CompTIA Security+ (SY0-501)
Practice Exam #1

Question 1:
Jennifer decided that the licensing cost for a piece of video editing software was too expensive. Instead, she decided to download a keygen program to generate her own license key and install a pirated version of the editing software. After she runs the keygen, a license key is created, but her system performance becomes very sluggish and her antimalware suite begins to display numerous alerts.

a) Worm
b) Trojan
c) Adware
d) Logic bomb

Question 2:
Jeffrey, the Security Operations Center director for Security Time Corporation, received a pop-up message on his workstation that said "You will regret firing me, just wait until Christmas!" He suspects the message that a disgruntled former employee may have setup a piece of software to create this pop-up on his machine, and is concerned what other code might be lurking that will create a negative effect on Christmas. He directs his team of cybersecurity analysts to begin search the network for this suspicious code. What type of malware are they searching for?

a) Worm
b) Trojan
c) Adware
d) Logic bomb

Question 3:
Your organization has been receiving a lot of phishing emails recently and you are trying to determine why they are effective in getting your users to click on their links. The latest email consists of what looks like an advertisement that is offering an exclusive early access opportunity to buy a new iPhone at a discounted price, but there are only 5 phones available at this price. What type of social engineering principle is being exploited here?

a) Familiarity
b) Scarcity
c) Intimidation
d) Trust

Question 4:
Tierra works as a cybersecurity analyst for a large multi-national oil and gas company. She is responding to an incident at her company in which their public-facing web server has been defaced with the words, “Killers of the Arctic”. She believes this was done in response to her company’s latest oil drilling project in the Arctic Circle. Which group is most likely to blame for the website defacement?

a) Script kiddies
b) Organized crime
c) APT
d) Hacktivist

Question 5:
During your annual cybersecurity awareness training in your company, the instructor states that employees should be careful as to what information they post on social media. According to the instructor, if you post too much personal information on social media, such as your name, birthday, hometown, and other personal details, it is much easier for an attacker to conduct which type of attack in order to break your passwords?

a) Birthday attack
b) Brute force attack
c) Cognitive password attack
d) Rainbow table attack

Question 6:
During a search of your network, you discovered an unauthorized device that is allowing access to networked resources. What type of attack is being used?

a) Bluesnarfing
b) Bluejacking
c) IV attack
d) Rogue access point

Question 7:
You are hiring a penetration testing firm to conduct an assessment of your company’s network. As part of the contract, your company has specified that they will not provide any details of the network to the penetration testing firm. Instead, the company wants to see how much information about the network the firm can find using open source research and by conducting scanning of the corporate network. What type of assessment is this?

a) White Box
b) Gray Box
c) Blue Box
d) Black Box

Question 8:
Your intrusion detection system has produced an alert based on its review of a series of network packets. After analysis, it is determined that the network packets did not contain any malicious activity. How would you classify this alert?

a) True positive
b) True negative
c) False positive
d) False negative

Question 9:
Lamont is in the process of debugging a software program. As he is examining the code, he discovers that it is written incorrectly. Due to the error, the code is not validating the

a) SQL injection
b) Cross-site scripting
c) Malicious logic
d) Buffer overflow

Question 10:
Ted, a file server administrator, has noticed that a large number of sensitive files have been transferred from a corporate workstation to an IP address outside of the local area network. Ted looks up the IP address and determines that it assigned to a country in Russia. Ted contacts his company's security analyst, Sally, who verifies that the workstation's antimalware solution is up-to-date and the network's firewall is properly configured. What type of attack most likely occurs to allow the exfiltration of the files from the workstation?

a) Session hijacking
b) Zero day
c) MAC spoofing
d) Impersonation

Question 11:
Dion Training Solutions has applied a new Group Policy to all student accounts that will lockout any student's account that enters their password incorrectly 3 times in a row. Once the account is locked out, the student must wait 15 minutes before they can attempt to login again. What type of attack is this mitigation strategy trying to prevent?

a) Privilege escalation
b) Brute force attack
c) Spoofing
d) Man-in-the-middle

Question 12:
You are working as part of a penetration testing team on an assessment. Your boss has requested that you search the recycle bins of the targeted company for any information that might be valuable during the reconnaissance phase of your attack. What type of social engineering method are you performing?

a) Dumpster diving
b) Whaling
c) Impersonation
d) Phishing

Question 13:
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, shutdown 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 5 Bitcoin to regain access to your personal files. What type of malware did you accidentally get installed while at the coffee shop?

a) Trojan
b) Spyware
c) Ransomware
d) Rootkit

Question 14:
What type of malware changes its binary pattern in its code on specific dates or times in order to avoid detection by an antimalware scan?

a) Logic bomb
b) Trojan
c) Ransomware
d) Polymorphic virus

Question 15:
What type of malware is designed to be difficult for malware analysts to reverse engineer?

a) Armored virus
b) Logic bomb
c) Rootkit
d) Trojan

Question 16:
Susan, a help desk technician, has received several trouble tickets today related to employees receiving the same email as part of a phishing campaign. She has determined that the malicious link in the email is not being blocked by your organization's content filter or web proxy. Susan, knowing you recently earned your Security+ certification, calls you up and asks what action she can perform to prevent a user from reaching the website that is associated with the malicious link in the phishing email. What action do you recommend she perform?

a) Block the IP address of the malicious domain in your firwall's ACL
b) Add the malicious domain name to your content filter and web proxy's blacklist
c) Enable TLS on your organization's mail server
d) Forward the phishing email to all employees with a warning not to click on the embedded links

Question 17:
You are attempting architect a new architecture for your company's website. The current architecture involves a single server that hosts the website in its entirety. Your company's newest product has been creating a lot of interest in the media, and your CIO is concerned that the single server will not be able to handle the increased load and demand that could results from this increased publicity. What technology should you implement in the new architecture to allow you to use multiple web servers to share the work of serving up the website to this expected increase in demand from new users?

a) VPN concentrator
b) DLP
c) RAID
d) Load balancing

Question 18:
What type of wireless security measure can easily be defeated by a hacker by spoofing the hardware address of a their network interface card?

a) MAC filtering
b) WEP
c) Disabled SSID broadcast
d) WPS

Question 19:
You are configuring the ACL for your network's perimeter firewall. You have just finished adding all the proper allow and deny rules. What should you place at the end of your ACL rules?

a) An implicit allow statement
b) An implicit deny statement
c) A time of day restriction
d) A SNMP deny string

Question 20:
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 alert to the appropriate security personnel?

a) SSL
b) UTM
c) DLP
d) MDM

Question 21:
You have been asked to determine if one of your company's web servers is vulnerable to a recently discovered attack on an old version of SSH. Which technique should you use to determine the current version of SSH running on the web server?

a) Vulnerability scan
b) Protocol analysis
c) Passive scan
d) Banner grabbing

Question 22:
Your company has recently experience a data breach and has lost nearly 1 GB of personally identifiable information about your 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 contains pictures of that user's recent trip to Australia. What is the most likely explanation of how the data left the network?

a) The user has used steganography to hide the leaked data inside their photos
b) The user connected to the corporate VPN from home and downloaded the files
c) The user hashed the data and emailed it to their personal email account
d) The user has encrypted the data and emailed it to their personal email account

Question 23:
During your lunch break, your phone begins to receive unsolicited messages. What might this be an example of?

a) Packet sniffing
b) Bluesnarfing
c) Bluejacking
d) Geotagging

Question 24:
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?

a) Reset the device's password
b) Perform a remote wipe of the device
c) Remotely encrypt the device
d) Identify the IP address of the smartphone

Question 25:
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?

a) Application whitelist
b) Disable removable media
c) Application blacklist
d) Application hardening

Question 26:
In an effort to improve the security of the network, a security administrator wants to update the configuration of their wireless network in order for it to have IPSec built into the protocol by default. Additionally, the security administrator would like for NAT to no longer be required for extending the number of IP addresses available. What protocol should the administrator implement on the wireless network to achieve their goals?

a) WEP
b) WPA2
c) IPv4
d) IPv6

Question 27:
You want to implement a technology to BEST mitigate the risk that a zero-day virus might infect your corporate workstations. Which of the following should you implement first?

a) Application whitelisting
b) Intrusion Detection System
c) Anti-malware solution
d) Host-based firewall

Question 28:
Michelle has just finished installing a new database application on her server. She then proceeds to uninstall the sample configuration files, properly configures the application settings, and updates the software to the latest version according to her company's policy. What best describes the actions Michelle just took?

a) Patch management
b) Input Validation
c) Application hardening
d) Vulnerability scanning

Question 29:
You are the network administrator for your company. The company just hired a new CIO and he has decided to allow employees to connect their devices to the corporate wireless network under a new BYOD policy. You have been asked to separate the corporate network into an administrative network (for corporate owned devices) and a untrusted network (for employee owned devices). What technology should you utilize to achieve this goal?

a) VPN
b) VLAN
c) WPA2
d) MAC filtering

Question 30:
Your company is concerned with the possibility of employees accessing other user's workstations in secured areas without their permission. Which of the following would BEST be able to prevent this from happening?

a) Require biometric identification for user logins
b) Require a username and a password for user logins
c) Enforce a policy that requires passwords to be changed every 30 days
d) Install security cameras in secure areas to monitor logins

Question 31:
You have recently been hired as a security analyst at Small Time Corporation. On your first day, your supervisor begins to explain the way their network is configured, showing you the physical and logical placement of each firewall, IDS sensor, host-based IPS installations, the networked spam filter, and the DMZ. What best describes how these various devices are incorporated into the network for the best level of security?

a) Network segmentation
b) Defense in depth
c) UTM security appliance
d) Load balancers

Question 32:
Your company utilizes both a wired network throughout the building to provide network connectivity. You are concerned that a visitor might be able to plug their laptop into a CAT 5e wall jack in the lobby and access the corporate network. What technology should you utilize to prevent the user from gaining access to network resources if they are able to plug their laptop into the network?

a) UTM
b) NAC
c) DMZ
d) VPN

Question 33:
William would like to use full-disk encryption on his laptop. He is worried about slow performance, though, so he has requested that the laptop have an onboard hardware-based cryptographic processor. Based on this requirement, what should William ensure the laptop contains?

a) AES
b) FDE
c) PAM
d) TPM

Question 34:
The local electrical power plant contains both business networks and ICS/SCADA networks to control their equipment. Which technology should the power plant's security administrators look to implement first as part of the critical defenses of the ICS/SCADA systems?

a) Intrusion Prevention System
b) Antivirus software
c) Automated patch deployment
d) Log consolidation

Question 35:
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?

a) Sandboxing
b) Virtualization
c) Purchase additional workstations
d) Bypass testing and deploy to the production environment

Question 36:
Jason has installed multiple virtual machines on a single physical server. He needs to ensure that the traffic is logically separated between each virtual machine. How can Jason best implement this requirement?

a) Configure a virtual switch on the physical server and create VLANs
b) Conduct system partitioning on the physical server to ensure the virtual disk images are on different partitions
c) Create a virtual router and disable the spanning tree protocol
d) Install a virtual firewall and establish an access control list

Question 37:
Your organization wants to install a new accounting system and is considering moving to a cloud-based solution to reduce cost, reduce the information technology overhead costs, to improve reliability, and to improve availability. Your Chief Information Officer is supportive of this move since it will be more fiscally responsible, but the Chief Risk Officer is concerned with housing all of the company's confidential financial data in a cloud provider's network that might be shared with other companies. Since the Chief Information Officer is determined to move to the cloud, what type of cloud-based solution would you recommend to account for the Chief Risk Officer's concerns?

a) PaaS in a community cloud
b) SaaS in a private cloud
c) PaaS in a hybrid cloud
d) SaaS in a public cloud

Question 38:
An analyst is review 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?

a) Implement a VLAN to separate the HVAC control system from the open wireless network
b) Install a IDS to protect the HVAC system
c) Enable NAC on the open wireless network
d) Enable WPA2 security on the open wireless network

Question 39:
You work for Big Data Incorporated 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) Install CCTV to monitor the entrance
b) Install a mantrap at the entrance
c) Require all employees to wear security badges when entering the building
d) Install an RFID badge reader at the entrance

Question 40:
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?

a) Motion sensors
b) Mobile device management
c) Cable locks
d) CCTV

Question 41:
You have decided to provide some training to your company's system administrators about the importance of proper patching of a system prior to deployment. To demonstrate the effects of deploying a new system without patching it first, you ask for the system administrators to provide you with an image of a brand new server they plan to deploy. How should you deploy the image to demonstrate the vulnerabilities that are being exposure while maintaining the security of the corporate network?

a) Deploy the image to a brand new physical server, connect it to the corporate network, then conduct a vulnerablity scan to demonstrate how many vulnerabilities are now on the network
b) Utilize a server with multiple virtual machine snapshots installed on it, restore from a known compromised image, and then scan it for vulnerabilities
c) Deploy the system image within a virtual machine, ensure it is in an isolated sandbox enviornment, and then scan it for vulnerabilities
d) Deploy the vulnerable image to a virtual machine on a physical server, create an ACL to restrict all incoming connections to the system, then scan it for vulnerabilities

Question 42:
Which of the following would be considered multi-factor authentication?

a) Username and password
b) Username and pin
c) Thumbprint and password
d) Thumbprint and retina scan

Question 43:
What type of access control provides the strongest level of protection?
a) RBAC
b) MAC
c) DAC
d) ABAC

Question 44:
Which protocol relies on mutual authentication of the client and the server for its security?
a) RADIUS
b) Two-factor authentication
c) Secure LDAP
d) CHAP

Question 45:
Which of the following features is only supported by Kerberos and not by RADIUS or diameter?
a) Only Kerberos provides services for authentication.
b) Only Kerberos provides single sign-on capability.
c) Only Kerberos utilizes tickets to identify authenticated users.
d) Only Kerberos uses XML for cross-platform interoperability.

Question 46:
Assuming that Company X trusts Company Y, and Company Y trusts Company Z, then we can assume Company X trusts Company Z, too. What concept of PKI does this represent?
a) Domain level trust
b) Certificate authority trust
c) Public key trust
d) Transitive trust

Question 47:
Which of the following is not a factor of authentication?
a) Something you know
b) Something you are
c) Something you have
d) Something you want

Question 48:
Dion Training Solutions is requiring students to logon using multifactor authentication in an effort to increase the security of the authentication and login process. Currently, the students logon to diontraining.com using a username and password. What proposed solution would best meet the goal of enabling multifactor authentication for the student logon process?

a) Require students to enter a cognitive password requirement (such as 'What is your dog's name?')

b) Require students to enter a unique 6 digit number that is sent to them by SMS after entering their username and password

c) Require students to create a unique pin that is entered after their username and password are accepted

d) Require students to choose an image to serve as a secondary password after logon

Question 49:
Julie was just hired to conduct a security assessment of your company'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?

a) More routine auditing

b) Increase password security

c) Increase individual accountability

d) More efficient baseline management

Question 50:
What is used as a measure of biometric performance to rate the system's ability to correctly authenticate an authorized user by measuring the rate that an unauthorized user is mistakenly permitted access?

a) False acceptance rate

b) False rejection rate

c) Crossover error rate

d) Failure to capture

Question 51:
Your organization has recently suffered a data breach due to a server being exploited. As a part of the remediation efforts, the company wants to ensure that the default administrator password on each of the 1250 workstations on the network is changed. What is the easiest way to perform this password change?

a) Deploy a new group policy
b) Create a new security group
c) Utilize the key escrow process
d) Revoke the digital certificate

Question 52:
During a penetration test of your company's network, the assessor came across a spreadsheet with the passwords being used for several of the servers. Four of the passwords recovered are listed below, which one is the weakest password and should be change FIRST in order to increase the password's complexity?

a) P@$$w0rd
b) Pa55w0rd
c) P@$$W0RD
d) pa55word

Question 53:
What is a major security risk that could occur when you co-mingle hosts/servers with different security requirements in a single network?

a) Password compromises
b) Privilege creep
c) Security policy violations
d) Zombie attacks

Question 54:
Sean has been asked to write a new security policy to reduce the risk of employees working together to steal information from the corporate network. Which of the following policies should Sean write to counter this threat?

a) Policy that requires mandatory vacations
b) Policy that requires least privilege
c) Privacy policy
d) Acceptable use policy

Question 55:
Your company is building a new data center. The group designing the facility has decided to provide additional HVAC capacity to ensure the data center maintains a consistently low temperature. What benefit might be achieved by increasing the HVAC capacity?

a) Higher data integrity due to more efficient SSD cooling
b) Longer UPS run time due to increase airflow
c) Increase availability of network services due to higher throughput
d) Longer MTBF of hardware due to lower operating temperatures

Question 56:
Your company has a $15,000 server that has been crashing frequently. Over the past 12 months, the server has crashed 10 times, requiring the server to be rebooted in order to recover from the crash. Each time, this has resulted in a 5% loss of functionality or data. Based on this information, what is the Annual Loss Expectancy (ALE) for this server?

a) $1,500
b) $2,500
c) $7,500
d) $15,000

Question 57:
You have been asked by the incident response team leader to perform a forensic examination on a workstation that is suspected to be infected with malware. You remember from your training that you must collect digital evidence in the proper order to protect it from being changed during your evidence collection efforts. Which of the following describes the correct sequence to collect the data from the workstation?

a) RAM, CPU cache, Swap, Hard drive
b) Hard drive, Swap, CPU Cache, RAM
c) CPU Cache, RAM, Swap, Hard drive
d) Swap, RAM, CPU Cache, Hard drive

Question 58:
You have been hired as a consultant to Small Time Corp Incorporated to review their current disaster recovery plans. The CEO has requested that the plans ensure that the company can limit downtime in the event of a disaster, but due to staffing concerns he simply cannot approve the budget to implement or maintain a fully redundant offsite location to ensure a 99.999% availability. Based on that limitation, what should you recommend to the CEO of Small Time Corp?

a) Recommend that the company install a set of redundnat servers to another part of the company's office building

b) Recommend that the company retain all hardware at their office building but ship their backups to an offsite facility for storage

c) Recommend that the company retain their backups in their office building, but install redundant services in a colocated datacenter within a different company

d) Recommend that the redundant hardware be maintained at the offsite location and configure it to be ready for the recovery of the company's backup data when needed

Question 59:
Hilda needs a cost-effective backup solution that would allow for the restoration of data within a 24 hour RPO. The disaster recovery plan requires that backups occur during a specific timeframe each week and then the backups should be transported to an offsite facility for storage. What strategy should Hilda choose to BEST meet these requirements?

a) Create a daily incremental backup to tape

b) Create disk-to-disk snapshots of the server every hour

c) Configure replication of the data to a set of servers located at a hot site

d) Conduct full backup daily to tape

Question 60:
Your company’s offices utilize an open concept floor plan. You are concerned that a visitor might attempt to steal an external hard drive and carry it out of the building. To mitigate this risk, your security department has recommended installing security cameras that are clearly visible to both employees and visitors. What type of security control do these camera represent?

a) Corrective

b) Compensating

c) Administrative

d) Deterrent

Question 61:
Your company has just finished replacing all of its computers with brand new workstations. Colleen, one of your coworkers, has asked the owner of the company if she can have the old computers that are about to be thrown away. Colleen would like to refurbish the old computers by reinstalling a new operating system and donate them to a local community center for disadvantaged children in the neighborhood. The owner thinks this is a great idea, but is concerned that the private and sensitive corporate data on the old computer's hard drives might be placed at risk of exposure. You have been asked to choose the best solution to sanitize or destroy the data while ensuring the computers will still be usable by the community center. What type of data destruction or sanitization method do you recommend?

a) Degaussing
b) Wiping
c) Purging
d) Shredding

Question 62:
James, an programmer at Apple Computers, is surfing the internet on his lunch break. He comes across a rumor site that is focused on providing details of the upcoming iPhone being released in a few months. James knows that Apple likes to keep their product details a secret until they are publically announced. As James is looking over the website, he sees a blog post with an embedded picture of a PDF containing detailed specifications for the next iPhone and labeled as "Proprietary Information – Internal Use Only". The new iPhone is still several months away from release. What should James do next?

a) Contact the website's owner and request they take down the PDF
b) Contact his team lead and ask what he should do next
c) Contact the service desk or incident response team to determine what to do next
d) Reply to the blog post and deny the accuracy of the specifications

Question 63:
A company is using RADIUS authentication to connect a network client to a networked file server by providing its authentication credentials. The file server then uses the authentication credentials to issue a RADIUS authentication request to the RADIUS server. The RADIUS server then is able to exchange RADIUS authentication messages with the file server on behalf of the client. Throughout this process, a shared secret is used to protect the communication. Which of the following technologies relies upon the shared secret?

a) RADIUS
b) Kerberos
c) PKI
d) LDAP

Question 64:
Dion Training Solutions has contracted a software development firm to create a bulk file upload utility for its website. During a requirements planning meeting, the developers asked what type of encryption is required for the project. After some discussion, Jason decides that the file upload tool should use a cipher that is capable of encrypting 8 bits of data at a time before transmitting the files from the web developer's workstation to the web server. What of the following should be selected to meet this security requirement?

a) Stream cipher
b) Block cipher
c) CRC
d) Hashing algorithm

Question 65:
Sarah is working at a startup that is focused on making secure banking apps for smartphones. Her company needs to select an asymmetric encryption algorithm to encrypt the data being used by the app. Due to the need for high security of the banking data, the company needs to ensure that whatever encryption they use is consider strong, but also need to minimize the processing power required since it will be running on a mobile device with lower computing power. Which algorithm should Sarah choose in order to provide the same level of high encryption strength with a lower overall key length?

a) Diffie-Hellman
b) RSA
c) ECC
d) Twofish

Question 66:
Your company has just suffered a website defacement of its public facing web server. The CEO believes this act of vandalism may have been done by the company's biggest competitor. The decision has been made to contact law enforcement so evidence can be collected properly for use in a potential court case. Laura is a digital forensics investigator assigned to collect the evidence. She create a bit-by-bit disk image of the web server's hard drive as part of her evidence collection. Which technology should Laura use after creating the disk image to verify the data integrity of the copy matches that of the original web server's hard disk?

a) SHA-256
b) RSA
c) AES
d) 3DES

Question 67:
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?

a) DES with a 56-bit key
b) AES with a 256-bit key
c) ECC with a 256-bit key
d) Randomized one-time use pad

Question 68:
Why would a company want to utilize a wildcard certificate for their servers?

a) To secure the certificate's private key
b) To increase the certificate's encryption key length
c) To reduce the certificate management burden
d) To extend the renewal data of the certificate

Question 69:
In an effort to increase the security of their passwords, Ted's company 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?

a) Key stretching
b) Rainbow table
c) Salting
d) Collision resistance

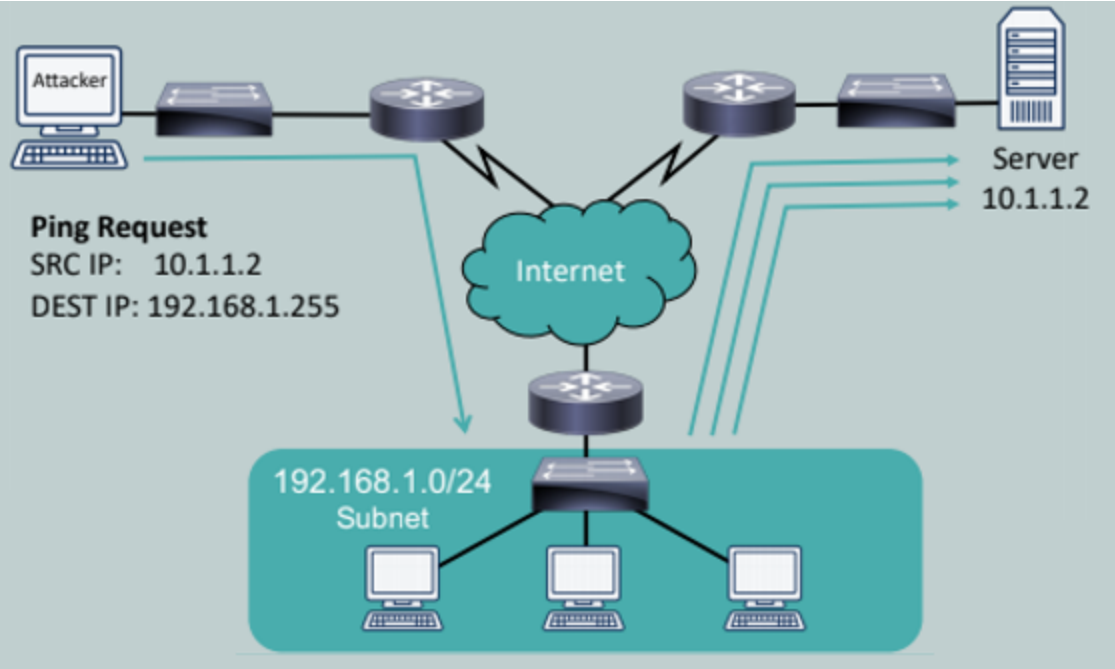
Question 70:
You just received an email from Bob, your investment banker, stating that he completed the wire transfer of $10,000 to your bank account in Vietnam. The problem is, you don't have a bank account in Vietnam! You immediately call Bob to ask what is happening. Bob explains that he received an email from you requesting the transfer. You insist you never sent that email to Bob initiating the transfer. What aspect of PKI is used to BEST ensure that a sender actually sent a particular email message?

a) CRL
b) Trust models
c) Recovery agents
d) Non-repudiation

Question 71:
What is the correct order of the Incident Response process?

a) Identification, Containment, Eradication, Preparation, Recovery, and Lessons Learned
b) Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
c) Containment, Eradication, Identification, Lessons Learned, Preparation, and Recovery
d) Lessons Learned, Recovery, Preparation, Identification, Containment, and Eradication

Question 72:
Which of the following best describes the attack being illustrated?



a) Ping of Death
b) XMAS Tree Attack
c) Man in the Middle
d) Smurf

Question 73:
A cybersecurity analyst has determined that an attack has occurred against your company's network. Fortunately, your company uses a good system of logging with a centralized SYSLOG server, so all the logs are available, were collected, and have been stored properly. According to the cybersecurity analyst, the logs indicate that the database server was the only company server on the network that appears to have been attacked. The network is a critical production network for your organization, therefore you have been asked to choose the LEAST disruptive actions on the network while performing the appropriate incident response actions. Which actions do you recommend to as part of the response efforts?

a) Capture network traffic using a sniffer, schedule a period of downtime to image and remediate the affected server, and maintain the chain of custody

b) Isolate the affected server from the network immediately, format the database server, reinstall from a known good backup

c) Immediately remove the database server from the network, create an image of its hard disk, maintain the chain of custody

d) Conduct a system restore of the database server, image the hard drive, and maintain the chain of custody

Question 74:
(1) An attacker has been collecting credit card details by calling victims and using false pretexts to trick them.

(2) An attacker sends out to 100,000 random email addresses. In the email the attacker sent, it claims that "Your Bank of American account has been locked out. Please click here to reset your password."

What type of attacks have occurred in (1) and (2)?

a) (1) Vishing and (2) Phishing
b) (1) Spearphishing and (2) Pharming
c) (1) Hoax and (2) Spearphishing
d) (1) Pharming and (2) Phishing

Question 75:
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? What type of data will be stored on Disk 1 and what type of Disk 2?

a) RAID 0 – Disk 1 (Stripe) and Disk 2 (Stripe)
b) RAID 0 – Disk 1 (Mirror) and Disk 2 (Mirror)
c) RAID 1 – Disk 1 (Stripe) and Disk 2 (Stripe)
d) RAID 1 – Disk 2 (Mirror) and Disk 2 (Mirror)

CompTIA Security+ (SY0-501)
Practice Exam #1

Answer Key

1	B
2	D
3	B
4	D
5	C
6	D
7	D
8	C
9	D
10	B
11	B
12	A
13	C
14	D
15	A
16	B
17	D
18	A
19	B
20	C
21	D
22	A
23	C
24	B
25	C

26	D
27	A
28	C
29	B
30	A
31	B
32	B
33	D
34	A
35	B
36	A
37	B
38	C
39	B
40	C
41	C
42	C
43	B
44	C
45	C
46	D
47	D
48	B
49	C
50	A

51	A
52	D
53	C
54	A
55	D
56	C
57	C
58	D
59	A
60	D
61	B
62	C
63	A
64	B
65	C
66	A
67	D
68	C
69	A
70	D
71	B
72	D
73	A
74	A
75	A