



**Vendor:** Cisco

**Exam Code:** 300-215

**Exam Name:** Conducting Forensic Analysis and Incident Response Using Cisco CyberOps Technologies

**Version:** DEMO

### QUESTION 1

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

**Answer: A**

### QUESTION 2

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.)

| 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**

General Details

A service was installed in the system.

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

- A. unauthorized system modification
- B. privilege escalation
- C. denial of service attack
- D. compromised root access
- E. malware outbreak

**Answer: AD**

### QUESTION 3

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

- A. cGRmZmlsZQ

- B. 706466666
- C. 255044462d
- D. 0a0ah4cg

**Answer: C**

#### QUESTION 4

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.

**Answer: D**

#### QUESTION 5

Refer to the exhibit. What do these artifacts indicate?

● **Artifact 32:** ☐ http-syracusecoffee.com-80-10-1

|   |   |
|---|---|
| <b>Src:</b> network<br><b>(GUI)</b> Intel 80386, for MS Windows<br><b>Size:</b> 270848<br><b>Imports:</b> 100<br><b>Exports:</b> 1<br><b>AV Sigs:</b> 0 | <b>Type:</b> EXE – PE32 executable<br><b>SHA256:</b><br>54665f8e84ea846e319408b23e65ad371cd09e0586c4980a199674034a3ab09<br><b>MD5:</b> f4a49b3e4aa82e1fc63adf48d133ae2a |
|---|---|

|                   |   |                   |  |
|-------------------|---|-------------------|--|
| <b>Path</b>       | http-syracusecoffee.com-80-10-1                   | <b>SHA1</b>       | 446e86e8d3b556afabe414bff4c250776e196c82 |
| <b>Mime Type</b>  | application/x-dosexec; charset=binary             | <b>Created At</b> | +142.693s                                |
| <b>Magic Type</b> | PE32 executable (GUI) Intel 80386, for MS Windows | <b>Related to</b> | <a href="#">stream 10</a>                |

● **PE Sections**

● **Headers**

● **Imported/Exported Symbols**

● **Artifact 33:** ☐ http-qstride.com-80-8-1

|   |   |
|---|---|
| <b>Src:</b> network<br><b>ASCII text</b><br><b>Size:</b> 318<br><b>Imports:</b> 0<br><b>Exports:</b> 0<br><b>AV Sigs:</b> 0 | <b>Type:</b> HTMLS – HTML document,<br><b>SHA256:</b><br>boc7e6712ecbf97a1e3a14f19e3aed5dbd6553f21a2852565bfc5518925713db<br><b>MD5:</b> fa172c77abd7b03605d33cd1ae373657 |
|---|---|

|                   |                             |                   |  |
|-------------------|-----------------------------|-------------------|--|
| <b>Path</b>       | http-qstride.com-80-8-1     | <b>SHA1</b>       | 9785fb3254695c25c621eb4cd81cf7a2a3c8258f |
| <b>Mime Type</b>  | text/html; charset=us-ascii | <b>Created At</b> | +141.865s                                |
| <b>Magic Type</b> | HTML document, ASCII text   | <b>Related to</b> | <a href="#">stream 8</a>                 |

- 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.

Answer: A

#### QUESTION 6

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

```
[**] [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:0x0 ID:20054 IpLen: 20 DgmLen:342 DF  
***AP*** Seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32  
[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```

- 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

Answer: C

#### QUESTION 7

Refer to the exhibit. Which type of code created the snippet?

```
function decrypt(rypted, key)
On Error Resume Next

Uf = rypted
sJs = "" '!!!
wWLu = ""
FETw = 1
for i=1 to len(Uf)
if ( asc(mid(Uf, i, 1)) > 47 and asc(mid(Uf, i, 1)) < 58) then
sJs = sJs + mid(Uf, 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
```

- A. VB Script
- B. Python
- C. PowerShell
- D. Bash Script

**Answer:** A

## Thank You for Trying Our Product

### Braindump2go Certification Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



**10% Discount Coupon Code: ASTR14**