5.1

1. According to CompTIA, which list of intelligence cycle phases is most correct?

- Requirements, Collection, Analysis, Dissemination, Feedback
- Planning, Processing, Intelligence, Dissemination, Feedback
- Direction, Collection, Processing, Dissemination, Lessons Learned
- Planning and Direction, Collection and Processing, Analysis, Sharing, Feedback
- None of the above.

2. Your chief information security officer (CISO) wants to develop a new collection and analysis platform that will enable the security team to extract actionable data from its assets. The CISO would like your input as far as which data sources to draw from as part of the new collection platform, worrying that collecting from too many sources, or not enough, could impede the company's ability to analyze information. Is this a valid concern, and how can it be addressed within an intelligence life-cycle model?

- Yes, it is a valid concern. The requirements (or planning and direction) phase of the intelligence cycle can be used to evaluate data sources and develop goals and objectives for producing strategic intelligence to support use cases demanded by intelligence consumers. You can also mention that the feedback phase of the cycle requires one to review sources and determine whether they are delivering valuable intelligence.
- No, it is not a valid concern. The requirements (or planning and direction) phase of the intelligence cycle cannot be used to evaluate data sources and develop goals and objectives for producing tactical intelligence to support use cases demanded by intelligence consumers. You can also mention that the feedback phase of the cycle does not provide the opportunity to review sources and determine whether they are delivering valuable intelligence.
- No, it is not a valid concern. The requirements (or planning and direction) phase of the intelligence cycle cannot be used to evaluate data sources and develop goals and objectives for producing general threat intelligence to support use cases demanded by intelligence consumers. You can also mention that the feedback phase of the cycle requires one to review sources and determine whether they are delivering valuable intelligence.
- Yes, it is a valid concern. The requirements (or planning and direction) phase of the intelligence cycle can be used to evaluate data sources and develop goals and objectives for producing actionable intelligence to support use cases demanded by intelligence consumers. You can also mention that the feedback phase of the cycle provides the opportunity to review sources and determine whether they are delivering valuable intelligence.
- None of the above correctly answer the question.

3. What are the characteristics to use to evaluate threat data and intelligence sources?

- They are categorized as proprietary/closed-source, public/open-source, or community-based, such as an ISAC. Within those categories, data feeds can be assessed for timeliness, relevancy, and accuracy. It is also important for analyst opinions and threat data points to be tagged with a confidence level.
- They are categorized as proprietary/closed-source, public/open-source, or community-based, such as an ISAC. Within those categories, data feeds can be assessed for timeliness and accuracy. Relevancy is not considered to be a good measure of intelligence. It is also important for analyst opinions and threat data points to be tagged with a confidence level.
- They are categorized as proprietary/closed-source, public/open-source, or community-based, such as an ISAC. Within those categories, data feeds can be assessed for relevancy and accuracy. Timeliness is not considered to be a good measure of intelligence. It is also important for analyst opinions and threat data points to be tagged with a threat level.
- They are categorized as proprietary/closed-source, public/open-source, or community-based, such as an ISAC. Within those categories, data feeds can be assessed for timeliness, relevancy, and accuracy. It is also important for analyst opinions and threat data points to be tagged with a threat level.
- None of the above.

4. Despite operating a patch management program, your company has been exposed to several attacks over the last few months. You have drafted a policy to require a lessons-learned incident report be created to review the historical attacks and to make this analysis a requirement following future attacks. How can this type of control be classified?

- Despite operating a patch management program, your company has been exposed to several attacks over the last few months. You have drafted a policy to require a lessons-learned incident report be created to review the historical attacks and to make this analysis a requirement following future attacks. How can this type of control be classified? It is implemented as an administrative control as it is strategic rather than technical in nature. Additionally, it is a managerial control rather than an operational control as it seeks oversight of day-to-day processes with a view to improving them. In terms of function, you can classify it as corrective, as it occurs after an attack has taken place.
- It is implemented as a managerial control as it is procedural rather than technical in nature. Additionally, it is a managerial control rather than an operational control as it seeks oversight of day-to-day processes with a view to improving them. In terms of function, you can classify it as preventative, as it occurs after an attack has taken place.
- It is implemented as an operational control as it is strategic rather than technical in nature. Additionally, it is a technical control rather than an operational control as it seeks oversight of day-to-day processes with a view to improving them. In terms of function, you can classify it as detective, as it occurs after an attack has taken place.
- It is implemented as a technical control as it is procedural rather than technical in nature. Additionally, it is an operational control rather than an operational control as it seeks oversight of day-to-day processes with a view to improving them. In terms of function, you can classify it as detective, as it occurs after an attack has taken place.
- None of the above correctly answer the question.

5. An application used by your company has been the target of malware. The developers have created signatures for the application's binaries, and these have been added to endpoint detection and response (EDR) scanning software running on each workstation. If a scan shows that a binary image no longer matches its signature, an administrative alert is generated. What type of security control is this?

- This is a technical control as it is implemented in software. In functional terms, it acts as a detective control because it does not stop malware from replacing the original file image (preventative control) or restore the original file automatically (preventative control).
- This is a managerial control as it is implemented in software. In functional terms, it acts as a strategic control because it does not stop malware from replacing the original file image (preventative control) or restore the original file automatically (corrective control).
- This is a corrective control as it is implemented in software. In functional terms, it acts as a operational control because it stops the malware from replacing the original file image (preventative control) and restores the original file automatically (corrective control).
- This is an access control as it is implemented in software. In functional terms, it acts as a managerial control because it stops the malware from replacing the original file image (corrective control) and restores the original file automatically (preventative control).
- None of the above statements correctly answer the question.

6. Your company is interested in implementing routine backups of all customer databases. This will help uphold availability because you will be able to quickly and easily restore the backed-up copy, and it will also help uphold integrity in case someone tampers with the database. Regarding this plan which of the following statements are most true?

- Encryption can be used as an additional layer of protection.
- You should consider the confidence level component.
- The backups contain the same privileged information as the live copy and so must be protected by compensation controls.
- Access controls can only be used to ensure that only authorized backup operators have access to the data.
- All the above
- None of the above

5.2

1. Your organization is planning to transition from using local clients to provisioning desktop instances via cloud-based infrastructure. Your CISO has asked you to outline a threat-modeling project to support selection and development of security controls to mitigate risks with this new service. What five methodologies should your outline contain?

- Adversary capability analysis, total attack surface analysis, attack vector analysis, impact analysis, and risk analysis.
- Adversary capability analysis, total attack surface analysis, MITRE ATT&CK vector analysis, impact analysis, and likelihood analysis.
- Adversary capability analysis, total surface area analysis, attack vector analysis, impact analysis, and likelihood analysis.
- Adversary capability analysis, total attack surface analysis, attack vector analysis, impact analysis, and likelihood analysis.
- None of the above.

2. Following a serious data breach affecting a supplier company, your CEO wants assurance that your company is not exposed to the same risk. The supplier is willing to share threat data gathered about the breach with you. You advise a threat hunting program as the most appropriate tool to use. Which is the following first steps is least wrong?

- Establish a hypothesis. You already have the basic scenario of the data breach at the supplier company. This does not require additional documenting and developing as the attacked supplier did that already. This means that you can then move on to profiling threat actors and activities and developing threat hunting tactics to query indicators from your own systems.
- Establish a chain of custody. You already have the detailed scenario of the data breach at the supplier company. This will require documenting and developing. Once the evidence is safely in a chain of custody, you should then move on to profiling threat actors and activities and developing threat hunting tactics to query indicators from your own systems.
- Secure the scene. You already have the working scenario of the data breach at the supplier company. This will require documenting and developing. You must then move on to profiling threat actors and activities and developing threat hunting tactics to query indicators from your own systems.
- Backup all critical data. You already have the memorandum of agreement (MOA) regarding the scenario of the data breach at the supplier company. This facilitates documenting and developing. You can then move on to profiling threat actors and activities and developing threat hunting tactics to query indicators from your own systems.
- None of the above.

3. As part of your threat hunting proposal, you need to identify benefits of the program. You have listed opportunities to close attack vectors, reduce the attack surface, and bundle critical assets within

additional layers of security controls. Which of the following is the best example of an additional benefit of threat hunting?

- Firstly, threat hunting develops integrated intelligence capabilities by which you create cyber-threat intelligence (CTI) with locally observed indicators. Secondly, the queries, filters, and tactics used can be redeployed to improve detection capabilities in conventional monitoring systems.
- Firstly, threat hunting develops integrated intelligence capabilities by which you create cyber-threat intelligence (CTI) with locally observed indicators. Secondly, the queries, filters, and tactics used can be redeployed to improve detection capabilities in conventional monitoring systems.
- Firstly, threat hunting develops integrated intelligence capabilities by which you create cyber-threat intelligence (CTI) with locally compared indices. Secondly, the queries, filters, and tactics used can be redeployed to create detection abilities in conventional monitoring systems.
- Firstly, threat hunting develops integrated intelligence capabilities by which you correlate cyber-threat intelligence (CTI) with locally observed indicators. Secondly, the queries, filters, and tactics used can be redeployed to implement detection capabilities in conventional monitoring systems.
- None of the above.

4. The security analyst determined that an email containing a malicious attachment was sent to several employees within the company, and it was not stopped by any of the email filtering devices. An incident was declared. During the investigation, it was determined that most users deleted the email, but one specific user executed the attachment. Based on the details gathered, which of the following actions should the security analyst perform NEXT?

- Obtain a copy of the email with the malicious attachment. Execute the file on another user's machine and observe the behavior. Document all findings.
- Acquire a full backup of the affected machine. Reimage the machine and then restore from the full backup.
- Take the affected machine off the network. Review local event logs looking for activity and processes related to unknown or unauthorized software.
- Take possession of the machine. Apply the latest OS updates and firmware. Discuss the problem with the user and return the machine.
- None of the above.

5. A security analyst has been asked to review permissions on accounts within Active Directory to determine if they are appropriate to the user's role. During this process, the analyst notices that a user from building maintenance is part of the Domain Admin group. Which of the following does this indicate?

- Cross-site scripting

- Session hijack
- Privilege escalation
- Rootkit
- None of the above.

6. A security analyst wants to capture data flowing in and out of a network. Which of the following would MOST likely assist in achieving this goal?

- Taking a screenshot.
- Analyzing network traffic and logs.
- Analyzing big data metadata.
- Capturing system image.
- None of the above.

7. Which of the following is the main benefit of sharing incident details with partner organizations or external trusted parties during the incident response process?

- It facilitates releasing incident results, findings and resolution to the media and all appropriate government agencies.
- It shortens the incident life cycle by allowing others to document incident details and prepare reports.
- It enhances the response process, as others may be able to recognize the observed behavior and provide valuable insight.
- It allows the security analyst to defer incident-handling activities until all parties agree on how to proceed with analysis.
- None of the above.

8. In the last six months, a company is seeing an increase in credential-harvesting attacks. The latest victim was the chief executive officer (CEO). Which of the following countermeasures would best render the attack ineffective?

- Use a complex password according to the company policy.
- Implement an intrusion-prevention system.
- Isolate the CEO's computer in a higher security zone.
- Implement multifactor authentication.

- None of the above.

5.3

1. Your company has suffered a data breach to an IP address subsequently found to appear on several threat reputation blacklists. What configuration change can you make to reduce the risk of further events of this type?

- At a minimum, configure outbound filtering on the firewall to block connections to "known-bad" IP addresses. You could also consider denying outbound connections to destinations that have not been approved on a whitelist. This configuration is more secure, but will generate more support incidents.
- At a minimum, configure inbound filtering on the firewall to block connections to "known-bad" IP addresses. You could also consider allowing outbound connections to destinations that have been approved on a whitelist. This configuration is more secure, but will generate more support incidents.
- At a minimum, configure outbound filtering on the firewall to block connections to "known-good" IP addresses. You could also consider denying outbound connections to destinations that have not been approved on a whitelist. This configuration is more secure, but will generate more support incidents.
- At a minimum, configure inbound filtering on the firewall to block connections to "known-good" IP addresses. You could also consider allowing outbound connections to destinations that have not been approved on a whitelist. This configuration is more secure, but will generate more support incidents.

2. You are reviewing a router configuration and notice a route to the null() interface. Is this a configuration weakness and IoC, or does it support a secure configuration

- This supports a secure configuration to mitigate DDoS. A route to a null interface is a means of dropping traffic (a black hole) without using as much resource on the router to process the unwanted connection.
- This supports a secure configuration to mitigate DDoS. A route to a null interface is a means of dropping traffic (a black hole) but taxes the resources on the router to process the unwanted connection.
- This is a configuration weakness and will not help mitigate DDoS. A route to a null interface is a means of dropping traffic (a black hole) without using as much resource on the router to process the unwanted connection.
- This is a configuration weakness and will not help mitigate mitigate DDoS. A route to a null interface is a means of dropping traffic (a black hole) but taxes the resources on the router to process the unwanted connection.

3. You are investigating a data exfiltration event and have obtained the web server logs of the host that data was exported to over the Internet from the hosting provider. The logs contain only the external IP address of your company's router/firewall and a high-level TCP port number. How can you use the log to identify the local host on your network that was used to perform the exfiltration?

- The router/firewall is performing port address translation. You can use the local router/firewall log to identify the local host from the port mapping recorded by the remote host.
- The router/firewall is performing name address translation. You can use the local router/firewall log to identify the local host from the NAT mapping recorded by the remote host.
- The router/firewall is performing port forwarding. You can use the local router/firewall log to identify the local host from the port forwarding recorded by the remote host.
- The router/firewall is performing MAC filtering. You can use the local router/firewall log to identify the local host from the MAC recorded by the remote host.

4. Attaching devices that are vulnerable to exploits to a network is a type of threat is NAC designed to mitigate?

- Ture
- False

5. What is the effect of running 'tcpdump -i eth0 -w server.pcap?

- Write the output of the packet capture running on network interface eth0 to the 'server.pcap file.
- Write the input of the packet capture running on network interface -i to the 'server.pcap file.
- Write the input of the packet capture running on network interface eth0 to the 'server.pcap file.
- Write the output of the packet capture running on network interface -i to the 'server.pcap file.

6. You need to log internet endpoints and bandwidth consumption between clients and servers on a local network, but do not have the resources to capture and store all network packets. You could use a NetFlow/Argus collector or simple network protocol (SNMP) collector. Another option is a scanner such as netstat that records traffic statistics and content selectively.

- True
- False

7. You are analyzing DNS logs for malicious traffic and come across two types of anomalous entry. The first type is for a single label with apparently random characters, in the form: VbhyofcyaewcfmozjycvrtbsaubliqThe other type is of the following form, but with different TLDs: nahekhrdizaiupfm.info tlaawnpkfcqorxuo.cn uwguhvpzqlzcmiug.org Which is more likely to be an indicator for DGA?

- The second type is more likely to be a domain generation algorithm. A query for a single label with no top level domain (TLD) will not resolve over the Internet, so the first type cannot be used for C&C. The first type is typical of a local client testing DNS. The Chrome browser performs this test to see how the local ISP handles NXDOMAIN errors, for instance.
- The second type is more likely to be a domain generation algorithm. A query for a single label with no top level domain (TLD) will still resolve over the Internet, so the first type can be used for C&C. The first type is typical of a local client testing NFC. The Chrome browser performs this test to see how the local ISP handles NXDOMAIN errors, for instance.
- The first type is more likely to be a domain generation algorithm. A query for a single label with no top level domain (TLD) will still resolve over the Internet, so the first type can be used for C&C. The first type is typical of a local client testing FTP. The Chrome browser performs this test to see how the local ISP handles NXDOMAIN errors, for instance.
- The first type is more likely to be a domain generation algorithm. A query for a single label with no top level domain (TLD) will not resolve over the Internet, so the first type cannot be used for C&C. The first type is typical of a local client testing OSPF. The Chrome browser performs this test to see how the local ISP handles NXDOMAIN errors, for instance.

5.4

1. The Domain-based Message Authentication, Reporting, and Conformance (DMARC) framework ensures that Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) are being utilized effectively. It also provides a reporting mechanism. This is framework assures the most comprehensive spoofing mitigation for email services.

- True
- False

2. Records for Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) are all published to DNS servers.

- True
- False

3. Is any other type of server other than SMTP required to implement S/MIME?

- Secure/Multipurpose Internet Mail Extensions (S/MIME) requires a S/SMTP server.
- Secure/Multipurpose Internet Mail Extensions (S/MIME) requires a CA server.
- Secure/Multipurpose Internet Mail Extensions (S/MIME) requires a SFTP server.
- Secure/Multipurpose Internet Mail Extensions (S/MIME) requires a SMB server.

4. An endpoint protection platform (EPP) bundles a number of security functions— signature-based malware detection and IDS, firewall, encryption, and so on—into a single software agent managed by a single console. Endpoint detection and response (EDR) focuses on logging and alerting functions rather than prevention per se. The aim is to alert administrators to an intrusion and allow them to respond quickly. User and entity behavior analytics (UEBA) is a server-side process that applies machine learning generated algorithms to security data to identify malicious behaviors by user and device accounts.

- True
- False

5. What are the principal techniques for reverse assembling malware code?

- The binary machine code can be disassembled to assembly code and potentially decompiled to low-level pseudocode. Another technique is to extract strings from the process image.
- The binary machine code can be disassembled to assembly code and potentially decompiled to high-level pseudocode. Another technique is to extract strings from the process image.
- The ASCII code can be disassembled to assembly code and potentially decompiled to low-level pseudocode. Another technique is to extract strings from the process image.
- The ASCII code can be disassembled to assembly code and potentially decompiled to high-level pseudocode. Another technique is to extract strings from the process image.

6. You suspect that a host is infected with malware but cannot identify a suspect process using locally installed tools. What is your best course of action?

- Contain the host within a sandbox for further analysis. The best approach is to monitor the host for inbound network connection attempts. If the host connects to suspicious domains or IP address ranges, you can identify the process responsible.
- Leave the host connected to the network for further analysis. The best approach is to monitor the host for outbound network connection attempts. If the host attempts to connect to suspicious domains or IP address ranges, you can identify the process responsible.

- Leave the host connected to the network for further analysis. The best approach is to monitor the host for inbound network connection attempts. If the host connects to suspicious domains or IP address ranges, you can identify the process responsible.
- Contain the host within a sandbox for further analysis. The best approach is to monitor the host for outbound network connection attempts. If the host attempts to connect to suspicious domains or IP address ranges, you can identify the process responsible.

7. Which of the following processes would you NOT expect to be running under services.exe? Csrss.exe, Lsass.exe, Svchost.exe, SearchIndexer.exe, Spoolsv. exe.

- Csrss.exe and Lsass.exe
- Svchost.exe and Lsass.exe
- Csrss.exe and Searchindexer.exe
- Searchindexer.exe and Spoolsv.exe

5.5

1. What options are there for ingesting data from a unified threat management (UTM) appliance deployed on the network edge to a SIEM?

- If supported, you could deploy agent software against the UTM. If an agent is not supported, you can push data to the SIEM using a protocol such as syslog. In the latter case, you will still need to use a filter to parse and normalize the logs. Most SIEMs come with filters for the major appliance platforms, but if not supported directly, you will need to configure a custom filter.
- If supported, you could deploy agent software to the UTM. If an agent is not supported, you cannot push data to the SIEM using a protocol such as syslog. In the latter case, you will still need to use a filter to parse and normalize the logs. Most SIEMs come with filters for the major appliance platforms, but if not supported directly, you will need to configure a custom filter.
- If supported, you could deploy agent software to the UTM. If an agent is not supported, you can push data to the SIEM using a protocol such as syslog. In the latter case, you will negate the need for a filter to parse and normalize the logs. Most SIEMs come with filters for the major appliance platforms, but if not supported directly, you will need to configure a custom filter.
- If supported, you could deploy agent software to the UTM. If an agent is not supported, you can push data to the SIEM using a protocol such as syslog. In the latter case, you will still need to use a filter to parse and normalize the logs. Most SIEMs come with filters for the major appliance platforms, but if not supported directly, you will need to configure a custom filter.

2. When correlating an event timeline using a SIEM you need to validate that all log sources were synchronized to the same time source. you also need to account for any variations in time zone for the different sources.

- (●) True
- ( ) False

3. Because syslog messages have a PRI code, header, and message structure, but the format of messages is application-specific, syslog uses a standard format for all message content.

- ( ) True
- (●) False

4. Which default port do you need to allow on any internal firewalls to allow a host to send messages by syslog to a SIEM management server?

- ( ) The default port for syslog is UDP 541. If the syslog implementation is using reliable delivery, the default TCP port is 1468.
- ( ) The default port for syslog is UDP 541. If the syslog implementation is using reliable delivery, the default TCP port is 1648.
- ( ) The default port for syslog is UDP 514. If the syslog implementation is using reliable delivery, the default TCP port is 1648.
- (●) The default port for syslog is UDP 514. If the syslog implementation is using reliable delivery, the default TCP port is 1468.

5. What type of visualization is most suitable for identifying traffic spikes?

- ( ) A pie chart is a good way of showing changes in volume over time.
- ( ) A relational graph is a good way of showing changes in volume over time.
- (●) A line graph is a good way of showing changes in volume over time.
- ( ) A real-time graph is a good way of showing changes in volume over time.

6. You need to analyze the destination IP address and port number from some firewall data. The data in the iptables file is in the following format:

- ( ) DATE,FACILITY,CHAIN,IN,SRC,DST,LEN,TOS,PREC,TTL,ID,PR0T0,SPT,DPT Jan 11 05:33:59,lx1 kernel: iptables,INPUT,eth0, 10.1.0.102,10.1.0.1,52,0x00,0x00,128,2242,TCP,2564,21
- (●) DATE,FACILITY,CHAIN,IN,SRC,DST,LEN,TOS,PREC,TTL,ID,PROTO,SPT,DPT Jan 11 05:33:59,lx1 kernel: iptables,INPUT,eth0, 10.1.0.102,10.1.0.1,52,0x00,0x00,128,2242,TCP,2564,21

- DATE,CHAIN,FACILITY,IN,SRC,DST,LEN,TOS,PREC,TTL,ID,PROTO,SPT,DPT Jan 11 05:33:59,lx1 kernel: iptables,INPUT,eth0, 10.1.0.102,10.1.0.1,52,0x00,0x00,128,2242,TCP,2564,21
- DATE,FACILITY,CHAIN,IN,SRC,DST,TOS,LEN,PREC,TTL,ID,PROTO,SPT,DPT Jan 11 05:33:59,lx1 kernel: iptables,INPUT,eth0, 10.1.0.102,10.1.0.1,52,0x00,0x00,128,2242,TCP,2564,21

6.1

1. Which four phases outline the procedures involved in a forensics investigation?

- Identification, collection, analysis, and reporting.
- Identification, acquisition, analysis, and reporting.
- Identification, collection, processing, and reporting.
- Identification, collection, analysis, and dissemination.
- None of the above

2. Why might a forensics investigator need to be hired on a work product retention basis?

- To protect analysis of evidence from discovery to opposing counsel, should a court case be involved.
- To protect analysis of evidence from disclosure to a jury, should a court case be involved.
- To protect analysis of evidence from disclosure to supporting counsel, should a court case be involved.
- To protect analysis of evidence from disclosure to opposing counsel, should a court case be involved.
- None of the above

3. To preserve evidence of a temporary file system mounted to a host, which system device must you target first for evidence collection?

- System memory (RAM)
- Hard disk drives (HDD)
- Solid state drives (SSD)
- USB flash drive

4. You must contain a host that is suspected of effecting a violation of security policy. No methods of live evidence acquisition are available. What is your best course of action to preserve the integrity of evidence?

- Pull the plug to terminate processes.
- Use a software shut-down routine.
- Shutdown the computer by the switch on the power supply.
- Send a shutdown command to the machine using remote procedure protocol.
- None of the above

5. A hard disk has been removed from a computer so that it can be subjected to forensic evidence collection. What steps should you take to complete this process? Which of the following is the most correct answer?

- Ideally, record or document the process. Attach the disk to a workstation, using a write blocker to prevent contaminating the source-disk contents. Make a hash of the disk contents. Make an image of the disk contents. Make a cryptographic hash of the image and verify it matches the source disk hash. Make a copy of the image and validate with a cryptographic hash. Perform analysis on the copy of the image.
- Ideally, record or document the process. Attach the disk to a forensic workstation, using a write blocker to prevent contaminating the source-disk contents. Make a cryptographic hash of the disk contents. Make an image of the disk contents. Make a cryptographic hash of the image and verify it matches the source disk hash. Make a copy of the image and validate with a cryptographic hash. Perform analysis on the copy of the image.
- Ideally, record or document the process. Attach the disk to a forensic workstation, using a write blocker to prevent contaminating the source-disk contents. Make a hash of the disk contents. Make an image of the disk contents. Make a copy of the image and validate with a cryptographic hash. Perform analysis on the copy of the image.
- Ideally, record or document the process. Attach the disk to a forensic workstation, using a write blocker to prevent contaminating the source-disk contents. Make a cryptographic hash of the disk contents. Make an image of the disk contents. Make a cryptographic hash of the image and verify it matches the source disk hash. Make a copy of the image and validate with a cryptographic hash. Perform analysis on the image.

6. Unallocated space (clusters marked as free for use in file-write operations) and slack space (cluster portions that were not overwritten when a new file was created) are the two types of space on a disk that can be analyzed by file-carving tools?

- True
- False

7. Which network-related potential indicator of compromise has been omitted from the following list? Bandwidth consumption, irregular peer-to-peer communication, rogue device on the network, scan/sweep, unusual traffic spike, common protocol over non-standard port.

- (•) Beaconing
- ( ) C&C Signaling
- ( ) Out-of-band communications
- ( ) Excessive number of login attempts
- ( ) None of the above

8. Which two main classes of attack would you suspect if you observe a bandwidth consumption IoC from a client workstation on the local network to a host on the Internet?

- ( ) You are most likely to suspect a cross site scripting attack, but it is also possible that the host has been infected with a bot and is being used for DDoS or spam.
- ( ) You are most likely to suspect a worm attack, but it is also possible that the host has been infected with a bot and is being used for DDoS or spam.
- (•) You are most likely to suspect a data exfiltration attack, but it is also possible that the host has been infected with a bot and is being used for DDoS or spam.
- ( ) You are most likely to suspect a downgrade attack, but it is also possible that the host has been infected with a bot and is being used for DDoS or spam.
- ( ) None of the above

9. What steps would you take to investigate irregular peer-to-peer communication? Which of the following is the most correct answer?

- ( ) Start an incident response ticket and log all actions taken. Identify the sending IP address. On the internet, work out the identity of each host and the accounts and services running on them. On the LAN, use IP reputation services and geolocation to identify the host(s). Raise the logging and packet capture level to monitor the communications. Try to identify the traffic—if it contains sensitive data, consider closing the channel to prevent further release of information.
- ( ) Start an incident response ticket and log all actions taken. Identify the IP addresses involved. On the internet, work out the identity of each host and the accounts and services running on them. Also, on the Internet, use IP reputation services and geolocation to identify the host(s). Raise the logging and packet capture level to monitor the communications. Try to identify the traffic—if it contains sensitive data, consider closing the channel to prevent further release of information.
- (•) Start an incident response ticket and log all actions taken. Identify the IP addresses involved. On a LAN, work out the identity of each host and the accounts and services running on

them. On the Internet, use IP reputation services and geolocation to identify the host(s). Raise the logging and packet capture level to monitor the communications. Try to identify the traffic—if it contains sensitive data, consider closing the channel to prevent further release of information.

- Start an incident response ticket and log all actions taken. Identify the IP addresses involved. On a LAN, work out the identity of the sending hosts and the accounts and services running on them. On the Internet, use IP reputation services and geolocation to identify the host(s). Lower the logging and packet capture level to monitor the communications. Try to identify the traffic—if it contains sensitive data, consider closing the channel to prevent further release of information.

10. Your firewall log shows that the following packet was dropped—what application protocol was the sender trying to access?

- IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=172.16.0.192 DST=192.168.0.22 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=4018 DF PROTO=TCP SPT=2584 DPT=135 WINDOW=64240 RES=0x00 SYN URGP=0 The destination port (DPT) is 139, which is Microsoft Remote Procedure Call (RPC). This advertises what RPC services are available in a Windows environment.
- IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=172.16.0.192 DST=192.168.0.22 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=4018 DF PROTO=TCP SPT=2584 DPT=135 WINDOW=64240 RES=0x00 SYN URGP=0 The destination port (DPT) is 135, which is VNC. This advertises what VNC services are available in a Windows environment.
- IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=172.16.0.192 DST=192.168.0.22 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=4018 DF PROTO=TCP SPT=2584 DPT=135 WINDOW=64240 RES=0x00 SYN URGP=0 The destination port (DPT) is 135, which is Netbios-ssn. This advertises what RPC services are available in a Windows environment.
- IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=172.16.0.192 DST=192.168.0.22 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=4018 DF PROTO=TCP SPT=2584 DPT=135 WINDOW=64240 RES=0x00 SYN URGP=0 The destination port (DPT) is 135, which is Microsoft Remote Procedure Call (RDP). This advertises what rdp services are available in a Windows environment.
- None of the above

11. Your border firewall uses a default allow policy, but you want to block outgoing requests for UPnP. Which port do you need to create a deny rule for?

- UDP port 1900
- TCP port 1900
- UDP port 1800
- TCP port 1800

- None of the above

6.2

1. Why might a host-related IoC manifest as abnormal OS process behavior rather than as a malicious process?

- A malicious process is relatively easy to identify. Advanced malware disguises its presence using techniques such as process limiting and DLL injection/sideloading to compromise legitimate OS and application processes.
- A malicious process is relatively easy to identify. Advanced malware disguises its presence using techniques such as process filling and SQL injection/sideloading to compromise legitimate OS and application processes.
- A malicious process is relatively difficult to identify. Advanced malware disguises its presence using techniques such as process hollowing and SQL injection/side-banding to compromise legitimate OS and application processes.
- A malicious process is relatively difficult to identify. Advanced malware disguises its presence using techniques such as process filling and DLL injection/sideloading to compromise legitimate OS and application processes.
- None of the above

2. Reverse engineer the code used by processes, discover how processes are interacting with the file system (handles) and Registry, examine network connections, retrieve cryptographic keys, and extract interesting strings are types of evidence can be retrieved from system memory analysis?

- True
- False

3. Why are CPU, memory, and disk space consumption IoCs used to identify incidents? Which of the following is LEAST correct?

- Detailed analysis of processes and file systems is detailed and time-consuming work. Anomalous resource consumption is easier to detect and can be used to prioritize cases for investigation. Depending on the tools there is little risk of false positives.
- Detailed analysis of processes and file systems is detailed and time-consuming work. Anomalous resource consumption is more difficult to detect but can be used to prioritize cases for investigation. Depending on the tools there is little risk of false positives.
- Detailed analysis of processes and file systems is difficult and time-consuming work. Anomalous resource consumption is easier to detect and can be used to prioritize cases for investigation, though there is a substantial risk of numerous false positives.

- Detailed analysis of processes and file systems is difficult and time-consuming work. Anomalous resource consumption is more difficult to detect. Sideloading can be used to prioritize cases for investigation, though there is a substantial risk of numerous false positives.
- None of the above

4. You can audit applications that have been most recently used (MRU) and look for use of persistence mechanisms in the Run, RunOnce, and Services keys. Another common tactic for malware is to change file associations via the Registry. Evidence of SQL injections can be identified in the HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce. These are the main types of IoCs that can be identified through analysis of the Registry?

- True
- False

5. You are assisting an incident responder with an overview of application- related IoCs. One approach is to analyze network protocol response packets for unusual size and content. Another is to correlate error messages or unexplained string output in the application UI. Attacks may attempt to layer form controls or objects over the legitimate app controls. Finally, there may be obvious or subtle defacement attacks against websites and other public services. These are the only unexpected output indicators of intrusion events?

- True
- False

6. In the context of digital forensics, what is VMI?

- Virtual Machine Infrastructure
- Vulnerable Matrix Indicators
- Vulnerable Maintenance Inspection
- Virtual Machine Introspection
- None of the above

7. Regarding mobile device forensics, manual extraction refers to using the device's user interface (UI) to observe and record data and settings. Logical extraction refers to using standard export, backup, synchronization, and debug tools to retrieve data and settings.

- True
- False

6.3

1. You can audit applications that have been most recently used (MRU) and look for use of persistence mechanisms in the Run, RunOnce, and Services keys. Another common tactic for malware is to change file associations via the Registry.

- (●) True
- ( ) False

2. One approach is to analyze network protocol response packets for unusual size and content. Another is to correlate error messages or unexplained string output in the application UI. Attacks may attempt to layer form controls or objects over the legitimate app controls. Finally, there may be obvious or subtle defacement attacks against websites and other public services. These are all of the unexpected output indicators of intrusion events.

- ( ) True
- (●) False

3. Virtual Machine Introspection (VMI) is a set of tools, commonly implemented by the hypervisor, to allow querying of the VM state when the instance is running, including dumping the contents of system memory for analysis.

- (●) True
- ( ) False

4. Manual extraction refers to using the device's user interface (UI) to observe and record data and settings. Logical extraction refers to using standard export, backup, synchronization, and debug tools to retrieve data and settings.

- (●) True
- ( ) False

5. Use lower privilege accounts to support users over remote desktop operational control can be used to prevent the abuse of domain administrator accounts by pass-the-hash attacks?

- (●) True
- ( ) False

6. Log-on and credential use events in the Windows Security log for the local host and on the domain are the only sources of security data can be used to detect pass the hash and golden ticket attacks?

- (●) True
- ( ) False

7. 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?

- ( ) Vulnerability feeds
- (●) open source
- ( ) Closed source
- ( ) Proprietary

8. During the reconnaissance stage of a penetration test, Cynthia needs to gather information about the target organization's network infrastructure without causing an IPS to alert the target to her information gathering. Which of the following is her best option?

- (●) perform a DNS brute-force attack
- ( ) Use an nmap ping sweep
- ( ) Perform a DNS zone transfer
- ( ) Use an nmap stealth scan

9. 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?

- ( ) Timeliness
- ( ) Expense
- ( ) Relevance
- (●) Accuracy

10. What markup language provides a standard mechanism for describing attack patterns, malware, threat actors, and tools?

- TAXII
- XML
- OpenIOC
- STIX

11. A port scan of a remote system shows that port 3306 is open on a remote database server. What database is the server most likely running?

- Oracle
- MySQL
- Postgress
- Microsoft SQL

12. 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)?

- Hacktivist
- Insider
- Organized crime
- Nation-State

13. Charles is working with leaders of his organization to determine the types of information that should be gathered in his new threat intelligence program. In what phase of the intelligence cycle is he participating?

- Dissemination
- Requirements
- Feedback
- Analysis

14. As Charles develops his threat intelligence program, he creates and shares threat reports with relevant technologists and leaders. What phase of the intelligence cycle is now occurring?

- Feedback

- Dissemination
- Collection
- Requirements

15. What term is used to describe the groups of related organizations who pool resources to share cybersecurity threat information and analyses?

- SOC
- CERT
- ISAC
- CIRT

16. Which one of the following threats is the most pervasive in modern computing environments?

- Advanced persistent threats
- Commodity hardware
- Zero-day attacks
- Insider threats

17. 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?

- Open source
- Behavioral
- Reputational
- Indicator of compromise

6.4

1. It is necessary to include marketing stakeholders in the incident response process because data breaches can cause lasting reputational damage, so communicating failures sensitively to the media and the wider public and protecting the company's brand is important.

- True

- ○ False

2. During a serious event, the essential point is to assume that internal communication channels might be compromised. Third-party messaging products with end-to-end encryption should be secure enough for most institutions, but those processing extremely sensitive information might require the use of bespoke products.

- ◉ True
- ○ False

3. What is PHI?

- ○ Proprietary Health Information (PHI)
- ○ Public Health Information (PHI)
- ○ Private Health Information (PHI)
- ◉ Protected Health Information (PHI)

4. Which class of data criticality factor has been omitted from the following list? PII, PHI, SPI, IP, financial and corporate information.

- ○ Heightened variable asset (HVA)
- ◉ High value asset (HVA)
- ○ High value attribute (HVA)
- ○ High volatility asset (HVA)

5. What is a CoA matrix?

- ○ A cost of action (CoA) matrix maps the controls available for each type of function to adversary tools and tactics.
- ○ A continuous offensive action (CoA) matrix maps the controls available for each type of function to adversary tools and tactics.
- ○ A corporate objective activity (CoA) matrix maps the controls available for each type of function to adversary tools and tactics.
- ◉ A course of action (CoA) matrix maps the controls available for each type of function to adversary tools and tactics.

6. Which two factors affecting severity level classification have been omitted from the following list? Downtime, detection time, data integrity, economic, system process criticality, reverse engineering.

- Data correction means combining locally observed indicators with cyber-threat intelligence (CTI) to identify adversary capabilities and motivations. Recovery time should be considered independently of downtime as complex systems may require lengthy work to fully remediate and protect against future attacks.
- Data correlation means combining locally observed indicators with cyber-threat intelligence (CTI) to identify adversary capabilities and motivations. Recovery time should be considered independently of downtime as complex systems may require lengthy work to fully remediate and protect against future attacks.
- Data connectivity means combining locally observed indicators with cyber-threat intelligence (CTI) to identify adversary capabilities and motivations. Recovery time should be considered independently of downtime as complex systems may require lengthy work to fully remediate and protect against future attacks.

7. You are explaining containment techniques to a junior analyst. What distinction can you make between isolation-based and segmentation-based containment? Which answer is the most correct?

- The terms are often used interchangeably, but segmentation is a network-specific method of containment that uses virtual LANs (VLAN), routing/subnets, VMs, and firewalls to restrict a host or group of hosts to an isolated network segment. This might be used as a sandbox or honeynet to perform further analysis. Isolation is any method of allowing a suspect host, account, or app from communicating with other hosts, including powering it off, pulling its network cable, and so on.
- The terms are often used interchangeably, but segmentation is a network-specific method of containment that uses virtual LANs (VLAN), routing/subnets, taps, and firewalls to allow a host or group of hosts to an isolated network segment. This might be used as a sandbox or honeynet to perform further analysis. Isolation is any method of allowing a suspect host, account, or app from communicating with other hosts, including powering it off, pulling its network cable, and so on.
- The terms are often used interchangeably, but segmentation is a network-specific method of containment that uses virtual LANs (VLAN), routing/subnets, IDS, and firewalls to restrict a host or group of hosts to an isolated network segment. This might be used as a sandbox or honeynet to perform further analysis. Isolation is any method of preventing a suspect host, account, or app from communicating with other hosts, including powering it off, pulling its network cable, and so on.
- The terms are often used interchangeably, but segmentation is a network-specific method of containment that uses virtual LANs (VLAN), routing/subnets, SIEMs, and firewalls to allow a host or group of hosts to an isolated network segment. This might be used as a sandbox or honeynet to perform further analysis. Isolation is any method of preventing a suspect host, account, or app from communicating with other hosts, including powering it off, pulling its network cable, and so on.

8. Your SIEM has alerted you to ongoing scanning activity directed against workstations and servers. The host intrusion detection on each target has blocked access to the source IP automatically. What are your options and considerations for investigating this incident? Which answer is least wrong?

- You will want to identify the actor behind the scanning attempts, possibly without alerting him or her to the fact that he/she has been discovered. Log the incident and initiate a confidential response process. Gather information about the source IP and how it has been compromised. Verify that no successful exploits have been launched against critical systems. Identify the insider threat actor. If you require additional evidence, consider using a honeypot to draw the attacker out. Ensure heightened monitoring across the network.
- You will want to identify the actor behind the scanning attempts, possibly without alerting him or her to the fact that he/she has been discovered. Log the incident and initiate a confidential response process. Gather information about the source IP and how it has been compromised. Verify that no successful exploits have been launched against critical systems. If you require additional evidence, consider using sensitive corporate data to draw the attacker out. Ensure heightened monitoring across the network.
- You will want to identify the actor behind the scanning attempts, possibly without alerting him or her to the fact that he/she has been discovered. Log the incident and initiate a confidential response process. Gather information about the source IP and how it has been compromised. Verify that no successful exploits have been launched against critical systems. If you require additional evidence, consider using a honeypot to draw the attacker out. Disable monitoring across the network to ensure the attacker is not alerted to your suspicions.
- You will want to identify the actor behind the scanning attempts, possibly without alerting him or her to the fact that he/she has been discovered. Log the incident and initiate a confidential response process. Gather information about the source IP and how it has been compromised. Verify that no successful exploits have been launched against critical systems. If you require additional evidence, consider using a honeypot to draw the attacker out. Ensure heightened monitoring across the network.

6.5

1. Vulnerability mitigation, reconstruction/reimaging, secure disposal, patching, sanitization, restoration of services, restoration of permissions, restoration of capabilities and services are the methods to restoration.

- True
- False

2. Evidence retention, lessons-learned report, change control process, incident summary report, indicator of compromise (IoC) generation, monitoring constitute the format for making the complete incident report.

- True
- False

3. A summary report is a technical report designed for internal use with a view to improving incident response processes. An lessons-learned report is designed for distribution to stakeholders to provide reassurance that the incident has been properly handled.

- ○ True
- ◉ False

4. While reviewing network flow logs, John sees that network flow on a particular segment suddenly dropped to zero. What is the most likely cause of this?

- ○ A denial-of-service attack
- ○ High bandwidth consumption
- ◉ A link failure
- ○ Beaconing

5. Charlotte is having a dispute with a coworker over access to information contained in a database maintained by her coworker's department. Charlotte insists that she needs the information to carry out her job responsibilities, whereas the coworker insists that nobody outside the department is allowed to access the information. Charlotte does not agree that the other department should be able to make this decision, and Charlotte's supervisor agrees with her. What type of policy could Charlotte turn to for the most applicable guidance?

- ○ Data classification policy
- ◉ Data ownership policy
- ○ Data retention policy
- ○ Acceptable use policy

6. Saanvi is conducting the recovery process after his organization experienced a security incident. During that process, he plans to apply patches to all of the systems in his environment. Which one of the following should be his highest priority for patching?

- ○ Windows systems
- ○ Linux systems
- ◉ Systems involved in the incident
- ○ Web servers

7. Susan's organization suffered from a major breach that was attributed to an advanced persistent threat (APT) that used exploits of zero-day vulnerabilities to gain control of systems on her company's network. Which of the following is the least appropriate solution for Susan to recommend to help prevent future attacks of this type?

- Heuristic attack detection
- Signature-based attack detection
- Segmentation
- Leverage threat intelligence

8. During his investigation of a Windows system, Eric discovered that files were deleted and wants to determine whether a specific file previously existed on the computer. Which of the following is the least likely to be a potential location to discover evidence supporting that theory?

- Windows registry
- Master File Table
- INDX files
- Event logs

9. As part of her duties as an SOC analyst, Emily is tasked with monitoring intrusion detection sensors that cover her employer's corporate headquarters network. During her shift, Emily's IDS alarms report that a network scan has occurred from a system with IP address 10.0.11.19 on the organization's WPA2 Enterprise wireless network aimed at systems in the finance division. What data source should she check first?

- Wireless authentication logs
- Host firewall logs
- AD authentication logs
- WAF logs

10. Casey's incident response process leads her to a production server that must stay online for her company's business to remain operational. What method should she use to capture the data she needs?

- Live image to an external drive.
- Live image to the system's primary drive.
- Take the system offline and image to an external drive.

- Take the system offline, install a write blocker on the system's primary drive, and then image it to an external drive.

11. During a routine upgrade, Maria inadvertently changes the permissions to a critical directory, causing an outage of her organization's RADIUS infrastructure. How should this threat be categorized using NIST's threat categories?

- Accidental
- Adversarial
- Structural
- Environmental

12. What does the nmap response “filtered” mean in port scan results?

- A firewall was detected.
- An IPS was detected.
- There is no application listening, but there may be one at any time.
- nmap cannot tell whether the port is open or closed.

13. Darcy is the security administrator for a hospital that operates in the United States and is subject to the Health Insurance Portability and Accountability Act (HIPAA). She is designing a vulnerability scanning program for the hospital's datacenter that stores and processes electronic protected health information (ePHI). What is the minimum scanning frequency for this environment, assuming that the scan shows no critical vulnerabilities?

- Every 30 days
- Every 90 days
- Every 180 days
- No scanning is required.

7.1

1. Your company is being targeted by a hacktivist group who are launching a DDoS attack against your e-commerce portal on a random day each month throughout the year. The portal generates $500,000 dollars each month and each attack reduces revenue by 10%. What is the annual loss expectancy of this malicious activity? What use is the ALE in determining selection of security controls?

- The single loss expectancy is the asset value ($500,000) multiplied by the exposure factor (10%), so $50,000. The ALE is $50,000*12 or $600,000. The ALE sets a budget for security control selection. For example, if you contract with a DDoS mitigation cloud provider at a cost of $100,000 per year and that reduces the exposure factor to 2%, you will have not achieved a reasonable return on security investment (ROSI).
- The single loss expectancy is the asset value ($500,000) multiplied by the exposure factor (10%), so $50,000. The ALE is $50,000*12 or $600,000. The ALE sets a budget for security control selection. For example, if you contract with a DDoS mitigation cloud provider at a cost of $100,000 per year and that reduces the exposure factor to 12%, you will have not achieved a reasonable return on security investment (ROSI).
- The single loss expectancy is the asset value ($500,000) multiplied by the exposure factor (10%), so $50,000. The ALE is $50,000*12 or $600,000. The ALE sets a budget for security control selection. For example, if you contract with a DDoS mitigation cloud provider at a cost of $100,000 per year and that reduces the exposure factor to 12%, you will have achieved a reasonable return on security investment (ROSI).
- The single loss expectancy is the asset value ($500,000) multiplied by the exposure factor (10%), so $50,000. The ALE is $50,000*12 or $600,000. The ALE sets a budget for security control selection. For example, if you contract with a DDoS mitigation cloud provider at a cost of $100,000 per year and that reduces the exposure factor to 2%, you will have achieved a reasonable return on security investment (ROSI).

2. The role of the blue team during a pen test is to operate the security system to detect and repel the intrusion.

- True
- False

3. True or false? Most pen tests should be defined with an open-ended scope to maximize the chance of detecting vulnerabilities.

- True
- False

4. What is a maturity model?

- A statement of how under-developed a system or business process (such as security assurance) is. Most maturity models progress in tiers from a naïve state to one where the organization demonstrates best practice and can assist other organizations in their development.
- A statement of how under-developed a system or business process (such as security assurance) is. Most maturity models progress in tiers from a intelligent state to one where the

organization demonstrates best practice and can assist other organizations in their development.

- A statement of how well-developed a system or business process (such as security assurance) is. Most maturity models progress in tiers from a intelligent state to one where the organization demonstrates best practice and can assist other organizations in their development.
- A statement of how well-developed a system or business process (such as security assurance) is. Most maturity models progress in tiers from a naïve state to one where the organization demonstrates best practice and can assist other organizations in their development.

5. Which type of framework allows greater local factors to have more influence over security control selection?

- A prescriptive-based framework encourages a bottom-up approach to control selection, driven by internal risk assessments. Prescriptive frameworks impose top-down selection of mandatory controls.
- A analytical-based framework encourages a bottom-up approach to control selection, driven by internal risk assessments. Prescriptive frameworks impose top-down selection of mandatory controls.
- A outcomes-based framework encourages a bottom-up approach to control selection, driven by internal risk assessments. Prescriptive frameworks impose top-down selection of mandatory controls.
- A risk-based framework encourages a bottom-up approach to control selection, driven by internal risk assessments. Prescriptive frameworks impose top-down selection of mandatory controls.

6. An evaluation is typically a very formal process completed against some sort of externally developed or enforced standard or framework. An audit is a less methodical process that is more dependent on the judgement of the evaluator.

- True
- False

7. Framework Profile part of the NIST Cybersecurity Framework is used to provide a statement of current cybersecurity outcomes?

- True
- False

7.2

1. Describe one advantage and one disadvantage of using the -T0 (Tee-Zero) switch when performing an Nmap scan.

- This sets an extremely short delay between probes, which may help to evade detection systems but will take a very short time to return results.
- This sets an extremely high delay between probes, which may help to evade detection systems but will take a very long time to return results.
- This sets an extremely short delay between probes, which may help to evade detection systems but will take a very short time to return results.
- This sets an extremely high delay between probes, which may help to evade detection systems but will take a very long time to return results.

2. UDP does not send ACK messages so the scan must use timeouts to interpret the port state. This makes scanning a wide range of UDP ports a lengthy process.

- True
- False

3. True or false? A port that is reported as "closed" by Nmap is likely to be one protected by a firewall.

- True
- False

4. What is the function of the -A switch in Nmap?

- Performs service redirection (verify that the packets delivered over a port correspond to the "well known" protocol associated with that port) and version detection (using the scripts marked "default").
- Performs service detection (verify that the packets delivered over a port correspond to the "well known" protocol associated with that port) and version detection (using the scripts marked "default").
- Performs service multicast (verify that the packets delivered over a port correspond to the "well known" protocol associated with that port) and version detection (using the scripts marked "default").
- Performs service stealth mode sweep (verify that the packets delivered over a port correspond to the "well known" protocol associated with that port) and version detection (using the scripts marked "default").

5. You can run a specific Nmap script or category of scripts by using the --script argument with the script name or path or category name.

- (•) True
- ( ) False

6. What is the advantage of the Nmap "grepable" output format?

- ( ) grep is a Linux command for running a irregular expression to search for a particular string. Nmap's grepable output is less resources intensive for this tool to parse.
- ( ) grep is a Linux command for running regular strings to search for a particular string. Nmap's grepable output is easier for this tool to parse.
- (•) grep is a Linux command for running a regular expression to search for a particular string. Nmap's grepable output is easier for this tool to parse.
- ( ) grep is a Linux command for running a regular expression to search for a particular string. Nmap's grepable output is more difficult for this tool to parse but it makes interpreting the output much simpler.

7. Packet injection is using software to write packets directly to the network stream, often to spoof or disrupt legitimate traffic.

- (•) True
- ( ) False

8. Analyze business processes and identify the ones that the business could not afford not to run is the best way to differentiate between critical assets distinguish non-critical from critical systems.

- (•) True
- ( ) False

9. The scan scope is configured by specifying a target IP address or IP address range.

- (•) True
- ( ) False

10. What type of vulnerability scanning is being performed if the scanner sniffs traffic passing over the local segment?

- Pervasive scanning
- Passive scanning
- Procursive scanning
- Predictive scanning

11. Scanning causes negligible system instability and consumes little network bandwidth. It is best performed when the network is heavily utilized or when the target systems are performing critical tasks in order to improve the accuracy of the results.

- True
- False

12. In regards to vulnerability management, an update refers to vulnerability patches in Tenable Nessus. A vulnerability feed contains information about known exploits and required security patches.

- True
- False

13. How does the regulatory environment affect vulnerability scanning?

- The regulator might require on the number of scans and scan level to remain compliant.
- The regulator might impose requirements on types of scans and scan frequency to remain compliant.
- The regulator will impose legal sanctions on your organization if certain types of scans and scan frequency are not met.
- The regulator, in an effort to determine maturity, might require you to run a Nmap -T0 to test you IDS capabilities.

7.3

1. Common Platform Enumeration (CPE) is a standardized way of referring to OS and application software and hardware appliances, maintained by NIST.

- True

- False

2. Does a CVSS score of 9.1 represent a critical vulnerability or a low-priority finding?

- Critical vulnerability
- Moderate vulnerability
- Zero vulnerability
- Intermediate vulnerability

3. Which CVSS base metric has been omitted from the following list? Access vector, access complexity, privileges required, scope, confidentiality, integrity, availability.

- User integration—Whether an exploit of the vulnerability depends on some local user action, such as executing a file attachment.
- User interoperability—Whether an exploit of the vulnerability depends on some local user action, such as executing a file attachment.
- User inter-ability—Whether an exploit of the vulnerability depends on some local user action, such as executing a file attachment.
- User interaction—Whether an exploit of the vulnerability depends on some local user action, such as executing a file attachment.

4. What can you do to reduce a high number of false positives returned when performing vulnerability scanning?

- Remove non-applicable vulnerabilities from the scan, update heuristics baselines, create exceptions, and run credentialed scans.
- Remove applicable vulnerabilities from the scan, update heuristics baselines, create exploits to run uncredentialled scans.
- Remove applicable vulnerabilities from the scan, revert to earlier heuristics baselines, create exploits to run uncredentialled scans.
- Remove non-applicable vulnerabilities from the scan, revert to earlier heuristics baselines, create exceptions, and run credentialed scans.

5. Repeat the scan (possibly using a different scanner), review logs and other data sources, and compare to compliance or configuration baselines. Run a differential backup to encrypt the the scan logs. You might also attempt to actively exploit a vulnerability using pen testing. These are some methods you can use to validate the results of a vulnerability scan.

- True
- False

6. The Qualys infrastructure vulnerability management engine is only available as a cloud service.

- True
- False

7. A mission essential function relies on a server running an unsupported OS, which can no longer be patched. The system can only be accessed from a hardened jump box management station and is physically stored in a lockable cabinet with CCTV monitoring. What type of remediation has been applied in this scenario?

- This is a combination of risk avoidance with compensating controls.
- This is a combination of risk acceptance with compensating controls.
- This is a combination of risk acceptance with competitive controls.
- This is a combination of risk avoidance with commandeering controls.

8. Which security controls support hardening?

- Hardening depends on configuration guidelines so that any necessary ports, services, and interfaces can be enabled and appropriate settings and permissions applied to software and the file system. Patch management procedures and endpoint security products are of less importance if system hardening protocols are in place.
- Hardening depends on configuration baselines so that any unnecessary ports, services, and interfaces can be disabled and appropriate settings and permissions applied to software and the file system. Effective patch management procedures and endpoint security products are also important.
- Hardening depends on configuration baselines so that any unnecessary ports, services, and interactions can be disabled and appropriate settings and permissions applied to software and the file system. Effective patch management procedures and endpoint security products are also important.
- Hardening depends on configuration baselines so that any unnecessary ports, services, and interoperabilities can be disabled and appropriate settings and permissions applied to software and the file system. Patch management procedures and endpoint security products are of less importance if system hardening protocols are in place.

9. Which inhibitor to remediation has been omitted from the following list? Memorandum of understanding (MoU), service level agreement (SLA), organizational governance, business process interruption, degrading functionality, proprietary systems.

- Actively supported proprietary system
- Legacy system
- Printer and fax scanning and spooling system
- Critical system

10. Why might an SLA be a barrier to remediating a vulnerability?

- A service level agreement (SLA) is likely to specify minimum downtime periods or maximum uptime guarantees. If remediating the vulnerability will cause downtime, the SLA may be breached. Also, maintenance windows might restrict the timing of service intervals. It is required to agree to exceptions in the SLA so that critical vulnerabilities can be patched promptly.
- A service level agreement (SLA) is likely to specify minimum downtime periods or maximum uptime guarantees. If remediating the vulnerability will cause downtime, the SLA may be breached. Also, maintenance windows might allow the timing of service intervals. It is required to agree to exceptions in the SLA so that critical vulnerabilities can be patched promptly.
- A service level agreement (SLA) is likely to specify maximum downtime periods or minimum uptime guarantees. If remediating the vulnerability will cause downtime, the SLA may be breached. Also, maintenance windows might allow the timing of service intervals. It is best to agree to exceptions in the SLA so that critical vulnerabilities can be patched promptly.
- A service level agreement (SLA) is likely to specify maximum downtime periods or minimum uptime guarantees. If remediating the vulnerability will cause downtime, the SLA may be breached. Also, maintenance windows might restrict the timing of service intervals. It is best to agree to exceptions in the SLA so that critical vulnerabilities can be patched promptly.

7.4

1. Public key infrastructure (PKI) cryptography—issuing hosts and signing executable code with digital certificates are mechanisms that can be used to prove the identity of hosts and software applications.

- True
- False

2. You are devising a password policy that is compliant with NIST 800-63b guidelines. Which factors for employee password creation are most important to enforce through system rules?

- Prevent the use of dictionary words and repetitive strings, and set a minimum length of at least thirty-two characters. The use of complexity rules (required use of mixed case, symbols, and so on) is detrimental.
- Prevent the use of dictionary words and repetitive strings, and set a minimum length of at least sixteen characters. The use of complexity rules (required use of mixed case, symbols, and so on) is depreciated.
- Prevent the use of dictionary words and repetitive strings, and set a minimum length of at least twenty-four characters. The use of complexity rules (required use of mixed case, symbols, and so on) is downgraded.
- Prevent the use of dictionary words and repetitive strings, and set a minimum length of at least eight characters. The use of complexity rules (required use of mixed case, symbols, and so on) is deprecated.

3. What administrative control(s) will best reduce the impact of an attack where a user gains control over an administrator's account?

- Ensure accounts are configured with the user-required privileges. This makes it less likely that a "root" or "domain admin" account will be compromised. Use logging and separation of duties to detect intrusions.
- Ensure accounts are configured with the user-requested privileges. This makes it less likely that a "root" or "domain admin" account will be compromised. Use logging and separation of duties to detect intrusions.
- Ensure accounts are configured with the user-recommended privileges. This makes it less likely that a "root" or "domain admin" account will be compromised. Use logging and separation of duties to detect intrusions.
- Ensure accounts are configured with the least privileges necessary. This makes it less likely that a "root" or "domain admin" account will be compromised. Use logging and separation of duties to detect intrusions.

4. If unauthorized access is suspected but has not been flagged by SIEM (discover and eliminate false negatives) a manual review of authentication logs should be required as part of reviewing security architecture.

- True
- False

5. In the context of federated identity management, what is automated provisioning?

- Using an administrator to communicate changes in account status and authorizations between systems rather than having software intervene to do it manually.

- Using an administrator to communicate changes in account status and authorizations between systems rather than having software intervene to do it automatically.
- Using software to communicate changes in account status and authorizations between systems rather than having an administrator intervene to do it manually.
- Using software to communicate changes in account status and authorizations between systems rather than having an administrator intervene to do it automatically.

6. A telecommunication acceptable use policy might include or supplement a BYOD policy.

- True
- False

7. You are advising a small company on cybersecurity. Employees have formed the habit of bringing personal devices into the workplace and attaching them to the network, which has been the cause of several security incidents. As a small company, authorized IT devices are drawn from a wide range of makes and models, making identification of rogue devices difficult. What solution do you suggest to make inspection of the IT infrastructure simpler?

- Use asset tagging to identify unauthorized devices. This will also assist the company in building an inventory of assets and ensuring more effective configuration and change management.
- Use asset tagging to identify unauthorized devices. This might also assist the company in building an inventory of assets and ensuring more effective configuration and change management.
- Use asset tagging to identify authorized devices. This will likely assist the company in building an inventory of assets and ensuring more effective configuration and change management.
- Use asset tagging to identify authorized devices. This will also assist the company in building an inventory of assets and ensuring more effective configuration and change management.

8. You want to provide controlled remote access to the remote administration interfaces of multiple servers hosted on a private cloud. Installing a jumpbox as a single point of entry for administration of servers within the cloud is the best choice for this requirement.

- True
- False

9. Which network architecture security solution for infrastructure management has been omitted from the following list, and what is its purpose? Physical, software-defined, virtual private cloud, serverless.

- Remote access virtual private networks (VPN) allow hosts on an external network to connect to resources on the local network over a public network, such as the Intranet. Use of VPN ports and remote dial-in privileges need to be subject to authentication and accounting mechanisms. VPNs always allow secure traffic between hosts and between sites.
- Remote access virtual private networks (VPN) allow hosts on an external network to connect to resources on the local network over a public network, such as the Internet. Because it is a VPN, user accounts are already authenticated and privileges authorized. VPNs can also be used to secure traffic between hosts and between sites.
- Remote access virtual private networks (VPN) allow hosts on an external network to connect to resources on the local network over a public network, such as the Internet. Because it is a VPN, user accounts are already authenticated and privileges authorized. VPNs always allow secure traffic between hosts and between sites.
- Remote access virtual private networks (VPN) allow hosts on an external network to connect to resources on the local network over a public network, such as the Internet. Use of VPN ports and remote dial-in privileges need to be subject to authentication and accounting mechanisms. VPNs can also be used to secure traffic between hosts and between sites.

10. Your company is developing a learning management system (LMS) app for provision as a hosted system to multiple clients. It is important that each customer's data be segmented from other instances. Which infrastructure security solution is a good choice to meet the requirements of this scenario? Which is the most correct?

- You could deploy each customer's instance as a separate virtual machine (VM). This should not involve additional resources and management.
- Containerization is adequate for the requirement to deploy a single application within an isolated cell.
- Segmentation is the best choice because of the increased network traffic.
- You could deploy each VM instance on-premise to ensure successful implementation and LMS access.

11. An air gap is the best type of system isolation that ensures that the host is physically disconnected from any network?

- True
- False

7.5

1. You are working for a small company. The owner wants to replace a server with a second-hand device sourced from an eBay vendor. You caution that the lack of vendor due diligence means there is some risk from this approach. The business owner retorts that the savings are well worth the minimal risk. The reality is that firmware-based exploits are relatively difficult to develop, so the owner is probably correct that there is little risk of a small company such as yours being targeted. That said, any larger companies that your firm contracts may take a different view. You can mitigate the risk by ensuring that the firmware is replaced and all disks sanitized before the server is put into production.

- (●) True
- ( ) False

2. The difference between a secure and measured boot is that a measured boot checks that the OS has a valid digital signature from a trusted OS vendor. Secure boot transmits an attestation report of key boot metrics and logs to a server for validation.

- ( ) True
- (●) False

3. What requirements must be met for an app to make use of a secure enclave? Which is the most correct answer?

- ( ) There must be RAM support for security extensions and the app developer must have obtained a digital signature from the RAM vendor.
- ( ) There must be RAM support for security extensions, the host must be running a trusted OS, and the app developer must have obtained a digital signature from the RAM vendor.
- ( ) There must be CPU support for security extensions and the host must be running a trusted OS.
- (●) There must be CPU support for security extensions, the host must be running a trusted OS, and the app developer must have obtained a digital signature from the computer manufacturer.

4. The dedicated nature of an RTOS makes it less susceptible to software-based exploits to perform remote code execution.

- ( ) True
- (●) False

5. The following are CAN bus attack vectors: A controller area network (CAN) bus is often implemented with no segmentation, making any connectivity channel a potential vector. Remote access can be accomplished over a cellular or Wi-Fi connection. Local access can be made via the OBD-II port. The media system may also support the attachment of mobile devices via USB or Apple Lightning connector. A secure boot TPM is vulnerable to attack by malicious firmware.

- ○ True
- ◉ False

6. Which network protocol is associated with SCADA and other OT networks? Which is the most correct answer?

- ○ Podbus. You might also mention EtherNet - TCP/IP, a variant of the Common Industrial Protocol, Distributed Network Protocol (DNP1), and Honeywell S4comms.
- ○ LANbus. You might also mention EtherNet/IP, a variant of the Common Industrial Protocol, Distributed Network Protocol (DNP2), and 3M S6comms.
- ◉ Bodbus. You might also mention EtherNet/IP, a variant of the Common Industrial Protocol, Distributed Network Protocol (DNP3), and Siemens S7comms.
- ○ WANbus. You might also mention EtherCap/IP, a variant of the Common Industrial Protocol, Distributed Network Protocol (DNP4), and Phillips S5comms.

7. What is a PACS?

- ○ A permission accessory control system (PACS) is a network of monitored locks, intruder alarms, and video surveillance.
- ◉ A physical access control system (PACS) is a network of monitored locks, intruder alarms, and video surveillance.
- ○ A persistent asset control system (PACS) is a network of monitored locks, intruder alarms, and video surveillance.
- ○ A partial access controller system (PACS) is a network of monitored locks, intruder alarms, and video surveillance.

8.1

1. True or false? Public information, information you could search for online, phone numbers, addresses, court documents, and other public record documents have no need for additional security attributes besides protecting access to the data by username and password.

- ○ True
- ◉ False

2. Which two non-technical controls for data privacy and protection have been omitted from the following list? Classification, ownership, retention, data types, retention standards, confidentiality, legal requirements, data minimization, non-disclosure agreement (NDA).

- ○ Data solvency refers to a jurisdiction preventing or restricting processing and storage from taking place on systems do not physically reside within that jurisdiction. Purpose integration means that private/personal can only be collected for a defined purpose to which the data subject gives explicit consent.
- ○ Data solitude refers to a jurisdiction preventing or restricting processing and storage from taking place on systems do not physically reside within that jurisdiction. Purpose inspection means that private/personal can only be collected for a defined purpose to which the data subject gives explicit consent.
- ○ Data solution refers to a jurisdiction preventing or restricting processing and storage from taking place on systems do not physically reside within that jurisdiction. Purpose litigation means that private/personal can only be collected for a defined purpose to which the data subject gives explicit consent.
- ◉ Data sovereignty refers to a jurisdiction preventing or restricting processing and storage from taking place on systems do not physically reside within that jurisdiction. Purpose limitation means that private/personal can only be collected for a defined purpose to which the data subject gives explicit consent.

3. An Exact Data Match (EDM) is a database of strings of actual private data converted to fingerprints through a hash process. A data loss prevention (DLP) policy enforcer can match these fingerprints in user documents and messages and take the appropriate enforcement action. Annualized Loss Expectancy (ALE) will improve when using EDM.

- ◉ True
- ○ False

4. What is the effect of the following command: chmod 644 sql.log

- chmod 644 sql.log sets write permission for the owner and read and write permission for group and world on the file sql.log.
- chmod 644 sql.log sets read and write permission for the owner and read permission for group and world on the file sql.log.
- chmod 644 sql.log sets read and execute permission for the owner and read and write permission for group and read-only world on the file sql.log.
- chmod 644 sql.log sets read, write and execute permission for the owner and read-only permission for group and no permissions for the world on the file sql.log.

5. What is the process for reidentifying tokenized data?

- Use the token server to look up the tenable value of the token.
- Use the token server to look up the IV value of the token.
- Use the token server to look up the original value of the token.
- Use the token server to look up the plain-text value of the token.

8.2

1. How can security issues be incorporated within the planning phase of an SDLC?

- Perform web app pentests regularly
- Train developers and testers in security issues, acquire security analysis tools, and ensure the security of the development environment.
- Do not allow developers admin priviledges
- SDLC is not necessary for secure application development

2. What is horizontal privilege escalation?

- When a user obtains access to resources at the same level of privilege but from a different domain. For example, a user in sales accessing data files restricted to use by the accounting department.
- When a user obtains access to resources at a higher level of privilege but from a different domain. For example gaining admin privileges from a user account stand point
- When a user removes access from another user.
- None of the above

3. What type of code exploit must malware make to install a rootkit with ring 0 privileges?

- It must exploit OS level processes
- It must exploit network protocols
- It must exploit a kernel-mode OS process, driver, or firmware
- It must exploit email server user accounts

4. What type of overflow attack is most likely to lead to arbitrary/remote code execution?

- Most attacks target vulnerabilities that occur in functions using stack buffers, especially in applications written in Python
- Most attacks target vulnerabilities that occur in functions using stack buffers, especially in applications written in C and C++.
- Most attacks target vulnerabilities that occur in functions using stack buffers, especially in applications written in Swift
- Most attacks target vulnerabilities that occur in functions using stack buffers, especially in applications written in HTML and Javascript

5. What is TOCTTOU?

- A time of check to time of use (TOCTTOU) is a type of race condition. It refers to a change in a resource between the time an app checks the resource and subsequently makes use of it.
- A time of check to time of use (TOCTTOU) is a type of integer overflow that is based on time values.
- A time of check to time of use (TOCTTOU) is an error with Network Time Protocol
- None of the above

6. Which class of software vulnerability has been omitted from the following list: Improper error handling, dereferencing, insecure object reference, race condition, broken authentication, sensitive data exposure, insecure components, weak or default configurations, use of insecure functions.

- Black Box
- White Box
- Insufficient logging and monitoring.
- Grey Box

7. What type of attack is being performed by the code shown below? http://www.target.foo/language.php?region=../../ phpinfo.php

- Directory transversal
- This is targeting a local file inclusion (LFI) vulnerability, where the web app allows the return of arbitrary files from the local file system.
- This is targeting a remote file inclusion (RFI) vulnerability, where the web app allows the return of arbitrary files from a remote file system.
- None of the above

8. What is a horizontal brute force attack?

- When an attacker tries to traverse through a network using various network attacks
- When an attacker is spoofing their IP address until one is listed as a valid whitelisted IP address on the network
- When an attacker is scanning a website with gobuster or dirbuster to try and find directories that are not meant to be accessed
- Password spraying refers to selecting obvious passwords and attempting them against multiple user names. This circumvents the account lockout policies that defeat attempts to brute force a password. Another technique is credential stuffing, which means testing username and password combinations against multiple sites.

9. Which secure coding best practice has been omitted from the following list? Input validation, output encoding, session management, authentication, data protection.

- Parameterized queries
- Encryption
- Hashing
- Obfuscation

10. Which secure coding technique(s) can be used to mitigate the risk of reflected and stored XSS attack

- Disabling dynamic content
- Using Javascript instead of PHP
- Input Validation
- Output validation

8.3

1. Security regression testing tries to prove that version updates have not reintroduced previously patched security issues?

- (•) True
- ( ) False

2. True or false? Static code analysis can only be performed manually by other programmers and testers in a process of code review.

- ( ) True
- (•) False

3. Interactive debugging, stress testing, and fuzzing are the three types main types of dynamic analysis are available for software testing?

- (•) True
- ( ) False

4. Which web application scanner has been omitted from the following list? OWASP Zed Attack Proxy, Burp Suite, Arachni.

- ( ) SANS
- ( ) GISW
- (•) Nikto
- ( ) Tennable

8.4

1. You are promoting a learning management system (LMS) app in which administrators can configure courses and classes via a cloud app but keep student's registration details in local storage. What type of cloud model is this?

- ○ This is an infrastructure as a service (IaaS) model and a hybrid deployment model.
- ◉ This is a software as a service (SaaS) model and a hybrid deployment model.
- ○ This is a logistics as a service (LaaS) model and a hybrid deployment model.
- ○ This is a platform as a service (PaaS) model and a hybrid deployment model.

2. What type of cloud model provisions unconfigured VM instances with support for the selection of multiple different operating systems?

- ○ Software as a service (SaaS). One key difference between SaaS and platform as a service (PaaS) is where responsibility for patch management and OS configuration lies. With SaaS, the CSP only manages the underlying hypervisor platform. Responsibility for managing each instance lies with the customer.
- ○ Infrastructure as a service (IaaS). One key difference between IaaS and platform as a service (PaaS) is where responsibility for patch management and OS configuration lies. With IaaS, the CSP only manages the underlying hypervisor platform and each VM instance.
- ◉ Infrastructure as a service (IaaS). One key difference between IaaS and platform as a service (PaaS) is where responsibility for patch management and OS configuration lies. With IaaS, the CSP only manages the underlying hypervisor platform. Responsibility for managing each instance lies with the customer.
- ○ Infrastructure as a service (IaaS). One key difference between IaaS and software as a service (SaaS) is where responsibility for patch management and OS configuration lies. With IaaS, the CSP only manages the underlying hypervisor platform and each VM instance.

3. Your company is moving from an on-premises network to hosting copies of its existing client desktops, servers, and business applications as virtual instances in a cloud-based network. What type of cloud model and security solution is being applied in this scenario.

- ◉ This is a public deployment model, infrastructure as a service (IaaS) service model, and makes use of a virtual private cloud (VPC).

4. Your company has experienced a severe security incident caused by an employee uploading a database to a cloud storage service. A cloud access security broker (CASB) can be used to prevent unauthorized use of cloud services from the local network. This will help to mitigate against this type of risk in the future.

- (●) True
- ( ) False

5. Microservices architecture calls for self-contained modules that can be developed and tested independently on one another. Depending on the nature of the project, that might reduce development times and provide better scope for reuse of modules in different contexts. Microservices are also more scalable than a monolithic app. Performance might only need to be increased in one or two modules, for instance. With a monolithic app, you would still need to provision extra resources for the whole app. With microservices, only the necessary modules can be provisioned with increased resource.

- (●) True
- ( ) False

6. The Security Assertions Markup Language (SAML) is often used for exchange of authentication, authorization, and accounting information in a Simple Object Access Protocol (SOAP)-based service-oriented architecture (SOA). SAML assertions are written in XML and exchanged using HTTPS.

- (●) True
- ( ) False

7. The application programming interface (API) provides the means of communicating with the platform. For example, the API might allow an agent to be registered with the platform and be authorized to submit reports and receive updates. Scripting allows you to automate use of the API. For example, you might write a Python or PowerShell script to run on local hosts to install the agent and register with the cloud platform, rather than configuring each host manually.

- (●) True
- ( ) False

8. The main principles of effective API key management are do not embed keys in source code, use least privileges policies for each account/ key, delete unused keys and regenerate live keys periodically, and only install keys to hardened developer workstations. What is missing from this list?

- ( ) Do not use port forwarding
- ( ) Require 32 character passwords when authenticating a system to another system.
- ( ) Store cryptographic keys in an accessible location so the AD can use them to authenticate sessions.
- (●) None of the above

9. Cloud storage can use complex permissions from different sources for containers and objects. A cloud infrastructure assessment tool can be used to assess the effect of these settings.

- (•) True
- ( ) False

10. Which cloud infrastructure assessment tool is best suited for use in penetration testing?

- ( ) Nicu
- (•) Pacu
- ( ) Seequ
- ( ) SaaS

8.5

1. How does DevSecOps support continuous integration and continuous delivery/deployment?

- ( ) A development/operations (DevOps) culture makes provisioning the platform elements of an app a seamless process, by breaking down artificial barriers and silo-based thinking where they are separate teams with separate goals and responsibilities. Adding security (DevSecOps) to this culture encourages "shift up" thinking, where risk assessment, threat modeling, and secure maintenance and monitoring are an integral part of the continuous development life cycle.
- ( ) A development/operations (DevOps) culture makes provisioning the platform elements of an app a seamless process, by breaking down artificial barriers and silo-based thinking where they are separate teams with separate goals and responsibilities. Adding security (DevSecOps) to this culture encourages "shift down" thinking, where risk assessment, threat modeling, and secure maintenance and monitoring are an integral part of the continuous development life cycle.
- (•) A development/operations (DevOps) culture makes provisioning the platform elements of an app a seamless process, by breaking down artificial barriers and silo-based thinking where they are separate teams with separate goals and responsibilities. Adding security (DevSecOps) to this culture encourages "shift left" thinking, where risk assessment, threat modeling, and secure maintenance and monitoring are an integral part of the continuous development life cycle.
- ( ) A development/operations (DevOps) culture makes provisioning the platform elements of an app a seamless process, by breaking down artificial barriers and silo-based thinking where they are separate teams with separate goals and responsibilities. Adding security (DevSecOps) to this culture encourages "shift right" thinking, where risk assessment, threat modeling, and secure maintenance and monitoring are an integral part of the continuous development life cycle.

2. Your CEO is thinking of hiring a couple of programmers to support a switch to an infrastructure as code approach to IT provision. Is this simple approach likely to be successful?

- No. While development expertise is essential, successfully deploying infrastructure as code (IaC) requires a comprehensive transition plan. Firstly, a DevSecOps culture has to be established, as IaC will affect all parts of IT service provision. Secondly, scripting, automation, and orchestration tools have to be selected and appropriately configured. Thirdly, IaC needs to replace entirely manual configuration and ad hoc deployments, or it will not really solve any of the problems with configuration drift that it is supposed to address.
- Yes. While development expertise is essential, successfully deploying infrastructure as code (IaC) requires a comprehensive transition plan. Firstly, a DevSecOps culture has to be established, as IaC will affect all parts of IT service provision. Secondly, scripting, automation, and orchestration tools have to be selected and appropriately configured. Thirdly, IaC needs to replace entirely manual configuration and admin deployments, or it will not really solve any of the problems with configuration drift that it is supposed to address.
- No. While development expertise is essential, successfully deploying infrastructure as code (IaC) requires a comprehensive transition plan. Firstly, a DevSecOps culture has to be established, as IaC will affect all parts of IT service provision. Secondly, scripting, automation, and orchestration tools have to be selected and appropriately configured. Thirdly, IaC needs to replace entirely manual configuration and de facto deployments, or it will not really solve any of the problems with configuration drift that it is supposed to address.
- Yes. While development expertise is essential, successfully deploying infrastructure as code (IaC) requires a comprehensive transition plan. Firstly, a DevSecOps culture has to be established, as IaC will affect all parts of IT service provision. Secondly, scripting, automation, and orchestration tools have to be selected and appropriately configured. Thirdly, IaC needs to replace entirely manual configuration and infrastructure deployments, or it will not really solve any of the problems with configuration drift that it is supposed to address.