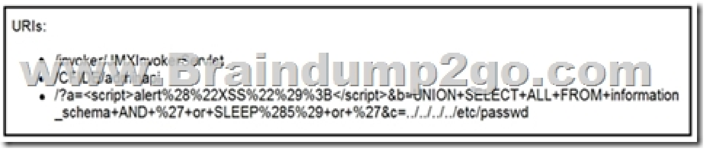
[February-2023Braindump2go 350-201 Free Dumps Download[Q46-Q76

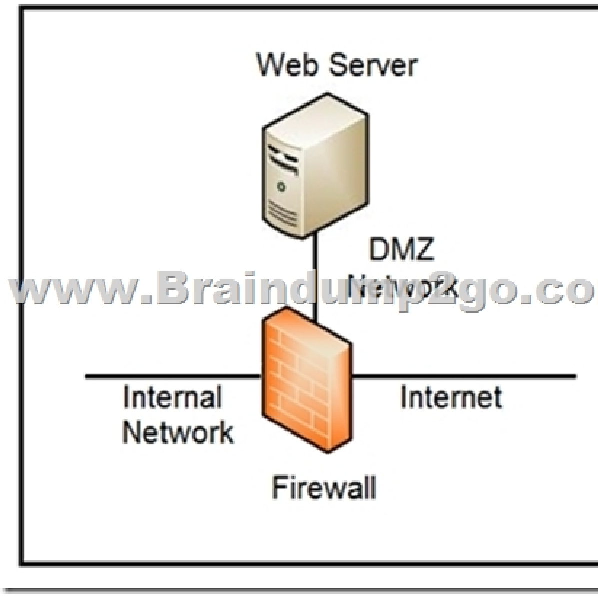
February/2023 Latest Braindump2go 350-201 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go 350-201 Real Exam Questions!QUESTION 46A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)A. incident response playbooksB. asset vulnerability assessmentC. report of staff members with asset relationsD. key assets and executivesE. malware analysis reportAnswer: BEExplanation:https://cloudogre.com/risk-assessment/QUESTION 47Refer 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?



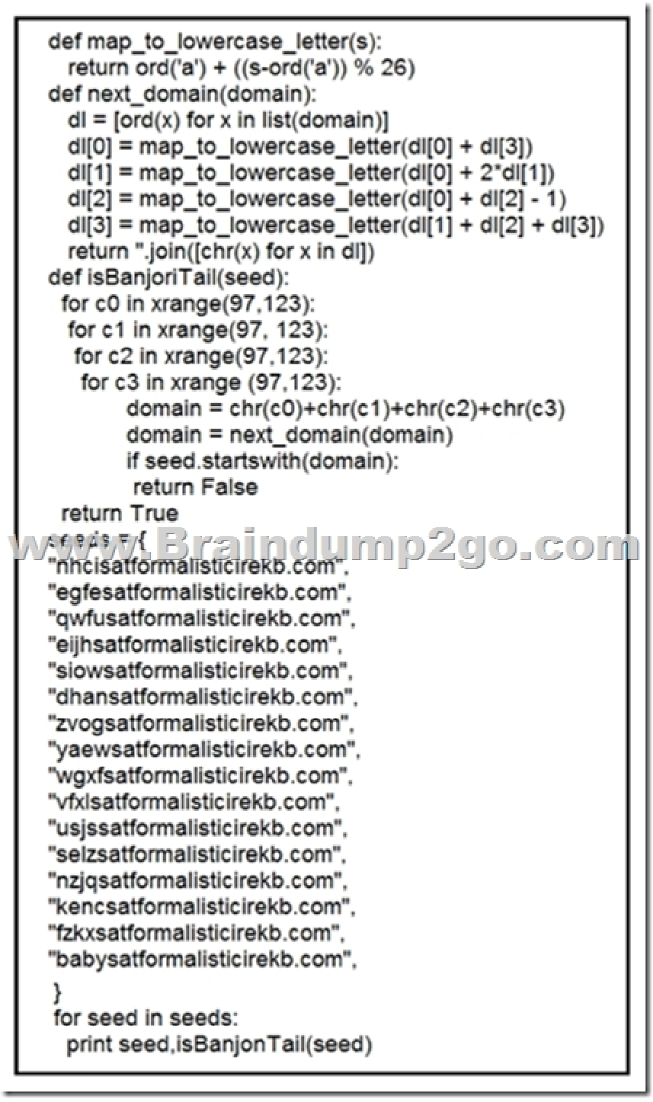
URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/administrator
- /?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

A. exploitationB. actions on objectivesC. deliveryD. reconnaissanceAnswer: CExplanation: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdfQUESTION 48What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?A. Tapping interrogation replicates signals to a separate port for analyzing trafficB. Tapping interrogations detect and block malicious trafficC. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policiesD. Inline interrogation detects malicious traffic but does not block the trafficAnswer: AQUESTION 49Refer to the exhibit. Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

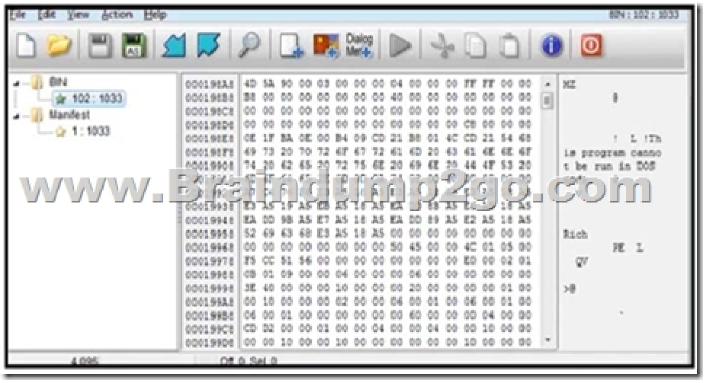


A. Create an ACL on the firewall to allow only TLS 1.3B. Implement a proxy server in the DMZ networkC. Create an ACL on the firewall to allow only external connectionsD. Move the webserver to the internal networkE. Move the webserver to the external networkAnswer: ABQUESTION 50According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?A. Perform a vulnerability assessmentB. Conduct a data protection impact assessmentC. Conduct penetration testingD. Perform awareness testingAnswer: BExplanation: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf QUESTION 51A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?A. Classify the criticality of the information, research the attacker's motives, and identify missing patchesB. Determine the damage to the business, extract reports, and save evidence according to a chain of custodyC. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploitedD. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation planAnswer: BQUESTION 52A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?A.   Identify the business applications running on the assetsB.   Update software to patch third-party softwareC.   Validate CSRF by executing exploits within MetasploitD.   Fix applications according to the risk scoresAnswer: DExplanation: Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious web site, email, blog, instant message, or program causes a user's web browser to perform an unwanted action on a trusted site when the user is authenticated. A CSRF attack works because browser requests automatically include all cookies including session cookies. Therefore, if the user is authenticated to the site, the site cannot distinguish between legitimate authorized requests and forged authenticated requests.QUESTION 53An 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.)A.   firewallB.   WiresharkC.   autopsyD.   SHA512E.   IPSAnswer: AEQUESTION 54A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?A.   HIPAAB.   PCI-DSSC.   Sarbanes-Oxley D.   GDPRAnswer: DExplanation: https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/QUESTION 55An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?A.   Host a discovery meeting and define configuration and policy updates B.   Update the IDS/IPS signatures and reimage the affected hostsC.   Identify the systems that have been affected and tools used to detect the attackD.   Identify the traffic with data capture using Wireshark and review email filtersAnswer: BQUESTION 56An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the engineer should take?A.   Investigate the vulnerability to prevent further spreadB.   Acknowledge the vulnerabilities and document the riskC.   Apply vendor patches or available hot fixesD.   Isolate the assets affected in a separate networkAnswer: BExplanation:Acknowledge issues are those which, for whatever reason, you decide not to resolve at present. There are valid reasons for not immediately resolving a vulnerability, and they should be recorded, along with the reasoning for acknowledging it and a review date given. If the level of risk they present is sufficiently high, record the issue in a risk register.QUESTION 57A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs.Which technology should be used to accomplish this task?A.   application whitelisting/blacklistingB.   network NGFWC.   host-based IDSD.   antivirus/antispyware softwareAnswer: AQUESTION 58Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?A.   chmod 666B.   chmod 774C.   chmod 775D.   chmod 777Answer: DExplanation: https://www.pluralsight.com/blog/it-ops/linux-file-permissionsQUESTION 59A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network.What is the next step in handling the incident?A.   Block the source IP from the firewallB.   Perform an antivirus scan on the laptopC.   Identify systems or services at riskD.   Identify lateral movementAnswer: CQUESTION 60A 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's infrastructure. Which steps should an engineer take at the recovery stage?A.   Determine the systems involved and deploy available patchesB.   Analyze event logs and restrict network accessC.   Review access lists and require users to increase password complexityD.   Identify the attack vector and update the IDS signature listAnswer: AQUESTION 61A patient views information that is not theirs when they sign in to the hospital's online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real- time. What is the first step the analyst should take to address this incident?A.   Evaluate visibility tools to determine if external access resulted in tamperingB.   Contact the third-party handling provider to respond to the incident as criticalC.   Turn off all access to the patient portal to secure patient recordsD.   Review system and application logs to identify errors in the portal codeAnswer: CQUESTION 62Refer to the exhibit. What results from this script?



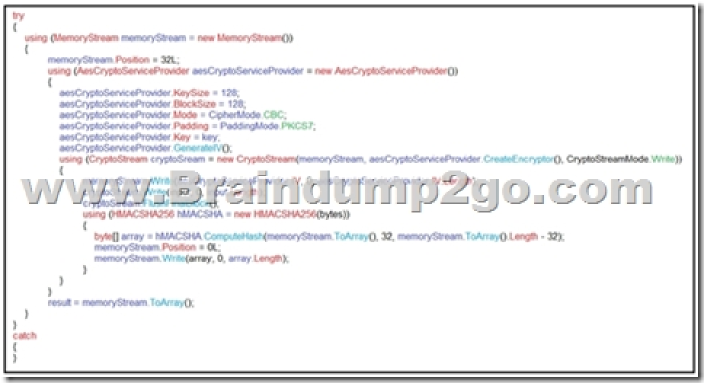
```
def map_to_lowercase_letter(s):
   return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
   dl = [ord(x) for x in list(domain)]
   dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
   dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
   dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
   dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
   return ''.join([chr(x) for x in dl])
def isBanjoriTail(seed):
  for c0 in xrange(97,123):
   for c1 in xrange(97, 123):
    for c2 in xrange(97,123):
     for c3 in xrange (97,123):
            domain = chr(c0)+chr(c1)+chr(c2)+chr(c3)
            domain = next_domain(domain)
            if seed.startswith(domain):
             return False
  return True
seeds = {
"nhcisatformalisticirekb.com",
"egfesatformalisticirekb.com",
"qwfusatformalisticirekb.com",
"eijhsatformalisticirekb.com",
"siowsatformalisticirekb.com",
"dhansatformalisticirekb.com",
"zvogsatformalisticirekb.com",
"yaewsatformalisticirekb.com",
"wgxfsatformalisticirekb.com",
"vfxlsatformalisticirekb.com",
"usjssatformalisticirekb.com",
"selzsatformalisticirekb.com",
"nzjqsatformalisticirekb.com",
"kencsatformalisticirekb.com",
"fzkxsatformalisticirekb.com",
"babysatformalisticirekb.com",
 }
 for seed in seeds:
   print seed,isBanjonTail(seed)
```

A. Seeds for existing domains are checkedB. A search is conducted for additional seedsC. Domains are compared to seed rules D. A list of domains as seeds is blockedAnswer: BQUESTION 63Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?



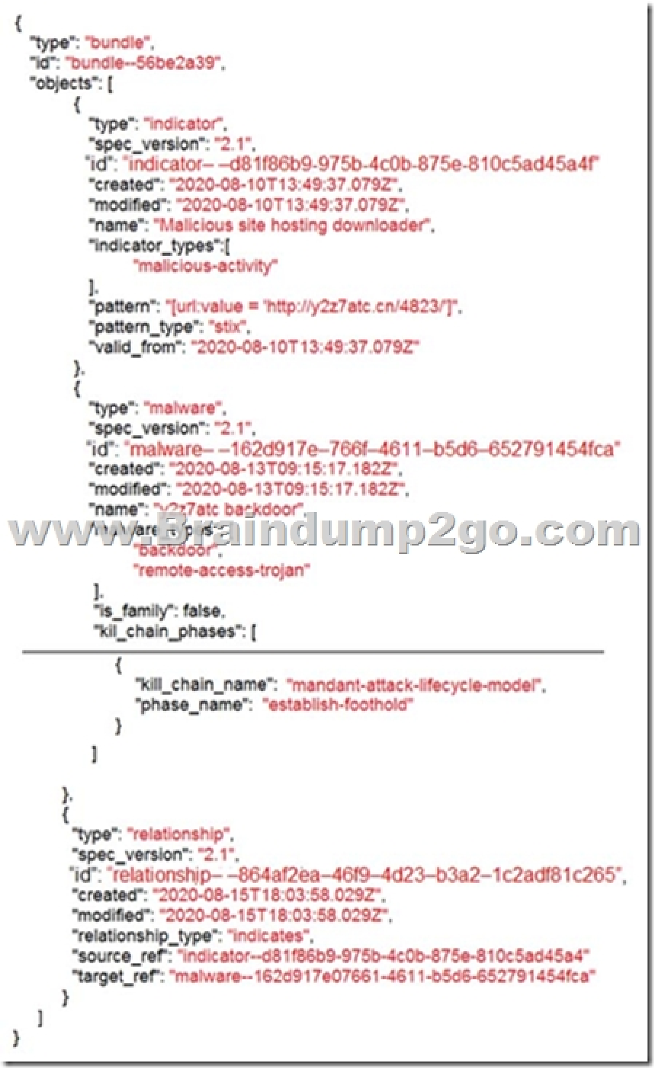
```
000198A8  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ
000198B8  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00         @
000198C8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000198D8  00 00 00 00 00 00 00 00 00 00 00 00 C8 00 00 00
000198E8  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68         !  L !Th
000198F8  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
00019908  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS
[illegible]
[illegible]
[illegible]
00019948  EA DD 9B A5 E7 A5 18 A5 EA DD 89 A5 E2 A5 18 A5
00019958  52 69 63 68 E3 A5 18 A5 00 00 00 00 00 00 00 00   Rich
00019968  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00         PE  L
00019978  F5 CC 51 56 00 00 00 00 00 00 00 00 E0 00 02 01     QV
00019988  0B 01 09 00 00 04 00 00 00 06 00 00 00 00 00 00
00019998  3E 40 00 00 00 10 00 00 00 20 00 00 00 00 01 00   >@
000199A8  00 10 00 00 00 02 00 00 06 00 01 00 06 00 01 00
000199B8  06 00 01 00 00 00 00 00 00 60 00 00 00 04 00 00
000199C8  CD D2 00 00 01 00 00 04 00 00 04 00 00 10 00 00
000199D8  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00
```

A. a DOS MZ executable formatB. a MS-DOS executable archiveC. an archived malwareD. a Windows executable fileAnswer: DQUESTION 64Refer to the exhibit. An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?



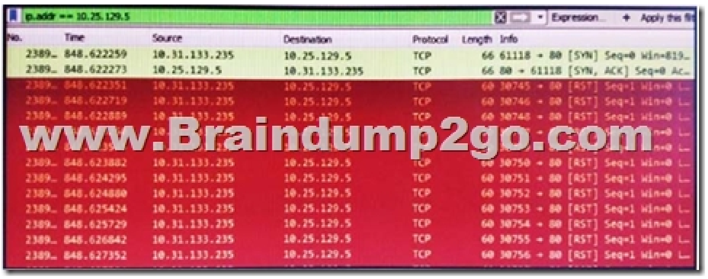
```
try
{
   using (MemoryStream memoryStream = new MemoryStream())
   {
         memoryStream.Position = 32L;
         using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
         {
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = key;
            aesCryptoServiceProvider.GenerateIV();
            using (CryptoStream cryptoSream = new CryptoStream(memoryStream, aesCryptoServiceProvider.CreateEncryptor(), CryptoStreamMode.Write))
            {
               memoryStream.Write([illegible]
               [illegible]Write([illegible]
               cryptoStream.Flush[illegible]();
               using (HMACSHA256 hMACSHA = new HMACSHA256(bytes))
               {
                  byte[] array = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray().Length - 32);
                  memoryStream.Position = 0L;
                  memoryStream.Write(array, 0, array.Length);
               }
            }
         }
         result = memoryStream.ToArray();
   }
}
catch
{
}
```

A. The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.B. The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.C. The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.D. The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.Answer: DExplanation: https://gist.github.com/yetanotherchris/810c5900616b6c76f78dedda9bf3be85QUESTION 65An 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?A. HIPAA B. FISMAC. COBITD. PCI DSSAnswer: DExplanation: https://upserve.com/restaurant-insider/restaurant-pos-pci-compliance-checklist/QUESTION 66A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device. Which should be disabled to resolve the issue?A. SNMPv2B. TCP small servicesC. port UDP 161 and 162D. UDP small servicesAnswer: AExplanation: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-snmpQUESTION 67Refer to the exhibit. Which indicator of compromise is represented by this STIX?



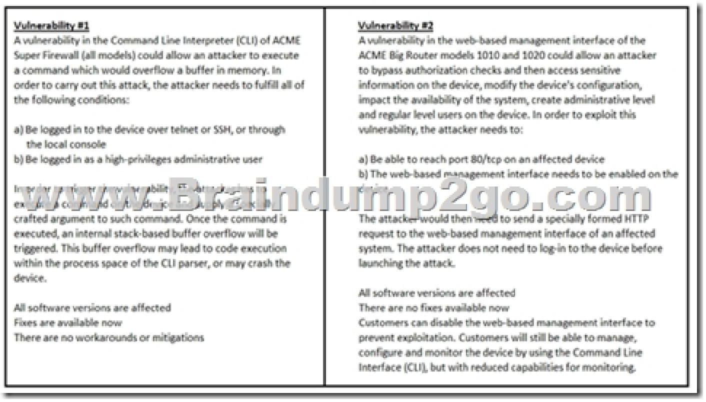
```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
      {
        "type": "indicator",
        "spec_version": "2.1",
       "id": "indicator– –d81f86b9-975b-4c0b-875e-810c5ad45a4f"
        "created": "2020-08-10T13:49:37.079Z",
        "modified": "2020-08-10T13:49:37.079Z",
        "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– –162d917e–766f–4611–b5d6–652791454fca"
        "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– –864af2ea–46f9–4d23–b3a2–1c2adf81c265",
      "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"
    }
  ]
}
```

A. website redirecting traffic to ransomware serverB. website hosting malware to download filesC. web server vulnerability exploited by malwareD. cross-site scripting vulnerability to backdoor serverAnswer: BQUESTION 68Refer to the exhibit. What is occurring in this packet capture?



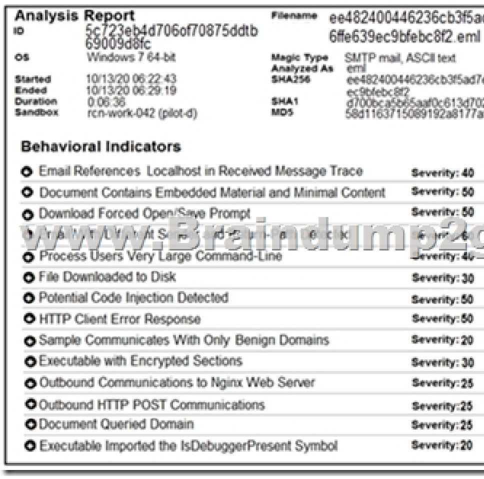
```
No.    Time          Source           Destination      Protocol  Length  Info
2389…  848.622259    10.31.133.235    10.25.129.5      TCP       66 61118 → 80 [SYN] Seq=0 Win=819…
2389…  848.622273    10.25.129.5      10.31.133.235    TCP       66 80 → 61118 [SYN, ACK] Seq=0 Ac…
2389…  848.622351    10.31.133.235    10.25.129.5      TCP       60 30745 → 80 [RST] Seq=1 Win=0 L…
2389…  848.622719    10.31.133.235    10.25.129.5      TCP       60 30746 → 80 [RST] Seq=1 Win=0 L…
2389…  848.622889    10.31.133.235    10.25.129.5      TCP       60 30748 → 80 [RST] Seq=1 Win=0 L…
[illegible]
[illegible]
2389…  848.623882    10.31.133.235    10.25.129.5      TCP       60 30750 → 80 [RST] Seq=1 Win=0 L…
2389…  848.624295    10.31.133.235    10.25.129.5      TCP       60 30751 → 80 [RST] Seq=1 Win=0 L…
2389…  848.624880    10.31.133.235    10.25.129.5      TCP       60 30752 → 80 [RST] Seq=1 Win=0 L…
2389…  848.625424    10.31.133.235    10.25.129.5      TCP       60 30753 → 80 [RST] Seq=1 Win=0 L…
2389…  848.625729    10.31.133.235    10.25.129.5      TCP       60 30754 → 80 [RST] Seq=1 Win=0 L…
2389…  848.626842    10.31.133.235    10.25.129.5      TCP       60 30755 → 80 [RST] Seq=1 Win=0 L…
2389…  848.627352    10.31.133.235    10.25.129.5      TCP       60 30756 → 80 [RST] Seq=1 Win=0 L…
```

A. TCP port scanB. TCP floodC. DNS floodD. DNS tunnelingAnswer: BQUESTION 69Refer to the exhibit. How must these advisories be prioritized for handling?



Vulnerability #1	Vulnerability #2
A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions: a) Be logged in to the device over telnet or SSH, or through the local console b) Be logged in as a high-privileges administrative user In order to trigger the vulnerability, the attacker [illegible] execute a command [illegible] supply a [illegible] crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device. All software versions are affected Fixes are available now There are no workarounds or mitigations	A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to: a) Be able to reach port 80/tcp on an affected device b) The web-based management interface needs to be enabled on the device. The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack. All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.

A. The highest priority for handling depends on the type of institution deploying the devicesB. Vulnerability #2 is the highest priority for every type of institutionC. Vulnerability #1 and vulnerability #2 have the same priorityD. Vulnerability #1 is the highest priority for every type of institutionAnswer: BExplanation:All that is needed is port 80 access on #2 whereas #1 requires a login by a privileged account to exploit.QUESTION 70The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?A. Conduct a risk assessment of systems and applicationsB. Isolate the infected host from the rest of the subnetC. Install malware prevention software on the hostD. Analyze network traffic on the host's subnetAnswer: BExplanation:Short-term containment - limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production server and routing to failover.QUESTION 71An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?A. diagnosticB. qualitativeC. predictiveD. statisticalAnswer: CExplanation:What Is Predictive Analytics?When you know what happened in the past and understand why it happened, you can then begin to predict what is likely to occur in the future based on that information. Predictive analytics takes the investigation a step further, using statistics, computational modeling, and machine learning to determine the probability of various outcomes.What Is Diagnostic Analytics?Once you know what happened, you'll want to know why it happened. That's where diagnostic analytics comes in. Understanding why a trend is developing or why a problem occurred will make your business intelligence actionable. It prevents your team from making inaccurate guesses, particularly related to confusing correlation and causality.QUESTION 72A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?A. Assess the network for unexpected behaviorB. Isolate critical hosts from the networkC. Patch detected vulnerabilities from critical hostsD. Perform analysis based on the established risk factorsAnswer: BQUESTION 73Refer to the exhibit. Cisco Advanced Malware Protection installed on an end-user desktop automatically submitted a low prevalence file to the Threat Grid analysis engine. What should be concluded from this report?



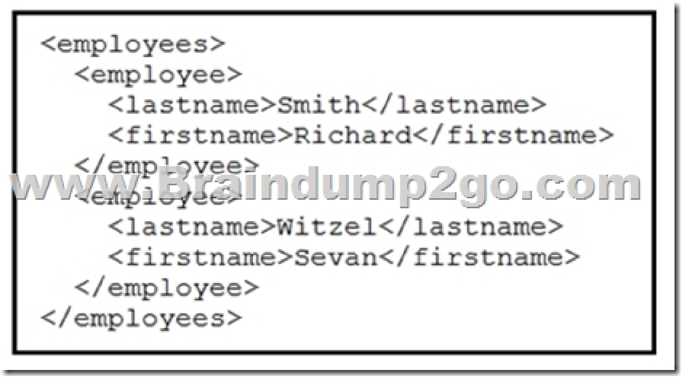
Analysis Report

ID	5c723eb4d706of70875ddtb 69009d8fc	Filename	ee482400446236cb3f5a 6ffe639ec9bfebc8f2.eml
OS	Windows 7 64-bit	Magic Type	SMTP mail, ASCII text
		Analyzed As	eml
Started	10/13/20 06:22:43	SHA256	ee482400446236cb3f5ad7 ec9bfebc8f2
Ended	10/13/20 06:29:19		
Duration	0:06:36	SHA1	d700bca5b65aaf0c613d70
Sandbox	rcn-work-042 (pilot-d)	MD5	58d1163715089192a8177a

Behavioral Indicators

Email References Localhost in Received Message Trace	Severity: 40
Document Contains Embedded Material and Minimal Content	Severity: 50
Download Forced Open/Save Prompt	Severity: 50
[illegible]	[illegible]
Process Users Very Large Command-Line	Severity: 40
File Downloaded to Disk	Severity: 30
Potential Code Injection Detected	Severity: 50
HTTP Client Error Response	Severity: 50
Sample Communicates With Only Benign Domains	Severity: 20
Executable with Encrypted Sections	Severity: 30
Outbound Communications to Nginx Web Server	Severity: 25
Outbound HTTP POST Communications	Severity: 25
Document Queried Domain	Severity: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20

A. Threat scores are high, malicious ransomware has been detected, and files have been modifiedB. Threat scores are low, malicious ransomware has been detected, and files have been modifiedC. Threat scores are high, malicious activity is detected, but files have not been modifiedD. Threat scores are low and no malicious file activity is detectedAnswer: DQUESTION 74An organization is using a PKI management server and a SOAR platform to manage the certificate lifecycle. The SOAR platform queries a certificate management tool to check all endpoints for SSL certificates that have either expired or are nearing expiration. Engineers are struggling to manage problematic certificates outside of PKI management since deploying certificates and tracking them requires searching server owners manually. Which action will improve workflow automation?A. Implement a new workflow within SOAR to create tickets in the incident response system, assign problematic certificate update requests to server owners, and register change requests.B. Integrate a PKI solution within SOAR to create certificates within the SOAR engines to track, update, and monitor problematic certificates.C. Implement a new workflow for SOAR to fetch a report of assets that are outside of the PKI zone, sort assets by certification management leads and automate alerts that updates are needed.D. Integrate a SOAR solution with Active Directory to pull server owner details from the AD and send an automated email for problematic certificates requesting updates.Answer: DQUESTION 75Refer to the exhibit. Which data format is being used?



```
<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
```

A. JSONB. HTMLC. XMLD. CSVAnswer: CQUESTION 76The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?A. Contain the malwareB. Install IPS softwareC. Determine the escalation pathD. Perform vulnerability assessmentAnswer: AResources From:1.2023 Latest Braindump2go 350-201 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/350-201.html2.2023 Latest Braindump2go 350-201 PDF and 350-201 VCE Dumps Free Share: https://drive.google.com/drive/folders/1AxXpeiNddgUeSboJXzaOVsnt5wFFoDnO?usp=sharingFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!