200-201$^{\text{Q\&As}}$

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

QUESTION 1

A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

A. the intellectual property that was stolen

B. the defense contractor who stored the intellectual property

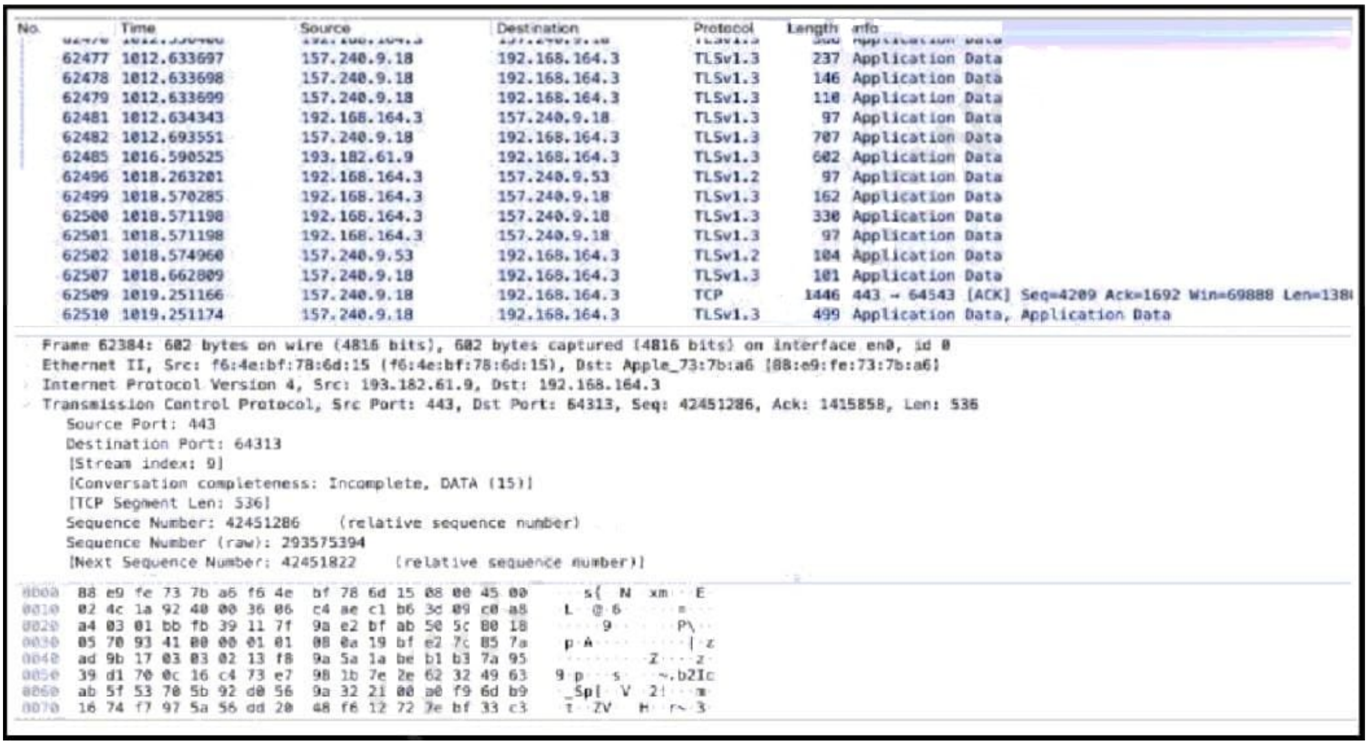
C. the method used to conduct the attack

D. the foreign government that conducted the attack

Correct Answer: D

QUESTION 2

Refer to exhibit.



```
No.    Time          Source          Destination     Protocol  Length  Info
62477  1012.633697   157.240.9.18    192.168.164.3   TLSv1.3      237  Application Data
62478  1012.633698   157.240.9.18    192.168.164.3   TLSv1.3      146  Application Data
62479  1012.633699   157.240.9.18    192.168.164.3   TLSv1.3      110  Application Data
62481  1012.634343   192.168.164.3   157.240.9.18    TLSv1.3       97  Application Data
62482  1012.693551   157.240.9.18    192.168.164.3   TLSv1.3      707  Application Data
62485  1016.590525   193.182.61.9    192.168.164.3   TLSv1.3      602  Application Data
62496  1018.263201   192.168.164.3   157.240.9.53    TLSv1.2       97  Application Data
62499  1018.570285   192.168.164.3   157.240.9.18    TLSv1.3      162  Application Data
62500  1018.571198   192.168.164.3   157.240.9.18    TLSv1.3      330  Application Data
62501  1018.571198   192.168.164.3   157.240.9.18    TLSv1.3       97  Application Data
62502  1018.574960   157.240.9.53    192.168.164.3   TLSv1.2      104  Application Data
62507  1018.662809   157.240.9.18    192.168.164.3   TLSv1.3      101  Application Data
62509  1019.251166   157.240.9.18    192.168.164.3   TCP         1446  443 → 64543 [ACK] Seq=4209 Ack=1692 Win=69888 Len=138
62510  1019.251174   157.240.9.18    192.168.164.3   TLSv1.3      499  Application Data, Application Data

  Frame 62384: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface en0, id 0
  Ethernet II, Src: f6:4e:bf:78:6d:15 (f6:4e:bf:78:6d:15), Dst: Apple_73:7b:a6 (88:e9:fe:73:7b:a6)
  Internet Protocol Version 4, Src: 193.182.61.9, Dst: 192.168.164.3
  Transmission Control Protocol, Src Port: 443, Dst Port: 64313, Seq: 42451286, Ack: 1415858, Len: 536
     Source Port: 443
     Destination Port: 64313
     [Stream index: 9]
     [Conversation completeness: Incomplete, DATA (15)]
     [TCP Segment Len: 536]
     Sequence Number: 42451286    (relative sequence number)
     Sequence Number (raw): 293575394
     [Next Sequence Number: 42451822    (relative sequence number)]

0000  88 e9 fe 73 7b a6 f6 4e  bf 78 6d 15 08 00 45 00   ···s{··N ·xm···E·
0010  02 4c 1a 92 40 00 36 06  c4 ae c1 b6 3d 09 c0 a8   ·L··@·6· ····=···
0020  a4 03 01 bb fb 39 11 7f  9a e2 bf ab 50 5c 80 18   ·····9·· ····P\··
0030  05 70 93 41 00 00 01 01  08 0a 19 bf e2 7c 85 7a   ·p·A···· ·····|·z
0040  ad 9b 17 03 03 02 13 f8  9a 5a 1a be b1 b3 7a 95   ········ ·Z····z·
0050  39 d1 70 0c 16 c4 73 e7  98 1b 7e 2e 62 32 49 63   9·p···s· ··~.b2Ic
0060  ab 5f 53 70 5b 92 d0 56  9a 32 21 00 a0 f9 6d b9   ·_Sp[··V ·2!···m·
0070  16 74 f7 97 5a 56 dd 20  48 f6 12 72 7e bf 33 c3   ·t··ZV·  H··r~·3·
```

An analyst performs the analysis of the pcap file to detect the suspicious activity. What challenges did the analyst face in terms of data visibility?

A. data encapsulation

B. code obfuscation

C. data encryption

D. IP fragmentation

Correct Answer: C

QUESTION 3

Which action prevents buffer overflow attacks?

A. variable randomization

B. using web based applications

C. input sanitization

D. using a Linux operating system

Correct Answer: C

QUESTION 4

Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis

B. preparation

C. eradication

D. containment

Correct Answer: A

Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity

Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information.Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively

communicate incident information (internal and external communications). Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

QUESTION 5

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.

Which information is available on the server certificate?

A. server name, trusted subordinate CA, and private key

B. trusted subordinate CA, public key, and cipher suites

C. trusted CA name, cipher suites, and private key

D. server name, trusted CA, and public key

Correct Answer: D