300-215 Q&As

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

QUESTION 1

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

QUESTION 2

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

QUESTION 3

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).

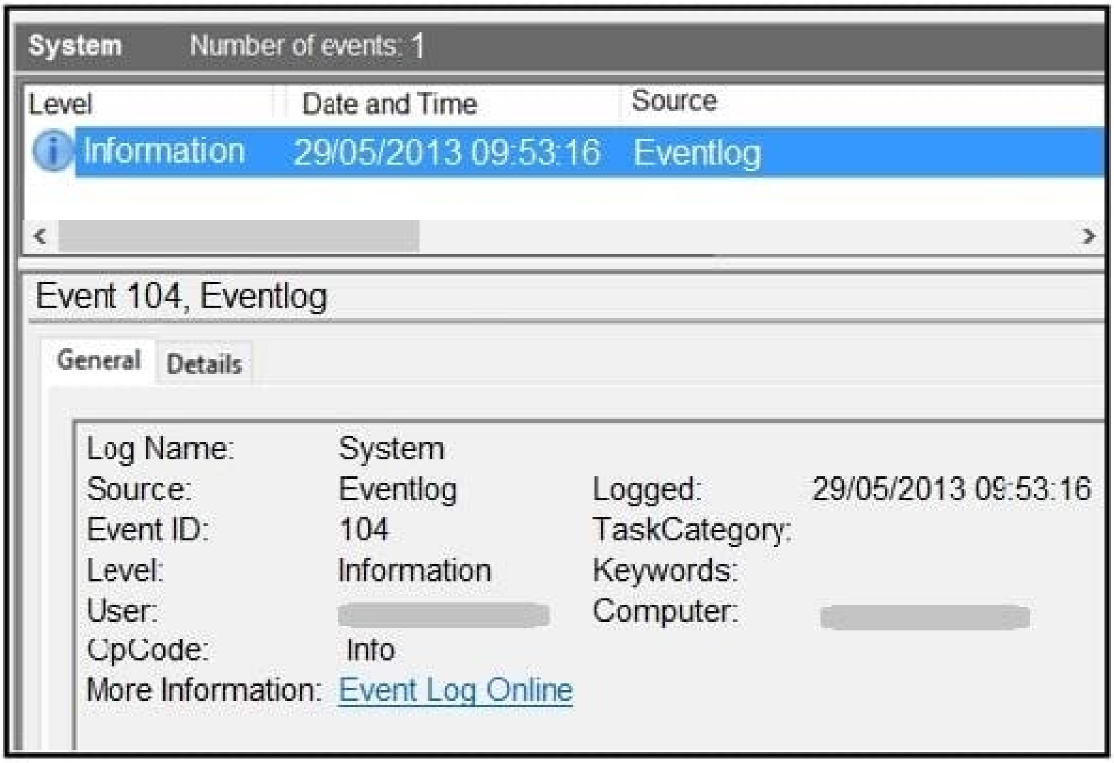
C. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).

D. Analyze the Magic File type in Cisco Umbrella.

E. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Correct Answer: BC

QUESTION 4



System Number of events: 1

Level	Date and Time	Source
Information	29/05/2013 09:53:16	Eventlog

Event 104, Eventlog

Log Name: System
Source: Eventlog
Event ID: 104
Level: Information
User: [redacted]
CpCode: Info
More Information: Event Log Online

Logged: 29/05/2013 09:53:16
TaskCategory:
Keywords:
Computer: [redacted]

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

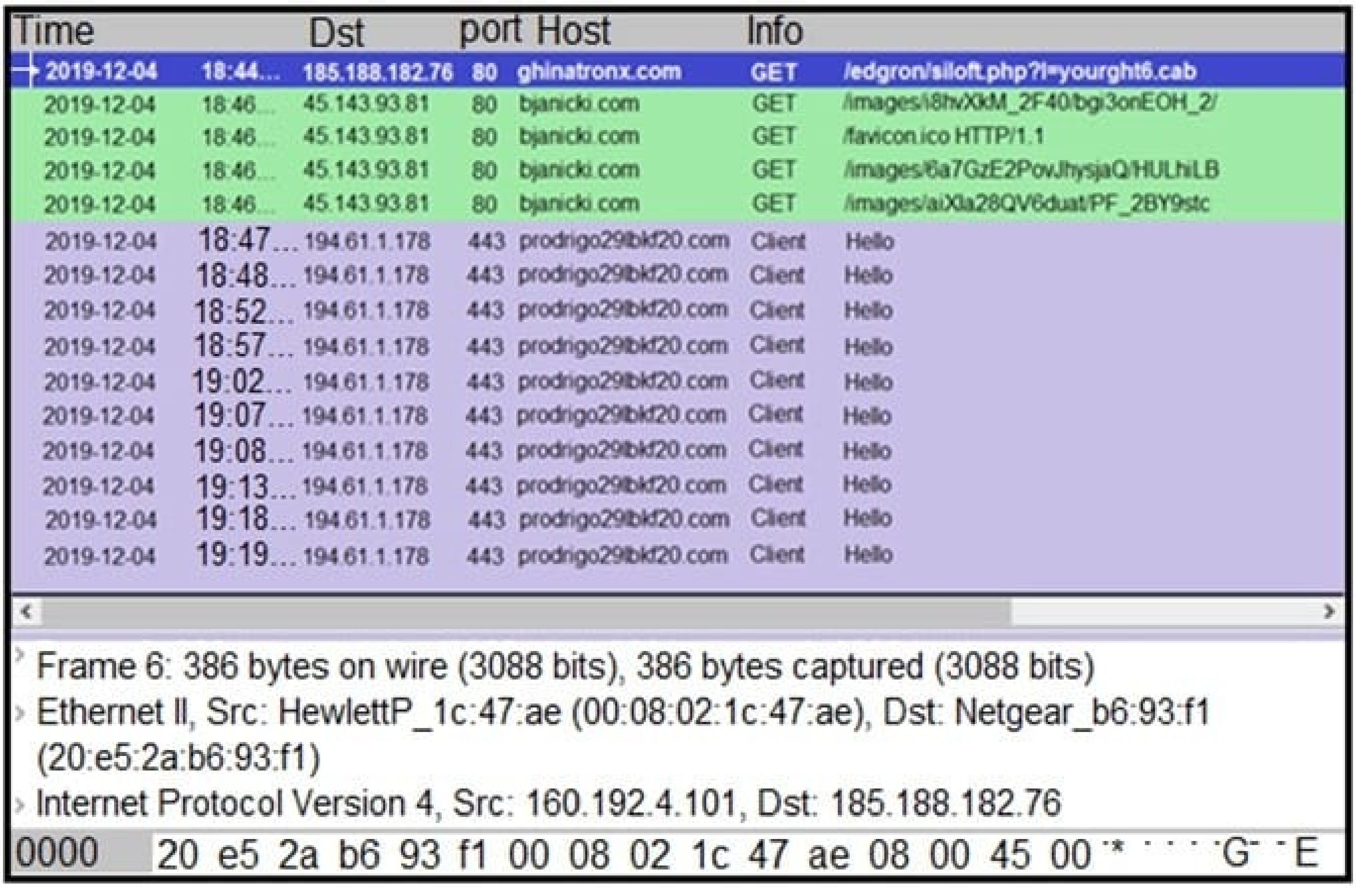
B. reconnaissance attack

C. brute-force attack

D. log tampering

Correct Answer: B

QUESTION 5



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

Reference:

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

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

[Latest 300-215 Dumps](#) [300-215 PDF Dumps](#) [300-215 Braindumps](#)