300-215.VCEplus.premium.exam.59q

Number: 300-215
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

300-215

Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps

Version 1.0

Exam A

QUESTION 1

A security team is discussing lessons learned and suggesting process changes after a security breach incident. During the incident, members of the security team failed to report the abnormal system activity due to a high project workload. Additionally, when the incident was identified, the response took six hours due to management being unavailable to provide the approvals needed. Which two steps will prevent these issues from occurring in the future? (Choose two.)

A. Introduce a priority rating for incident response workloads.
B. Provide phishing awareness training for the fill security team.
C. Conduct a risk audit of the incident response workflow.
D. Create an executive team delegation plan.
E. Automate security alert timeframes with escalation triggers.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

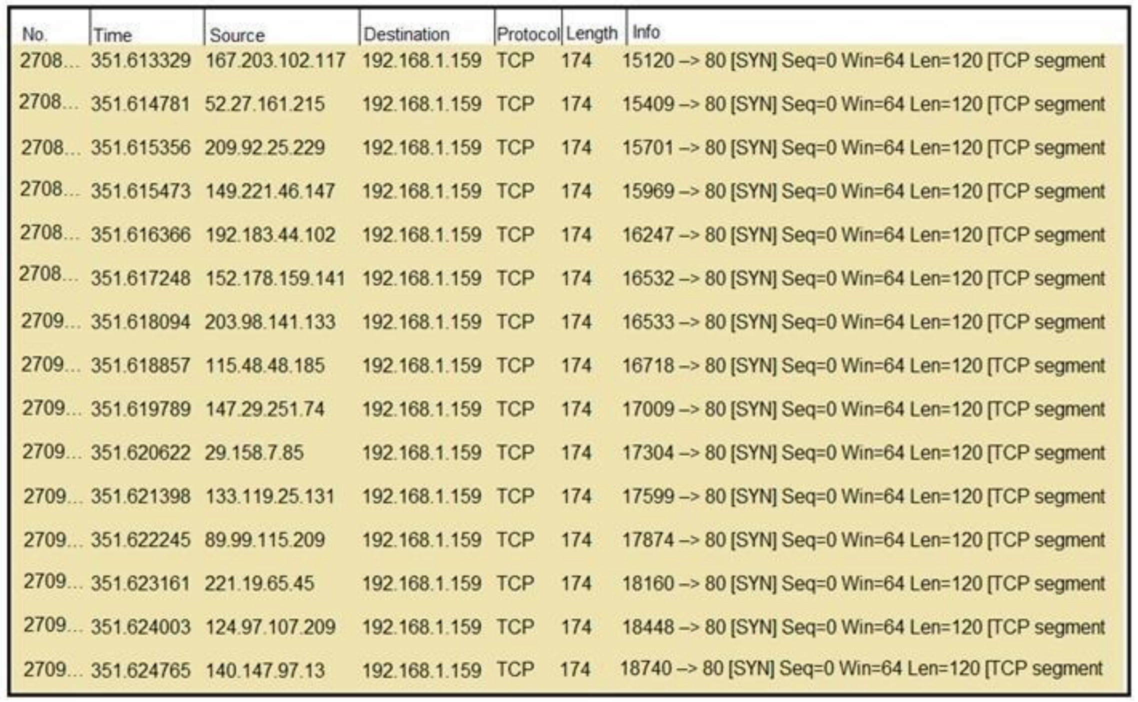
An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

A. Restore to a system recovery point.
B. Replace the faulty CPU.
C. Disconnect from the network.
D. Format the workstation drives.
E. Take an image of the workstation.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3



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

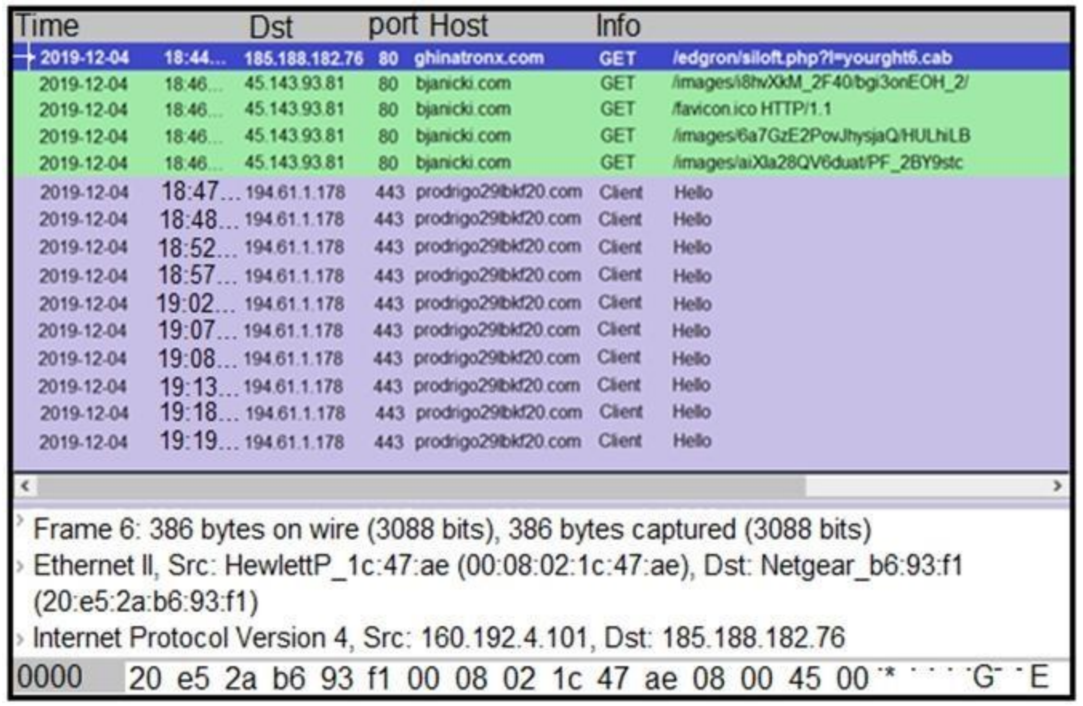
Refer to the exhibit. What should an engineer determine from this Wireshark capture of suspicious network traffic?

A. There are signs of SYN flood attack, and the engineer should increase the backlog and recycle the oldest half-open TCP connections.
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 a DNS attack, and the engineer should hide the BIND version and restrict zone transfers as a countermeasure.
D. There are signs of ARP spoofing, and the engineer should use Static ARP entries and IP address-to-MAC address mappings as a countermeasure.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4



```
Time                 Dst            port Host                  Info
2019-12-04  18:44... 185.188.182.76  80  ghinatronx.com        GET    /edgron/siloft.php?l=yourght6.cab
2019-12-04  18:46... 45.143.93.81    80  bjanicki.com          GET    /images/i8hvXkM_2F40/bgi3onEOH_2/
2019-12-04  18:46... 45.143.93.81    80  bjanicki.com          GET    /favicon.ico HTTP/1.1
2019-12-04  18:46... 45.143.93.81    80  bjanicki.com          GET    /images/6a7GzE2PovJhysjaQ/HULhiLB
2019-12-04  18:46... 45.143.93.81    80  bjanicki.com          GET    /images/aiXla28QV6duat/PF_2BY9stc
2019-12-04  18:47... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  18:48... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  18:52... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  18:57... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  19:02... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  19:07... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  19:08... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  19:13... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  19:18... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello
2019-12-04  19:19... 194.61.1.178   443  prodrigo29lbkf20.com  Client Hello

> Frame 6: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1
  (20:e5:2a:b6:93:f1)
> Internet Protocol Version 4, Src: 160.192.4.101, Dst: 185.188.182.76
0000  20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00  *····G··E
```

Refer to the exhibit. A network engineer is analyzing a Wireshark file to determine the HTTP request that caused the initial Ursnif banking Trojan binary to download. Which filter did the engineer apply to sort the Wireshark traffic logs?

A. http.request.un matches
B. tls.handshake.type ==1
C. tcp.port eq 25
D. tcp.window_size ==0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://www.malware-traffic-analysis.net/2018/11/08/index.html
https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/

QUESTION 5 What is a concern for gathering forensics evidence in public cloud environments?

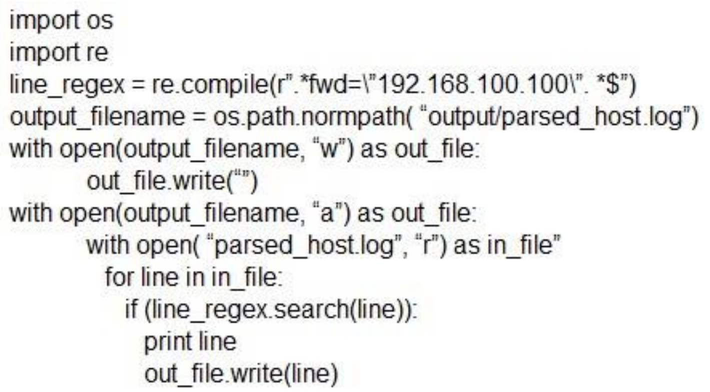
A. High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.
B. Configuration: Implementing security zones and proper network segmentation.

C. Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.
D. Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

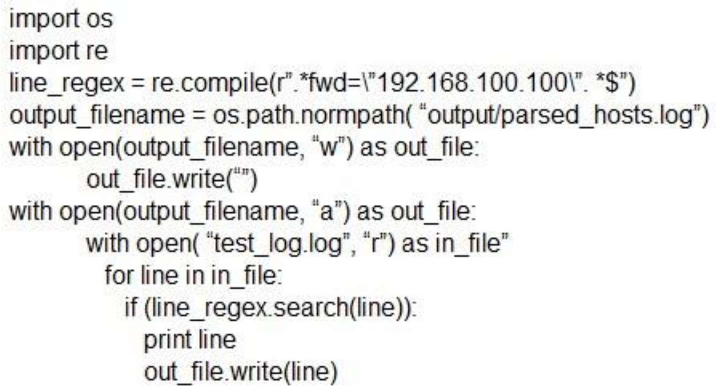
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.researchgate.net/publication/307871954_About_Cloud_Forensics_Challenges_and_Solutions

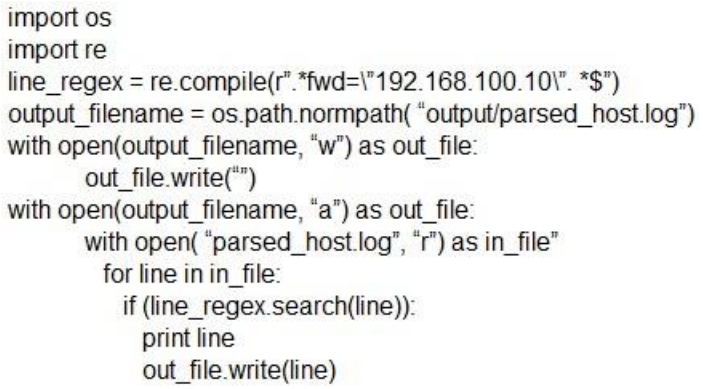
QUESTION 6
Which scripts will search a log file for the IP address of 192.168.100.100 and create an output file named parsed_host.log while printing results to the console? A.



```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( “output/parsed_host.log”)
with open(output_filename, “w”) as out_file:
        out_file.write(“”)
with open(output_filename, “a”) as out_file:
        with open( “parsed_host.log”, “r”) as in_file”
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```



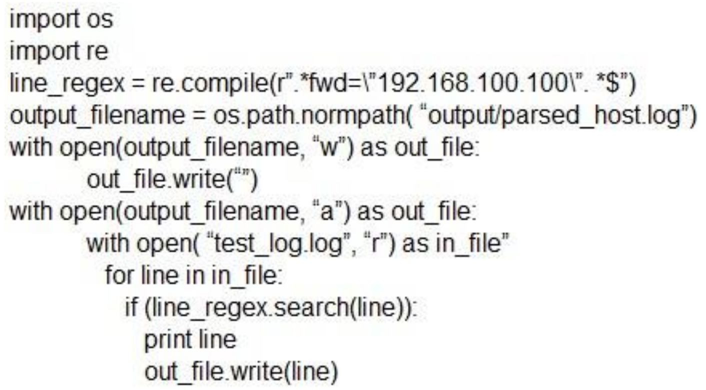
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( “output/parsed_hosts.log”)
with open(output_filename, “w”) as out_file:
        out_file.write(“”)
with open(output_filename, “a”) as out_file:
        with open( “test_log.log”, “r”) as in_file”
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```



```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.10\". *$")
output_filename = os.path.normpath( “output/parsed_host.log”)
with open(output_filename, “w”) as out_file:
        out_file.write(“”)
with open(output_filename, “a”) as out_file:
        with open( “parsed_host.log”, “r”) as in_file”
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

B.

C.



```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( "output/parsed_host.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "test_log.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 8 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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 9
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.)

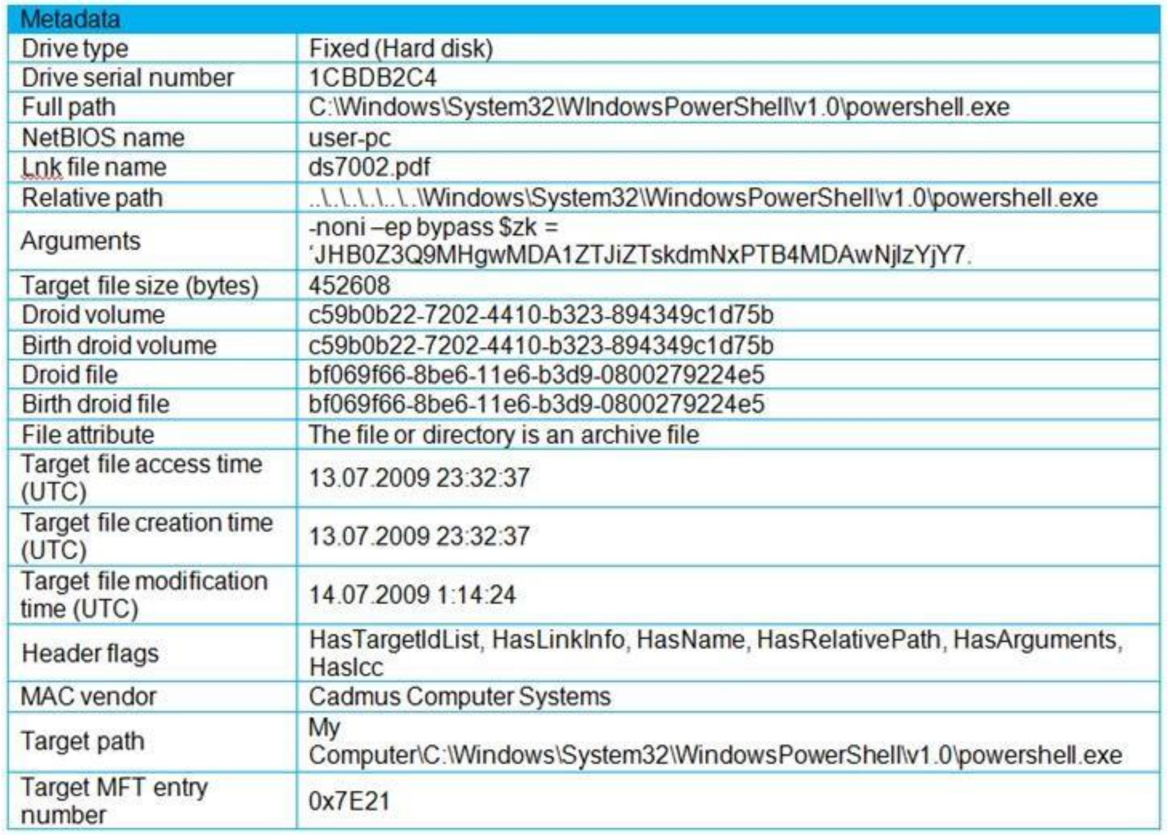
A. Inspect registry entries
B. Inspect processes.
C. Inspect file hash.

D. Inspect file type.
E. Inspect PE header.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a

QUESTION 10



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 = 'JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjlzYjY7.
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

Refer to the exhibit. 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. Delete the suspicious email with the attachment as the file is a shortcut extension and does not represent any threat.
B. 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.
C. Quarantine the file within the endpoint antivirus solution as the file is a ransomware which will encrypt the documents of a victim.
D. Open the file in a sandbox environment for further behavioral analysis as the file contains a malicious script that runs on execution.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 An investigator is analyzing an attack in which malicious files were loaded on the network and were undetected. Several of the images received during the attack include repetitive patterns. Which anti-forensic technique was used?

A. spoofing
B. obfuscation
C. tunneling
D. steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://doi.org/10.5120/1398-1887
https://www.carbonblack.com/blog/steganography-in-the-modern-attack-landscape/

QUESTION 12
A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook. Which two elements are part of the eradication phase for this incident? (Choose two.)

A. anti-malware software
B. data and workload isolation
C. centralized user management
D. intrusion prevention system
E. enterprise block listing solution

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

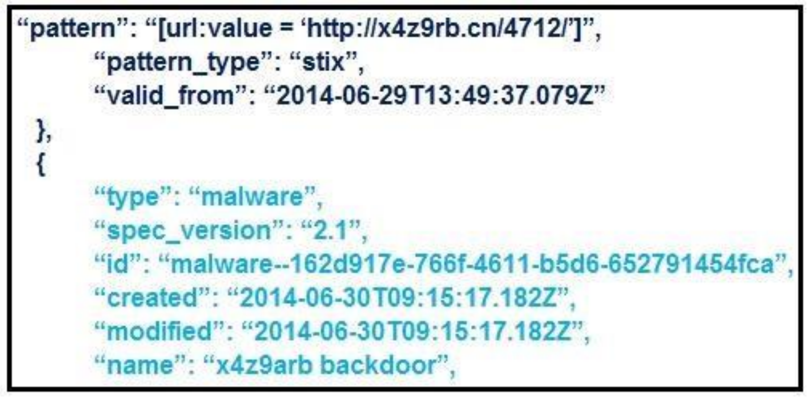
QUESTION 13 Which tool conducts memory analysis?

A. MemDump
B. Sysinternals Autoruns
C. Volatility
D. Memoryze

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://resources.infosecinstitute.com/topic/memory-forensics-and-analysis-using-volatility/

QUESTION 14



```
“pattern”: “[url:value = ‘http://x4z9rb.cn/4712/’]”,
        “pattern_type”: “stix”,
        “valid_from”: “2014-06-29T13:49:37.079Z”
  },
  {
        “type”: “malware”,
        “spec_version”: “2.1”,
        “id”: “malware--162d917e-766f-4611-b5d6-652791454fca”,
        “created”: “2014-06-30T09:15:17.182Z”,
        “modified”: “2014-06-30T09:15:17.182Z”,
        “name”: “x4z9arb backdoor”,
```

Refer to the exhibit. What is the IOC threat and URL in this STIX JSON snippet?

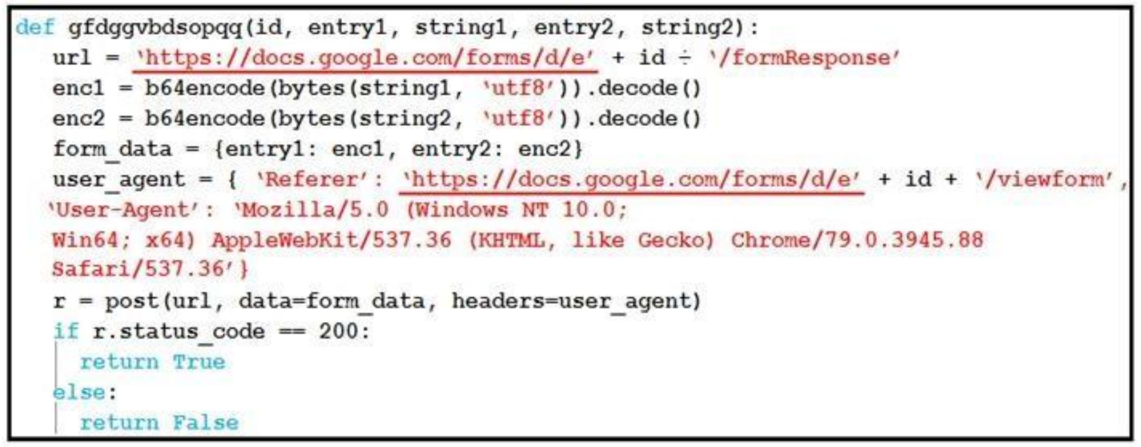
A. malware; ‘http://x4z9arb.cn/4712/’
B. malware; x4z9arb backdoor

C. x4z9arb backdoor; http://x4z9arb.cn/4712/
D. malware; malware--162d917e-766f-4611-b5d6-652791454fca
E. stix; ‘http://x4z9arb.cn/4712/’

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15



```
def gfdggvbdsopqq(id, entry1, string1, entry2, string2):
   url = 'https://docs.google.com/forms/d/e' + id ÷ '/formResponse'
   enc1 = b64encode(bytes(string1, 'utf8')).decode()
   enc2 = b64encode(bytes(string2, 'utf8')).decode()
   form_data = {entry1: enc1, entry2: enc2}
   user_agent = { 'Referer': 'https://docs.google.com/forms/d/e' + id + '/viewform',
  'User-Agent': 'Mozilla/5.0 (Windows NT 10.0;
   Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88
   Safari/537.36'}
   r = post(url, data=form_data, headers=user_agent)
   if r.status_code == 200:
     return True
   else:
     return False
```

Refer to the exhibit. Which type of code is being used?

A. Shell
B. VBScript
C. BASH
D. Python

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://scholar.google.co.in/scholar?q=disassembler+aids+performing+static+malware+analysis&hl=en&as_sdt=0&as_vis=1&oi=scholart

QUESTION 17
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.monitoring.doc/GUID-832A2618-6B11-4A28-9672-93296DA931D0.html

QUESTION 18
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. privilege escalation
B. internal user errors
C. malicious insider
D. external exfiltration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

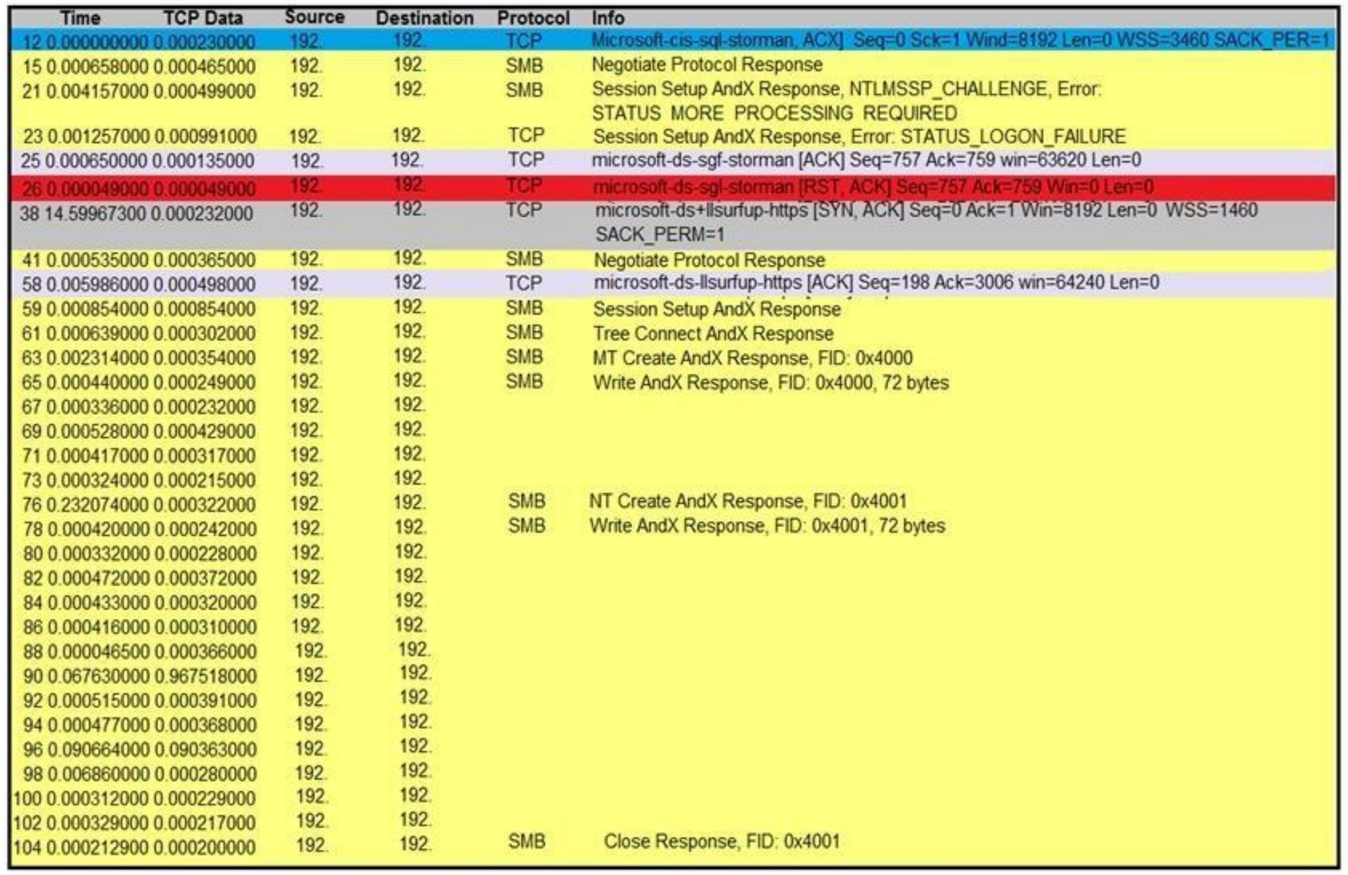
QUESTION 19
A website administrator has an output of an FTP session that runs nightly to download and unzip files to a local staging server. The download includes thousands of files, and the manual process used to find how many files failed to download is time-consuming. The administrator is working on a PowerShell script that will parse a log file and summarize how many files were successfully downloaded versus ones that failed. Which script will read the contents of the file one line at a time and return a collection of objects?

A. Get-Content-Folder \\Server\FTPFolder\Logfiles\ftpfiles.log | Show-From “ERROR”, “SUCCESS”
B. Get-Content –ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked “ERROR”, “SUCCESS”
C. Get-Content –Directory \\Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result “ERROR”, “SUCCESS”D. Get-Content –Path \\Server\FTPFolder\Logfiles\ftpfiles.log | Select-String “ERROR”, “SUCCESS”

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20



Time	TCP Data	Source	Destination	Protocol	Info
12 0.000000000	0.000230000	192.	192.	TCP	Microsoft-cis-sql-storman, ACX] 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

Refer to the exhibit. An engineer is analyzing a TCP stream in a 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 What is the goal of an incident response plan?

A. to identify critical systems and resources in an organization
B. to ensure systems are in place to prevent an attack
C. to determine security weaknesses and recommend solutions
D. to contain an attack and prevent it from spreading

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.forcepoint.com/cyber-edu/incident-response

QUESTION 22

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).

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

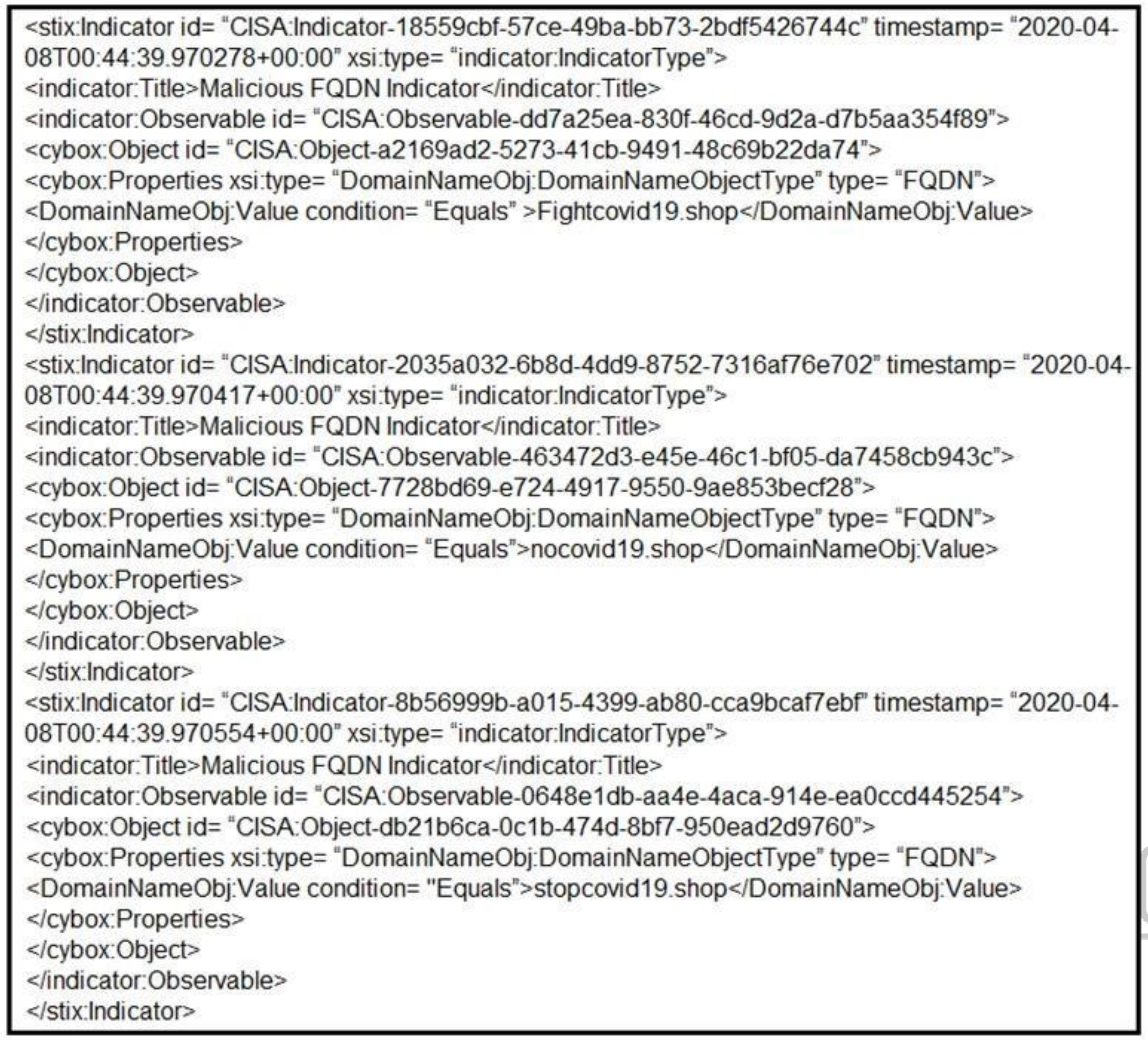
QUESTION 23
An employee receives an email from a “trusted” person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24



```
<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>
```

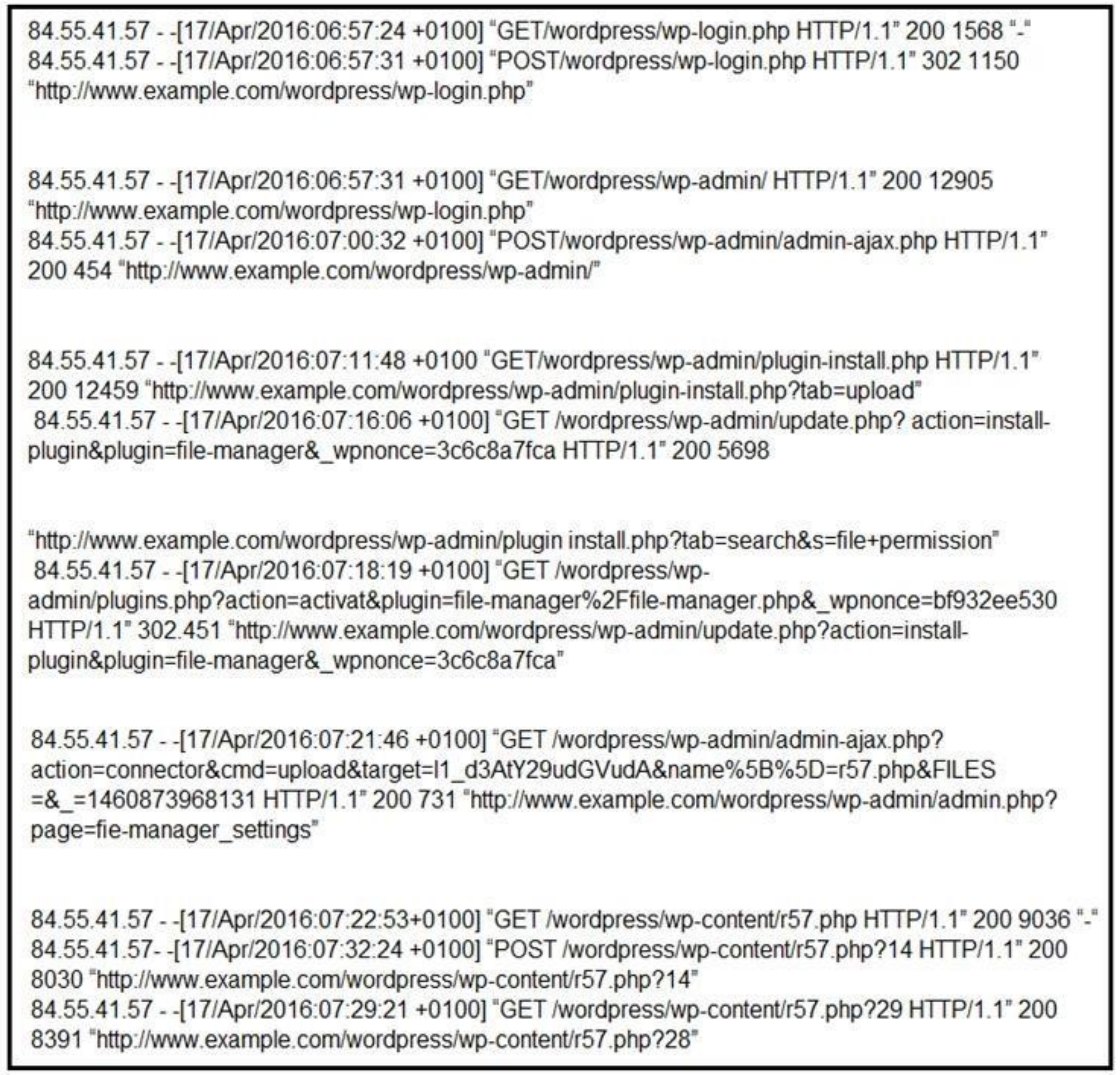
Refer to the exhibit. Which two actions should be taken based on the intelligence information? (Choose two.)

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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25



```
84.55.41.57 - -[17/Apr/2016:06:57:24 +0100] "GET/wordpress/wp-login.php HTTP/1.1" 200 1568 "-"
84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] "POST/wordpress/wp-login.php HTTP/1.1" 302 1150
"http://www.example.com/wordpress/wp-login.php"


84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] "GET/wordpress/wp-admin/ HTTP/1.1" 200 12905
"http://www.example.com/wordpress/wp-login.php"
84.55.41.57 - -[17/Apr/2016:07:00:32 +0100] "POST/wordpress/wp-admin/admin-ajax.php HTTP/1.1"
200 454 "http://www.example.com/wordpress/wp-admin/"


84.55.41.57 - -[17/Apr/2016:07:11:48 +0100 "GET/wordpress/wp-admin/plugin-install.php HTTP/1.1"
200 12459 "http://www.example.com/wordpress/wp-admin/plugin-install.php?tab=upload"
 84.55.41.57 - -[17/Apr/2016:07:16:06 +0100] "GET /wordpress/wp-admin/update.php? action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca HTTP/1.1" 200 5698


"http://www.example.com/wordpress/wp-admin/plugin install.php?tab=search&s=file+permission"
 84.55.41.57 - -[17/Apr/2016:07:18:19 +0100] "GET /wordpress/wp-
admin/plugins.php?action=activat&plugin=file-manager%2Ffile-manager.php&_wpnonce=bf932ee530
HTTP/1.1" 302.451 "http://www.example.com/wordpress/wp-admin/update.php?action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca"


84.55.41.57 - -[17/Apr/2016:07:21:46 +0100] "GET /wordpress/wp-admin/admin-ajax.php?
action=connector&cmd=upload&target=l1_d3AtY29udGVudA&name%5B%5D=r57.php&FILES
=&_=1460873968131 HTTP/1.1" 200 731 "http://www.example.com/wordpress/wp-admin/admin.php?
page=fie-manager_settings"


84.55.41.57 - -[17/Apr/2016:07:22:53+0100] "GET /wordpress/wp-content/r57.php HTTP/1.1" 200 9036 "-"
84.55.41.57- -[17/Apr/2016:07:32:24 +0100] "POST /wordpress/wp-content/r57.php?14 HTTP/1.1" 200
8030 "http://www.example.com/wordpress/wp-content/r57.php?14"
84.55.41.57 - -[17/Apr/2016:07:29:21 +0100] "GET /wordpress/wp-content/r57.php?29 HTTP/1.1" 200
8391 "http://www.example.com/wordpress/wp-content/r57.php?28"
```

Refer to the exhibit. Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

A. The attacker used r57 exploit to elevate their privilege.
B. The attacker uploaded the word press file manager trojan.
C. The attacker performed a brute force attack against word press and used sql injection against the backend database.
D. The attacker used the word press file manager plugin to upoad r57.php.
E. The attacker logged on normally to word press admin page.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
An attacker embedded a macro within a word processing file opened by a user in an organization’s legal department. The attacker used this technique to gain access to confidential financial data. Which two recommendations should a security expert make to mitigate this type of attack? (Choose two.)

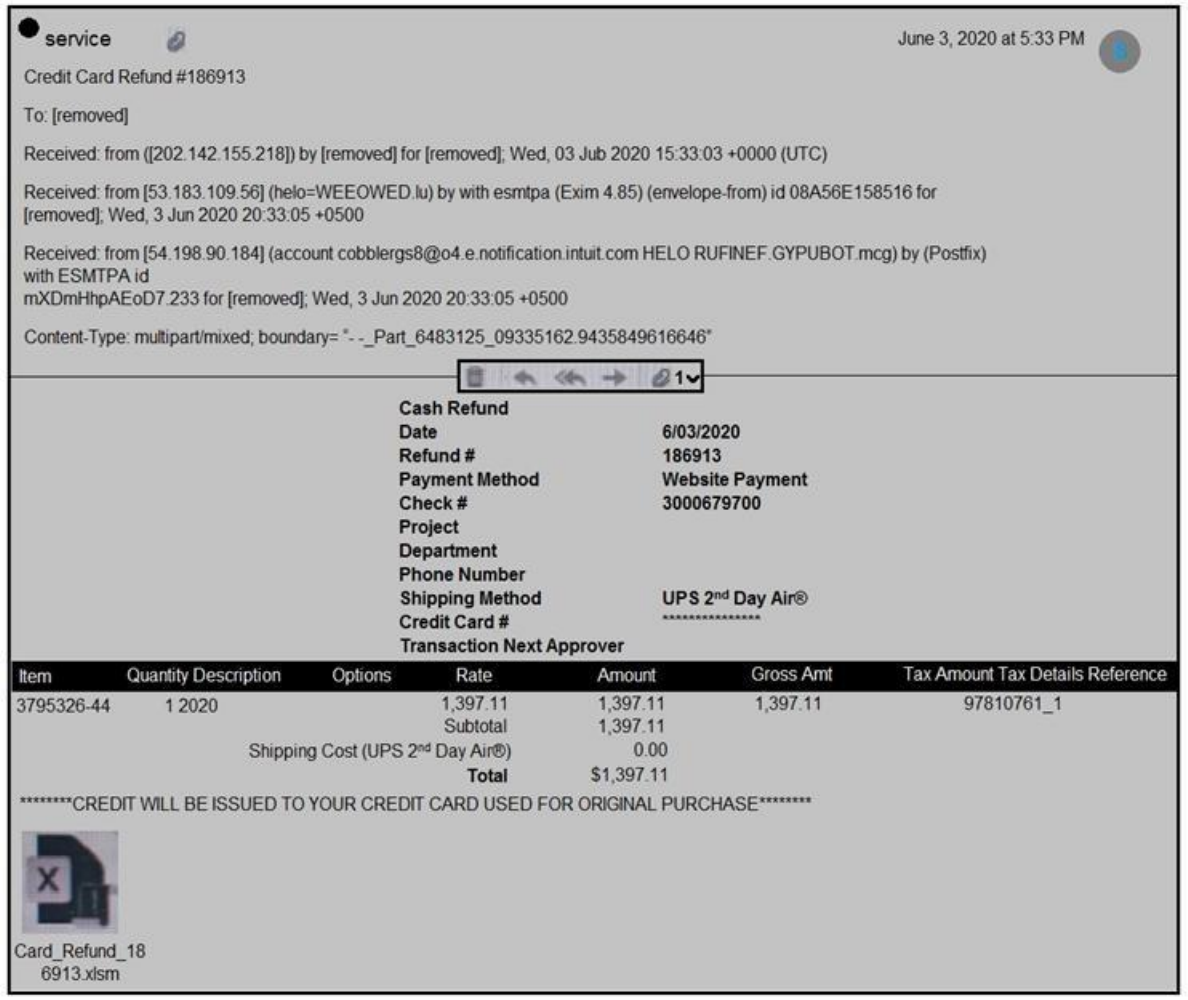
A. controlled folder access
B. removable device restrictions
C. signed macro requirements

D. firewall rules creation
E. network access control

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27



● service

June 3, 2020 at 5:33 PM

Credit Card Refund #186913

To: [removed]

Received: from ([202.142.155.218]) by [removed] for [removed]; Wed, 03 Jub 2020 15:33:03 +0000 (UTC)

Received: from [53.183.109.56] (helo=WEEOWED.lu) by with esmtpa (Exim 4.85) (envelope-from) id 08A56E158516 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Received: from [54.198.90.184] (account cobblergs8@o4.e.notification.intuit.com HELO RUFINEF.GYPUBOT.mcg) by (Postfix) with ESMTPA id mXDmHhpAEoD7.233 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Content-Type: multipart/mixed; boundary= "- -_Part_6483125_09335162.9435849616646"

Cash Refund

Date	**6/03/2020**
Refund #	**186913**
Payment Method	**Website Payment**
Check #	**3000679700**
Project	
Department	
Phone Number	
Shipping Method	**UPS 2nd Day Air®**
Credit Card #	***************
Transaction Next Approver	

Item	Quantity Description	Options	Rate	Amount	Gross Amt	Tax Amount Tax Details Reference
3795326-44	1 2020		1,397.11	1,397.11	1,397.11	97810761_1
			Subtotal	1,397.11		
			Shipping Cost (UPS 2nd Day Air®)	0.00		
			Total	$1,397.11		

********CREDIT WILL BE ISSUED TO YOUR CREDIT CARD USED FOR ORIGINAL PURCHASE********

Card_Refund_186913.xlsm

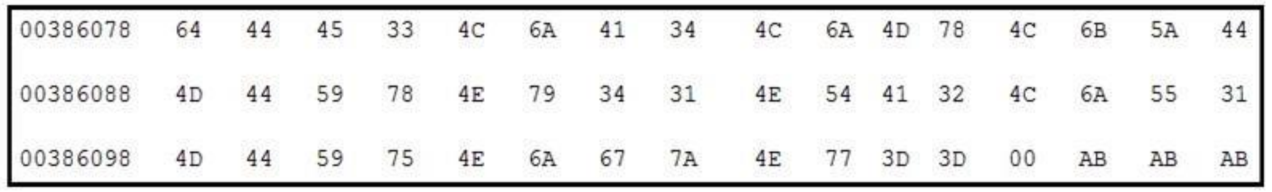
Refer to the exhibit. Which element in this email is an indicator of attack?

A. IP Address: 202.142.155.218
B. content-Type: multipart/mixed
C. attachment: “Card-Refund”
D. subject: “Service Credit Card”

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28



```
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
```

Refer to the exhibit. Which encoding technique is represented by this HEX string?

A. Unicode
B. Binary
C. Base64
D. Charcode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.suse.com/c/making-sense-hexdump/

QUESTION 29
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)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 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.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which information is provided bout the object file by the "-h" option in the objdump line command **objdump –b oasys –m vax –h fu.o**?

A. bfdname
B. debugging
C. help
D. headers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sourceware.org/binutils/docs/binutils/objdump.html

QUESTION 33
A threat actor attempts to avoid detection by turning data into a code that shifts numbers to the right four times. Which anti-forensics technique is being used?

A. encryption
B. tunneling
C. obfuscation
D. poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.vadesecure.com/en/malware-analysis-understanding-code-obfuscation-techniques/#:~:text=Obfuscation%20of%20character%20strings%20is,data%20when%20the%20code%20executes.

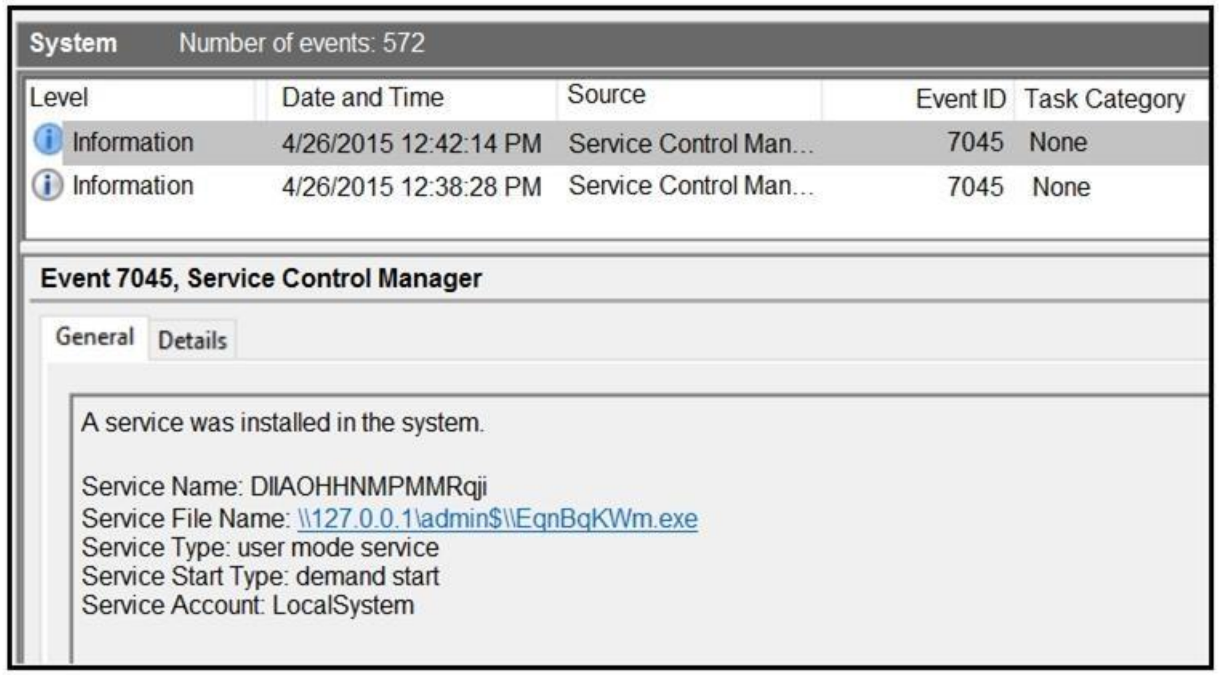
QUESTION 34
Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

A. process injection
B. privilege escalation
C. GPO modification
D. token manipulation

Correct Answer: A
Section: (none)

Explanation
Explanation/Reference:
Reference: https://attack.mitre.org/techniques/T1055/

QUESTION 35



System Number of events: 572

Level	Date and Time	Source	Event ID	Task Category
ⓘ Information	4/26/2015 12:42:14 PM	Service Control Man...	7045	None
ⓘ Information	4/26/2015 12:38:28 PM	Service Control Man...	7045	None

Event 7045, Service Control Manager

A service was installed in the system.

Service Name: DIIAOHHNMPMMRqji
Service File Name: \\127.0.0.1\admin$\\EqnBqKWm.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

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. privilege escalation
C. denial of service attack
D. compromised root access
E. malware outbreak

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 Which magic byte indicates that an analyzed file is a pdf file?

A. cGRmZmlsZQ
B. 706466666
C. 255044462d
D. 0a0ah4cg

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37

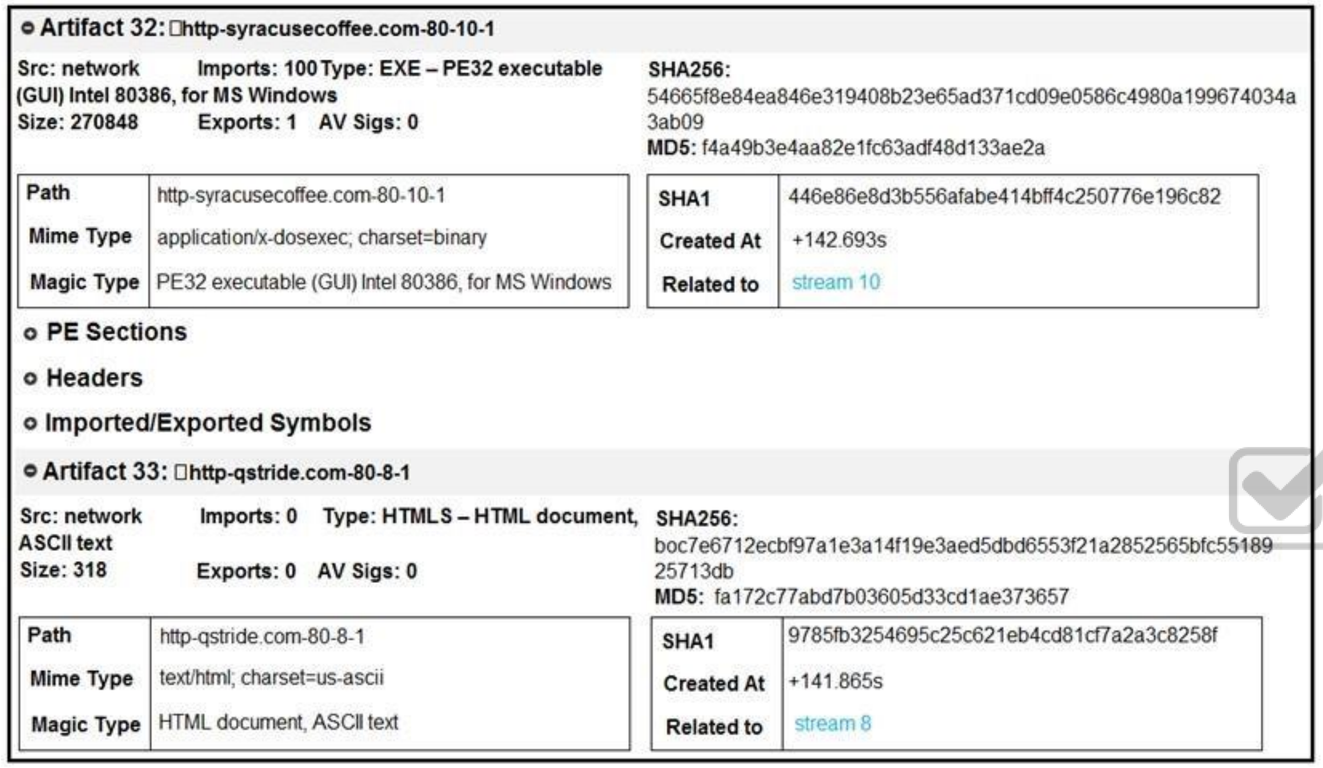
An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

A. An engineer should check the list of usernames currently logged in by running the command **$ who | cut –d' ' -f1| sort | uniq**
B. An engineer should check the server's processes by running commands **ps -aux** and **sudo ps -a**.
C. An engineer should check the services on the machine by running the command **service -status-all**.
D. An engineer should check the last hundred entries of a web server with the command **sudo tail -100 /var/log/apache2/access.log**.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38



Artifact 32: □http-syracusecoffee.com-80-10-1

Src: network Imports: 100 Type: EXE – PE32 executable (GUI) Intel 80386, for MS Windows
Size: 270848 Exports: 1 AV Sigs: 0

SHA256: 54665f8e84ea846e319408b23e65ad371cd09e0586c4980a199674034a3ab09
MD5: f4a49b3e4aa82e1fc63adf48d133ae2a

Path	http-syracusecoffee.com-80-10-1
Mime Type	application/x-dosexec; charset=binary
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows

SHA1	446e86e8d3b556afabe414bff4c250776e196c82
Created At	+142.693s
Related to	stream 10

- PE Sections
- Headers
- Imported/Exported Symbols

Artifact 33: □http-qstride.com-80-8-1

Src: network Imports: 0 Type: HTMLS – HTML document, ASCII text
Size: 318 Exports: 0 AV Sigs: 0

SHA256: boc7e6712ecbf97a1e3a14f19e3aed5dbd6553f21a2852565bfc5518925713db
MD5: fa172c77abd7b03605d33cd1ae373657

Path	http-qstride.com-80-8-1
Mime Type	text/html; charset=us-ascii
Magic Type	HTML document, ASCII text

SHA1	9785fb3254695c25c621eb4cd81cf7a2a3c8258f
Created At	+141.865s
Related to	stream 8

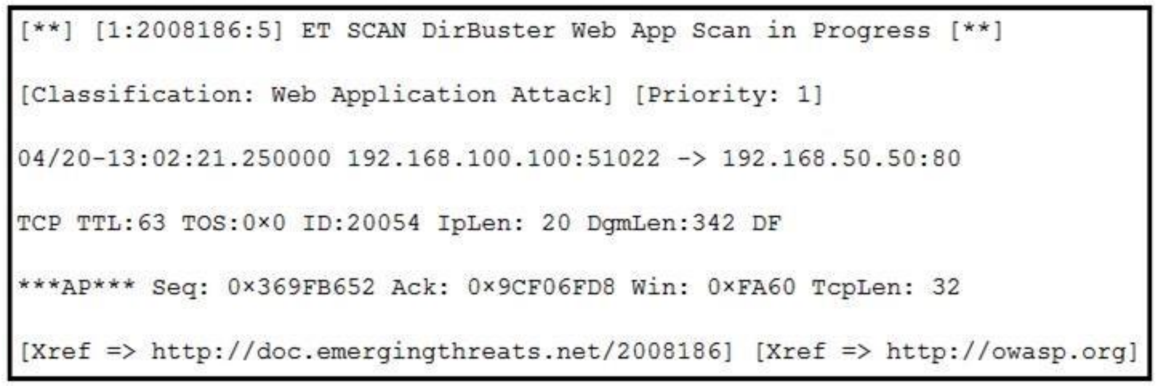
Refer to the exhibit. What do these artifacts indicate?

A. An executable file is requesting an application download.
B. A malicious file is redirecting users to different domains.
C. The MD5 of a file is identified as a virus and is being blocked.
D. A forged DNS request is forwarding users to malicious websites.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39



```
[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]

[Classification: Web Application Attack] [Priority: 1]

04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80

TCP TTL:63 TOS:0×0 ID:20054 IpLen: 20 DgmLen:342 DF

***AP*** Seq: 0×369FB652 Ack: 0×9CF06FD8 Win: 0×FA60 TcpLen: 32

[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```

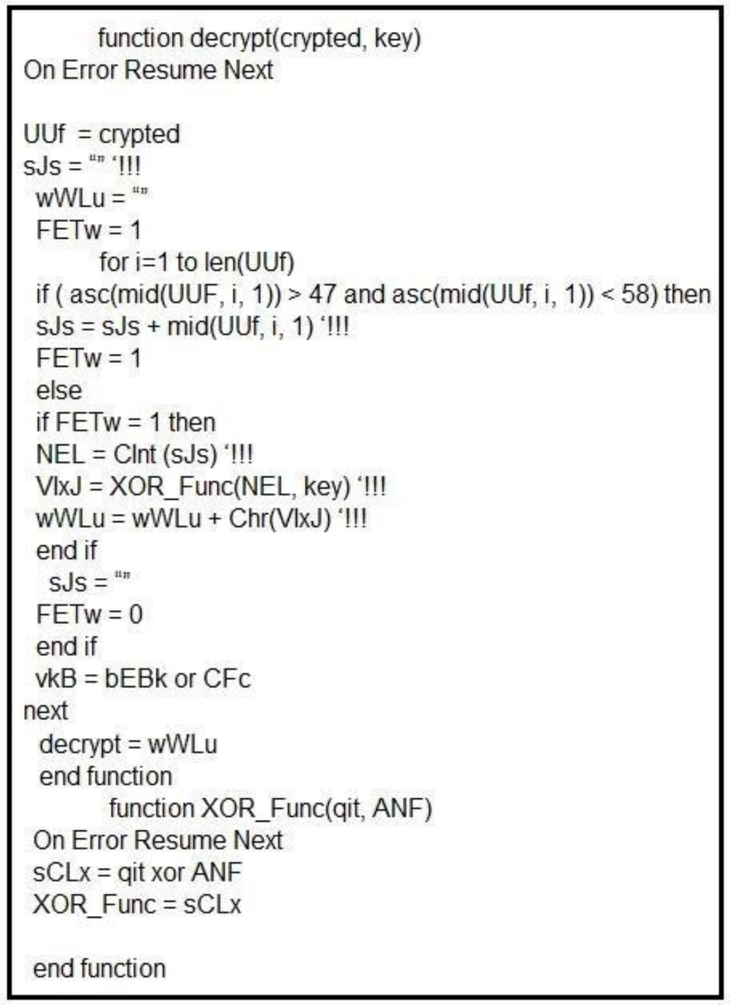
Refer to the exhibit. According to the SNORT alert, what is the attacker performing?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40



```
          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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
DRAG DROP

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

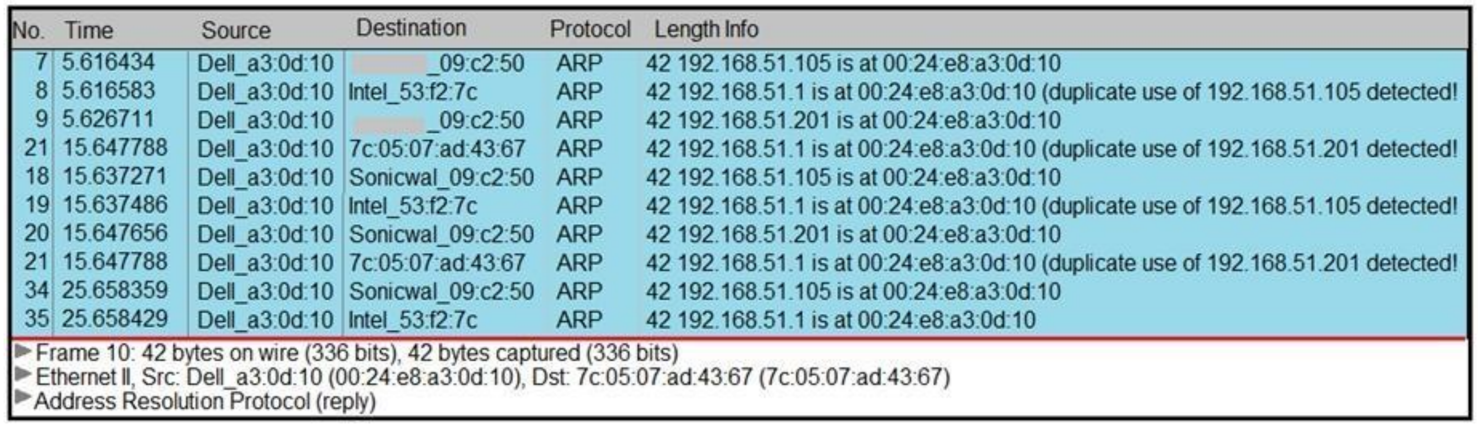
Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 42



No.	Time	Source	Destination	Protocol	Length	Info
7	5.616434	Dell_a3:0d:10	[redacted]_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	[redacted]_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)

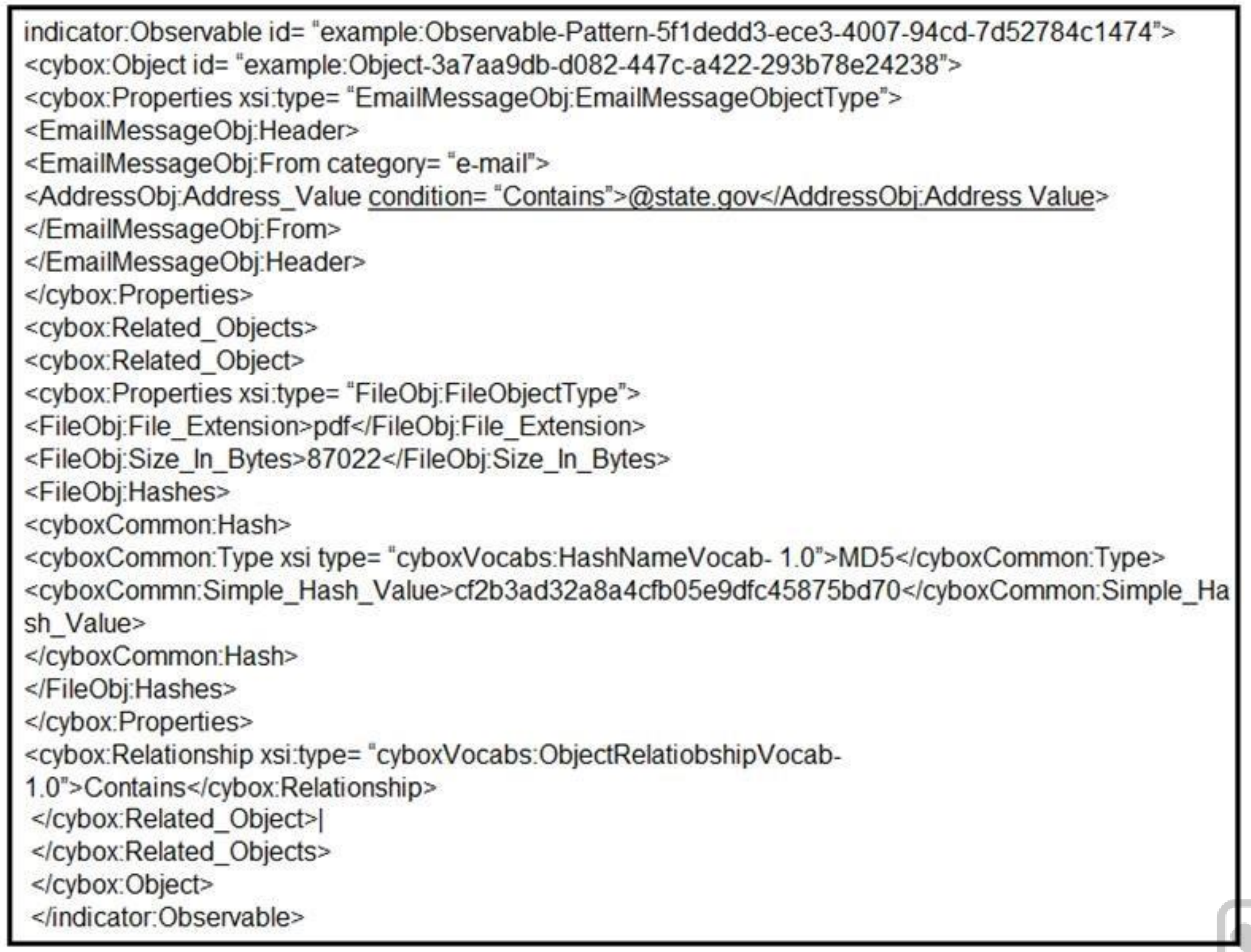
Refer to the exhibit. A security analyst notices unusual connections while monitoring traffic. What is the attack vector, and which action should be taken to prevent this type of event?

A. DNS spoofing; encrypt communication protocols
B. SYN flooding, block malicious packets
C. ARP spoofing; configure port security
D. MAC flooding; assign static entries

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43



```
indicator:Observable id= "example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
<cybox:Object id= "example:Object-3a7aa9db-d082-447c-a422-293b78e24238">
<cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
<EmailMessageObj:Header>
<EmailMessageObj:From category= "e-mail">
<AddressObj:Address_Value condition= "Contains">@state.gov</AddressObj:Address_Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= "FileObj:FileObjectType">
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi type= "cyboxVocabs:HashNameVocab- 1.0">MD5</cyboxCommon:Type>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelatiobshipVocab-
1.0">Contains</cybox:Relationship>
 </cybox:Related_Object>|
 </cybox:Related_Objects>
 </cybox:Object>
 </indicator:Observable>
```

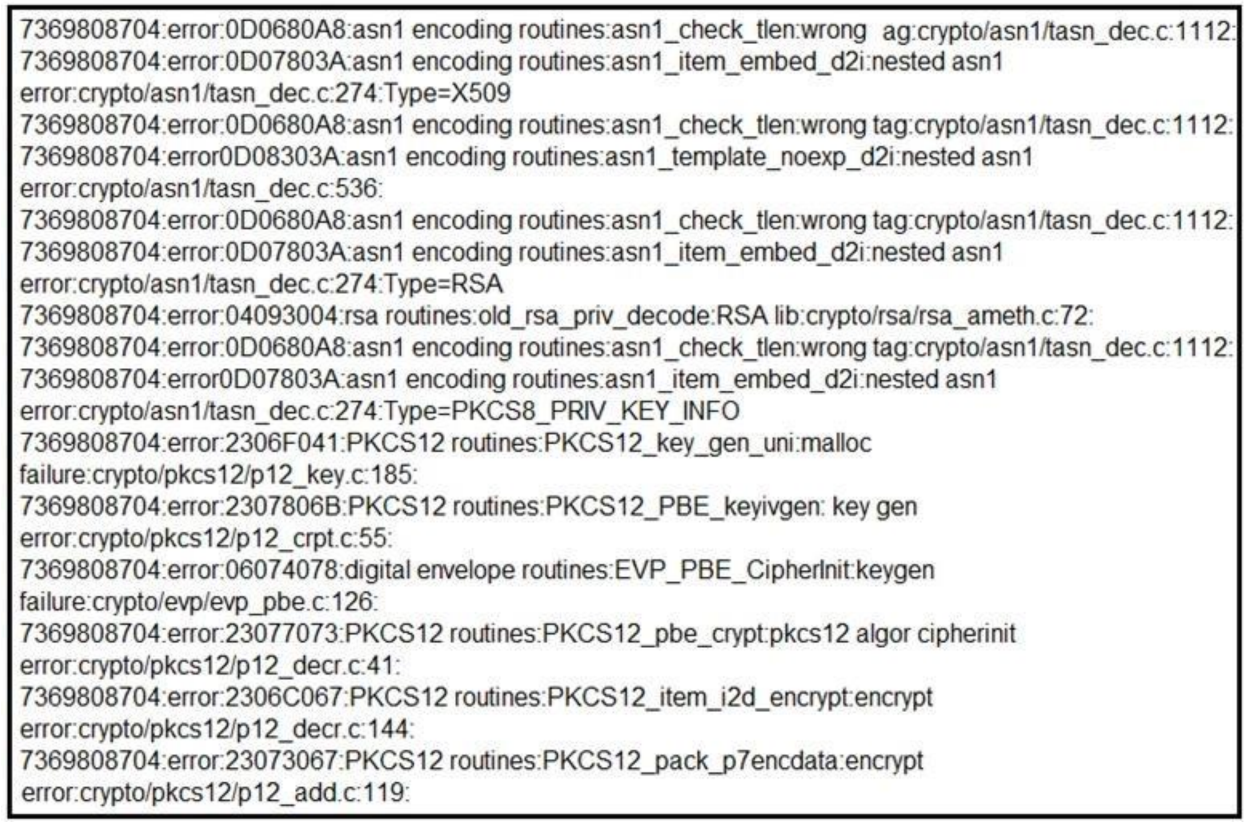
Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

A. Update the AV to block any file with hash “cf2b3ad32a8a4cfb05e9dfc45875bd70”.
B. Block all emails sent from an @state.gov address.
C. Block all emails with pdf attachments.
D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash “cf2b3ad32a8a4cfb05e9dfc45875bd70”.
E. Block all emails with subject containing “cf2b3ad32a8a4cfb05e9dfc45875bd70”.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44



```
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong  ag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=X509
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error0D08303A:asn1 encoding routines:asn1_template_noexp_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:536:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=RSA
7369808704:error:04093004:rsa routines:old_rsa_priv_decode:RSA lib:crypto/rsa/rsa_ameth.c:72:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=PKCS8_PRIV_KEY_INFO
7369808704:error:2306F041:PKCS12 routines:PKCS12_key_gen_uni:malloc
failure:crypto/pkcs12/p12_key.c:185:
7369808704:error:2307806B:PKCS12 routines:PKCS12_PBE_keyivgen: key gen
error:crypto/pkcs12/p12_crpt.c:55:
7369808704:error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen
failure:crypto/evp/evp_pbe.c:126:
7369808704:error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit
error:crypto/pkcs12/p12_decr.c:41:
7369808704:error:2306C067:PKCS12 routines:PKCS12_item_i2d_encrypt:encrypt
error:crypto/pkcs12/p12_decr.c:144:
7369808704:error:23073067:PKCS12 routines:PKCS12_pack_p7encdata:encrypt
error:crypto/pkcs12/p12_add.c:119:
```

Refer to the exhibit. What should be determined from this Apache log?

A. A module named mod_ssl is needed to make SSL connections.
B. The private key does not match with the SSL certificate.
C. The certificate file has been maliciously modified
D. The SSL traffic setup is improper

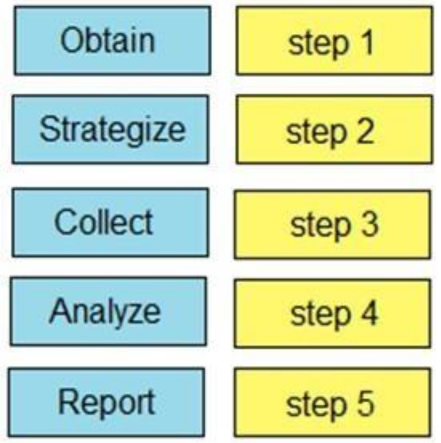
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
DRAG DROP

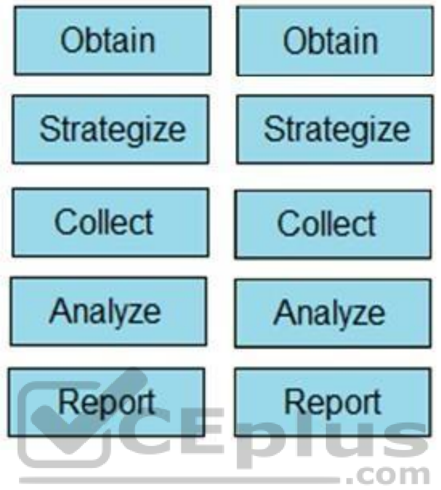
Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

Select and Place:



Obtain	step 1
Strategize	step 2
Collect	step 3
Analyze	step 4
Report	step 5

Correct Answer:



Obtain	Obtain
Strategize	Strategize
Collect	Collect
Analyze	Analyze
Report	Report

Section: (none)
Explanation

Explanation/Reference:
Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lvl1sec12/network-forensics-investigation-methodology

QUESTION 46 Which tool is used for reverse engineering malware?

A. Ghidra
B. SNORT
C. Wireshark
D. NMAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.nsa.gov/resources/everyone/ghidra/#:~:text=Ghidra%20is%20a%20software%20reverse,in%20their%20networks%20and%20systems.

QUESTION 47
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. email security appliance
B. DNS server

C. Antivirus solution
D. network device

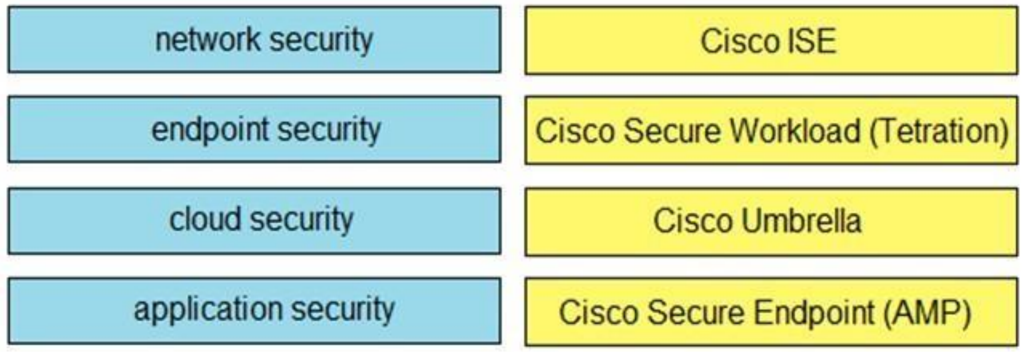
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
DRAG DROP

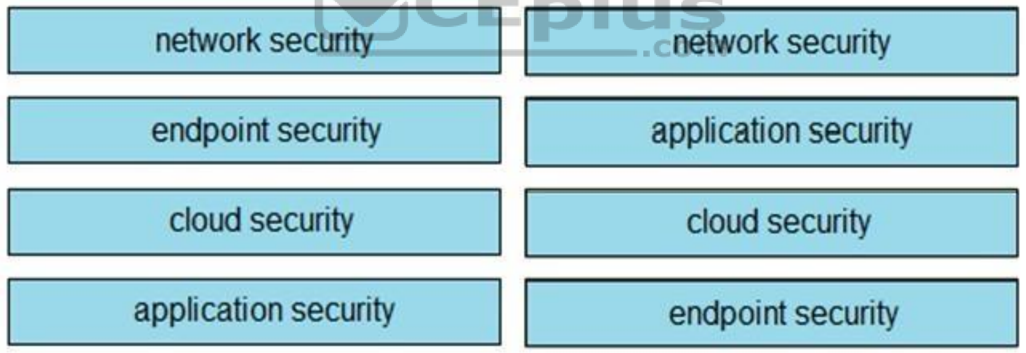
Drag and drop the capabilities on the left onto the Cisco security solutions on the right.

Select and Place:



network security	Cisco ISE
endpoint security	Cisco Secure Workload (Tetration)
cloud security	Cisco Umbrella
application security	Cisco Secure Endpoint (AMP)

Correct Answer:



network security	network security
endpoint security	application security
cloud security	cloud security
application security	endpoint security

Section: (none)
Explanation

Explanation/Reference:

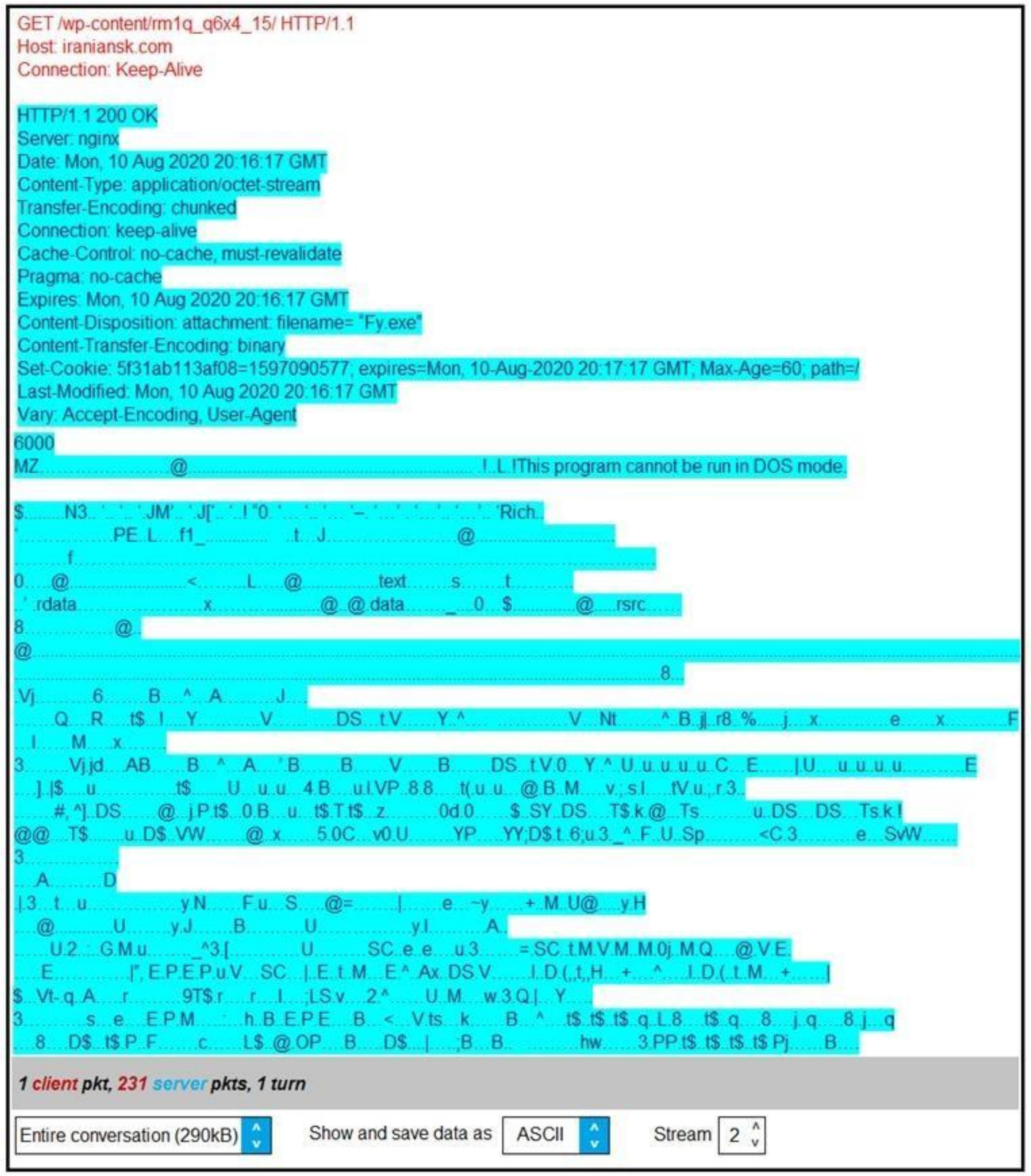
QUESTION 49
What are YARA rules based upon?

A. binary patterns
B. HTML code
C. network artifacts
D. IP addresses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/YARA#:~:text=YARA%20is%20the%20name%20of,strings%20and%20a%20boolean%20expression.

QUESTION 50



```
GET /wp-content/rm1q_q6x4_15/ HTTP/1.1
Host: iraniansk.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 10 Aug 2020 20:16:17 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 10 Aug 2020 20:16:17 GMT
Content-Disposition: attachment; filename= "Fy.exe"
Content-Transfer-Encoding: binary
Set-Cookie: 5f31ab113af08=1597090577; expires=Mon, 10-Aug-2020 20:17:17 GMT; Max-Age=60; path=/
Last-Modified: Mon, 10 Aug 2020 20:16:17 GMT
Vary: Accept-Encoding, User-Agent
6000
MZ......................@..................................................!..L.!This program cannot be run in DOS mode.

$.......N3..'..'..'.JM'..'.J['..'.!."0.'....'...'....'–.'.....'...'...'...'..'Rich..
'..................PE..L....f1_............t...J.........................@.....................
.........f................................................................................
0.....@......................<.........L.....@..............text........s.........t.............
..'..rdata..........................x...........................@..@.data........_....0....$...........@.....rsrc.......
8...............@..
@.........................................................................................................................
.............................................................................................8...
.Vj.........6.........B.....^....A..........J....
........Q.....R.....t$...l....Y............V............DS....t.V.......Y..^..................V....Nt.........^..B..jj..r8...%.......j....x..............e........x.............F
...I.......M.....x...........
3.........Vj.jd....AB.......B....^....A.....'B..........B.........V.........B.........DS...t.V.0....Y..^..U..u..u..u..u..C.....E.........|.U.....u..u..u..u...............E
.....]..|$......u.......................t$..........U.....u..u.....4.B.....u.I.VP..8.8.......t(.u..u.....@.B..M.......v.;.s.I.......tV.u.,.r.3..
..........#,.^].DS..........@....j.P.t$....0.B.....u.....t$.T.t$...z...........0d.0.........$..SY..DS.......T$.k.@....Ts.............u..DS.....DS.....Ts.k.!
@@.....T$.........u..D$..VW..........@..x.........5.0C.....v0.U............YP.......YY;D$.t..6;u.3._^..F..U..Sp............<C.3............e.....SvW........
3....................
.....A...........D
.|.3....t....u..........................y.N.........F.u.....S.......@=............|...........e.....~y..........+..M..U@......y.H
.....@..............U.........y.J..........B.............U.........................y.I.............A...
.........U.2...:..G.M.u..........._^3.[..................U...............SC..e..e.......u.3.........=.SC..t.M.V.M..M.0j..M.Q......@.V.E.
.......E.......................|",.E.P.E.P.u.V.....SC.....|..E..t..M.....E.^..Ax..DS.V...........I..D.(.,t,.H......+........^........I..D.(..t.M.......+..........|
$....Vt-.q..A.......r...............9T$.r.........r.......I........;LS.v......2.^.............U..M.......w.3.Q.|.......Y.......
3.....................s.....e.......E.P.M..............h..B..E.P.E.......B.....<.......V.ts.....k.............B.......^.......t$..t$..t$..q..L.8.......t$..q........8.......j..q.........8..j.....q
.......8......D$...t$.P..F............c.............L$..@.OP........B.........D$.....|........;B.....B...........................hw...........3.PP.t$..t$...t$..t$.Pj..........B......
```

1 client pkt, 231 server pkts, 1 turn

Entire conversation (290kB) Show and save data as ASCII Stream 2

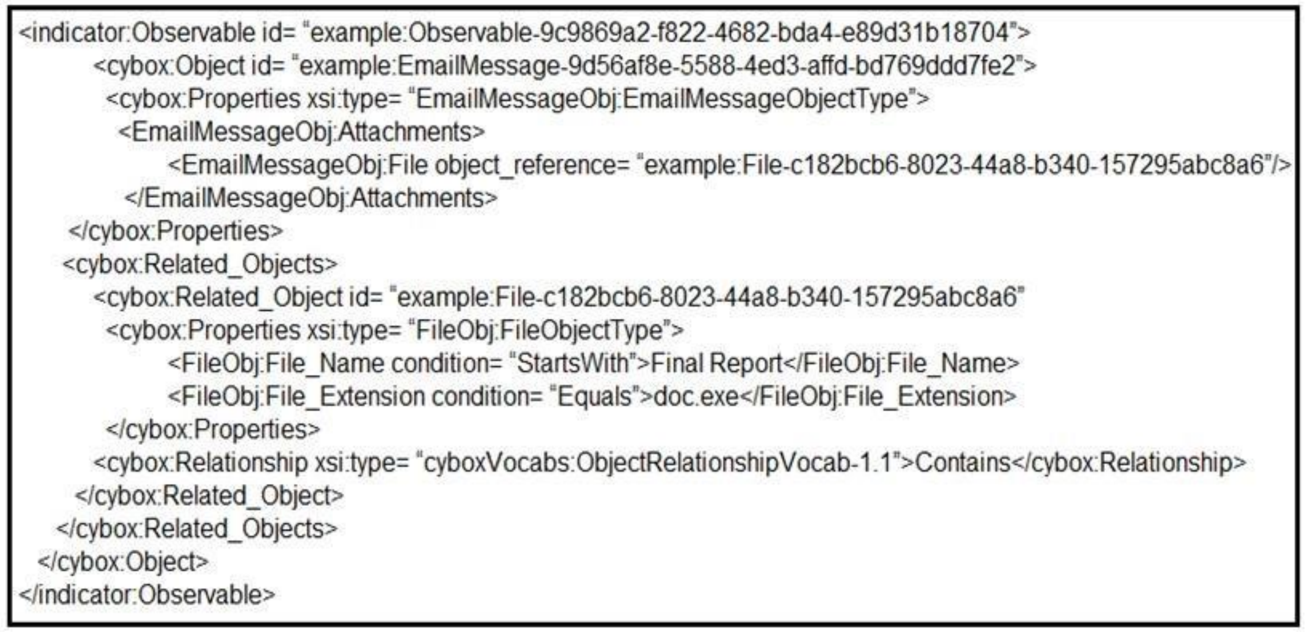
Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name:iraniansk.com
B. Server: nginx
C. Hash value: 5f31ab113af08=1597090577
D. filename= "Fy.exe"
E. Content-Type: application/octet-stream

Correct Answer: CE
Section: (none)

Explanation
Explanation/Reference:

QUESTION 51



```
<indicator:Observable id= "example:Observable-9c9869a2-f822-4682-bda4-e89d31b18704">
        <cybox:Object id= "example:EmailMessage-9d56af8e-5588-4ed3-affd-bd769ddd7fe2">
         <cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
          <EmailMessageObj:Attachments>
               <EmailMessageObj:File object_reference= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"/>
           </EmailMessageObj:Attachments>
     </cybox:Properties>
    <cybox:Related_Objects>
        <cybox:Related_Object id= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"
         <cybox:Properties xsi:type= "FileObj:FileObjectType">
               <FileObj:File_Name condition= "StartsWith">Final Report</FileObj:File_Name>
               <FileObj:File_Extension condition= "Equals">doc.exe</FileObj:File_Extension>
         </cybox:Properties>
        <cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelationshipVocab-1.1">Contains</cybox:Relationship>
      </cybox:Related_Object>
    </cybox:Related_Objects>
  </cybox:Object>
</indicator:Observable>
```

Refer to the exhibit. Which determination should be made by a security analyst?

A. An email was sent with an attachment named “Grades.doc.exe”.
B. An email was sent with an attachment named “Grades.doc”.
C. An email was sent with an attachment named “Final Report.doc”.
D. An email was sent with an attachment named “Final Report.doc.exe”.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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. verify the breadth of the attack
B. collect logs
C. request packet capture
D. remove vulnerabilities
E. scan hosts with updated signatures

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/window-event-log

QUESTION 54
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. Monitor processes as this a standard behavior of Word macro embedded documents.
C. Contain the threat for further analysis as this is an indication of suspicious activity.
D. Investigate the sender of the email and communicate with the employee to determine the motives.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
An engineer is analyzing a ticket for an unexpected server shutdown and discovers that the web-server ran out of useable memory and crashed.

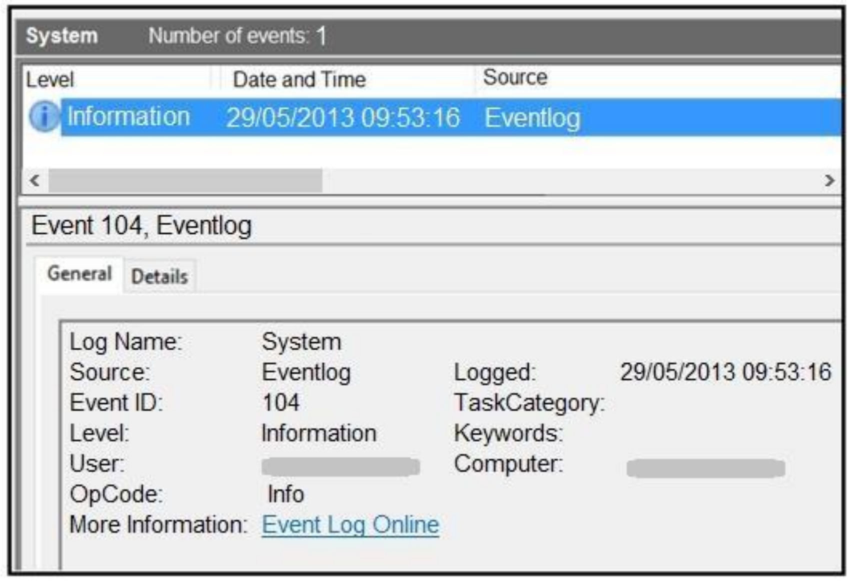
Which data is needed for further investigation?

A. /var/log/access.log
B. /var/log/messages.log
C. /var/log/httpd/messages.log
D. /var/log/httpd/access.log

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56



```
System    Number of events: 1
Level          Date and Time          Source
Information    29/05/2013 09:53:16    Eventlog

Event 104, Eventlog
General  Details

Log Name:          System
Source:            Eventlog          Logged:         29/05/2013 09:53:16
Event ID:          104               TaskCategory:
Level:             Information       Keywords:
User:              [redacted]        Computer:       [redacted]
OpCode:            Info
More Information:  Event Log Online
```

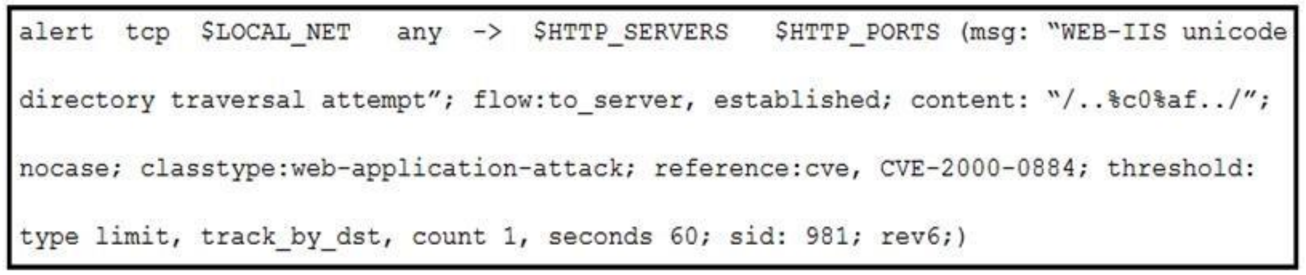
Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

A. data obfuscation
B. reconnaissance attack
C. brute-force attack
D. log tampering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57



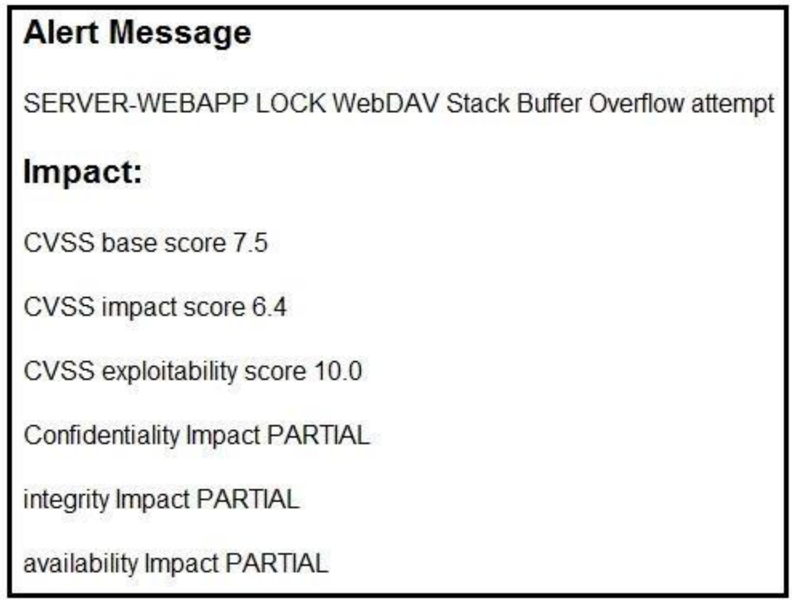
```
alert  tcp  $LOCAL_NET   any  ->  $HTTP_SERVERS   $HTTP_PORTS (msg: "WEB-IIS unicode

directory traversal attempt"; flow:to_server, established; content: "/..%c0%af../";

nocase; classtype:web-application-attack; reference:cve, CVE-2000-0884; threshold:

type limit, track_by_dst, count 1, seconds 60; sid: 981; rev6;)
```

Refer to the exhibit. A company that uses only the Unix platform implemented an intrusion detection system. After the initial configuration, the number of alerts is overwhelming, and an engineer needs to analyze and classify the alerts. The highest number of alerts were generated from the signature shown in the exhibit. Which classification should the engineer assign to this event?

A. True Negative alert
B. False Negative alert
C. False Positive alert
D. True Positive alert

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 58



Alert Message

SERVER-WEBAPP LOCK WebDAV Stack Buffer Overflow attempt

Impact:

CVSS base score 7.5

CVSS impact score 6.4

CVSS exploitability score 10.0

Confidentiality Impact PARTIAL

integrity Impact PARTIAL

availability Impact PARTIAL

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. encapsulation
B. NOP sled technique
C. address space randomization
D. heap-based security
E. data execution prevention

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: