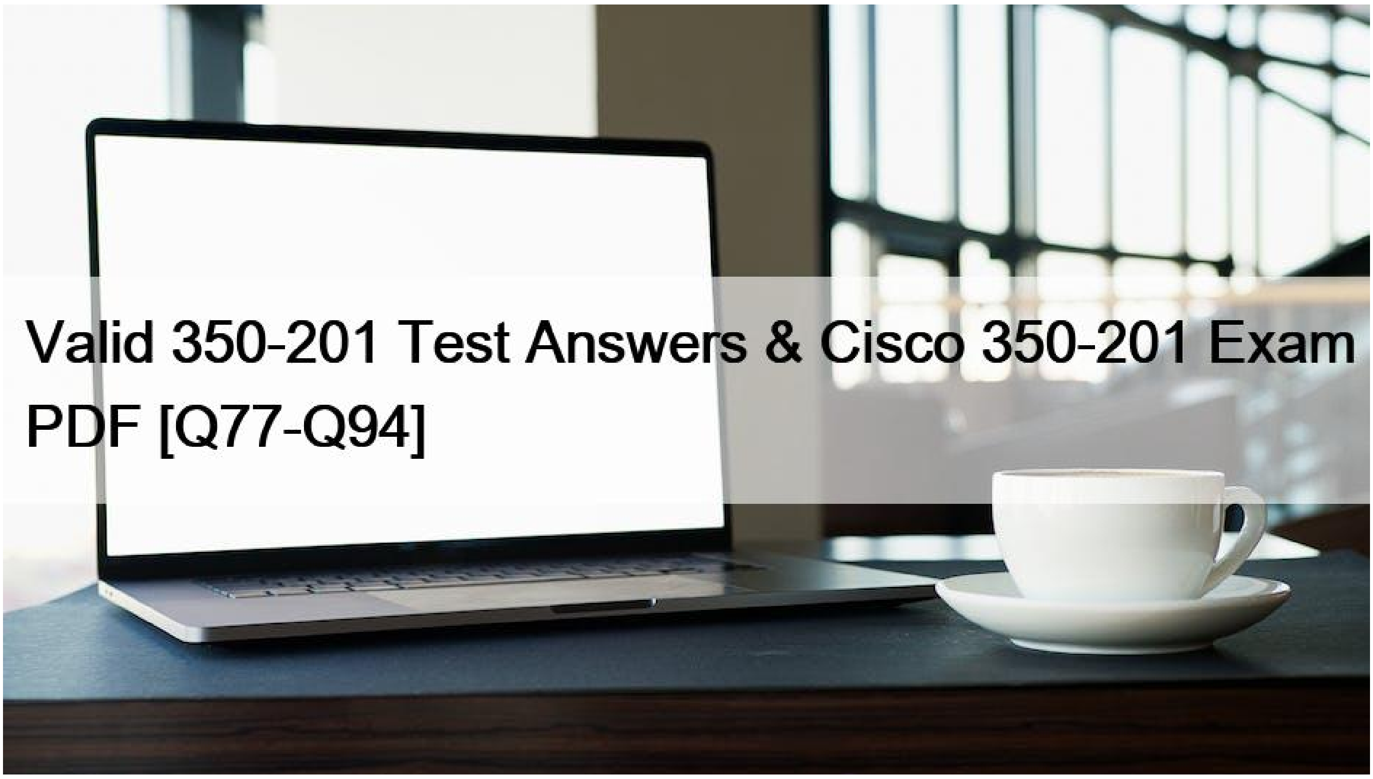
Valid 350-201 Test Answers & Cisco 350-201 Exam PDF [Q77-Q94



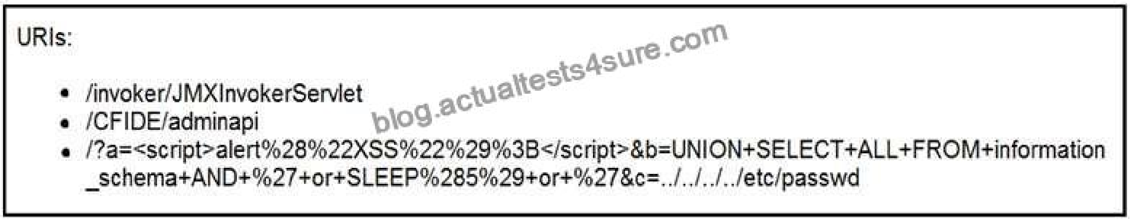
Valid 350-201 Test Answers & Cisco 350-201 Exam PDF
Cisco 350-201 Certification Real 2024 Mock Exam

Q77. An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal.

Which compliance regulations must the audit apply to the company?
* HIPAA
* FISMA
* COBIT
* PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is the compliance regulation that must be applied to a company that accepts credit card payments. PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Since the small business in question has acquired a POS terminal to handle credit card transactions, it falls under the purview of PCI DSS compliance.

Q78.



URIs:

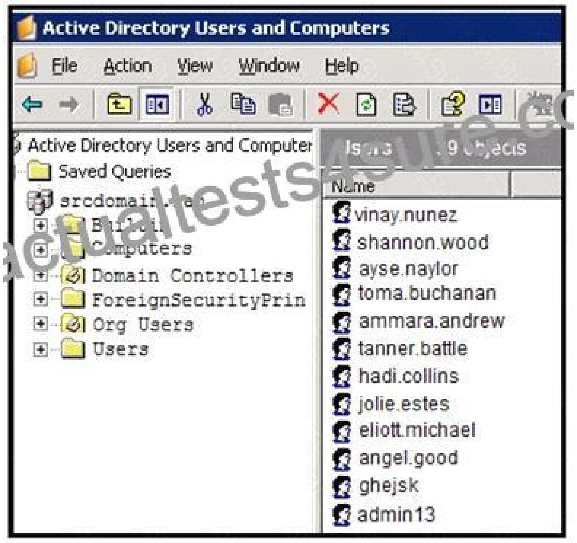
- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

Refer to the exhibit. At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?
* exploitation
* actions on objectives
* delivery
* reconnaissance
Explanation/Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf

Q79. What is needed to assess risk mitigation effectiveness in an organization?
* analysis of key performance indicators
* compliance with security standards
* cost-effectiveness of control measures
* updated list of vulnerable systems

Q80. An engineer is analyzing a possible compromise that happened a week ago when the company database servers unexpectedly went down. The analysis reveals that attackers tampered with Microsoft SQL Server Resolution Protocol and launched a DDoS attack. The engineer must act quickly to ensure that all systems are protected. Which two tools should be used to detect and mitigate this type of future attack? (Choose two.)
* firewall
* Wireshark
* autopsy
* SHA512
* IPS

Q81. Refer to the exhibit.



Active Directory Users and Computer
Saved Queries
srcdomain
Builtin
Computers
Domain Controllers
ForeignSecurityPrin
Org Users
Users

vinay.nunez
shannon.wood
ayse.naylor
toma.buchanan
ammara.andrew
tanner.battle
hadi.collins
jolie.estes
eliott.michael
angel.good
ghejsk
admin13

An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior.

Which type of compromise is occurring?
* compromised insider
* compromised root access
* compromised database tables
* compromised network

The creation of privileged user accounts in the Active Directory that coincide with suspicious network traffic suggests a network compromise. This type of activity is often indicative of an attacker gaining sufficient access to create accounts with elevated privileges, which can be used for further malicious activities within the network. The cross-correlation of events from other sources that align with the timing of these account creations strengthens the case for a compromised network. This scenario is consistent with tactics used by attackers to maintain persistence and establish control over network resources for ongoing exploitation1.

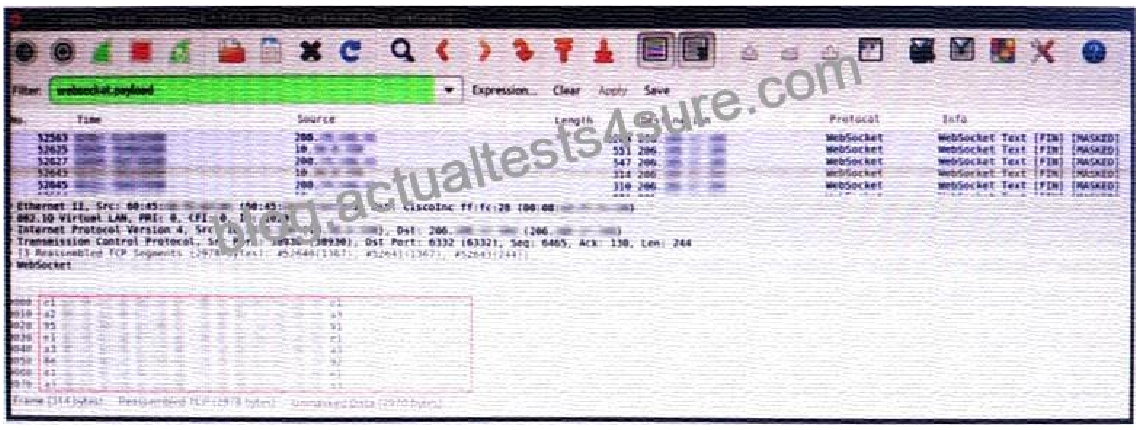
References:

* The Performing CyberOps Using Cisco Security Technologies (CBRCOR) course covers the fundamentals of cybersecurity operations, including the identification and analysis of security incidents and network compromises1.

* The Cisco Certified CyberOps Associate certification provides knowledge on monitoring, detecting, and responding to cybersecurity threats, which includes understanding the signs of a compromised network2

Q82. A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?
* Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
* Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
* Review the server backup and identify server content and data criticality to assess the intrusion risk
* Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

Q83. Refer to the exhibit.



```
Filter: websocket.payload

No.    Time          Source          Length  Destination   Protocol   Info
52563  [redacted]    200.[redacted]  [illegible] 206.[redacted]  WebSocket  WebSocket Text [FIN] [MASKED]
52625  [redacted]    10.[redacted]   551     206.[redacted]  WebSocket  WebSocket Text [FIN] [MASKED]
52627  [redacted]    200.[redacted]  547     206.[redacted]  WebSocket  WebSocket Text [FIN] [MASKED]
52643  [redacted]    10.[redacted]   314     206.[redacted]  WebSocket  WebSocket Text [FIN] [MASKED]
52645  [redacted]    200.[redacted]  310     206.[redacted]  WebSocket  WebSocket Text [FIN] [MASKED]

Ethernet II, Src: 00:45:[redacted] (00:45:[redacted]), Dst: CiscoInc ff:fc:28 (00:00:[redacted])
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: [illegible]
Internet Protocol Version 4, Src: 10.[redacted] (10.[redacted]), Dst: 206.[redacted] (206.[redacted])
Transmission Control Protocol, Src Port: 30930 (30930), Dst Port: 6332 (6332), Seq: 6465, Ack: 130, Len: 244
[3 Reassembled TCP Segments (2978 bytes): #52640(1367), #52641(1367), #52643(244)]
WebSocket

0000  e1 [redacted]   e1
0010  a2 [redacted]   a?
0020  95 [redacted]   91
0030  e1 [redacted]   e1
0040  a3 [redacted]   a3
0050  8e [redacted]   92
0060  e1 [redacted]   e1
0070  a1 [redacted]   11

Frame (314 bytes)   Reassembled TCP (2978 bytes)   Unmasked Data (2970 bytes)
```

An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable. What does this STIX indicate?
* The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible

* The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information
* There is a possible data leak because payloads should be encoded as UTF-8 text
* There is a malware that is communicating via encrypted channels to the command and control server

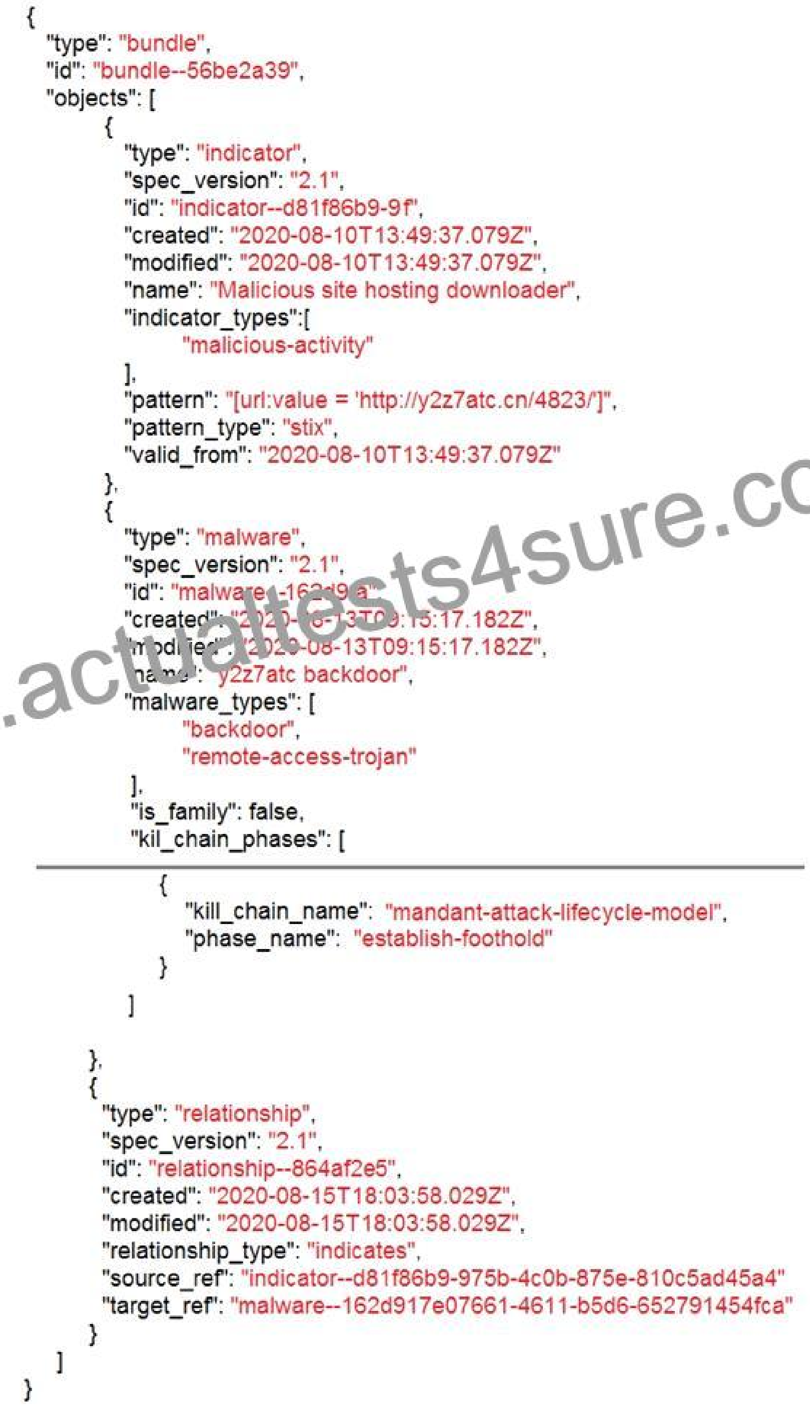
The STIX (Structured Threat Information eXpression) in the context of the exhibit indicates a scenario where a Google Chrome extension is initiating direct IP connections using the WebSocket protocol, and the payloads are obfuscated and unreadable. This behavior is suspicious and suggests that the extension could be a front for malware that is using encrypted channels to communicate with a command and control server. The use of WebSockets and the obfuscation of payloads are common tactics used by malware authors to evade detection and maintain persistent control over compromised systems. The fact that the payloads cannot be decoded or read as UTF-8 text further supports the likelihood of malicious activity, as legitimate extensions would not typically need to obfuscate their communications.

References :=

* STIX/TAXII is a framework for sharing cyber threat intelligence, which would include indicators of such suspicious activities1.

* Understanding the implications of obfuscated payloads in network traffic, as described in cybersecurity resources23.

Q84. Refer to the exhibit.

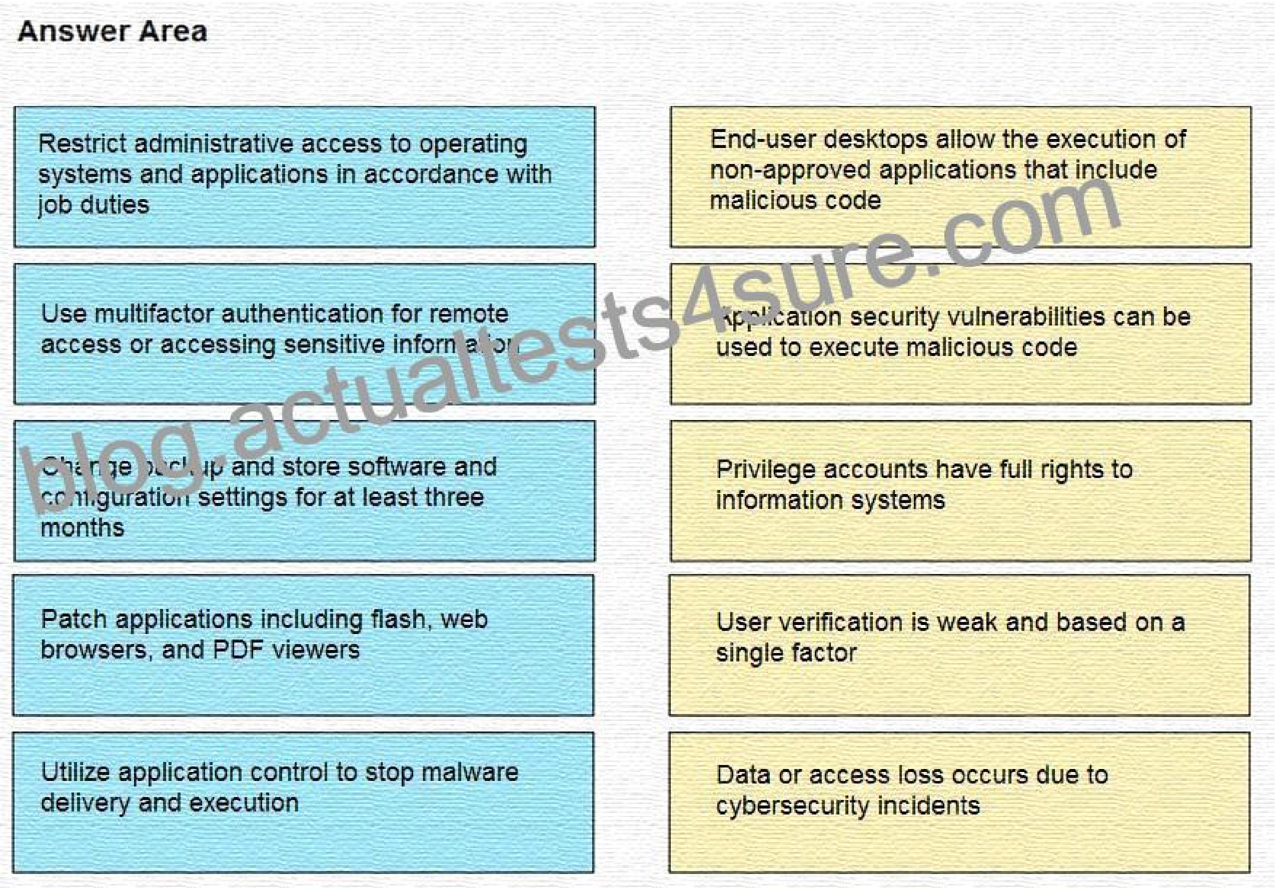


```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
        {
          "type": "indicator",
          "spec_version": "2.1",
          "id": "indicator--d81f86b9-9f",
          "created": "2020-08-10T13:49:37.079Z",
          "modified": "2020-08-10T13:49:37.079Z",
          "name": "Malicious site hosting downloader",
          "indicator_types":[
                "malicious-activity"
          ],
          "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
          "pattern_type": "stix",
          "valid_from": "2020-08-10T13:49:37.079Z"
        },
        {
          "type": "malware",
          "spec_version": "2.1",
          "id": "malware--162d9a",
          "created": "2020-08-13T09:15:17.182Z",
          "modified": "2020-08-13T09:15:17.182Z",
          "name": "y2z7atc backdoor",
          "malware_types": [
                "backdoor",
                "remote-access-trojan"
           ],
           "is_family": false,
           "kil_chain_phases": [
               {
                  "kill_chain_name":  "mandant-attack-lifecycle-model",
                  "phase_name":  "establish-foothold"
               }
           ]

      },
      {
        "type": "relationship",
        "spec_version": "2.1",
        "id": "relationship--864af2e5",
        "created": "2020-08-15T18:03:58.029Z",
        "modified": "2020-08-15T18:03:58.029Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4"
        "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
      }
    ]
}
```

Which indicator of compromise is represented by this STIX?

* website redirecting traffic to ransomware server
* website hosting malware to download files
* web server vulnerability exploited by malware
* cross-site scripting vulnerability to backdoor server

Q85. Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.



Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties

Use multifactor authentication for remote access or accessing sensitive information

Change backup and store software and configuration settings for at least three months

Patch applications including flash, web browsers, and PDF viewers

Utilize application control to stop malware delivery and execution

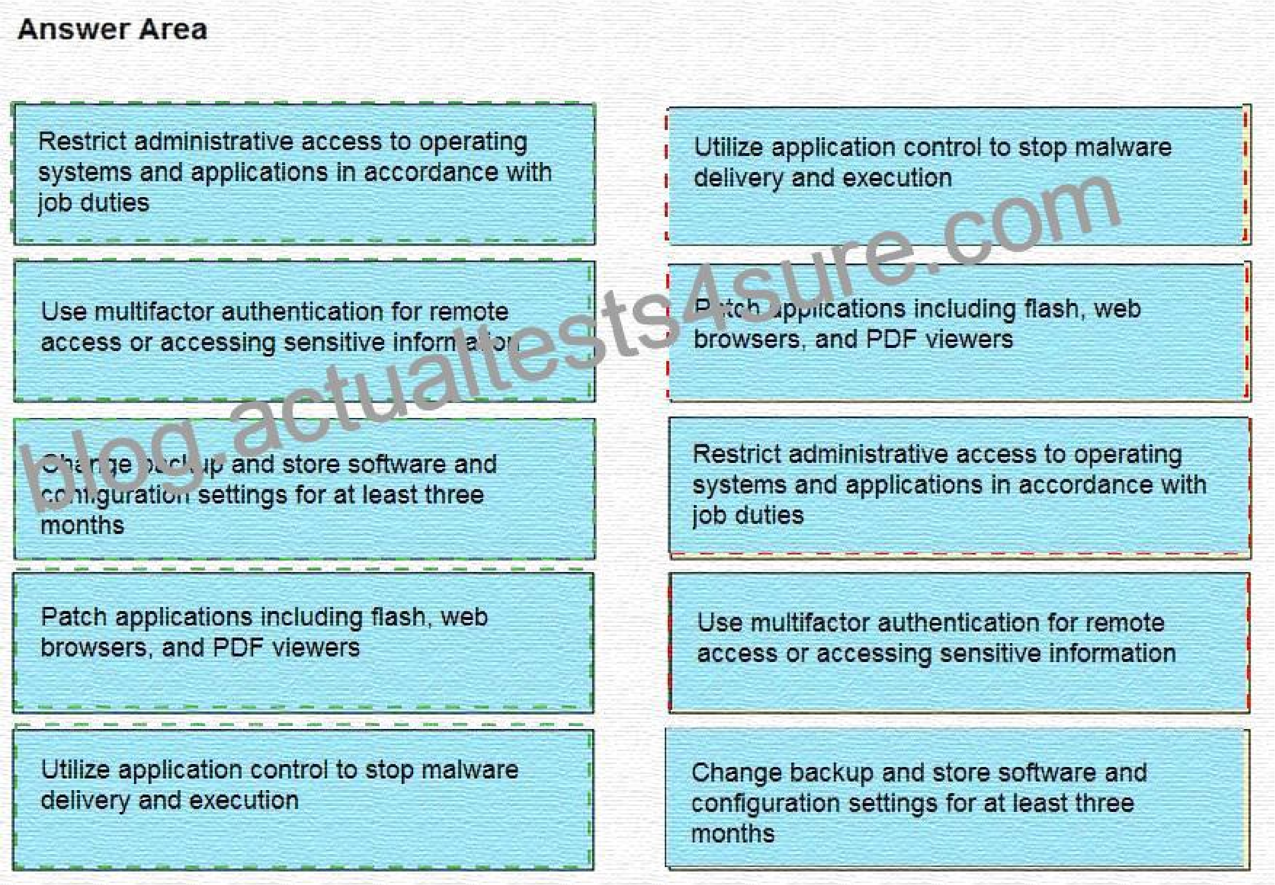
End-user desktops allow the execution of non-approved applications that include malicious code

Application security vulnerabilities can be used to execute malicious code

Privilege accounts have full rights to information systems

User verification is weak and based on a single factor

Data or access loss occurs due to cybersecurity incidents



Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties

Use multifactor authentication for remote access or accessing sensitive information

Change backup and store software and configuration settings for at least three months

Patch applications including flash, web browsers, and PDF viewers

Utilize application control to stop malware delivery and execution

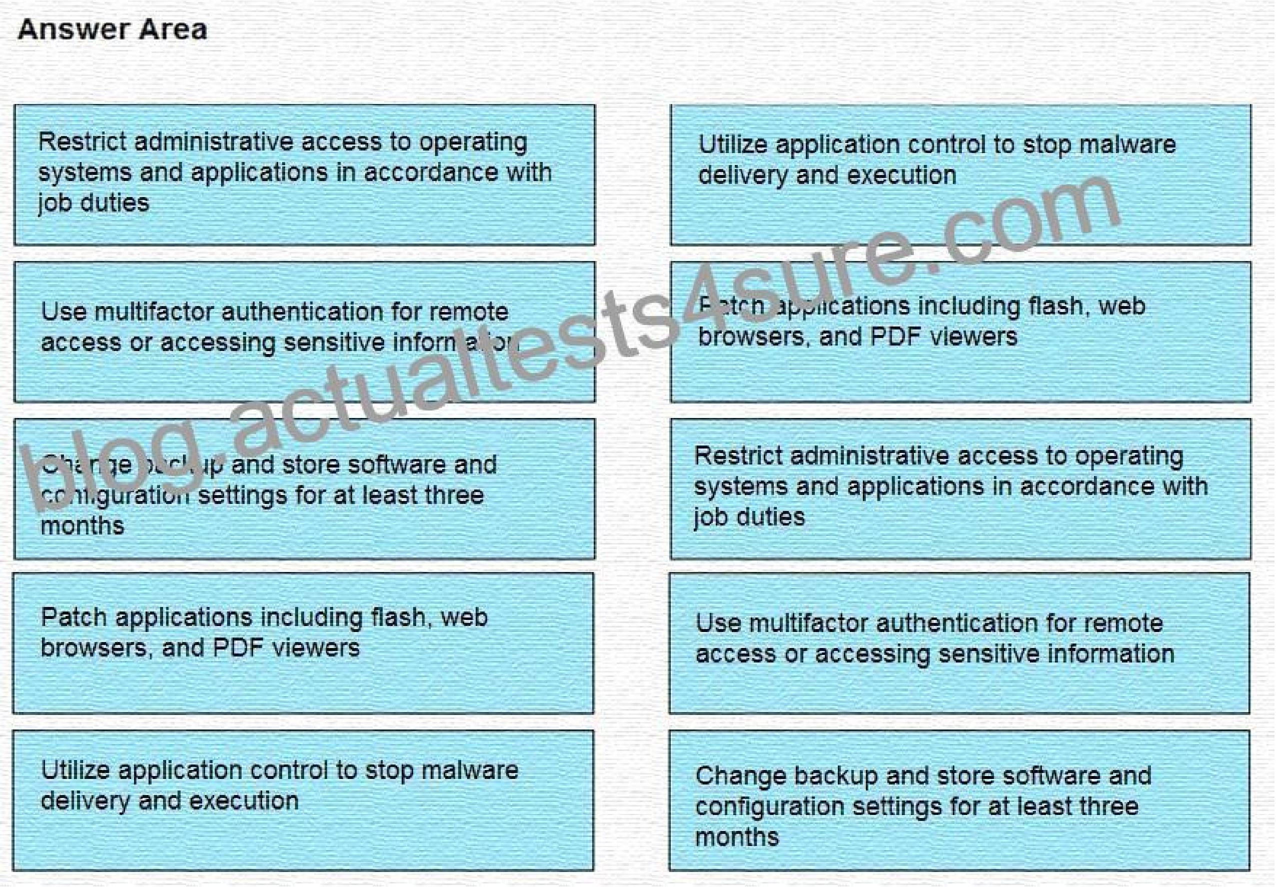
Utilize application control to stop malware delivery and execution

Patch applications including flash, web browsers, and PDF viewers

Restrict administrative access to operating systems and applications in accordance with job duties

Use multifactor authentication for remote access or accessing sensitive information

Change backup and store software and configuration settings for at least three months



Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	Utilize application control to stop malware delivery and execution
Use multifactor authentication for remote access or accessing sensitive information	Patch applications including flash, web browsers, and PDF viewers
Change backup and store software and configuration settings for at least three months	Restrict administrative access to operating systems and applications in accordance with job duties
Patch applications including flash, web browsers, and PDF viewers	Use multifactor authentication for remote access or accessing sensitive information
Utilize application control to stop malware delivery and execution	Change backup and store software and configuration settings for at least three months

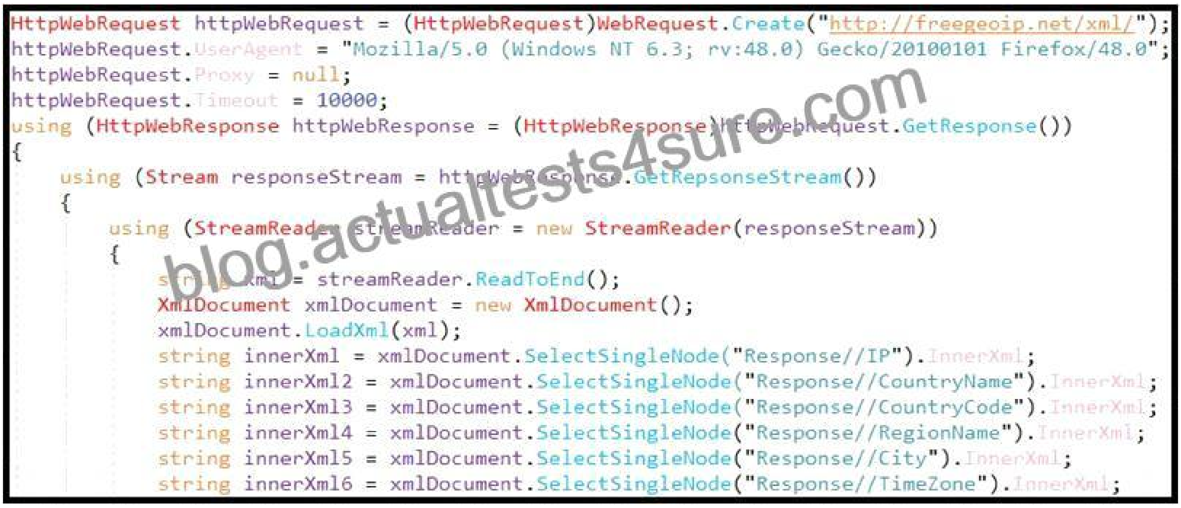
Q86. An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

- ExecutedMalware.ioc
- Crossrider.ioc
- ConnectToSuspiciousDomain.ioc
- W32 AccesschkUtility.ioc

Q87. A SOC analyst detected a ransomware outbreak in the organization coming from a malicious email attachment. Affected parties are notified, and the incident response team is assigned to the case. According to the NIST incident response handbook, what is the next step in handling the incident?

- Create a follow-up report based on the incident documentation.
- Perform a vulnerability assessment to find existing vulnerabilities.
- Eradicate malicious software from the infected machines.
- Collect evidence and maintain a chain-of-custody during further analysis.

Q88. Refer to the exhibit.



```
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create("http://freegeoip.net/xml/");
httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0";
httpWebRequest.Proxy = null;
httpWebRequest.Timeout = 10000;
using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
{
    using (Stream responseStream = httpWebResponse.GetRepsonseStream())
    {
        using (StreamReader streamReader = new StreamReader(responseStream))
        {
            string xml = streamReader.ReadToEnd();
            XmlDocument xmlDocument = new XmlDocument();
            xmlDocument.LoadXml(xml);
            string innerXml = xmlDocument.SelectSingleNode("Response//IP").InnerXml;
            string innerXml2 = xmlDocument.SelectSingleNode("Response//CountryName").InnerXml;
            string innerXml3 = xmlDocument.SelectSingleNode("Response//CountryCode").InnerXml;
            string innerXml4 = xmlDocument.SelectSingleNode("Response//RegionName").InnerXml;
            string innerXml5 = xmlDocument.SelectSingleNode("Response//City").InnerXml;
            string innerXml6 = xmlDocument.SelectSingleNode("Response//TimeZone").InnerXml;
```

An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?
* The file is redirecting users to a website that requests privilege escalations from the user.
* The file is redirecting users to the website that is downloading ransomware to encrypt files.
* The file is redirecting users to a website that harvests cookies and stored account information.
* The file is redirecting users to a website that is determining users&#8217; geographic location.
The STIX (Structured Threat Information eXpression) provided in the exhibit indicates a risk associated with a file that redirects users to a malicious website. The code snippet shows an HTTP request being made to a URL known fordistributing ransomware. This type of threat involves tricking users into downloading and executing malicious software that encrypts their files and then demands payment for decryption. The static analysis of the file&#8217;s behavior, as shown in the code, supports the conclusion that the file poses a risk of ransomware infection1.

References:

* Cisco CyberOps Using Core Security Technologies documentation.

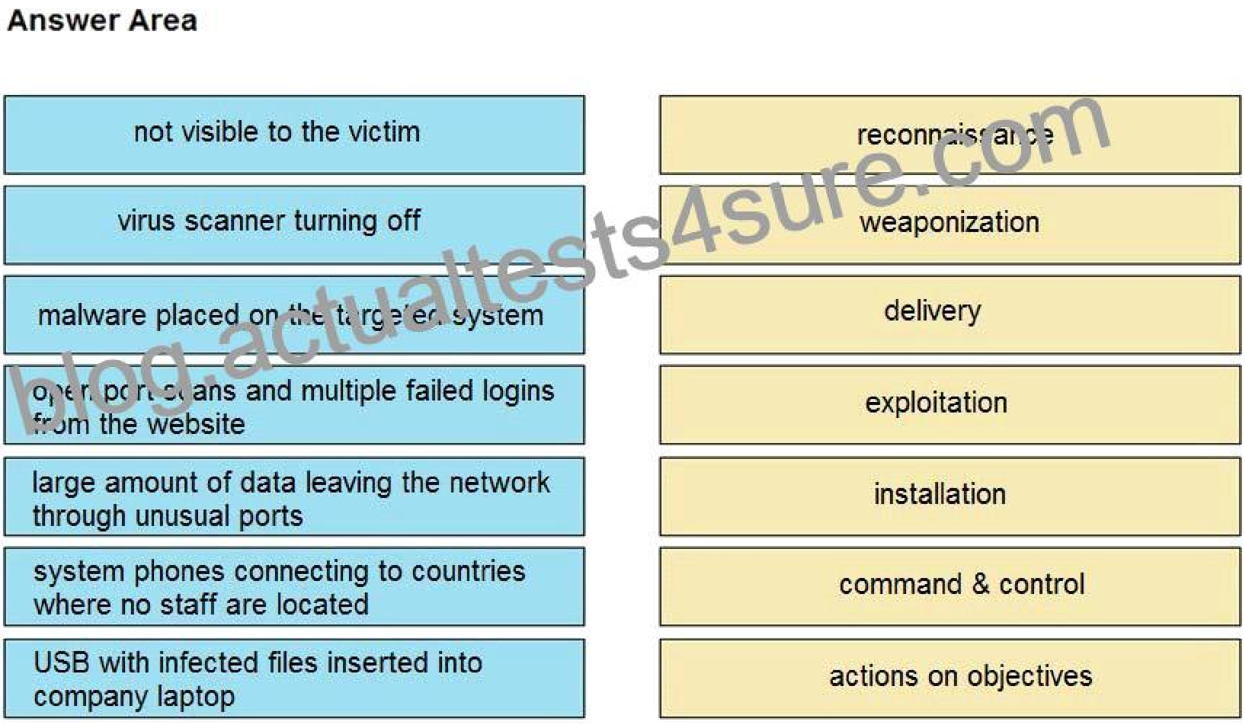
* Understanding Cisco CyberOps Using Core Security Technologies from Cisco&#8217;s official training and certifications resources.

* Foundation Topics > Security Principles | Cisco Press1.

* Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR) v1.02.

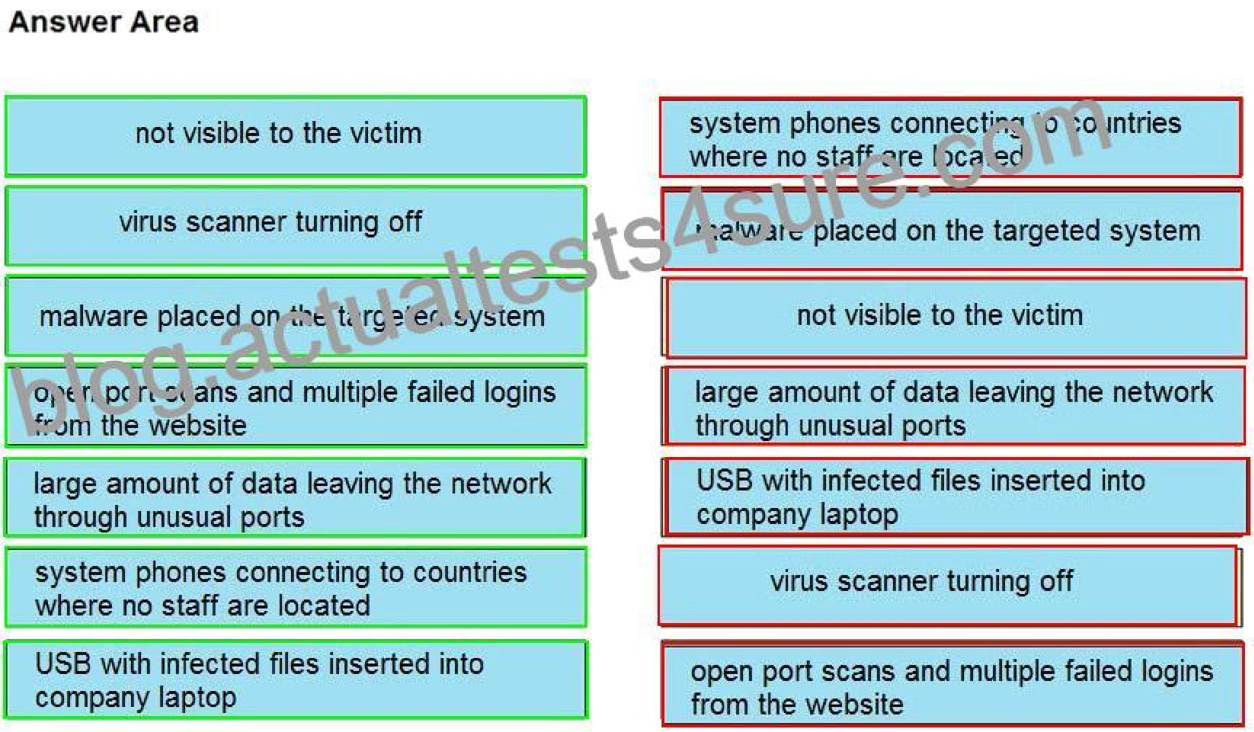
* CBRFIR Exam Topics &#8211; Cisco Learning Network

Q89. Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.



Answer Area

not visible to the victim	reconnaissance
virus scanner turning off	weaponization
malware placed on the targeted system	delivery
open port scans and multiple failed logins from the website	exploitation
large amount of data leaving the network through unusual ports	installation
system phones connecting to countries where no staff are located	command & control
USB with infected files inserted into company laptop	actions on objectives



Answer Area

not visible to the victim	system phones connecting to countries where no staff are located
virus scanner turning off	malware placed on the targeted system
malware placed on the targeted system	not visible to the victim
open port scans and multiple failed logins from the website	large amount of data leaving the network through unusual ports
large amount of data leaving the network through unusual ports	USB with infected files inserted into company laptop
system phones connecting to countries where no staff are located	virus scanner turning off
USB with infected files inserted into company laptop	open port scans and multiple failed logins from the website

Q90. An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to prevent this type of attack from reoccurring? (Choose two.)

* Implement a patch management process.

* Scan the company server files for known viruses.

* Apply existing patches to the company servers.
* Automate antivirus scans of the company servers.
* Define roles and responsibilities in the incident response playbook.

To prevent a security breach exploiting the Netlogon Remote Protocol vulnerability from reoccurring, the incident response team should implement a patch management process and apply existing patches to the company servers5. Patch management ensures that all systems are up-to-date with the latest security patches, which can prevent known vulnerabilities from being exploited6. Applying existing patches is a critical step in securing systems against identified threats, such as the Netlogon Remote Protocol vulnerability5.

Q91. A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

* DLP for data in motion
* DLP for removable data
* DLP for data in use
* DLP for data at rest

Data Loss Prevention (DLP) for data in use is designed to detect and prevent unauthorized attempts to copy or move sensitive data, particularly within an active processing environment. This type of DLP monitors and controls endpoint activities, ensuring that sensitive data is not transferred out of the network through unapproved applications or removable storage devices.

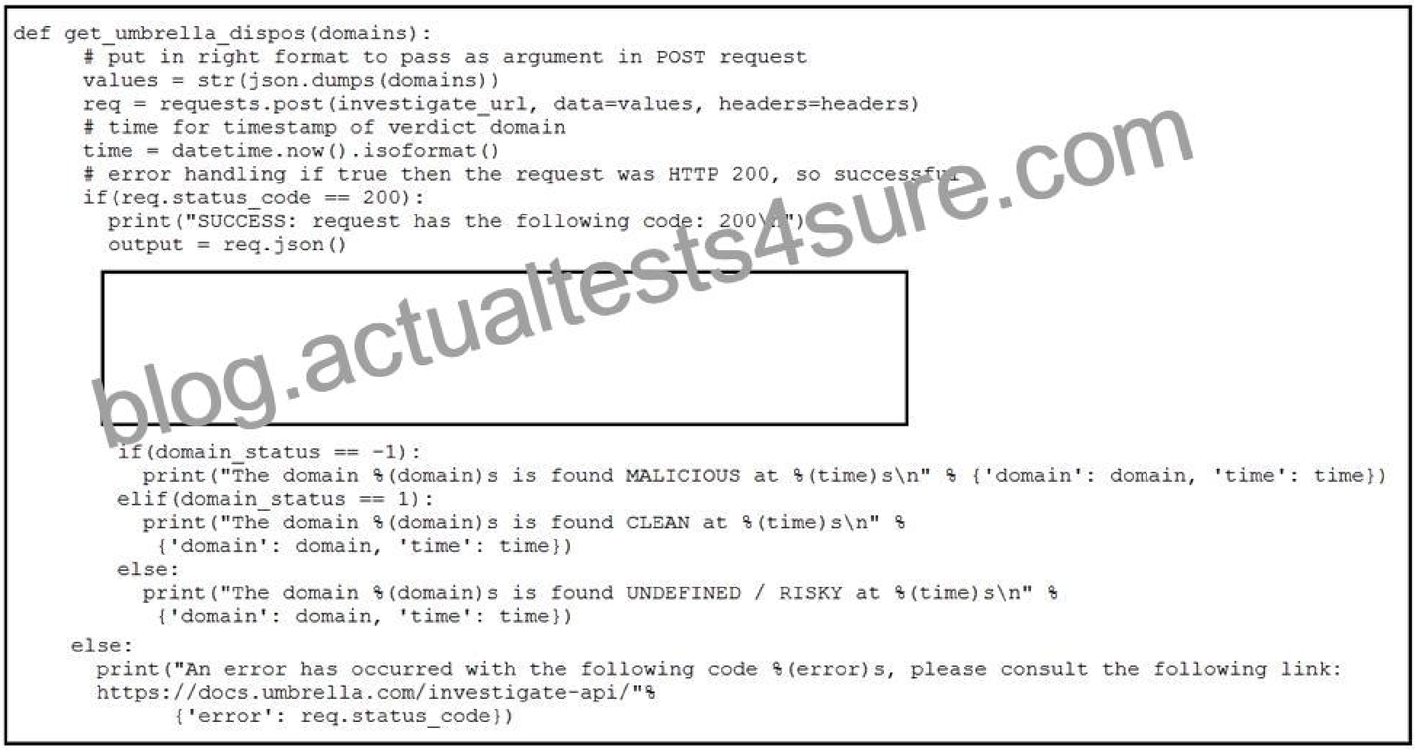
Q92. A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company&#8217;s infrastructure. Which steps should an engineer take at the recovery stage?

* Determine the systems involved and deploy available patches
* Analyze event logs and restrict network access
* Review access lists and require users to increase password complexity
* Identify the attack vector and update the IDS signature list

Q93. A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

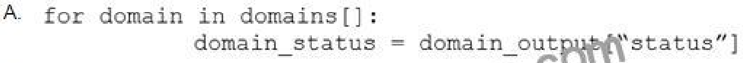
* Run the sudo sysdiagnose command
* Run the sh command
* Run the w command
* Run the who command

Q94. Refer to the exhibit.

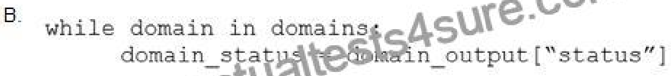


```
def get_umbrella_dispos(domains):
      # put in right format to pass as argument in POST request
      values = str(json.dumps(domains))
      req = requests.post(investigate_url, data=values, headers=headers)
      # time for timestamp of verdict domain
      time = datetime.now().isoformat()
      # error handling if true then the request was HTTP 200, so successful
      if(req.status_code == 200):
        print("SUCCESS: request has the following code: 200\n")
        output = req.json()



         if(domain_status == -1):
           print("The domain %(domain)s is found MALICIOUS at %(time)s\n" % {'domain': domain, 'time': time})
         elif(domain_status == 1):
           print("The domain %(domain)s is found CLEAN at %(time)s\n" %
             {'domain': domain, 'time': time})
         else:
           print("The domain %(domain)s is found UNDEFINED / RISKY at %(time)s\n" %
             {'domain': domain, 'time': time})
     else:
       print("An error has occurred with the following code %(error)s, please consult the following link:
       https://docs.umbrella.com/investigate-api/"%
             {'error': req.status_code})
```

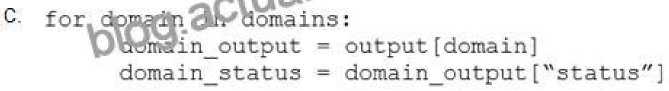
Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?



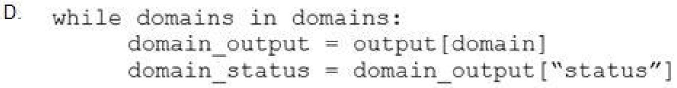
```
A. for domain in domains[]:
               domain_status = domain_output["status"]
```



```
B. while domain in domains:
         domain_status = domain_output["status"]
```



```
C. for domain in domains:
         domain_output = output[domain]
         domain_status = domain_output["status"]
```



```
D. while domains in domains:
         domain_output = output[domain]
         domain_status = domain_output["status"]
```

* Option A
* Option B
* Option C
* Option D

350-201 Exam Questions and Valid 350-201 Dumps PDF: https://www.actualtests4sure.com/350-201-test-questions.html]