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.pass4itsure.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

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)
```

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. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 2

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

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

QUESTION 3

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

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

QUESTION 4

What are YARA rules based upon?

A. binary patterns

B. HTML code

C. network artifacts

D. IP addresses

Correct Answer: A

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

QUESTION 5

Which tool conducts memory analysis?

A. MemDump

B. Sysinternals Autoruns

C. Volatility

D. Memoryze

Correct Answer: C

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