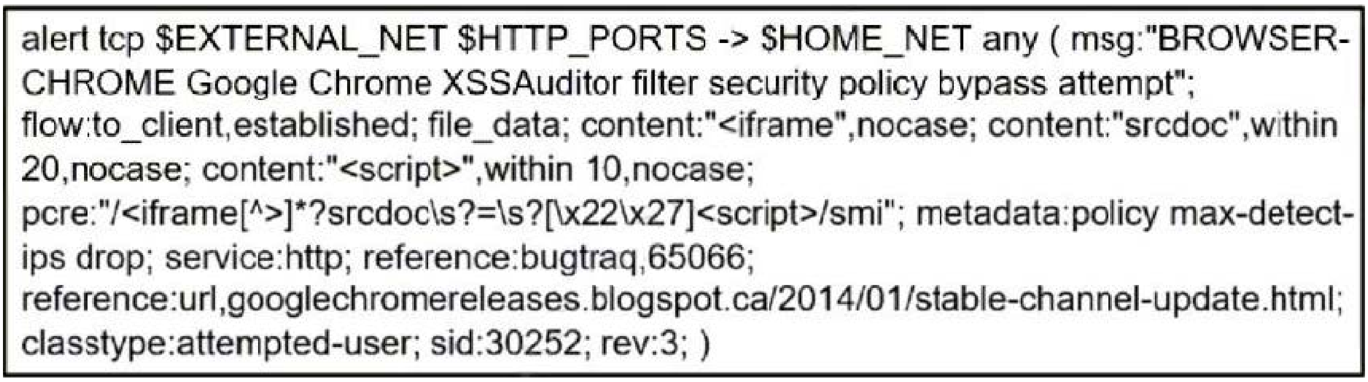
200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

QUESTION 1

Refer to the exhibit.



```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any ( msg:"BROWSER-
CHROME Google Chrome XSSAuditor filter security policy bypass attempt";
flow:to_client,established; file_data; content:"<iframe",nocase; content:"srcdoc",within
20,nocase; content:"<script>",within 10,nocase;
pcre:"/<iframe[^>]*?srcdoc\s?=\s?[\x22\x27]<script>/smi"; metadata:policy max-detect-
ips drop; service:http; reference:bugtraq,65066;
reference:url,googlechromereleases.blogspot.ca/2014/01/stable-channel-update.html;
classtype:attempted-user; sid:30252; rev:3; )
```

A company\\'s user HTTP connection to a malicious site was blocked according to configured policy. What is the source technology used for this measure?

A. network application control

B. firewall

C. IPS

D. web proxy

Correct Answer: C

QUESTION 2

How does certificate authority impact a security system?

A. It authenticates client identity when requesting SSL certificate

B. It validates domain identity of a SSL certificate

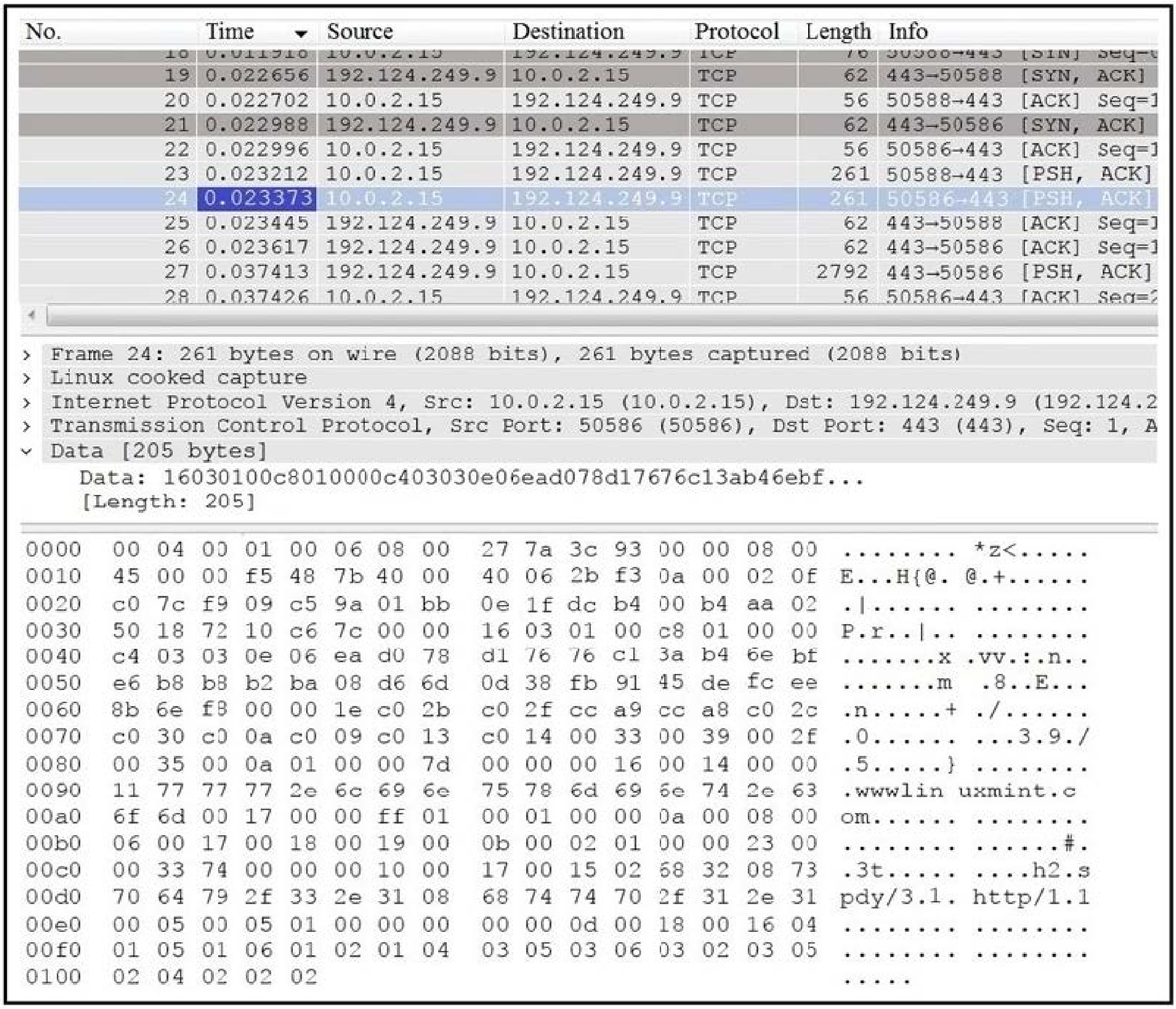
C. It authenticates domain identity when requesting SSL certificate

D. It validates client identity when communicating with the se

Correct Answer: B

QUESTION 3

Refer to the exhibit.



```
No.      Time      Source          Destination     Protocol Length Info
      18 0.011918  10.0.2.15       192.124.249.9   TCP          76 50588→443 [SYN] Seq=0
      19 0.022656  192.124.249.9   10.0.2.15       TCP          62 443→50588 [SYN, ACK]
      20 0.022702  10.0.2.15       192.124.249.9   TCP          56 50588→443 [ACK] Seq=1
      21 0.022988  192.124.249.9   10.0.2.15       TCP          62 443→50586 [SYN, ACK]
      22 0.022996  10.0.2.15       192.124.249.9   TCP          56 50586→443 [ACK] Seq=1
      23 0.023212  10.0.2.15       192.124.249.9   TCP         261 50588→443 [PSH, ACK]
      24 0.023373  10.0.2.15       192.124.249.9   TCP         261 50586→443 [PSH, ACK]
      25 0.023445  192.124.249.9   10.0.2.15       TCP          62 443→50588 [ACK] Seq=1
      26 0.023617  192.124.249.9   10.0.2.15       TCP          62 443→50586 [ACK] Seq=1
      27 0.037413  192.124.249.9   10.0.2.15       TCP        2792 443→50586 [PSH, ACK]
      28 0.037426  10.0.2.15       192.124.249.9   TCP          56 50586→443 [ACK] Seq=2
```

```
> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.2
> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
v Data [205 bytes]
    Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...
    [Length: 205]
```

```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ *z<.....
0010  45 00 00 f5 48 7b 40 00  40 06 2b f3 0a 00 02 0f  E...H{@. @.+.....
0020  c0 7c f9 09 c5 9a 01 bb  0e 1f dc b4 00 b4 aa 02  .|...... ........
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 0e 06 ea d0 78  d1 76 76 c1 3a b4 6e bf  .......x .vv.:.n..
0050  e6 b8 b8 b2 ba 08 d6 6d  0d 38 fb 91 45 de fc ee  .......m  .8..E...
0060  8b 6e f8 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c  .n.....+ ./......
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f  .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00  .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00  om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00  ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73  .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31  pdy/3.1. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04  ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05  ........ ........
0100  02 04 02 02 02                                    .....
```

Which application protocol is in this PCAP file?

A. SSH

B. TCP

C. TLS

D. HTTP

Correct Answer: C

QUESTION 4

An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.

B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.

C. Run "ps -ef" to understand which processes are taking a high amount of resources.

D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Correct Answer: C

Reference: https://unix.stackexchange.com/questions/62182/please-explain-this-output-of-ps-ef-command

QUESTION 5

What describes the concept of data consistently and readily being accessible for legitimate users?

A. integrity

B. availability

C. accessibility

D. confidentiality

Correct Answer: B

QUESTION 6

An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

A. The computer has a HIPS installed on it.

B. The computer has a NIPS installed on it.

C. The computer has a HIDS installed on it.

D. The computer has a NIDS installed on it.

Correct Answer: C

QUESTION 7

A forensic investigator is analyzing a recent breach case. An external USB drive was discovered to be connected and transmitting the data outside of the organization, and the owner of the USB drive could not be identified. Video surveillance shows six people during a two-month period had close contact with the affected asset. How must this type of evidence be categorized?

A. best evidence

B. indirect evidence

C. direct evidence

D. corroborative evidence

Correct Answer: B

QUESTION 8

A security incident occurred with the potential of impacting business services. Who performs the attack?

A. malware author

B. threat actor

C. bug bounty hunter

D. direct competitor

Correct Answer: B

Reference: https://www.paubox.com/blog/what-is-threat-actor/#:~:text=The%20term%20threat%20actor%20refers,CTA)%20when%20referencing%20cybersecurity%20issues

QUESTION 9

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. known-plaintext

B. replay

C. dictionary

D. man-in-the-middle

Correct Answer: D

QUESTION 10

What is the impact of encryption?

A. Confidentiality of the data is kept secure and permissions are validated

B. Data is accessible and available to permitted individuals

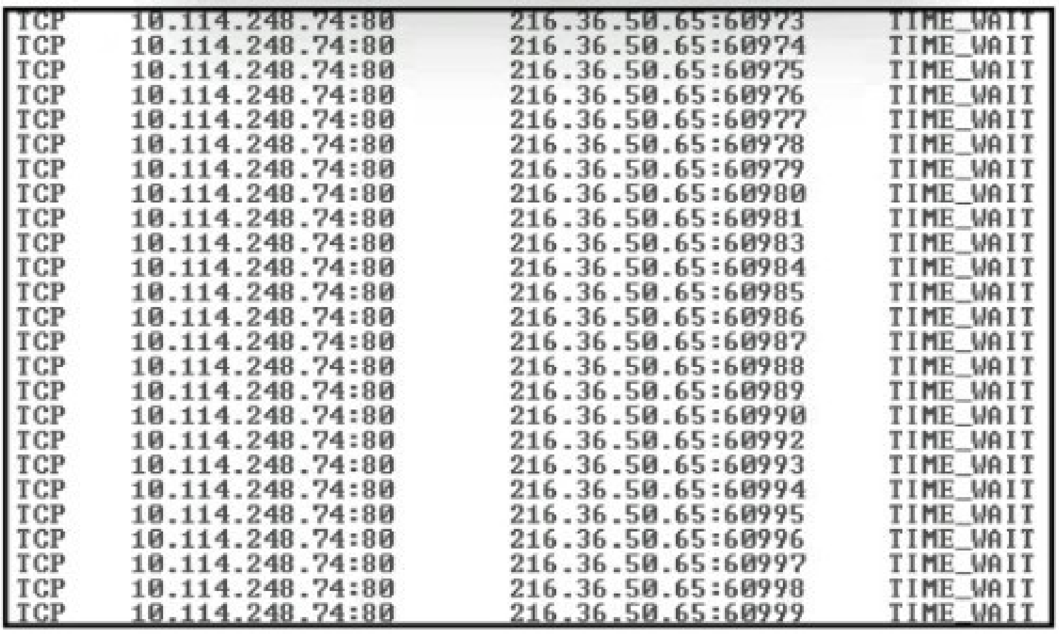
C. Data is unaltered and its integrity is preserved

D. Data is secure and unreadable without decrypting it

Correct Answer: D

QUESTION 11

Refer to the exhibit.



```
TCP    10.114.248.74:80    216.36.50.65:60973    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60974    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60975    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60976    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60977    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60978    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60979    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60980    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60981    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60983    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60984    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60985    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60986    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60987    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60988    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60989    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60990    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60992    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60993    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60994    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60995    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60996    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60997    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60998    TIME_WAIT
TCP    10.114.248.74:80    216.36.50.65:60999    TIME_WAIT
```

An engineer received a ticket about a slowed-down web application The engineer runs the #netstat -an command. How must the engineer interpret the results?

A. The web application is receiving a common, legitimate traffic

B. The engineer must gather more data.

C. The web application server is under a denial-of-service attack.

D. The server is under a man-in-the-middle attack between the web application and its database

Correct Answer: C

QUESTION 12

What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

A. additional PPTP traffic due to Windows clients

B. unauthorized peer-to-peer traffic

C. deployment of a GRE network on top of an existing Layer 3 network

D. attempts to tunnel IPv6 traffic through an IPv4 network

Correct Answer: D

QUESTION 13

Which of these is a defense-in-depth strategy principle?

A. Identify the minimum resource required per employee.

B. Provide the minimum permissions needed to perform job functions.

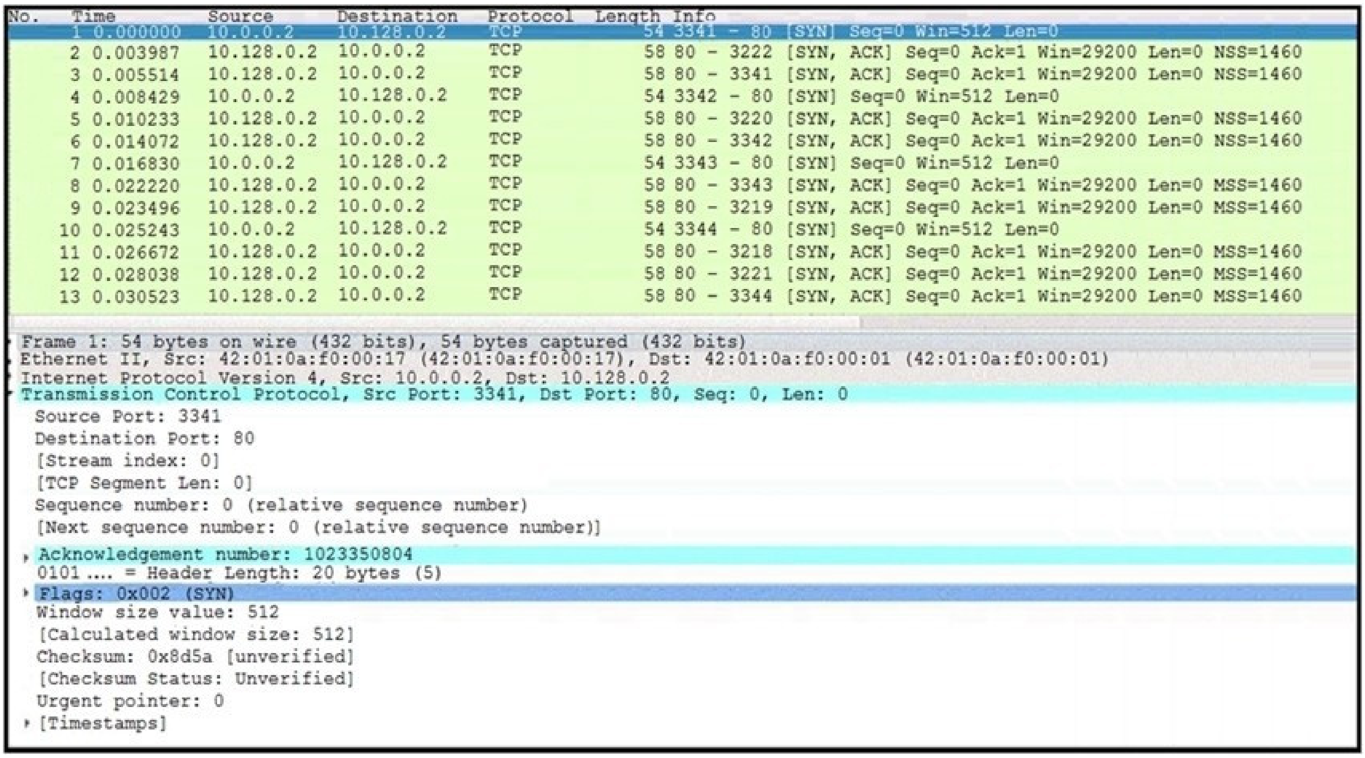
C. Disable administrative accounts to avoid unauthorized changes.

D. Assign the least network privileges to segment network permissions.

Correct Answer: D

QUESTION 14

Refer to the exhibit.



```
No.   Time       Source      Destination  Protocol  Length Info
    1 0.000000   10.0.0.2    10.128.0.2   TCP           54 3341 - 80 [SYN] Seq=0 Win=512 Len=0
    2 0.003987   10.128.0.2  10.0.0.2     TCP           58 80 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    3 0.005514   10.128.0.2  10.0.0.2     TCP           58 80 - 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    4 0.008429   10.0.0.2    10.128.0.2   TCP           54 3342 - 80 [SYN] Seq=0 Win=512 Len=0
    5 0.010233   10.128.0.2  10.0.0.2     TCP           58 80 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    6 0.014072   10.128.0.2  10.0.0.2     TCP           58 80 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
    7 0.016830   10.0.0.2    10.128.0.2   TCP           54 3343 - 80 [SYN] Seq=0 Win=512 Len=0
    8 0.022220   10.128.0.2  10.0.0.2     TCP           58 80 - 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
    9 0.023496   10.128.0.2  10.0.0.2     TCP           58 80 - 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   10 0.025243   10.0.0.2    10.128.0.2   TCP           54 3344 - 80 [SYN] Seq=0 Win=512 Len=0
   11 0.026672   10.128.0.2  10.0.0.2     TCP           58 80 - 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   12 0.028038   10.128.0.2  10.0.0.2     TCP           58 80 - 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   13 0.030523   10.128.0.2  10.0.0.2     TCP           58 80 - 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 3341
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
  Acknowledgement number: 1023350804
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x002 (SYN)
  Window size value: 512
  [Calculated window size: 512]
  Checksum: 0x8d5a [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [Timestamps]
```

What is occurring in this network traffic?

A. High rate of SYN packets being sent from a multiple source towards a single destination IP.

B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.

C. Flood of ACK packets coming from a single source IP to multiple destination IPs.

D. Flood of SYN packets coming from a single source IP to a single destination IP.

Correct Answer: D

QUESTION 15

What is the purpose of a ransomware attack?

A. to escalate privileges

B. to make files inaccessible by encrypting the data

C. to send keystrokes to a threat actor

D. to decrypt encrypted data and disks

Correct Answer: B