300-215 Q&As

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Pass Cisco 300-215 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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.

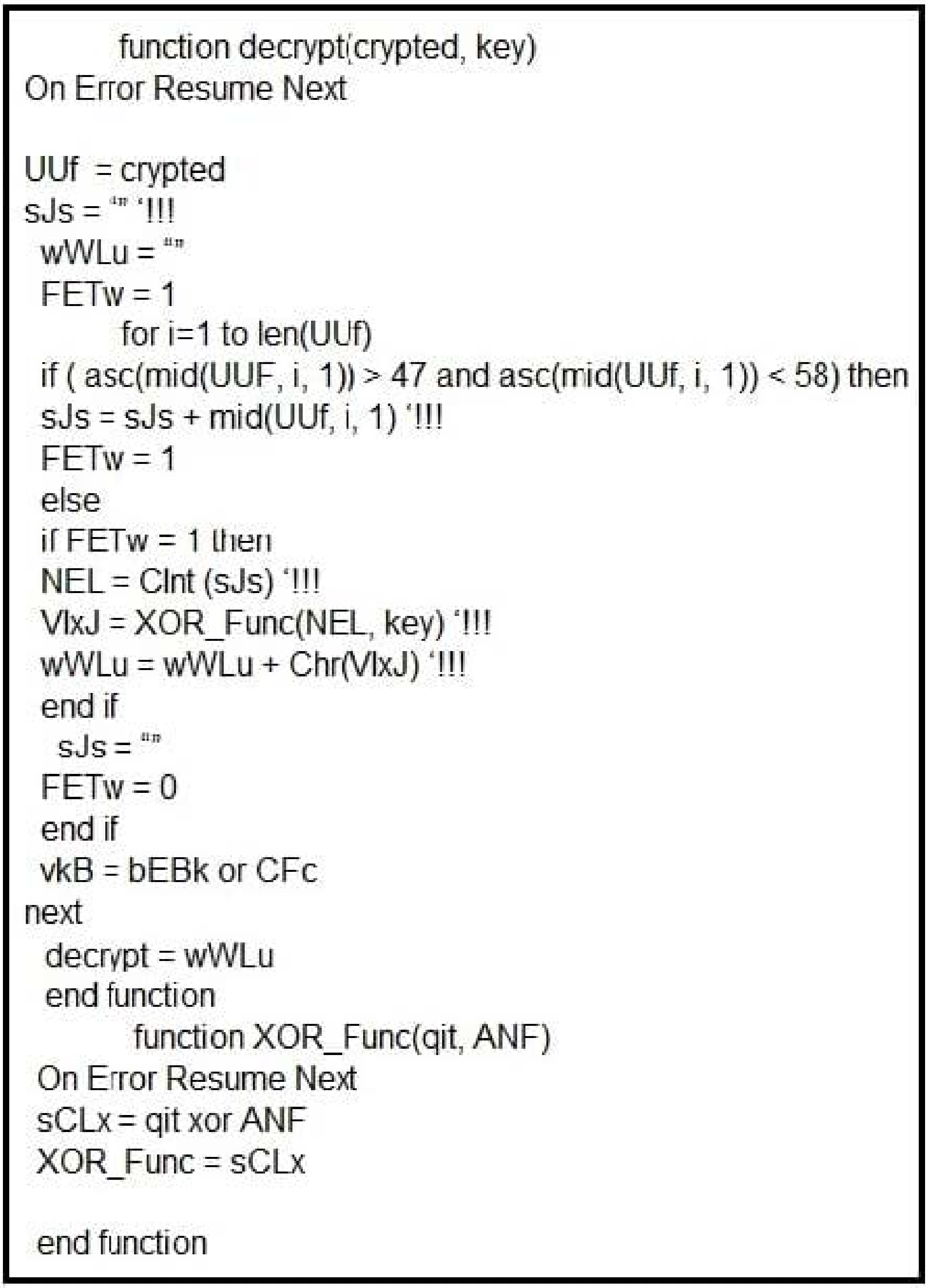
C. Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.

D. Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

Correct Answer: D

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

QUESTION 2



```
        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

QUESTION 3

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

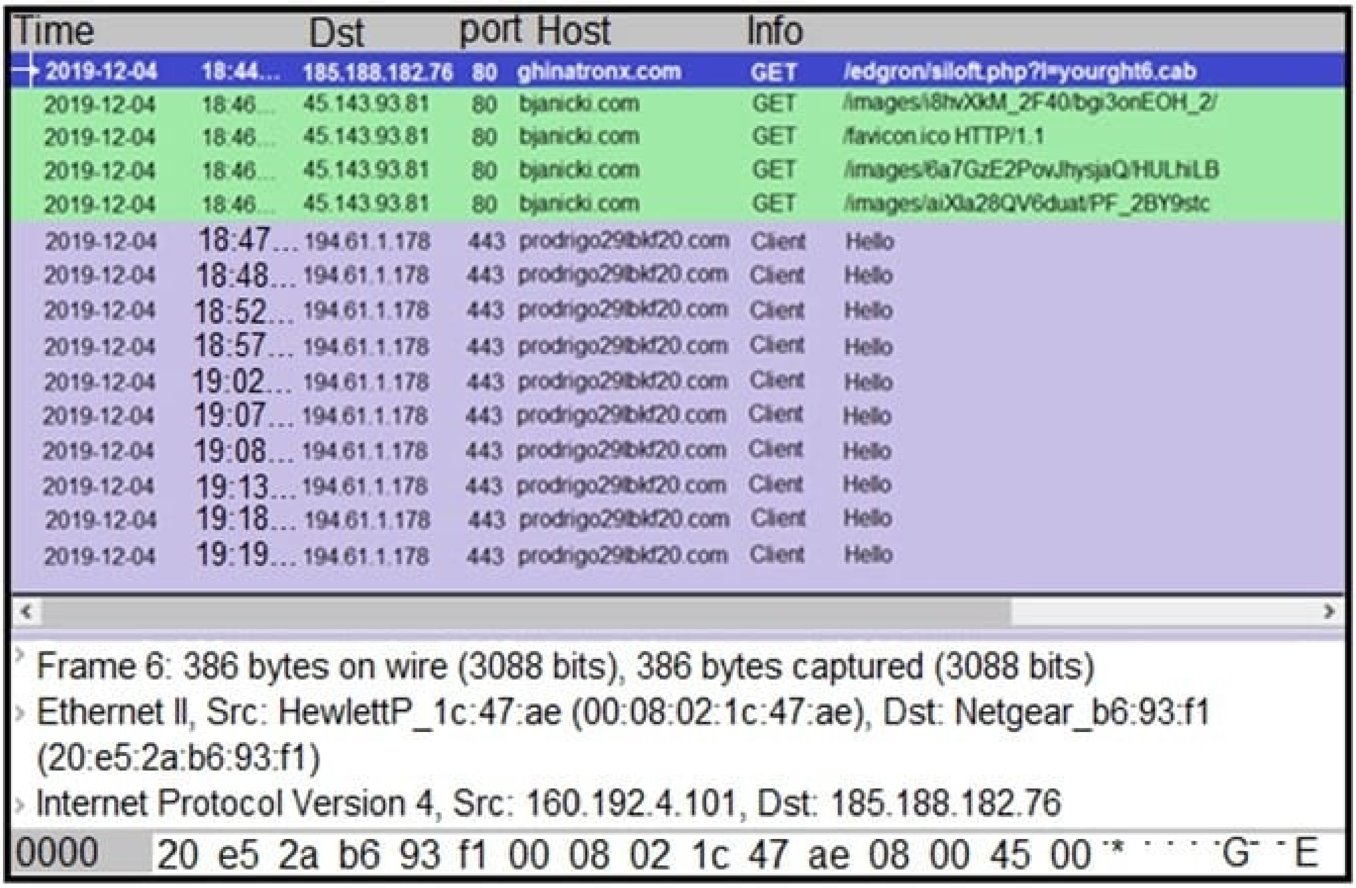
C. HKEY_CURRENT_USER\Software\Classes\Winlog

D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser

Correct Answer: A

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

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/6a7GzE2PowJhysjaQ/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

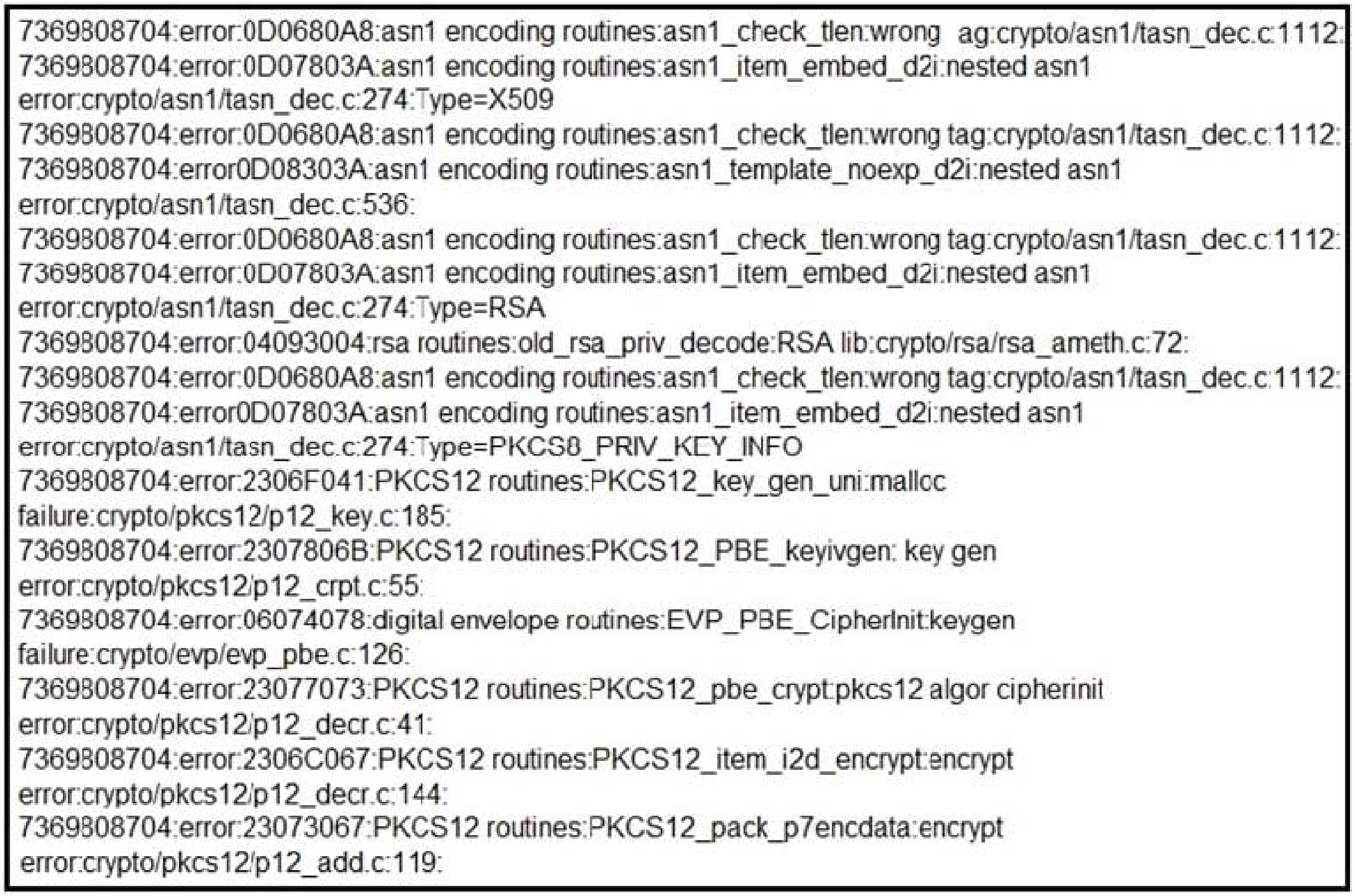
Correct Answer: B

Reference:

https://www.malware-traffic-analysis.net/2018/11/08/index.html

https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/

QUESTION 5



```
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.

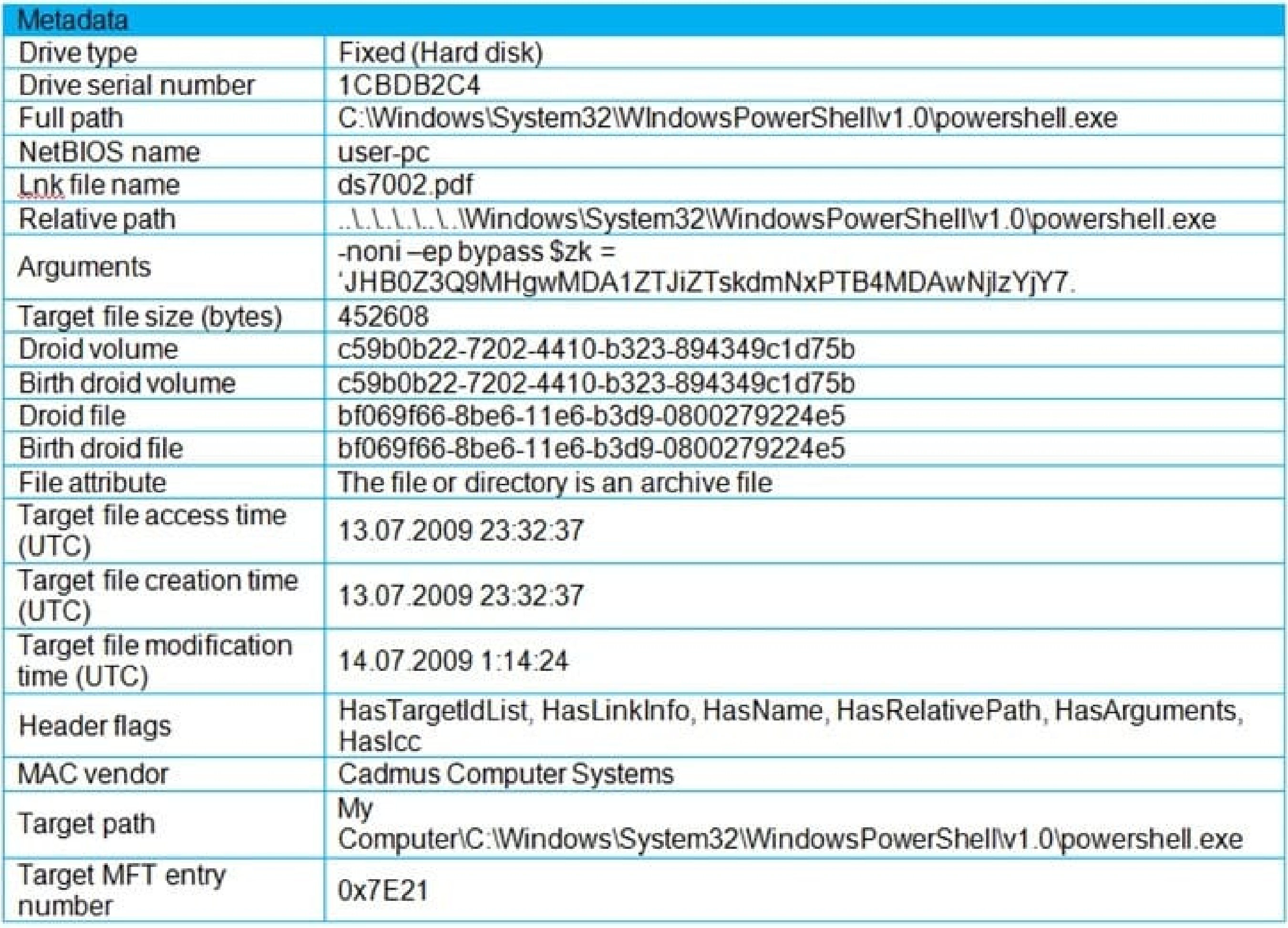
B. The private key does not match with the SSL certificate.

C. The certificate file has been maliciously modified

D. The SSL traffic setup is improper

Correct Answer: D

QUESTION 6



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.

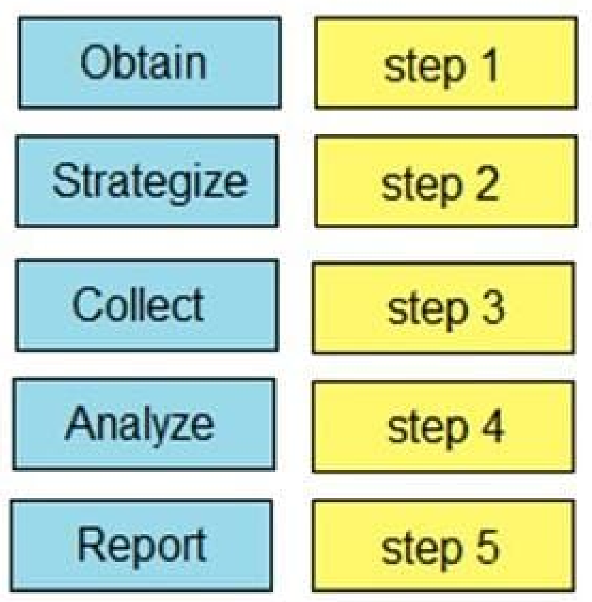
Correct Answer: D

QUESTION 7

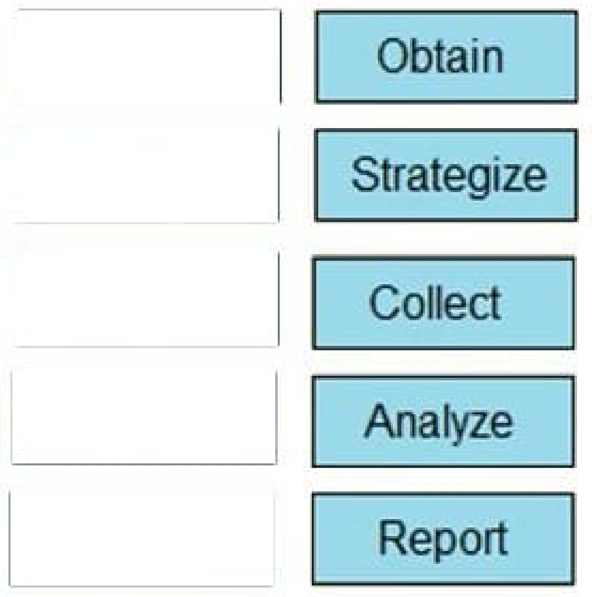
DRAG DROP

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

Select and Place:



Correct Answer:



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

QUESTION 8

Which tool is used for reverse engineering malware?

A. Ghidra

B. SNORT

C. Wireshark

D. NMAP

Correct Answer: A

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

QUESTION 9

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

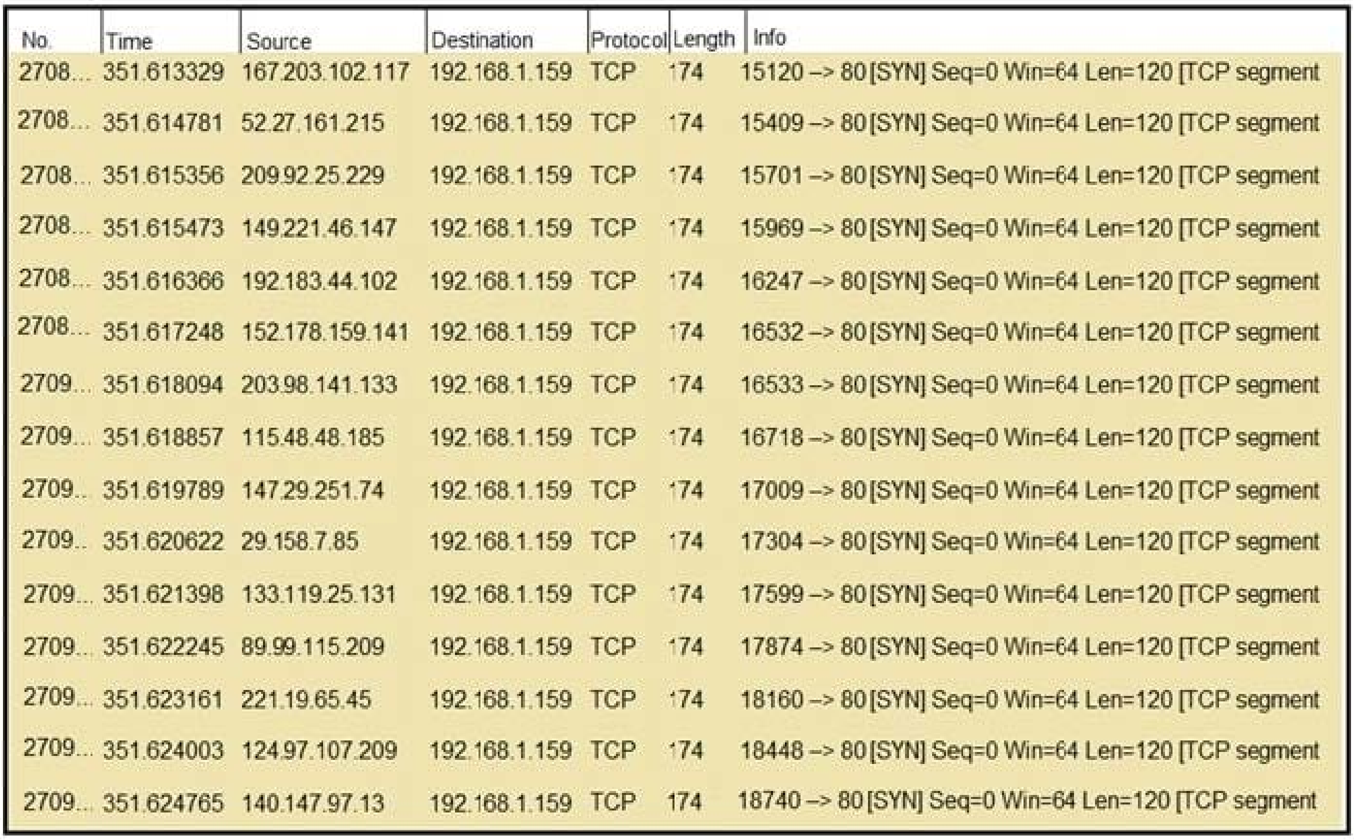
B. cause and effect

C. risk and RPN

D. motive and factors

Correct Answer: D

QUESTION 10



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