Free Questions for 300-215 by certsinside

Shared by Gregory on 12-12-2023

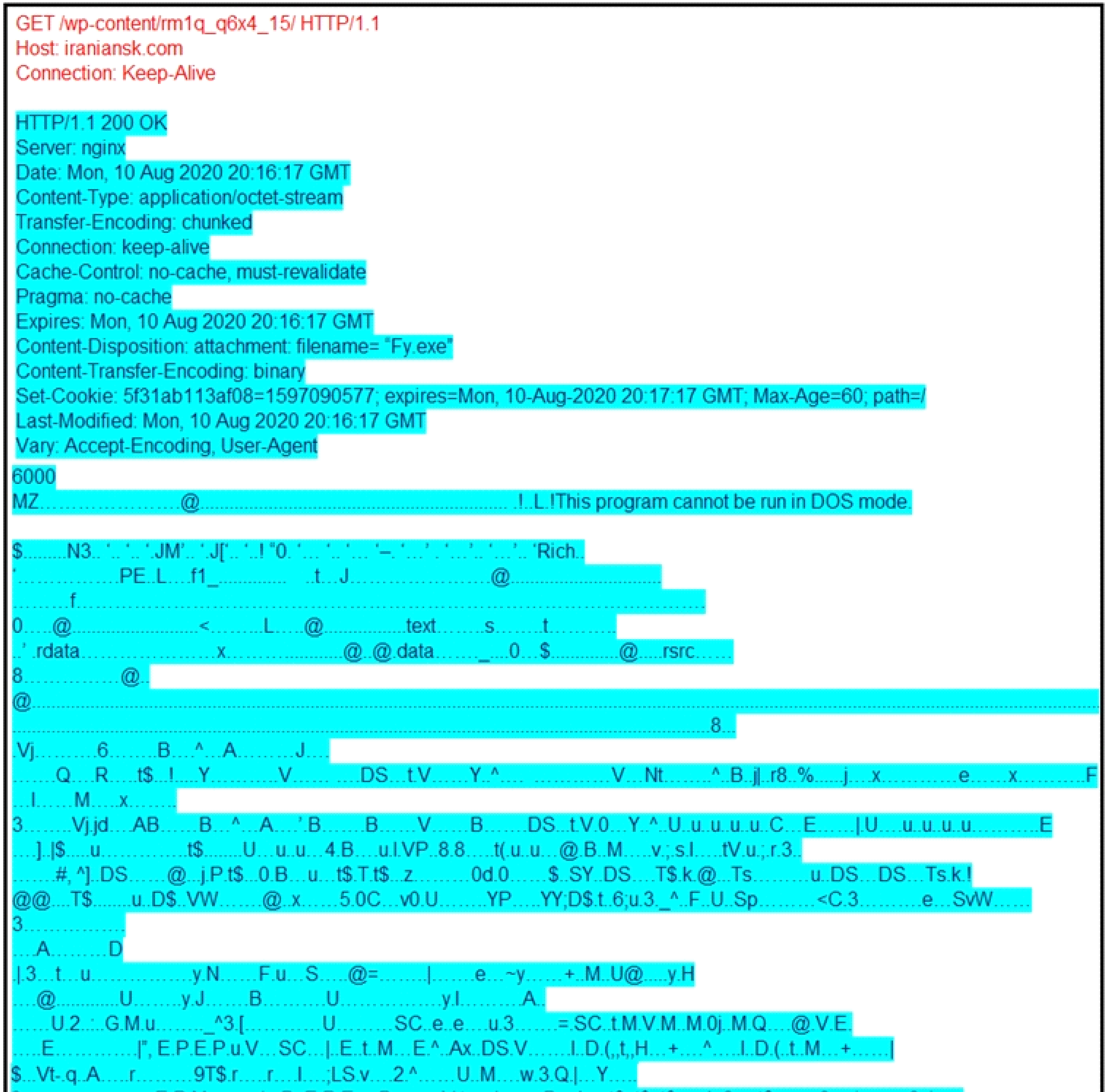
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



```
GET /wp-content/rm1q_q6x4_15/ HTTP/1.1
Host: iraniansk.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 10 Aug 2020 20:16:17 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 10 Aug 2020 20:16:17 GMT
Content-Disposition: attachment: filename= "Fy.exe"
Content-Transfer-Encoding: binary
Set-Cookie: 5f31ab113af08=1597090577; expires=Mon, 10-Aug-2020 20:17:17 GMT; Max-Age=60; path=/
Last-Modified: Mon, 10 Aug 2020 20:16:17 GMT
Vary: Accept-Encoding, User-Agent
6000
MZ…………………@.....................................................!..L.!This program cannot be run in DOS mode.

$.........N3.. '.. '.. '.JM'.. '.J['.. '..! "0. '… '.. '… '–. '…' . '…'.. '…'.. 'Rich..
'……………..PE..L….f1_.............   ..t…J………………….@...............................
……….f.....................................................................................................................
0…..@............................<……….L…..@...............text……..s……..t…………
..' .rdata…………………….x……………..........@..@.data……._….0…$.............@…..rsrc……
8……………..@..
@...........................................................................................................................................
...........................................................................................................................8...
.Vj……….6……..B….^…A……….J….
……..Q….R…..t$...!….Y…………V……   ….DS….t.V……Y..^….   ……………V….Nt………^..B..j|..r8..%…..j….x…………e……x…………F
…I……M…..x……..
3……..Vj.jd….AB……B…^….A….'.B…….B……V……B…….DS...t.V.0….Y..^..U..u..u..u..u..C….E……|.U…..u..u..u..u…………E
….]..|$.....u…………….t$.........U….u..u….4.B….u.l.VP..8.8…..t(.u..u….@.B..M…..v.;.s.l…..tV.u.;.r.3..
……..#, ^]..DS……@...j.P.t$...0.B….u…..t$.T.t$...z………..0d.0……..$..SY..DS…..T$.k.@....Ts………..u..DS….DS….Ts.k.!
@@....T$.........u..D$..VW……..@..x…….5.0C….v0.U………YP…..YY;D$.t..6;u.3._^..F..U..Sp……….<C.3…………e….SvW……
3……………..
….A………D
.|.3….t….u……………….y.N……F.u….S…..@=………|……..e….~y…….+..M..U@…..y.H
….@.............U……..y.J…….B…………U…………………y.l…………A..
……U.2..:..G.M.u………_^3.[…………….U………..SC..e..e…..u.3…….=.SC..t.M.V.M..M.0j..M.Q…..@.V.E.
…..E…………….|", E.P.E.P.u.V….SC….|..E..t..M….E.^..Ax..DS.V…….I..D.(,,t,,H….+….^……I..D.(..t..M….+……|
$...Vt-.q..A…..r…………9T$.r…..r…..I….;LS.v….2.^…….U..M…..w.3.Q.|….Y…..
```

According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

Options:

A- Domain name:iraniansk.com

B- Server: nginx

C- Hash value: 5f31ab113af08=1597090577

D- filename= "Fy.exe"

E- Content-Type: application/octet-stream

Answer:

C, E

Question 2

Question Type: **MultipleChoice**

What are YARA rules based upon?

Options:

A- binary patterns

B- HTML code

C- network artifacts

D- IP addresses

Answer:

A

Question 3

Question Type: **MultipleChoice**

A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file's behavior. Which logs should be reviewed next to evaluate this file further?

Options:

A- email security appliance

B- DNS server

C- Antivirus solution

D- network device

Answer:

B

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.

```
        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
```

Which type of code created the snippet?

Options:

A- VB Script

B- Python

C- PowerShell

D- Bash Script

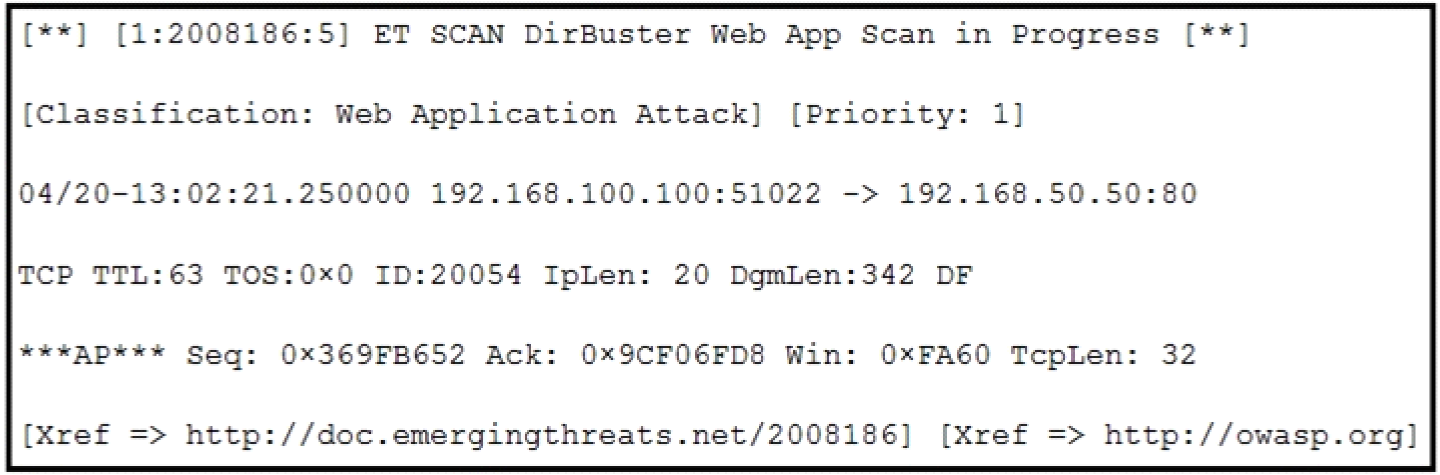
Answer:

A

Question 5

Question Type: **MultipleChoice**

Refer to the exhibit.



```
[**] [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]
```

According to the SNORT alert, what is the attacker performing?

Options:

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

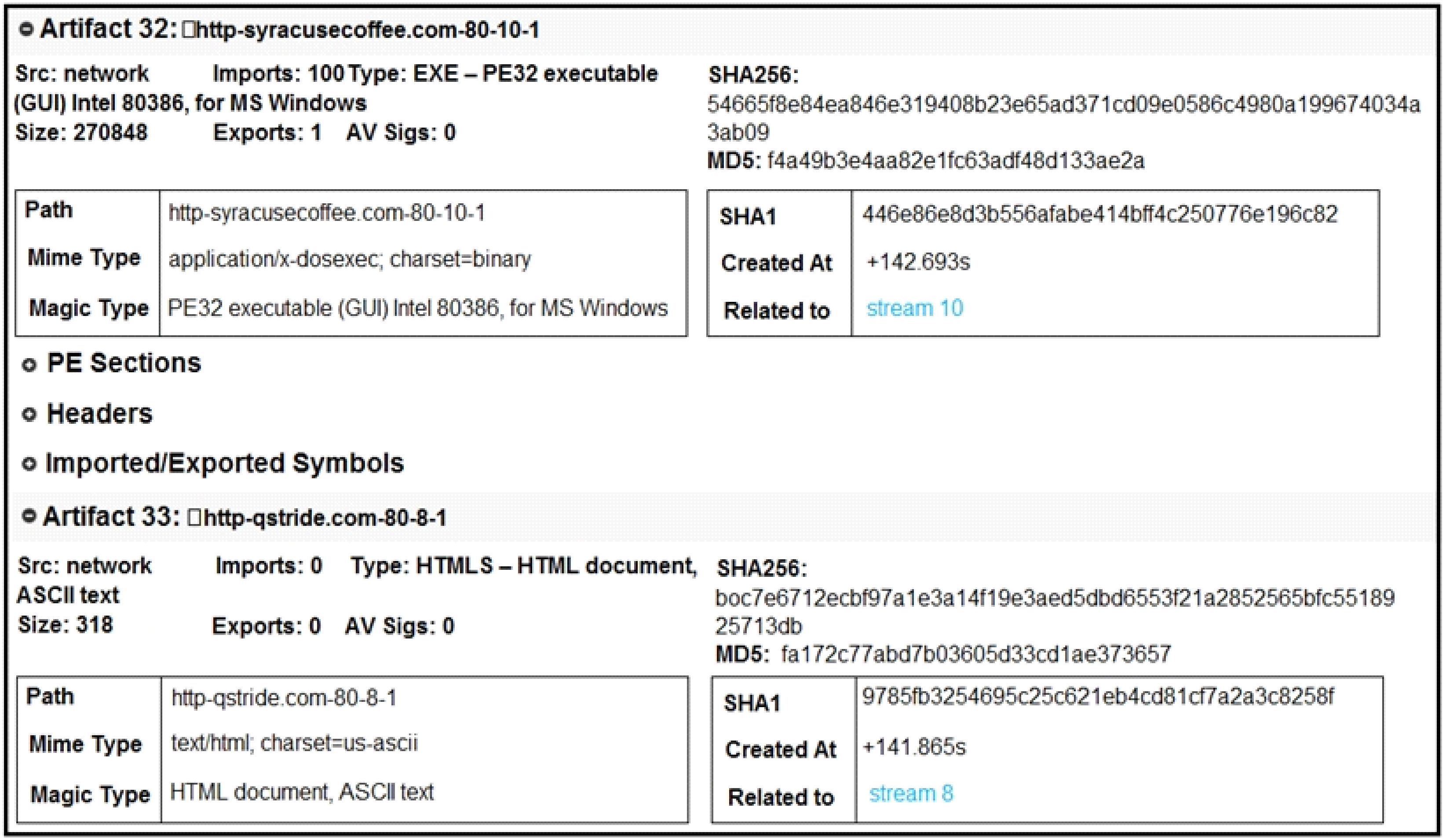
Answer:

C

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.



○ **Artifact 32: □http-syracusecoffee.com-80-10-1**

Src: network **Imports: 100** **Type: EXE – PE32 executable (GUI) Intel 80386, for MS Windows**
Size: 270848 **Exports: 1** **AV Sigs: 0**

SHA256: 54665f8e84ea846e319408b23e65ad371cd09e0586c4980a199674034a3ab09
MD5: f4a49b3e4aa82e1fc63adf48d133ae2a

Path	http-syracusecoffee.com-80-10-1
Mime Type	application/x-dosexec; charset=binary
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows

SHA1	446e86e8d3b556afabe414bff4c250776e196c82
Created At	+142.693s
Related to	stream 10

○ **PE Sections**

○ **Headers**

○ **Imported/Exported Symbols**

○ **Artifact 33: □http-qstride.com-80-8-1**

Src: network **Imports: 0** **Type: HTMLS – HTML document, ASCII text**
Size: 318 **Exports: 0** **AV Sigs: 0**

SHA256: boc7e6712ecbf97a1e3a14f19e3aed5dbd6553f21a2852565bfc5518925713db
MD5: fa172c77abd7b03605d33cd1ae373657

Path	http-qstride.com-80-8-1
Mime Type	text/html; charset=us-ascii
Magic Type	HTML document, ASCII text

SHA1	9785fb3254695c25c621eb4cd81cf7a2a3c8258f
Created At	+141.865s
Related to	stream 8

What do these artifacts indicate?

Options:

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 7

Question Type: **MultipleChoice**

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?

Options:

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