[Lead2pass Professional SY0-401 Latest Dumps Free Download From Lead2pass (326-350)

Lead2pass 2017 September New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! CompTIA New Released Exam SY0-401 exam questions are now can be downloaded from Lead2pass! All questions and answers are the latest! 100% exam pass guarantee! Get this IT exam certification in a short time! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 326An administrator is assigned to monitor servers in a data center. A web server connected to the Internet suddenly experiences a large spike in CPU activity. Which of the following is the MOST likely cause? A. SpywareB. TrojanC. Privilege escalationD. DoSAnswer: DExplanation:A Distributed Denial of Service (DDoS) attack is a DoS attack from multiple computers whereas a DoS attack is from a single computer. In terms of the actual method of attack, DDoS and DoS attacks are the same.One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack. QUESTION 327Which of the following attacks could be used to initiate a subsequent man-in-the-middle attack? A. ARP poisoningB. DoSC. ReplayD. Brute force Answer: CExplanation:A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve. Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one- time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation.Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication. One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems.Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check.Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed. QUESTION 328A network analyst received a number of reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks? A. ReplayB. DDoSC. SmurfD. Ping of Death Answer: AExplanation:A replay attack (also known as playback attack) is a form of

network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack). For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve. Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation.Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication. One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems.Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check.Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed. QUESTION 329Timestamps and sequence numbers act as countermeasures against which of the following types of attacks? A. SmurfB. DoSC. VishingD. Replay Answer: DExplanation:A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack). For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve. Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one- time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation.Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication. One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems.Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check.Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed. QUESTION 330Which of the following BEST describes the type of attack that is occurring? A. Smurf AttackB. Man in the middleC. BackdoorD. ReplayE. Spear PhishingF. Xmas AttackG. Blue JackingH. Ping of Death Answer: AExplanation:The exhibit shows that all the computers on the network are being `pinged'. This indicates that the ping request was sent to the network broadcast address. We can also see that all the replies were received by one (probably with a spoofed address) host on the network. This is typical of a smurf attack.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. QUESTION 331Which of the following will help prevent smurf attacks? A. Allowing necessary UDP packets in and out of the networkB. Disabling directed broadcast on border routersC. Disabling unused services on the gateway firewallD. Flash the BIOS with the latest firmware Answer: BExplanation:A smurf attack involves sending PING requests to a broadcast address. Therefore, we can prevent smurf attacks by blocking broadcast packets on our external routers. 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. QUESTION 332Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card? A. WEPB. MAC filteringC. Disabled SSID broadcastD. TKIP Answer: BExplanation:MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC (via airodumping) and then spoofing one's own MAC into a validated one. QUESTION 333Which of the following BEST describes the type of attack that is occurring? (Select TWO). A. DNS spoofingB. Man-in-the-middleC. BackdoorD. ReplayE. ARP attackF. Spear phishingG. Xmas attack Answer: AEExplanation:We have a legit bank web site and a hacker bank web site. The hacker has a laptop connected to the network. The hacker is redirecting bank web site users to the hacker bank web site instead of the legit bank web site. This can be done using two methods: DNS Spoofing and ARP Attack (ARP Poisoning). A: DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer). A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time, so that, if it receives another request for the same translation, it can reply without having to ask the other server again.When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (in this case, the hacker bank web site server). E: Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user. ARP poisoning is also known as ARP cache poisoning or ARP poison routing (APR). QUESTION 334Mike, a user, states that he is receiving several unwanted emails about home loans. Which of the following is this an example of? A. Spear phishingB. HoaxesC. SpoofingD. Spam Answer: DExplanation:Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However,

if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.There is some debate about why it is called spam, but the generally accepted version is that it comes from the Monty Python song, "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam". Like the song, spam is an endless repetition of worthless text. Another school of thought maintains that it comes from the computer group lab at the University of Southern California who gave it the name because it has many of the same characteristics as the lunch meat Spam:Nobody wants it or ever asks for it.No one ever eats it; it is the first item to be pushed to the side when eating the entree. Sometimes it is actually tasty, like 1% of junk mail that is really useful to some people. The term spam can also be used to describe any "unwanted" email from a company or website -- typically at some point a user would have agreed to receive the email via subscription list opt-in -- a newer term called graymail is used to describe this particular type of spam. QUESTION 335Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following? A. Trojan virusB. BotnetC. Worm outbreakD. Logic bomb Answer: CExplanation:A worm is similar to a virus but is typically less malicious. A virus will usually cause damage to the system or files whereas a worm will usually just spread itself either using the network or by sending emails.A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. QUESTION 336A security administrator notices large amounts of traffic within the network heading out to an external website. The website seems to be a fake bank site with a phone number that when called, asks for sensitive information. After further investigation, the security administrator notices that a fake link was sent to several users. This is an example of which of the following attacks? A. VishingB. PhishingC. WhalingD. SPAME. SPIM Answer: BExplanation:Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage.Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. QUESTION 337Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described? A. PhishingB. TailgatingC. PharmingD. Vishing Answer: DExplanation:Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency. Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless. Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with. QUESTION 338Purchasing receives an automated phone call from a bank asking to input and verify credit card information. The phone number displayed on the caller ID matches the bank. Which of the following attack types is this? A. HoaxB. PhishingC. VishingD. Whaling Answer: CExplanation:Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical

financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency. Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless. Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with. QUESTION 339A company's employees were victims of a spear phishing campaign impersonating the CEO. The company would now like to implement a solution to improve the overall security posture by assuring their employees that email originated from the CEO. Which of the following controls could they implement to BEST meet this goal? A. Spam filterB. Digital signaturesC. Antivirus softwareD. Digital certificates Answer: BExplanation:A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing. QUESTION 340A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user's host: Old `hosts' file:127.0.0.1 localhostNew `hosts' file:127.0.0.1 localhost5.5.5.5 www.comptia.com Which of the following attacks has taken place? A. Spear phishingB. PharmingC. PhishingD. Vishing Answer: BExplanation:We can see in this question that a fraudulent entry has been added to the user's hosts file. This will point the URL: www.comptia.com to 5.5.5.5 instead of the correct IP address. Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server (or hosts file) by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing. QUESTION 341Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following? A. Evil twinB. DNS poisoningC. VishingD. Session hijacking Answer: BExplanation:DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer). A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time, so that, if it receives another request for the same translation, it can reply without having to ask the other server again.When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (in this case, the server hosting the web page with derogatory content). QUESTION 342Which of the following is described as an attack against an application using a malicious file? A. Client side attackB. SpamC. Impersonation attackD. Phishing attack Answer: AExplanation:In this question, a malicious file is used to attack an application. If the application is running on a client computer, this would be a client side attack. Attacking a service or application on a server would be a server side attack.Client-side attacks target vulnerabilities in client applications interacting with a malicious data. The difference is the client is

the one initiating the bad connection. Client-side attacks are becoming more popular. This is because server side attacks are not as easy as they once were according to apache.org.Attackers are finding success going after weaknesses in desktop applications such as browsers, media players, common office applications and e-mail clients. To defend against client-side attacks keep-up the most current application patch levels, keep antivirus software updated and keep authorized software to a minimum. QUESTION 343Which of the following would BEST deter an attacker trying to brute force 4-digit PIN numbers to access an account at a bank teller machine? A. Account expiration settingsB. Complexity of PINC. Account lockout settingsD. PIN history requirements Answer: CExplanation:Account lockout settings determine the number of failed login attempts before the account gets locked and how long the account will be locked out for. For example, an account can be configured to lock if three incorrect passwords (or in this case PIN's) are entered. The account can then be configured to automatically unlock after a period of time or stay locked until someone manually unlocks it. QUESTION 344Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file? A. Cognitive passwordB. Password sniffingC. Brute forceD. Social engineering Answer: CExplanation:One way to recover a user's forgotten password on a password protected file is to guess it. A brute force attack is an automated attempt to open the file by using many different passwords.A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.A brute force attack may also be referred to as brute force cracking. For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers.An attack of this nature can be time- and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm. QUESTION 345A security administrator must implement all requirements in the following corporate policy:Passwords shall be protected against offline password brute force attacks. Passwords shall be protected against online password brute force attacks. Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE). A. Account lockoutB. Account expirationC. Screen locksD. Password complexityE. Minimum password lifetimeF. Minimum password length Answer: ADFExplanation:A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.A brute force attack may also be referred to as brute force cracking. For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers. The best defense against brute force attacks strong passwords. The following password policies will ensure that users have strong (difficult to guess) passwords:F: Minimum password length. This policy specifies the minimum number of characters a password should have. For example: a minimum password length of 8 characters is regarded as good security practice.D: Password complexity determines what characters a password should include. For example, you could require a password to contain uppercase and lowercase letters and numbers. This will ensure that passwords don't consist of dictionary words which are easy to crack using brute force techniques.A: Account lockout policy: This policy ensures that a user account is locked after a number of incorrect password entries. For example, you could specify that if a wrong password is entered three times, the account will be locked for a period of time or indefinitely until the account is unlocked by an administrator. QUESTION 346A recent spike in virus detections has been attributed to end-users visiting www.compnay.com. The business has an established relationship with an organization using the URL of www.company.com but not with the site that has been causing the infections. Which of the following would BEST describe this type of attack? A. Typo squattingB. Session hijackingC. Cross-site scriptingD. Spear phishing Answer: AExplanation:Typosquatting, also called URL hijacking or fake url, is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL (including an alternative website owned by a cybersquatter).The typosquatter's URL will usually be one of four kinds, all similar to the victim site address:(In the following, the intended website is "example.com") A common misspelling, or foreign language spelling, of the intended site: exemple.com A misspelling based on typing errors: xample.com or examlpe.com A differently phrased domain name: examples.comA different top-level domain: example.orgOnce in the typosquatter's site, the user may also be tricked into thinking that they are in fact in the real site; through the use of copied or similar logos, website layouts or content. Incorrect Answers:B: In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a

computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. In this question, the users went to www.compnay.com instead of www.company.com. Therefore, this is not a case of hijacking a valid session; it's a case of users going to the wrong URL. Therefore, this answer is incorrect. C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug- in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. The question is not describing an XSS attack. Therefore, this answer is incorrect. D: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. The attack described in the question is not an example of spear phishing. Therefore, this answer is incorrect. http://en.wikipedia.org/wiki/Typosquatting http://en.wikipedia.org/wiki/Session_hijackinghttp://searchsecurity.techtarget.com/definition/spear-phishing QUESTION 347Using proximity card readers instead of the traditional key punch doors would help to mitigate: A. ImpersonationB. TailgatingC. Dumpster divingD. Shoulder surfing Answer: DExplanation:Using a traditional key punch door, a person enters a code into a keypad to unlock the door. Someone could be watching the code being entered. They would then be able to open the door by entering the code. The process of watching the key code being entered is known as shoulder surfing.Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. QUESTION 348Ann an employee is visiting Joe, an employee in the Human Resources Department. While talking to Joe, Ann notices a spreadsheet open on Joe's computer that lists the salaries of all employees in her department. Which of the following forms of social engineering would BEST describe this situation? A. ImpersonationB. Dumpster divingC. TailgatingD. Shoulder surfing Answer: DExplanation:Ann was able to see the Spreadsheet on Joe's computer. This direct observation is known as shoulder surfing. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. QUESTION 349An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place? A. Shoulder surfingB. Dumpster divingC. Whaling attackD. Vishing attack Answer: AExplanation:The CCTV camera has recorded people entering their PINs in the ATMs. This is known as shoulder surfing.Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. QUESTION 350All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate? A. Dumpster DivingB. ImpersonationC. Shoulder SurfingD. Whaling Answer: CExplanation:Viewing confidential information on someone's monitor is known as shoulder surfing. By moving their monitors so they cannot be seen, the executives are preventing users passing by `shoulder surfing'.Shoulder surfing is using direct observation techniques, such as looking

over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Lead2pass gives the latest, authoritative and complete SY0-401 braindumps for SY0-401 exam, because of that, all of our candidates pass SY0-401 certification without any problem. The biggest feature is the regular update of SY0-401 PDF and VCE, which keeps our candidates' knowledge up to date and ensures their SY0-401 exam success. 2017 CompTIA SY0-401 (All 1868 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]