CompTIA Security+ (SY0-601) Complete Course & Exam

Study online at https://quizlet.com/_ebfdp1

You are at the doctor's office and waiting for the physician to enter the room to examine you. You look across the room and see a pile of patient records on the physician's desk. There is no one in the room and your curiosity has gotten the better of you, so you walk across the room and start reading through the other patient records on the desk. Which tenent of security have you just violated?	Confidentiality ensures that data or information has not been disclosed to unauthorized people. In this case, you are not the doctor or the patient whose records you looked at, therefore, confidentiality has been breached.
You have just walked up to the bank teller and requested to withdraw $100 from checking account #7654123 (your account). The teller asks for your name and driver's license before conducting this transaction. After she looks at your driver's license, she thanks you for your business, pulls out $100 from the cash drawer, and hands you back the license and the $100 bill. What category best describes what the bank teller just did?	Authentication occurs when a person's identity is established with proof and confirmed by a system. In this case, the bank teller verified you were the account holder by verifying your name and looking over your photo identification (driver's license) prior to giving you the cash being withdrawn.
You are in the kitchen cooking dinner while your spouse is in the other room watching the news on the television. The top story is about how hackers have been able to gain access to one of the state's election systems and tamper with the results. Unfortunately, you only heard a fraction of the story, but your spouse knows that you have been learning about hackers in your Security+ course and asks you, "Which type of hacker do you think would be able to do this?"	APTs
A user has reported that their workstation is running very slowly. A technician begins to investigate the issue and notices a lot of unknown processes running in the background. The technician determines that the user has recently downloaded a new application from the internet and may have become infected with malware. Which of the following types of infections does the workstation MOST likely have?	A trojan is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. The most common form of a trojan is a Remote Access Trojan (RAT), which is used to allow an attacker to remotely control a workstation or steal information from it. To operate, a trojan will create numerous processes that run in the background of the system.
On your lunch break, you walked down to the coffee shop on the corner. You open your laptop and connect to their wireless network. After a few minutes of surfing the Internet, a pop-up is displayed on your screen. You close the pop-up, finish your lunch break, shut down the laptop, and put it back into your backpack. When you get back to the office, you take out the laptop and turn it on, but instead of your normal desktop background, you are greeted by a full screen image with a padlock and a message stating you have to pay 1 BTC to regain access to your personal files. What type of malware has infected your laptop?	Ransomware
A computer is infected with a piece of malware that has infected the Windows kernel in an effort to hide. Which type of malware MOST likely infected this computer?	Rootkit
Your company's Security Operations Center (SOC) is currently detecting an ongoing DDoS attack against your network's file server. One of the cybersecurity analysts has identified forty internal workstations on the network that are conducting the attack against your network's file server. The cybersecurity analyst believes these internal workstations are infected with malware and places them into a quarantined area of the network. The analyst then submits a service desk ticket to have the workstations scanned and cleaned of the infection. What type of malware was the workstation likely a victim of based on the scenario provided?	Botnet
The Security Operations Center Director for Dion Training received a pop-up message on his workstation that said, "You will regret firing me; just wait until Christmas!" He suspects the message came from a disgruntled former employee that may have set up a piece of software to create this pop-up on his machine. The director is now concerned that other code might be lurking within the network that could create a negative effect on Christmas. He	Logic Bomb

directs his team of cybersecurity analysts to begin searching the network for this suspicious code. What type of malware should they be searching for?	
In which type of attack does the attacker begin with a normal user account and then seeks to gain additional access rights?	Privilege escalation
You have been investigating how a malicious actor was able to exfiltrate confidential data from a web server to a remote host. After an in-depth forensic review, you determine that the web server's BIOS had been modified by the installation of a rootkit. After you remove the rootkit and reflash the BIOS to a known good image, what should you do in order to prevent the malicious actor from affecting the BIOS again?	Utilize secure boot
Your company recently suffered a small data breach that was caused by an employee emailing themselves a copy of the current customer's names, account numbers, and credit card limits. You are determined that something like this shall never happen again. Which of the following logical security concepts should you implement to prevent a trusted insider from stealing your corporate data?	DLP
You are trying to select the best device to install in order to detect an outside attacker who is trying to reach into your internal network. The device should log the event, but it should not take any action to stop it. Which of the following devices would be the BEST for you to select?	IDS
Which mobile device strategy is most likely to result in the introduction of vulnerable devices to a corporate network?	BYOD
Your smartphone begins to receive unsolicited messages while you are eating lunch at the restaurant across the street from your office. What might cause this to occur?	Bluejacking
Tim, a help desk technician, receives a call from a frantic executive who states that their company-issued smartphone was stolen during their lunch meeting with a rival company's executive. Tim quickly checks the MDM administration tool and identifies that the user's smartphone is still communicating with the MDM and displays the location of the device on a map. What should Tim do next to ensure the data on the stolen device remains confidential and inaccessible to the thief?	Perform a remote wipe of the device
Which type of threat will patches NOT effectively combat as a security control?	Zero-day attacks
What should administrators perform to reduce the attack surface of a system and to remove unnecessary software, services, and insecure configuration settings?	Hardening
Which of the following security controls provides Windows system administrators with an efficient way to deploy system configuration settings across a large number of devices?	GPO
Which of the following BEST describes when a third-party takes components produced by a legitimate manufacturer and assembles an unauthorized replica that is sold in the general marketplace?	Counterfeiting
Which of the following programs was designed to secure the manufacturing infrastructure for information technology vendors providing hardware to the military?	Trusted Foundry (TF)
Following a root cause analysis of the unexpected failure of an edge router, a cybersecurity analyst discovered that the system administrator had purchased the device from an unauthorized reseller. The analyst suspects that the router may be a counterfeit	Conduct anti-counterfeit training

device. Which of the following controls would have been most effective in preventing this issue?	
What is the lowest layer (bottom layer) of a bare-metal virtualization environment?	Physical hardware
You need to determine the best way to test operating system patches in a lab environment prior to deploying them to your automated patch management system. Unfortunately, your network has several different operating systems in use, but you only have one machine available to test the patches on. What is the best environment to utilize to perform the testing of the patches prior to deployment?	Virtualization
Which of the following vulnerabilities involves leveraging access from a single virtual machine to other machines on a hypervisor?	VM escape
A web developer wants to protect their new web application from a man-in-the-middle attack. Which of the following controls would best prevent an attacker from stealing tokens stored in cookies?	Setting the secure attribute on the cookie
A user reports that every time they try to access https://www.dion-training.com, they receive an error stating "Invalid or Expired Security Certificate". The technician attempts to connect to the same site from other computers on the network, and no errors or issues are observed. Which of the following settings needs to be changed on the user's workstation to fix the "Invalid or Expired Security Certificate" error?	Date and time
Your company has created a baseline image for all of its workstations using Windows 10. Unfortunately, the image included a copy of Solitaire, and the CIO has created a policy to prevent anyone from playing the game on the company's computers. You have been asked to create a technical control to enforce the policy (administrative control) that was recently published. What should you implement?	Application blacklist
You are reviewing the IDS logs and notice the following log entry:-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-(where email=support@diontraining.com and password=' or 7==7')-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-What type of attack is being performed?	SQL injection
While conducting a penetration test of an organization's web applications, you attempt to insert the following script into the search form on the company's web site:-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-<script>alert("This site is vulnerable to an attack!")</script>-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-Then, you clicked the search button, and a pop-up box appears on your screen showing the following text, "This site is vulnerable to an attack!" Based on this response, what vulnerability have you uncovered in the web application?	Cross-site scripting
You are analyzing the SIEM for your company's ecommerce server when you notice the following URL in the logs of your SIEM:-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-https://www.dion-training.com/add_to_cart.php?itemId=5"+perItemPrice="0.00"+quantity="100"+/><item+id="5&quantity=0-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-Based on this line, what type of attack do you expect has been attempted?	XML injection
A supplier needs to connect several laptops to an organization's network as part of their service agreement. These laptops will be operated and maintained by the supplier. Victor, a cybersecurity analyst for the organization, is concerned that these laptops could potentially contain some vulnerabilities that could weaken the security posture of the network. What can Victor do to mitigate	Implement a jumpbox system

the risk to other devices on the network without having direct administrative access to the supplier's laptops?	
An analyst is reviewing the configuration of a triple-homed firewall that connects to the internet, a private network, and one other network. Which of the following would best describe the third network connected to this firewall?	DMZ
Dion Training allows its visiting business partners from CompTIA to use an available Ethernet port in their conference room to establish a VPN connection back to the CompTIA internal network. The CompTIA employees should be able to obtain internet access from the Ethernet port in the conference room, but nowhere else in the building. Additionally, if a Dion Training employee uses the same Ethernet port in the conference room, they should be able to access Dion Training's secure internal network. Which of the following technologies would allow you to configure this port and support both requirements?	Implement NAC
You have just received some unusual alerts on your SIEM dashboard and want to collect the payload associated with it. Which of the following should you implement to effectively collect these malicious payloads that the attackers are sending towards your systems without impacting your organization's normal business operations?	Honeypot
You are trying to select the best device to install in order to detect an outside attacker who is trying to reach into your internal network. The device should log the event, but it should not take any action to stop it. Which of the following devices would be the BEST for you to select? (1)	NIDS
During a security audit, you discovered that customer service employees have been sending unencrypted confidential information to their personal email accounts via email. What technology could you employ to detect these occurrences in the future and send an automated alert to the security team?	DLP
The Pass Certs Fast corporation has recently been embarrassed by a number of high profile data breaches. The CIO proposes improving the cybersecurity posture of the company by migrating images of all the current servers and infrastructure into a cloud-based environment. What, if any, is the flaw in moving forward with this approach?	This approach only changes the location of the network and not the attack surface of it
Which of the following would a virtual private cloud infrastructure be classified as?	IaaS
Dave's company utilizes Google's G-Suite environment for file sharing and office productivity, Slack for internal messaging, and AWS for hosting their web servers. Which of the following cloud models type of cloud deployment models is being used?	Multi-cloud
Which term is used in software development to refer to the method in which app and platform updates are committed to a production environment rapidly?	Continuous deployment
Which of the following utilizes a well-written set of carefully developed and tested scripts to orchestrate runbooks and generate consistent server builds across an enterprise?	IAC
Which type of system would classify traffic as malicious or benign based on explicitly defined examples of malicious and benign traffic?	Machine Learning
Port 21 / TCP	FTP (File Transfer Protocol)
Port 22 TCP & UDP	SSH, SCP, SFTP
Port 23 TCP & UDP	Telnet - Unencrypted method to remotely administer network devices (should not be used)

Port 25 TCP	SMTP
Port 53 (TCP/UDP)	Domain Name Server (DNS)
Port 69 UDP	TFTP - Trivial FTP is used as a simplified version of FTP to put a file on a remote host, or get a file from a remote host
Port 80 TCP	HTTP - Hyper Text Transfer Protocol is used to transmit web page data to a client for unsecured web browsing
Port 88 TCP & UDP	Kerberos - used for network authentication using a system of tickets within a Windows domain
Port 110 TCP	POP3 - Post Office Protocol v3 is used to receive email from a mail server
Port 119 TCP	NNTP
Port 135 TCP & UDP	RPC/DCOM-scan
Ports 137-139 TCP & UDP	NetBIOS is used to conduct name querying, sending of data, and other functions over a NetBIOS connection
Port 143 TCP	IMAP (Internet Message Access Protocol)
Port 161 UDP	SNMP - Simple Network Management Protocol is used to remotely monitor network devices
Port 162 TCP & UDP	SNMPTRAP Used to send Trap and InformRequests to the SNMP Manager on a network
Port 389 TCP & UDP	LDAP (Lightweight Directory Access Protocol)
Port 443 TCP	HTTPS - Hyper Text Transfer Protocol Secure is used to transmit web page data to a client over an SSL/TLS-encrypted connection
Port 445 TCP	SMB (Server Message Block)
Port 465/587 TCP	SMTP with SSL/TLS Simple Mail Transfer Protocol used to send email over the Internet with an SSL and TLS secured connection
Port 514 UDP	Syslog - used to conduct computer message logging, especially for routers and firewall logs
Port 636 TCP & UDP	LDAP SSL/TLS - LDAP is used to maintain directories of users and other objects over an encrypted SSL/TLS connection
Port 860 TCP	iSCSI - used for linking data storage facilities over IP
Port 989/990 TCP	FTPS File Transfer Protocol Secure is used to transfer files from host to host over an encrypted connection
Port 993 TCP	IMAP4 with SSL/TLS - Internet Message Access Protocol used to receive email from a mail server over an SSL/TLS encrypted connection
Port 995 TCP	POP3 (SSL/TLS) Post Office Protocol v3 is used to receive email from a mail server using an SSL/TLS-encrypted connection
Port 1433 TCP	Ms-sql-s Microsoft SQL server is used to receive SQL database queries from clients
Port 1645/1646 (UDP)	RADIUS (alternative) Remote Authentication Dial-In User Service is used for authentication and authorization (1645) and accounting (1646)
Port 1701 UDP	L2TP
Port 1723 TCP & UDP	PPTP - Point-to-Point Tunneling Protocol is an underlying VPN protocol with built-in security
Ports 1812 & 1813 (UDP)	RADIUS (authentication & authorization)
Port 3225 TCP & UDP	FCIP - Fibre Channel IP is used to encapsulate Fibre Channel frames within TCP/IP packets
Port 3260 TCP	iSCSI Target is a listening port for iSCSI targeted devices when linking data storage facilities over IP

Port 3389 TCP & UDP	RDP - Remote Desktop Protocol is used to remotely view and control other Windows systems via a Graphical User Interface
Port 3868 TCP	Diameter - A more advanced AAA protocol that is a replacement for RADIUS
Port 6514 TCP	Syslog over TLS - used to conduct computer message logging, especially for routers and firewall logs, over a TLS encrypted connection
Which of the following types of attacks are usually used as part of a man-in-the-middle attack?	Spoofing
An analyst just completed a port scan and received the following results of open ports:-=- TCP: 80 TCP: 110 TCP: 443 TCP: 1433 TCP: 3306 TCP: 3389-=-Based on these scan results, which of the following services are NOT currently operating?	SSH
Richard attempted to visit a website and received a DNS response from the DNS cache server pointing to the wrong IP address. Which of the following attacks has occurred?	DNS poisoning
If you are asked about Open Wireless	Look for the answer with no security or protection provided
If you are asked about WEP	Look for the answer with IV
If you are asked about WPA	Look for the answer with TKIP and RC4
If you are asked about WPA2	Look for the answer with CCMP and AES
Bluejacking ____ information	Sends
Bluesnarfing _____ information	takes
You are installing a new wireless network in your office building and want to ensure it is secure. Which of the following configurations would create the MOST secure wireless network?	WPA2 and AES
Your home network is configured with a long, strong, and complex pre-shared key for its WPA2 encryption. You noticed that your wireless network has been running slow, so you checked the list of "connected clients" and see that "Bob's Laptop" is connected to it. Bob lives downstairs and is the maintenance man for your apartment building. You know that you never gave Bob your password, but somehow he has figured out how to connect to your wireless network. Which of the following actions should you take to prevent anyone from connecting to your wireless network without the WPA2 password?	Disable WPS
Which of the following is the LEAST secure wireless security and encryption protocol?	WEP
Which of the following physical security controls would be the most effective in preventing an attacker from driving a vehicle through the glass doors at the front of the organization's headquarters?	Bollards
You work for Dion Training as a physical security manager. You are concerned that the physical security at the entrance to the company is not sufficient. To increase your security, you are determined to prevent piggybacking. What technique should you implement first?	A mantrap is a device that only allows a single person to enter per authentication. This authentication can be done by RFID, a pin number, or other methods. Once verified, the mantrap lets a single person enter through a system, such as a turnstile or rotating door. CCTV will not stop piggybacking, but it could be used as a detective control after an occurrence happened. Wearing security badges is useful, but it won't stop piggybacking by a skilled social engineer. RFID badges may be used as part of your entry requirements, but it won't stop a determined piggyback who follows an employee in.

The public library has had a recent issue with their laptops being stolen from their computer lab. Since this is a public library, it is not a high security area and is fully accessible by patrons during the day. What is the best way to prevent the theft of the laptops?	Cable Locks
Which of the following is NOT considered part of the Internet of Things?	Laptop
Syed is developing a vulnerability scanner program for a large network of sensors that are used to monitor his company's transcontinental oil pipeline. What type of network is this?	SCADA
An analyst is reviewing the logs from the network and notices that there have been multiple attempts from the open wireless network to access the networked HVAC control system. The open wireless network must remain openly available so that visitors are able to access the internet. How can this type of attack be prevented from occurring in the future?	Implement a VLAN to separate the HVAC control system from the open wireless network
David noticed that port 3389 was open on one of the POS terminals in a store during a scheduled PCI compliance scan. Based on the scan results, what service should he expect to find enabled on this terminal?	RDP
Which of the following authentication protocols was developed by Cisco to provide authentication, authorization, and accounting services?	TACACS+ (Port 49)
What access control model will a network switch utilize if it requires multilayer switches to use authentication via RADIUS/TACACS+?	802.1x
Which of the following access control methods utilizes a set of organizational roles in which users are assigned to gain permissions and access rights?	RBAC
Julie was just hired to conduct a security assessment of Dion Training's security policies. During her assessment, she noticed that there were many group accounts being shared by users to conduct their work roles. Julie recommended that the group accounts be eliminated and instead have an account created for each user. What improvement will this recommended action provide for the company?	Increase individual accountability
Marta's organization is concerned with the vulnerability of a user's account being vulnerable for an extended period of time if their password was compromised. Which of the following controls should be configured as part of their password policy to minimize this vulnerability?	Password expiration
After completing an assessment, you create a chart listing the associated risks based on the vulnerabilities identified with your organization's privacy policy. The chart contains listings such as high, medium, and low. It also utilizes red, yellow, and green colors based on the likelihood and impact of a given incident. Which of the following types of assessments did you just complete?	This describes a qualitative risk assessment since it categorizes things based on the likelihood and impact of a given incident using non-numerical terms, such as high, medium, and low. If the risk assessment provided exact numbers or percentages of risk, then it would be a quantitative risk assessment.
Jamie's organization is attempting to budget for the next fiscal year. Jamie has calculated that the asset value of the data is $120,000. Based on her analysis, she believes that a data breach will occur once every four years and have an exposure factor is 30%. What is the ALE for a data breach within Jamie's organization?	The single loss expectancy (SLE) is the amount that would be lost in a single occurrence (AV) times the exposure factor (EF). The annual loss expectancy (ALE) is the total cost of a risk to an organization on an annual basis. This is determined by multiplying the SLE by the annual rate of occurrence (ARO).
Dion Training is concerned with the possibility of a data breach causing a financial loss to the company. After performing a risk analysis, the COO decides to purchase data breach insurance to protect the company in the event of an incident. Which of the following best describes the company's risk response?	Transference

Which of the following command-line tools would you use to identify open ports and services on a host along with the version of the application that is associated with them?	nmap
A cybersecurity analyst in your company notices that an attacker is trying to crack the WPS pin associated with a wireless printer. The device logs show that the attacker tried 00000000, 00000001, 00000002, and continued to increment by 1 number each time until they found the correct PIN of 13252342. Which of the following type of password cracking was being performed by the attacker?	Brute-force
Nick is participating in a security exercise as part of the network defense team for his organization. Which team is Nick playing on?	Blue team
Which of the following protocols is commonly used to collect information about CPU utilization and memory usage from network devices?	SNMP
Which security tool is used to facilitate incident response, threat hunting, and security configuration by orchestrating automated runbooks and delivering data enrichment?	SOAR
You are conducting an intensive vulnerability scan to detect which ports might be open to exploitation. During the scan, one of the network services becomes disabled and causes an impact on the production server. Which of the following sources of information would provide you with the most relevant information for you to use in determining which network service was interrupted and why?	Syslog
If you are not sure on the exam, choose....	Block cipher except for RC4, RC5, RC6
Symmetric algorithms	DES, 3DES, IDEA, AES, Blowfish, Twofish, RC4, RC5, RC6
Asymmetric encryption is known as _____________	Public Key Cryptography. Two keys are used in public key cryptography.
Which of the following cryptographic algorithms is classified as asymmetric?	ECC
Frank and John have started a secret club together. They want to ensure that when they send messages to each other, they are truly unbreakable. What encryption key would provide the STRONGEST and MOST secure encryption?	The only truly unbreakable encryption is one that uses a one-time use pad. This ensures that every message is encrypted with a different shared key that only the two owners of the one-time use pad would know. This technique ensures that there is no pattern in the key for an attacker to guess or find. Even if one of the messages could be broken, all of the other messages would remain secure since they use different keys to encrypt them. Unfortunately, one-time use pads require that two identical copies of the pad are produced and distributed securely before they can be used.
A company has recently experienced a data breach and has lost nearly 1 GB of personally identifiable information about its customers. You have been assigned as part of the incident response team to identify how the data was leaked from the network. Your team has conducted an extensive investigation, and so far, the only evidence of a large amount of data leaving the network is from the email server. There is one user that has sent numerous large attachments out of the network to their personal email address. Upon closer inspection, those emails only contain pictures of that user's recent trip to Australia. What is the most likely explanation for how the data left the network?	Steganography was used to hide the leaked photos from the trip
md5 or sha1	md5 or sha1
Keith wants to validate the application file that he downloaded from the vendor of the application. Which of the following should he compare against the file to verify the integrity of the downloaded application?	md5 or sha1

Which of the following hashing algorithms results in a 160-bit fixed output?	SHA-1 creates a 160-bit fixed output. SHA-2 creates a 256-bit fixed output. NTLM creates a 128-bit fixed output. MD-5 creates a 128-bit fixed output.
In an effort to increase the security of their passwords, Dion Training has added a salt and cryptographic hash to their passwords prior to storing them. To further increase security, they run this process many times before storing the passwords. What is this technique called?	In cryptography, key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources it takes to test each possible key. The question describes one such key stretching technique (using a salt + hash combination aka a rainbow table)
Assuming that Dion Training trusts Thor Teaches, and Thor Teaches trusts Udemy, then we can assume Dion Training also trusts Udemy. What concept of PKI does the previous statement represent?	Transitive trust
You just received an email from Bob, your investment banker, stating that he completed the wire transfer of $10,000 to your bank account in Vietnam. The problem is, you do not have a bank account in Vietnam!, so you immediately call Bob to ask what happened. Bob explains that he received an email from you requesting the transfer. You insist you never sent that email to Bob initiating this wire transfer. What aspect of PKI could be used to BEST ensure that a sender actually sent a particular email message and avoid this type of situation?	Non-repudiation
The digital certificate on the Dion Training web server is about to expire. Which of the following should Jason submit to the CA in order to renew the server's certificate? CSR	A CSR (certificate signing request) is what is submitted to the CA (certificate authority) to request a digital certificate. Key escrow stores keys, CRL is a list of revoked certificate, and the OCSP is a status of certificates that provides validity such as good, revoked, or unknown.
A cybersecurity analyst is attempting to classify network traffic within an organization. The analyst runs the tcpdump command and receives the following output:-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-$ tcpdump -n -i eth0 15:01:35.170763 IP 10.0.19.121.52497 > 11.154.12.121.ssh: P 105:157(52) ack 18060 win 16549 15:01:35.170776 IP 11.154.12.121.ssh > 10.0.19.121.52497: P 23988:24136(148) ack 157 win 113 15:01:35.170894 IP 11.154.12.121.ssh > 10.0.19.121.52497: P 24136:24380(244) ack 157 win 113-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-Which of the following statements is true based on this output?	10.0.19.121 is a client that is accessing an SSH server over port 52497
Which of the protocols listed is NOT likely to be a trigger for a vulnerability scan alert when it is used to support a virtual private network (VPN)?	IPSec is the most secure protocol that works with VPNs. The use of PPTP and SSL is discouraged for VPN security. Due to this, the use of PPTP and SSL for a VPN will likely alert during a vulnerability scan as an issue to be remediated.
IPSec is the most secure protocol that works with VPNs. The use of PPTP and SSL is discouraged for VPN security. Due to this, the use of PPTP and SSL for a VPN will likely alert during a vulnerability scan as an issue to be remediated.	443
Fault-tolerant RAID	Protects against the loss of the array's data if a single component fails (RAID 1, RAID 5, RAID 6)
Disaster-tolerant RAID	Provides two independent zones with full access to the data (RAID 10)
10 Tape Rotation	Each tape is used once per day for two weeks and then the entire set is reused
Recovery Time Objective (RTO)	The length of time it takes after an event to resume normal business operations and activities.
Work Recovery Time (WRT)	The length of time in addition to the RTO of individual systems to perform reintegration and testing of a restored or upgraded system following an event

Recovery Point Objective (RPO)	The longest period of time that an organization can tolerate lost data being unrecoverable.
MTD and RPO help to determine	which business functions are critical and to specify appropriate risk countermeasures
You are configuring a RAID drive for a Media Streaming Server. Your primary concern is speed of delivery of the data. This server has two hard disks installed. What type of RAID should you install, and what type of data will be stored on Disk 1 and Disk 2?	Since this is a Media Streaming Server, you should implement a RAID 0 which provides disk stripping across both drives. This will increase the speed of the data delivery, but provides no redundancy. If you were concerned with redundancy, then you should choose a RAID 1 which uses a mirror of the data on both hard disks. You cannot use a RAID 5, since this requires a minimum of 3 disk drives and stripes the data across the hard disks. You also can not use a RAID 6 since this requires at least 4 hard disks with dual parity and disk stripping.
Dion Training has performed an assessment as part of their disaster recovery planning. The assessment found that the organization's RAID takes, on average, about 8 hours to repair when two drives within the RAID fail. Which of the following metrics would best represent this time period?	Mean time to repair (MTTR) is a basic measure of the maintainability of repairable items. It represents the average time required to repair a failed component or device.
Karen lives in an area that is prone to hurricanes and other extreme weather conditions. She asks you to recommend an electrical conditioning device that will prevent her files from being corrupted if the power to the building is unstable or lost. Additionally, she would like the computer to maintain power for up to an hour of uptime to allow for a graceful shutdown of her programs and computer. Which of the following should you recommend?	An uninterruptible power supply or uninterruptible power source (UPS) is an electrical apparatus that provides emergency power to a load when the input power source becomes too low, or the main power fails. A UPS provides near-instantaneous protection from input power interruptions by using a battery backup. The on-battery run-time of most uninterruptible power sources is usually short (less than 60 minutes) but sufficient to properly shut down a computer system.
Spear Phishing	An attempt to fraudulently obtain information from a user, usually by email that targets a specific individual
Whaling	A form of spear phishing that directly targets the CEO, CFO, CIO, CSO, or other high-value target in an organization
Smishing	Phishing attacks committed using text messages (SMS).
Vishing	Phishing attacks committed using telephone calls or VoIP systems.
Invoice Scam	A scam in which a person is tricked into paying for a fake invoice for a service or product that they did not order
Prepending	A technical method used in social engineering to trick users into entering their username and passwords by adding an invisible string before the weblink they click
Which attack method is MOST likely to be used by a malicious employee or insider who is trying to obtain another user's passwords?	While all of the methods listed could be used by a malicious employee or insider to obtain another user's passwords, shoulder surfing is the MOST likely to be used. Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder. Since a malicious employee or insider can work in close proximity to their victims (other users), they could easily use this technique to collect the passwords of the victimized users.
Which type of threat actor can accidentally or inadvertently cause a security incident in your organization?	Insider threat
Several users have contacted the help desk to report that they received an email from a well-known bank stating that their accounts have been compromised and they need to "click here" to reset their banking password. Some of these users are not even customers of this particular bank, though. Which of the following best describes this type of attack?	Phishing

Which of the following is a senior role with the ultimate responsibility for maintaining confidentiality, integrity, and availability in a system?	Data owner
Your company is setting up a system to accept credit cards in their retail and online locations. Which of the following compliance types should you be MOST concerned within dealing with credit cards?	PCI-DSS
Your company is expanding its operations in the European Union and is concerned about additional governmental regulations that may apply. Which of the following regulations applies when processing personal data within the European Union?	GDPR
Six steps for incident response	- Preparation - Identification - Containment - Eradication - Recovery - Lessons Learned
During which incident response phase is the preservation of evidence performed?	A cybersecurity analyst must preserve evidence during the containment, eradication, and recovery phase. They must preserve forensic and incident information for future needs, to prevent future attacks, or to bring up an attacker on criminal charges. Restoration and recovery are often prioritized over analysis by business operations personnel, but taking time to create a forensic image is crucial to preserve the evidence for further analysis and investigation.
You are the first forensic analyst to arrive on the scene of a data breach. You have been asked to begin evidence collection on the server while waiting for the rest of your team to arrive. Which of the following evidence should you capture first?	When collecting evidence, you should always follow the order of volatility. This will allow you to collect the most volatile evidence (most likely to change) first, and the least volatile (least likely to change) last. You should always begin the collection with the CPU registers and cache memory (L1/L2/L3/GPU). The contents of system memory (RAM), including a routing table, ARP cache, process tables, kernel statistics, and temporary file systems/swap space/virtual memory. Next, you would move onto the collection of data storage devices like hard drives, SSDs, and flash memory devices.
Which of the following is required for evidence to be admissible in a court of law?	The chain of custody is used to document the collection and preservation of evidence from its initial acquisition, throughout the handling leading up to a trial, and during its preservation in case of an appeal or retrial.