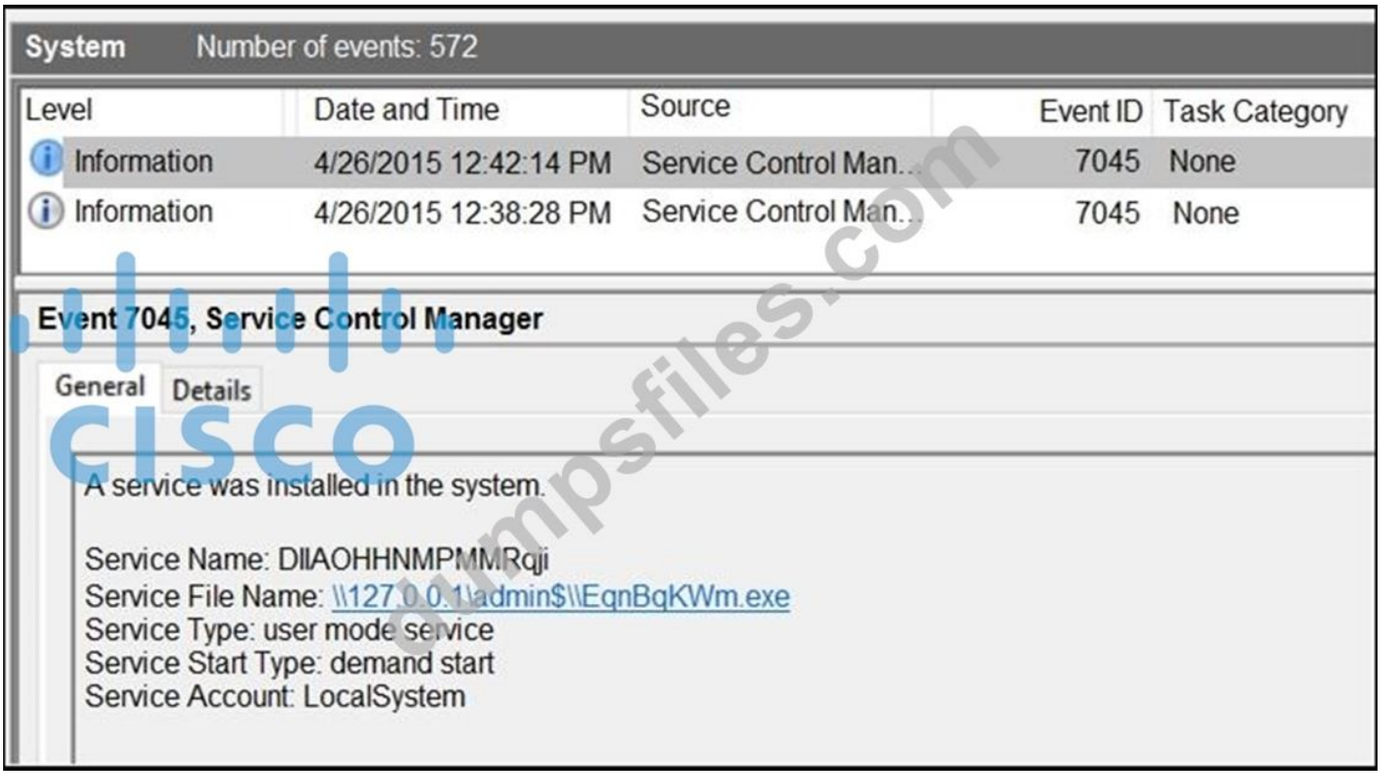
C. /var/log/access.log

D. /var/log/messages.log

Answer: D (LEAVE A REPLY)

NEW QUESTION: 52

Refer to the exhibit.

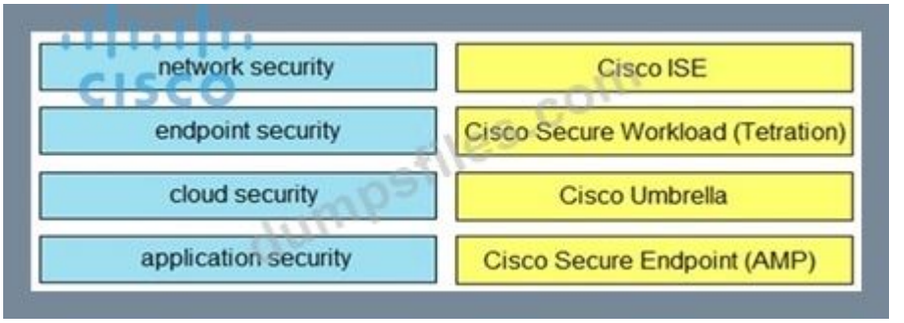


An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hours prior. Which two indicators of compromise should be determined from this information? (Choose two.)

A. unauthorized system modification
B. privilege escalation
C. denial of service attack
D. compromised root access
E. malware outbreak
Answer: A,E (LEAVE A REPLY)
According to the event log, a suspicious service was installed (DIAOHHNMPMMRgji) with a service file pointing to a remote share (\\127.0.0.1\admin$\EqnBqKWm.exe). This type of activity strongly suggests:
* A. Unauthorized system modification: Installation of a service without proper authorization, especially with a random or obfuscated name, directly fits the description of system modification. The use of admin$ (administrative share) further implies this wasn't part of standard operations.
* E. Malware outbreak: The use of a service that points to an executable with a seemingly random name and the demand start configuration indicate a potential backdoor or remote-controlled malware. As stated in the Cisco CyberOps Associate guide, event ID 7045 with unusual service names or file paths is a strongIndicator of Compromise (IoC)for malware or persistence mechanisms.
Options like privilege escalation or DoS are not directly evidenced in the event log shown. There's no indication that the LocalSystem account was elevated beyond its default, nor that system resources were overwhelmed (as would be typical in DoS).

NEW QUESTION: 53
An organization recovered from a recent ransomware outbreak that resulted in significant business damage. Leadership requested a report that identifies the problems that triggered the incident and the security team's approach to address these problems to prevent a reoccurrence. Which components of the incident should an engineer analyze first for this report?
A. impact and flow
B. cause and effect
C. risk and RPN
D. motive and factors
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Drag and drop the capabilities on the left onto the Cisco security solutions on the right.



Answer:

NEW QUESTION: 55
An incident response analyst is preparing to scan memory using a YARA rule. How is this task completed?
A. deobfuscation
B. XML injection
C. string matching
D. data diddling
Answer: (SHOW ANSWER)
YARA rules are pattern-matching rules used to identify malware based on specific strings, conditions, and binary patterns. They are most effective in memory or file scans where analysts search for known indicators or unique signatures via string matching.
Correct answer: C. string matching.

NEW QUESTION: 56
Refer to the exhibit.

Metadata	
Drive type	Fixed (Hard disk)
Drive serial number	1CBDB2C4
Full path	C:\Windows\System32\WIndowsPowerShell\v1.0\powershell.exe
NetBIOS name	user-pc
Lnk file name	ds7002.pdf
Relative path	..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments	-noni –ep bypass $zk = 'JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjIzYjY7.
Target file size (bytes)	452608
Droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Birth droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
Birth droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
File attribute	The file or directory is an archive file
Target file access time (UTC)	13.07.2009 23:32:37
Target file creation time (UTC)	13.07.2009 23:32:37
Target file modification time (UTC)	14.07.2009 1:14:24
Header flags	HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, HasArguments, HasIcc
MAC vendor	Cadmus Computer Systems
Target path	My Computer\C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Target MFT entry number	0x7E21

An engineer is analyzing a .LNK (shortcut) file recently received as an email attachment and blocked by email security as suspicious. What is the next step an engineer should take?

A. Open the file in a sandbox environment for further behavioral analysis as the file contains a malicious script that runs on execution.

B. Quarantine the file within the endpoint antivirus solution as the file is a ransomware which will encrypt the documents of a victim.

C. Delete the suspicious email with the attachment as the file is a shortcut extension and does not represent any threat.

D. Upload the file to a virus checking engine to compare with well-known viruses as the file is a virus disguised as a legitimate extension.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 57

Refer to the exhibit.

Process Name	Process Arguments	Process Path	Parent Process Name
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
cmd.exe	/c powershell.exe [Byte[]] SrOWg = [system.Convert]::FromBase64string((New-Object...	\Device\HarddiskVolume3\Windows\System32\cmd.exe	WScript.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe
RegSvcs.exe	--	\Device\HarddiskVolume3\Windows\Microsoft.NET\Framew...	powershell.exe

An alert came with a potentially suspicious activity from a machine in HR department. Which two IOCs should the security analyst flag? (Choose two.)

A. powershell.exe used on HR machine

B. cmd.exe executing from \Device\HarddiskVolume3\

C. WScript.exe initiated by powershell.exe

D. cmd.exe starting powershell.exe with Base64 conversion

E. WScript.exe acting as a parent of cmd.exe

Answer: D,E (LEAVE A REPLY)

The exhibit shows a series of process executions that form a suspicious chain involving scripting engines and obfuscated commands:

* One critical indicator iscmd.exe executing PowerShell with obfuscated (Base64-encoded) arguments

. The use of Base64 is a known method used by attackers to mask malicious commands. This aligns with attack techniques defined under MITRE ATT&CK T1059 (Command and Scripting Interpreter) and T1086 (PowerShell abuse). Therefore, option D is valid.

* Another important IOC isWScript.exe acting as a parent of cmd.exe, which is abnormal in typical business environments. This indicates potential misuse of Windows Script Host (WSH) to launch commands, often seen in phishing or malware dropper scenarios. Thus, option E is also valid.

Options A and B by themselves are not definitive IOCs-PowerShell and cmd.exe are legitimate administrative tools and frequently used in Windows environments.

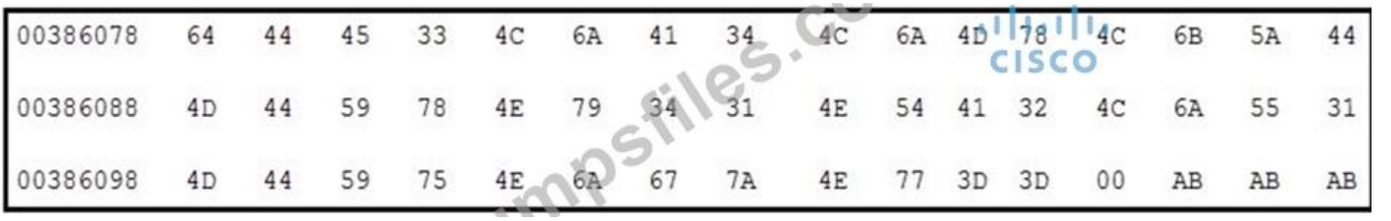
Option C is not supported by the exhibit-the reverse (powershell.exe initiated by WScript.exe) is what's seen, not the other way around.

These patterns align with theCyberOps Technologies (CBRFIR) 300-215 study guide, which specifies that chaining of interpreters (e.g., WScript # cmd # PowerShell) with encoded commands is a key indicator of compromise during forensic analysis.

Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Identifying Malicious Activity in Host-Based Artifacts and Command-Line Analysis.

NEW QUESTION: 58

Refer to the exhibit.



00386078	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	44	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Which encoding technique is represented by this HEX string?

A. Binary

B. Unicode

C. Base64

D. Charcode

Answer: A (LEAVE A REPLY)

NEW QUESTION: 59

An incident response team is recommending changes after analyzing a recent compromise in which:

* a large number of events and logs were involved;
* team members were not able to identify the anomalous behavior and escalate it in a timely manner;
* several network systems were affected as a result of the latency in detection;
* security engineers were able to mitigate the threat and bring systems back to a stable state; and
* the issue reoccurred shortly after and systems became unstable again because the correct information was not gathered during the initial identification phase.

Which two recommendations should be made for improving the incident response process? (Choose two.)

A. Formalize reporting requirements and responsibilities to update management and internal stakeholders throughout the incident-handling process effectively.

B. Improve the mitigation phase to ensure causes can be quickly identified, and systems returned to a functioning state.

C. Implement an automated operation to pull systems events/logs and bring them into an organizational context.

D. Allocate additional resources for the containment phase to stabilize systems in a timely manner and reduce an attack's breadth.

E. Modify the incident handling playbook and checklist to ensure alignment and agreement on roles, responsibilities, and steps before an incident occurs.

Answer: (SHOW ANSWER)

The Cisco study material recommends integrating automation for log/event collection and contextual analysis to reduce detection delays and ensure rapid identification of anomalies. It also emphasizes the need for pre- defined roles and documented steps in anIncident Handling Playbook, following NIST SP 800-61 Rev.2 standards, to improve consistency and readiness during incidents.

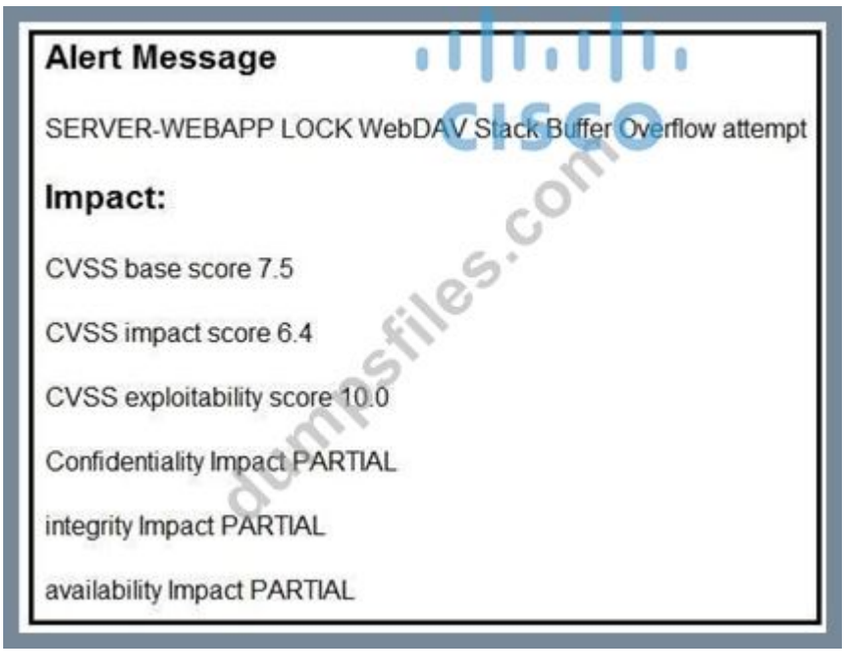
NEW QUESTION: 60
An investigator notices that GRE packets are going undetected over the public network. What is occurring?
A. encryption
B. tunneling
C. decryption
D. steganography
Answer: B (LEAVE A REPLY)
Generic Routing Encapsulation (GRE) is a tunneling protocol used to encapsulate a wide variety of network layer protocols inside point-to-point connections. If packets encapsulated with GRE are bypassing monitoring tools, it's likely due to tunneling-where payloads are hidden within another protocol. Tunneling can obscure malicious content or lateral movement in a network and is a common method used in data exfiltration.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Network Protocols and Evasion Techniques.
-

NEW QUESTION: 61
What is the steganography anti-forensics technique?
A. hiding a section of a malicious file in unused areas of a file
B. changing the file header of a malicious file to another file type
C. sending malicious files over a public network by encapsulation
D. concealing malicious files in ordinary or unsuspecting places
Answer: (SHOW ANSWER)
Steganography is the anti-forensics technique of hiding malicious content within seemingly innocent files, such as image, audio, or video files. The goal is to conceal data or code in a way that avoids suspicion and detection, thereby making traditional security inspection tools ineffective unless they are explicitly designed to detect hidden data within media files.
Steganography differs from encryption because it does not simply make data unreadable; it hides the existence of the data itself. It is commonly used in cyber operations to hide command-and-control instructions or to exfiltrate sensitive information in covert ways.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Evasion and Obfuscation Techniques, Anti-Forensics, Steganography Section.

NEW QUESTION: 62
An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)
A. Format the workstation drives.
B. Restore to a system recovery point.
C. Disconnect from the network.
D. Replace the faulty CPU.
E. Take an image of the workstation.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
What is the transmogrify anti-forensics technique?
A. hiding a section of a malicious file in unused areas of a file
B. sending malicious files over a public network by encapsulation
C. concealing malicious files in ordinary or unsuspecting places
D. changing the file header of a malicious file to another file type
Answer: D (LEAVE A REPLY)
Explanation/Reference:
https://www.csoonline.com/article/2122329/the-rise-of-anti-forensics.html#:~:text=Transmogrify%20is%
20similarly%20wise%20to,a%20file%20from%2C%20say%2C%20.

NEW QUESTION: 64



Refer to the exhibit. After a cyber attack, an engineer is analyzing an alert that was missed on the intrusion detection system. The attack exploited a vulnerability in a business critical, web-based application and violated its availability. Which two migration techniques should the engineer recommend? (Choose two.)

A. heap-based security
B. data execution prevention
C. address space randomization
D. NOP sled technique
E. encapsulation
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 65
Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

A. process injection
B. privilege escalation
C. GPO modification
D. token manipulation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
Snort detects traffic that is targeting vulnerabilities in files that belong to software in the Microsoft Office suite. On a SIEM tool, the SOC analyst sees an alert from Cisco FMC. Cisco FMC is implemented with Snort IDs. Which alert message is shown?

A. FILE-OFFICE Microsoft Graphics buffer overflow
B. FILE-OFFICE Microsoft Graphics cross site scripting (XSS)
C. FILE-OFFICE Microsoft Graphics SQL INJECTION

D. FILE-OFFICE Microsoft Graphics remote code execution attempt

Answer: D (LEAVE A REPLY)

Cisco Firepower Management Center (FMC), when configured with Snort rules, classifies attacks with signature categories such as FILE-OFFICE for Microsoft Office-based exploits. One of the critical threats involving Microsoft Office is a known vector involving Microsoft Graphics, which attackers exploit for remote code execution (RCE). RCE vulnerabilities enable attackers to execute arbitrary commands or code on the target machine-making this classification high-severity.

The alert "FILE-OFFICE Microsoft Graphics remote code execution attempt" is consistent with what Cisco and Snort define for such threats and appears in rulesets addressing vulnerabilities like CVE-2017-0001.

Reference: Cisco Secure Firewall Threat Defense and Snort rule categories in the Cisco CyberOps v1.2 Guide.

-

NEW QUESTION: 67

What is the function of a disassembler?

A. aids performing static malware analysis

B. aids viewing and changing the running state

C. aids transforming symbolic language into machine code

D. aids defining breakpoints in program execution

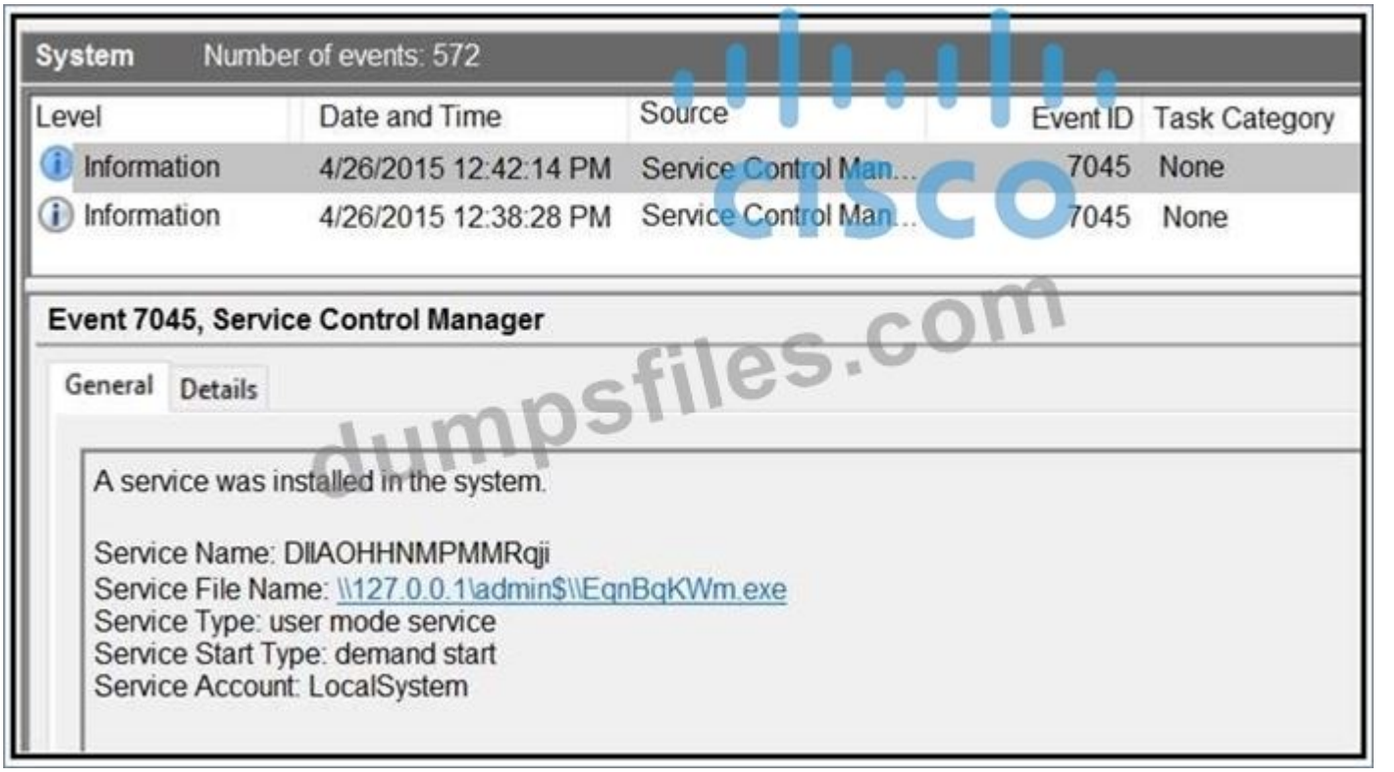
Answer: A (LEAVE A REPLY)

A disassembler is a forensic and reverse engineering tool that translates machine-level code (binary) back into human-readable assembly language. This is used during static malware analysis to understand how the malware is constructed and what it is designed to do without actually executing the code.

According to theCyberOps Technologies (CBRFIR) 300-215 study guide, "Disassembler tools are used to assist with reverse malware engineering by allowing a security professional to examine the binary and understand the functionality of the malware code".

-

NEW QUESTION: 68

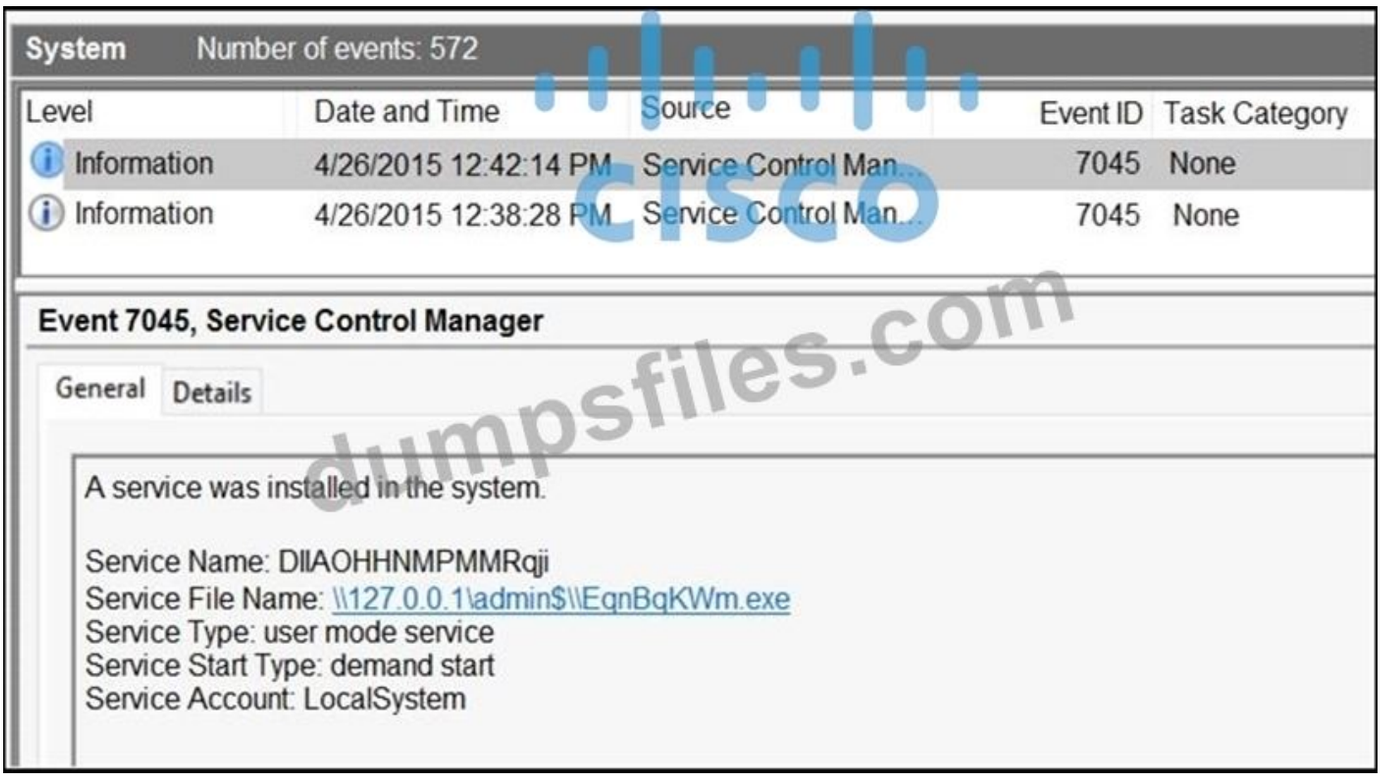


Refer to the exhibit. An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hour prior. Which two indicators of compromise should be determined from this information?
(Choose two.)

A. unauthorized system modification
B. compromised root access
C. denial of service attack
D. privilege escalation
E. malware outbreak

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 69
Refer to the exhibit.



An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hour prior. Which two indicators of compromise should be determined from this information? (Choose two.)

A. privilege escalation

B. unauthorized system modification

C. malware outbreak

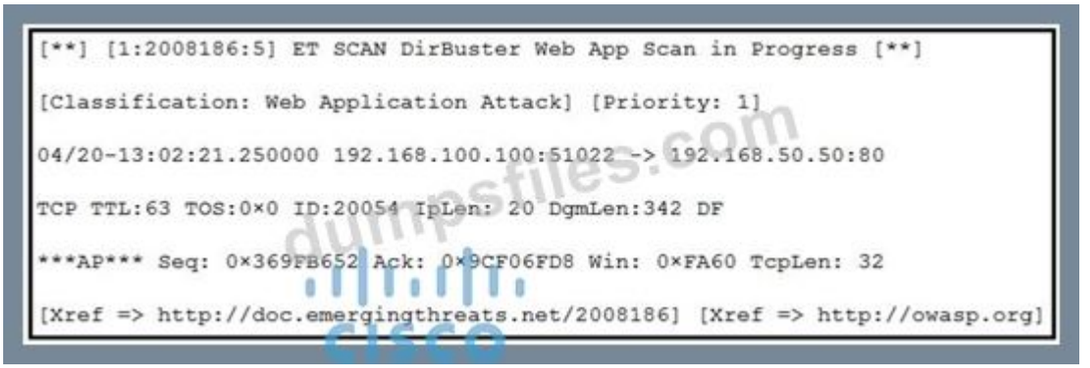
D. compromised root access

E. denial of service attack

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 70

Refer to the exhibit.



According to the SNORT alert, what is the attacker performing?

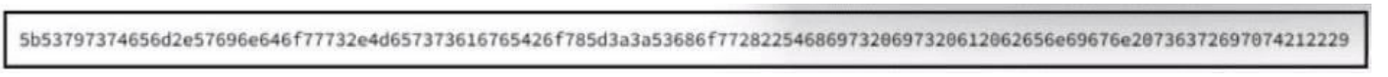
A. brute-force attack against the web application user accounts

B. XSS attack against the target webserver

C. brute-force attack against directories and files on the target webserver
D. SQL injection attack against the target webserver
Answer: C (LEAVE A REPLY)
The alert clearly identifies ET SCAN DirBuster Web App Scan in Progress, referencingSID 2008186, which is a Snort signature that specifically detectsDirBusteractivity. DirBuster is a well-known tool used for brute- forcing hidden directories and files on web servers.
The Cisco CyberOps Associate guide and OWASP both identifydirectory brute-forcingas a reconnaissance technique to find unprotected or misconfigured endpoints on web applications, typically prior to launching deeper attacks.
Therefore, the correct interpretation of the alert is:
C). brute-force attack against directories and files on the target webserver.

NEW QUESTION: 71
An organization uses a Windows 7 workstation for access tracking in one of their physical data centers on which a guard documents entrance/exit activities of all personnel. A server shut down unexpectedly in this data center, and a security specialist is analyzing the case. Initial checks show that the previous two days of entrance/exit logs are missing, and the guard is confident that the logs were entered on the workstation. Where should the security specialist look next to continue investigating this case?
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList
C. HKEY_CURRENT_USER\Software\Classes\Winlog
D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser
Answer: (SHOW ANSWER)
The correct registry path to investigate user profiles and login details is:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList This location stores information about each user profile on the machine, including login activity and the LastWrite time for forensic tracking.

NEW QUESTION: 72
Refer to the exhibit.



A. hex encoding
B. metamorphic encoding
C. ASCII85 encoding
D. Base64 encoding
Answer: (SHOW ANSWER)
The string shown is long, alphanumeric, and includes both uppercase and lowercase letters with numbers- characteristics of Base64 encoding. This format is widely used to obfuscate payloads in

malicious scripts, particularly in phishing or malware campaigns. Base64 encoding is also supported by Python and other platforms for data transformation.
-

NEW QUESTION: 73
A new zero-day vulnerability is discovered in the web application. Vulnerability does not require physical access and can be exploited remotely. Attackers are exploiting the new vulnerability by submitting a form with malicious content that grants them access to the server. After exploitation, attackers delete the log files to hide traces. Which two actions should the security engineer take next? (Choose two.)
A. Validate input upon submission.
B. Block connections on port 443.
C. Install antivirus.
D. Update web application to the latest version.
E. Enable file integrity monitoring.
Answer: (SHOW ANSWER)
* Input validation (A) is a critical countermeasure to defend against command injection and related vulnerabilities, as discussed in the Cisco guide. Proper validation ensures that malicious commands or payloads are not accepted or executed by the web application.
* File integrity monitoring (E) helps detect unauthorized changes such as log deletion or binary modification, making it a crucial tool in recognizing and investigating tampering attempts.Blocking port
443 (B) would disable HTTPS and is not a practical solution. Antivirus (C) does not prevent form-based application attacks, and merely updating the application (D) may not be sufficient without addressing the underlying input validation flaw.
-