300-215 Q&As

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

QUESTION 1

A website administrator has an output of an FTP session that runs nightly to download and unzip files to a local staging server. The download includes thousands of files, and the manual process used to find how many files failed to download is time-consuming. The administrator is working on a PowerShell script that will parse a log file and summarize how many files were successfully downloaded versus ones that failed. Which script will read the contents of the file one line at a time and return a collection of objects?

A. Get-Content-Folder \\Server\FTPFolder\Logfiles\ftpfiles.log | Show-From "ERROR", "SUCCESS"

B. Get-Content –ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked “ERROR”, “SUCCESS”

C. Get-Content –Directory \\Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result “ERROR”, “SUCCESS”

D. Get-Content –Path \\Server\FTPFolder\Logfiles\ftpfiles.log | Select-String “ERROR”, “SUCCESS”

Correct Answer: D

QUESTION 2

A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook. Which two elements are part of the eradication phase for this incident? (Choose two.)

A. anti-malware software

B. data and workload isolation

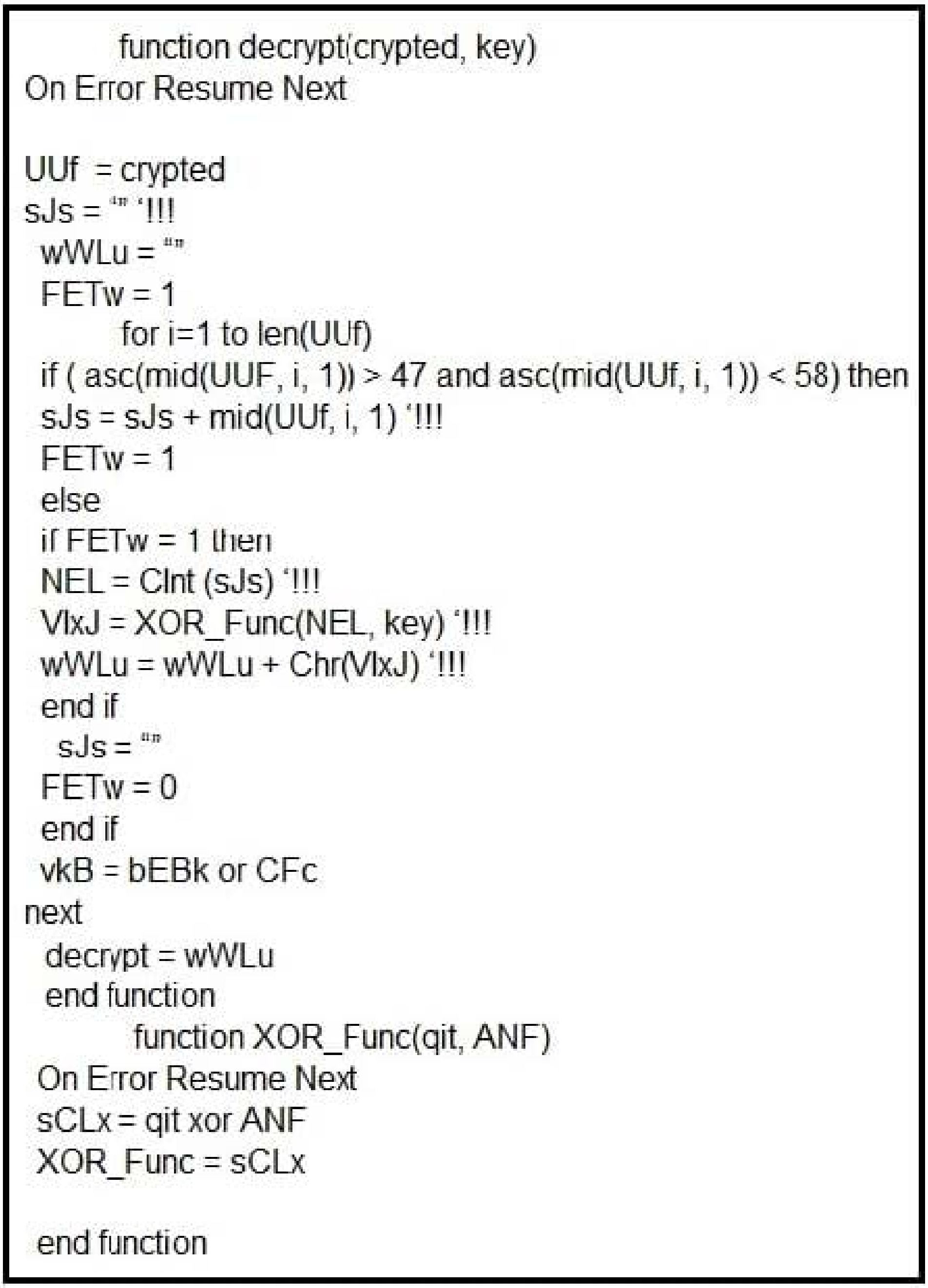
C. centralized user management

D. intrusion prevention system

E. enterprise block listing solution

Correct Answer: CD

QUESTION 3



```
        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
```

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

A. VB Script

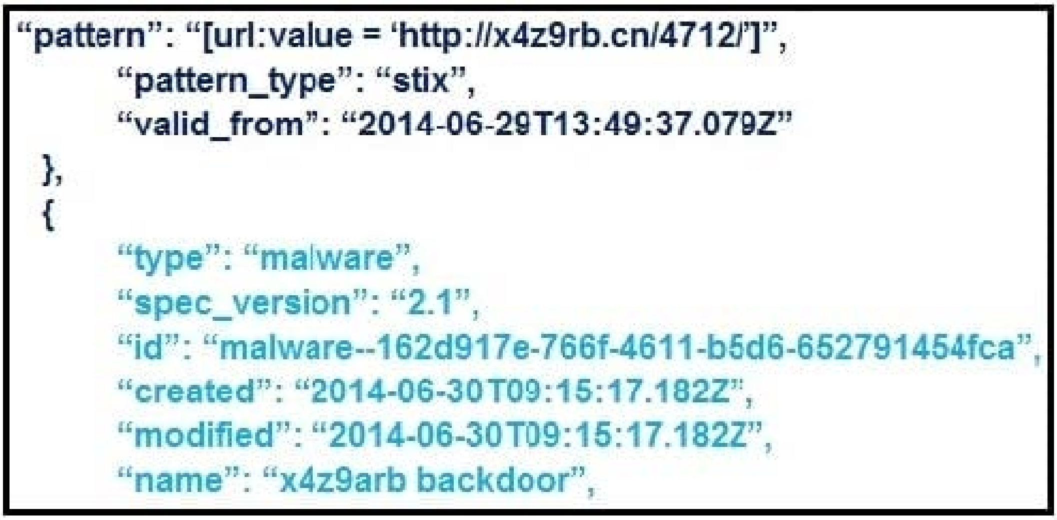
B. Python

C. PowerShell

D. Bash Script

Correct Answer: A

QUESTION 4



```
“pattern”: “[url:value = ‘http://x4z9rb.cn/4712/’]”,
        “pattern_type”: “stix”,
        “valid_from”: “2014-06-29T13:49:37.079Z”
  },
  {
        “type”: “malware”,
        “spec_version”: “2.1”,
        “id”: “malware--162d917e-766f-4611-b5d6-652791454fca”,
        “created”: “2014-06-30T09:15:17.182Z”,
        “modified”: “2014-06-30T09:15:17.182Z”,
        “name”: “x4z9arb backdoor”,
```

Refer to the exhibit. What is the IOC threat and URL in this STIX JSON snippet?

A. malware; `http://x4z9arb.cn/4712/\\'

B. malware; x4z9arb backdoor

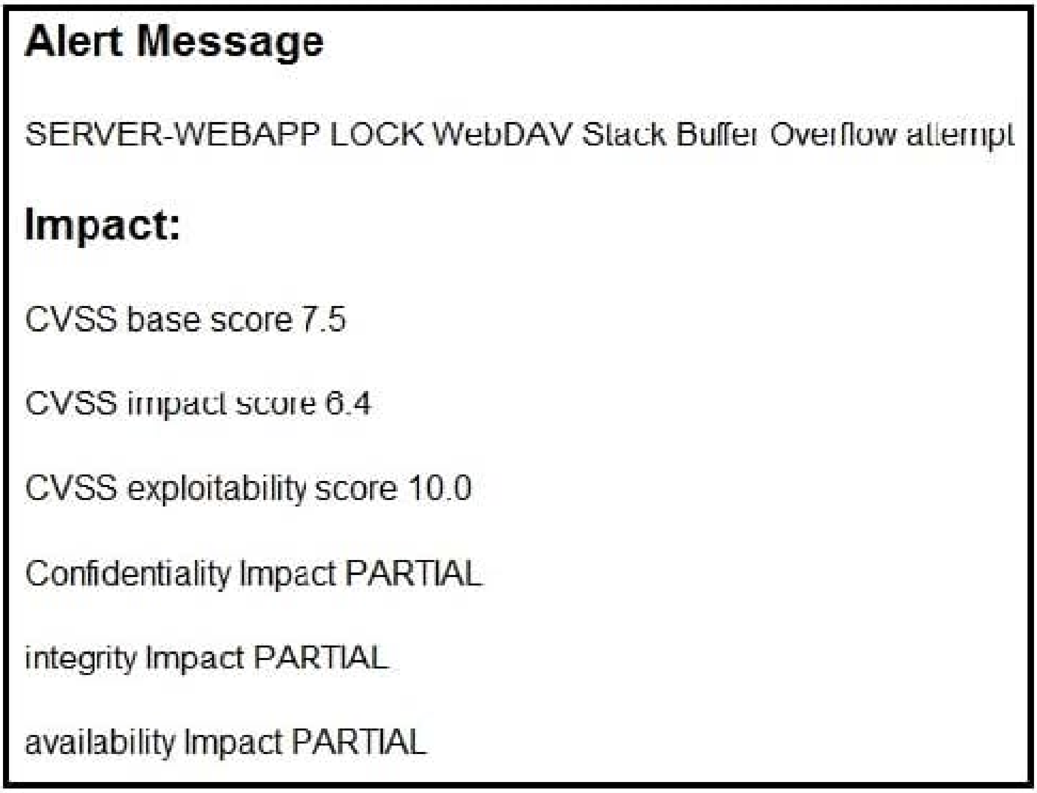
C. x4z9arb backdoor; http://x4z9arb.cn/4712/

D. malware; malware--162d917e-766f-4611-b5d6-652791454fca

E. stix; `http://x4z9arb.cn/4712/\\'

Correct Answer: D

QUESTION 5



Alert Message

SERVER-WEBAPP LOCK WebDAV Stack Buffer Overflow attempt

Impact:

CVSS base score 7.5

CVSS impact score 6.4

CVSS exploitability score 10.0

Confidentiality Impact PARTIAL

integrity Impact PARTIAL

availability Impact PARTIAL

Refer to the exhibit. After a cyber attack, an engineer is analyzing an alert that was missed on the intrusion detection system. The attack exploited a vulnerability in a business critical, web-based application and violated its availability. Which two migration techniques should the engineer recommend? (Choose two.)

A. encapsulation

B. NOP sled technique

C. address space randomization

D. heap-based security

E. data execution prevention

Correct Answer: CE

Latest 300-215 Dumps 300-215 VCE Dumps 300-215 Exam Questions