Vendor: Cisco

Exam Code: 300-215

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

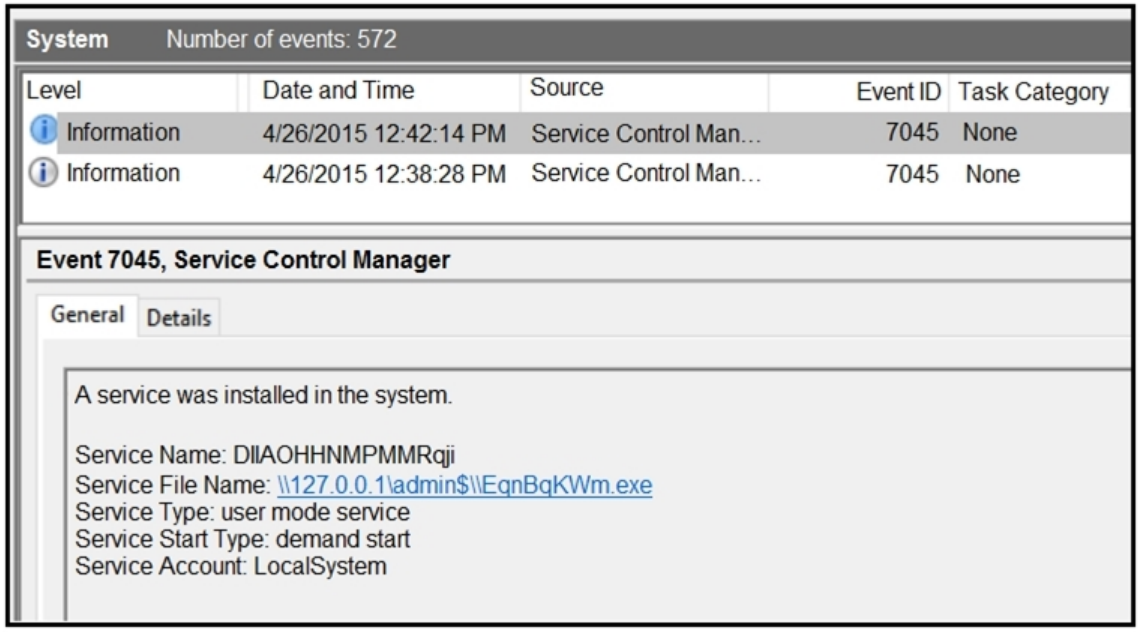
Version: DEMO

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.)



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

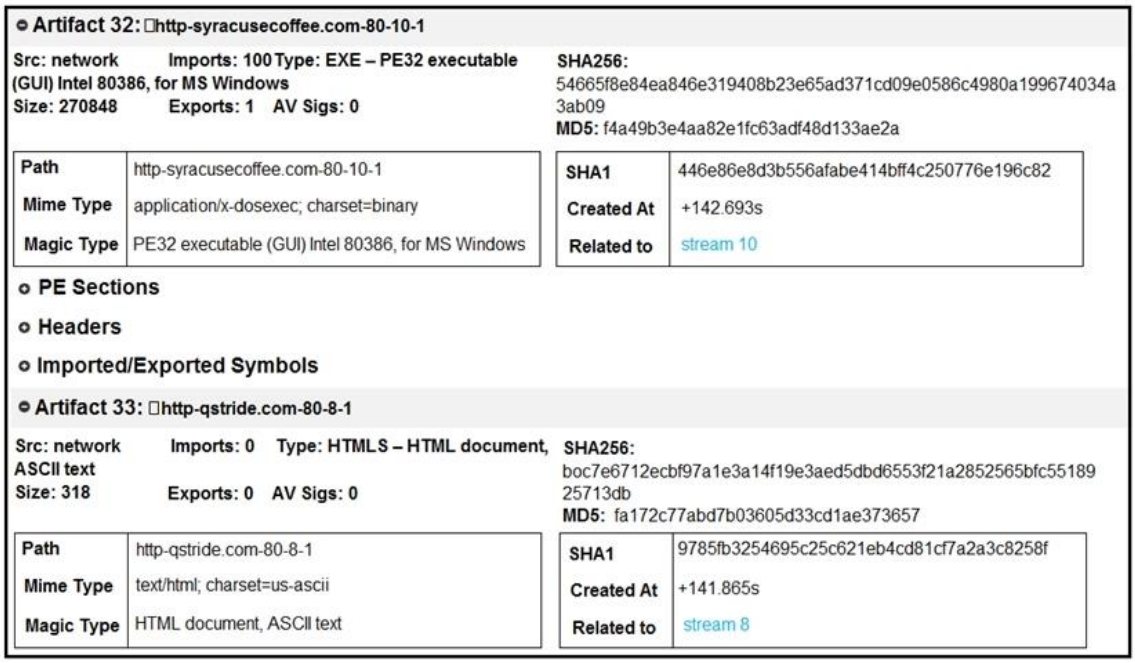
Answer: C

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?



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(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
```

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**