OPERATIONS AND INCIDENT RESPONSE

16%

OPERATIONS AND INCIDENT RESPONSE

- The command **nslookup** is used to perform DNS queries and receive: domain names, IP addresses, an DNS Records such as A records, MX records or any other DNS Record.
- The command that finds the MX records from your email server is: $ nslookup -query=mx yourdomain.com

- The command **tracert** is a utility designed for displaying the time it takes for a packet of information to travel between a local computer and a destination IP address or domain. It’s used to show several details such as the number of hops about the path that a packet takes from the computer or device you’re on to whatever destination you specify.

- The **route** command is used to view and manipulate the IP routing table.

OPERATIONS AND INCIDENT RESPONSE

- The command **ping** sends a request over the network to a specific device to see if a networked device is reachable. In other words, the ping command is used to find out whether an IP connection exists for a particular host.

- To command **ipconfig** displays the basic TCP/IP configuration such as IPv4, IPv6, subnet mask, and default gateway for all adapters.

- **Tcpdump** is a command-line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.

OPERATIONS AND INCIDENT RESPONSE

- The **head** command is a UNIX and Linux command for outputting the first part of the files. Examples of outputting the first five lines of a file, limiting the number of lines, limiting the number of bytes, showing multiple files, and using pipes.

- The **tail** command is a command-line utility for outputting the last part of files given to it via standard input. It writes results to standard output.

- **Tcpdump** is a command-line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.

OPERATIONS AND INCIDENT RESPONSE

- The **cat** (short for concatenate) command is one of the most frequently used command in Linux/Unix like operating systems. cat command allows us to create single or multiple files, concatenate files and redirect output in terminal or files.

- The **chmod** command is used to change the access permissions of file. Let’s say you are the owner of a file named yourfile, and you want to set its permissions so that the user can read, write, and execute it, then the final command is: chmod u=rwx

OPERATIONS AND INCIDENT RESPONSE

- The command **dig** is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups. The dig command replaces older tool such as nslookup and the host.
- The **netstat** command displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

OPERATIONS AND INCIDENT RESPONSE

- The **arp** command allows you to display and modify the Address Resolution Protocol (ARP) cache. An ARP cache is a simple mapping of IP addresses to MAC addresses. Each time a computer's TCP/IP stack uses ARP to determine the Media Access Control (MAC) address for an IP address, it records the mapping in the ARP cache so that future ARP lookups go faster.

- The **Wireshark** is indeed a tool that captures and analyzes network traffic that goes through your system but is not a command-line utility. Wireshark is the world's leading network traffic analyzer and an essential tool for any security professional or systems administrator. It lets you analyze network traffic in real-time, and is often the best tool for troubleshooting issues on your network.

OPERATIONS AND INCIDENT RESPONSE

- **Business continuity planning** is a strategy, that ensures continuity of operations with minimal service outage or downtime. It is designed to protect personnel or assets and make sure they can function quickly when a disaster strikes such as natural disasters or cyber-attacks.

- Business **disaster recovery** plan can restore data and critical applications in the event your systems are destroyed when disaster strikes.

OPERATIONS AND INCIDENT RESPONSE

- The difference between a business continuity plan and disaster recovery plan is:
  - A business continuity plan is a strategy businesses put in place to continue operating with minimal disruption in the event of a disaster.
  - The disaster recovery plan refers more specifically to the steps and technologies for recovering from a disruptive event, especially as it pertains to restoring lost data, infrastructure failure, or other technological components.

OPERATIONS AND INCIDENT RESPONSE

- An **incident response team** is a group of IT professionals in charge of preparing for and reacting to any type of organizational emergency. Responsibilities of an incident response team include developing an incident response plan, testing for and resolving system vulnerabilities, maintaining strong security best practices, and providing support for all incident handling measures.

- A **retention policy** is a key part of the lifecycle of a record. It describes how long a business needs to keep a piece of information (a record), where it’s stored, and how to dispose of the record when its time.

Governance, Risk, and Compliance

14%

GOVERNANCE, RISK AND COMPLIANCE

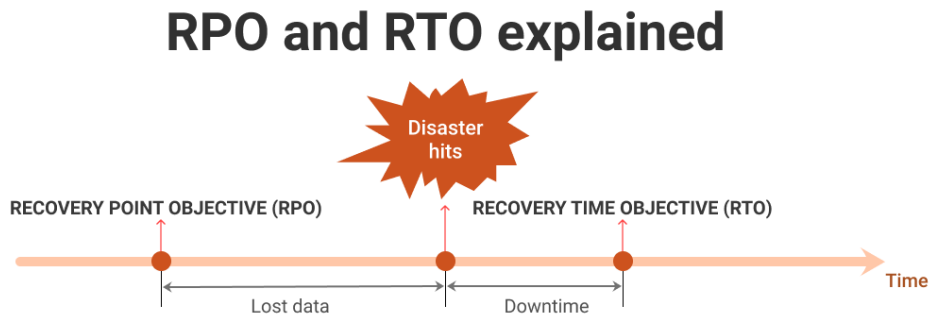
- **Mean time between failures (MTBF)** measures the predicted time that passes between one previous failure of a mechanical/ electrical system to the next failure during normal operation. In simpler terms, MTBF helps you predict how long an asset can run before the next unplanned breakdown happens.

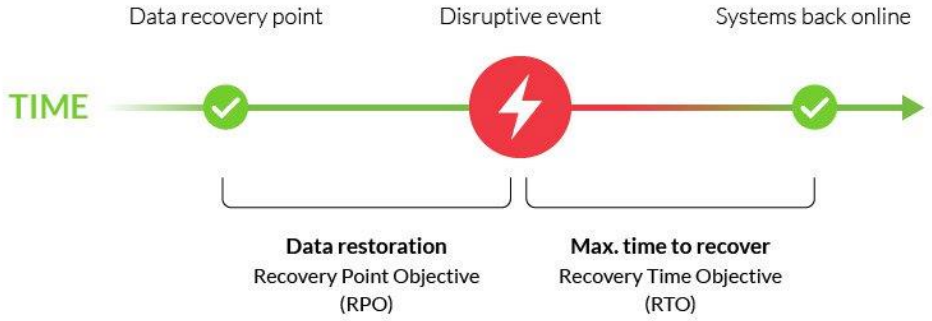
- **Recovery point objective (RPO)** describes a period of time in which an enterprise's operations must be restored following a disruptive event, e.g., a cyberattack, natural disaster, or communications failure.

GOVERNANCE, RISK AND COMPLIANCE

- **MTTR** (mean time to recovery or mean time to repair) is the average time it takes to recover from a product or system failure. This includes the full time of the outage—from the time the system or product fails to the time that it becomes fully operational again.

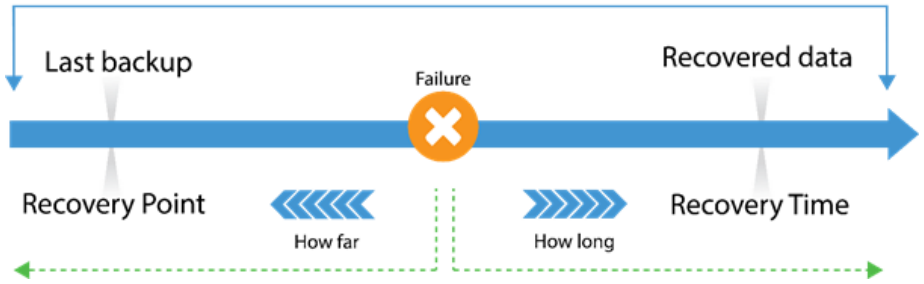
- The **Recovery Time Objective** (RTO) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.





Recovery Objectives

- Two of the important parameters that define a BCDR plan are the **Recovery Point Objective (RPO)** and **Recovery Time Objective (RTO).** For those of you who are not familiar with these terms, let me give you a brief description:
  - **RPO** limits how far to roll back in time, and defines the maximum allowable amount of lost data measured in time from a failure occurrence to the last valid backup.
  - **RTO** is related to downtime and represents how long it takes to restore from the incident until normal operations are available to users



GOVERNANCE, RISK AND COMPLIANCE

- **General Data Protection Regulation** is a set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy. Under the terms of GDPR, not only do organizations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it are obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners – or face penalties for not doing so

GOVERNANCE, RISK AND COMPLIANCE

- The **Payment Card Industry Data Security Standard** (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

- **National Institute of Standards and Technology (NIST)** - NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life.

GOVERNANCE, RISK AND COMPLIANCE

- **International Organization for Standardization (ISO)-**ISO develops and publishes standards for a vast range of products, materials, and processes. The organization's standards catalog is divided into 97 fields which include healthcare technology, railway engineering, jewelry, clothing, metallurgy, weapons, paint, civil engineering, agriculture, and aircraft.

GOVERNANCE, RISK AND COMPLIANCE

- **The annualized rate of occurrence (ARO)** is described as an estimated frequency of the threat occurring in one year. ARO is used to calculate ALE (annualized loss expectancy). ALE is calculated as follows: ALE = SLE x ARO. ALE is $15,000 ($30,000 x 0.5), when ARO is estimated to be 0.5 (once in two years). As we can see, the risk is about the impact of the vulnerability on the business and the probability of the vulnerability to be exploited.

GOVERNANCE, RISK AND COMPLIANCE

- Single loss expectancy (SLE) - SLE tells us what kind of monetary loss we can expect if an asset is compromised because of a risk. Calculating SLE requires knowledge of the asset value (AV) and the range of loss that can be expected if a risk is exploited, which is known as the exposure factor (EF). EF is a percentage determined by how much of an impact we can expect based on the risk, the highest being 1 (signifying 100%).

  In formulaic terms, SLE = AV * EF

AV = $500
EF = 50%
SLE = $250
$500 x 50/100 = 1/2

Laptop

ALE = SLE x ARO

2/year

250 x 2 = $500

GOVERNANCE, RISK AND COMPLIANCE

- **Annualized loss expectancy (ALE)** - Annualized loss expectancy is the loss that can be expected for an asset due to risk over a one-year period. It's useful for working out whether a business decision is worthwhile.

- **A Memorandum of understanding (MOU)** is an agreement between two or more parties outlined in a formal document. It is not legally binding but signals the willingness of the parties to move forward with a contract.

    - The MOU can be seen as the starting point for negotiations as it defines the scope and purpose of the talks. Such memoranda are most often seen in international treaty negotiations but also may be used in high-stakes business dealings such as merger talks.

GOVERNANCE, RISK AND COMPLIANCE

- **End of life (EOL)** is the final stage of a product's existence. The particular concerns of endof-life depend on the product in question and whether the perspective is that of the manufacturer or the user. For the manufacturer, EOL concerns involve not only discontinuing production but also continuing to address the market needs that the product addresses — which might lead to the development of a new product. For the business using the product, EOL concerns include disposing of the existing product responsibly, transitioning to a different product, and ensuring that disruption will be minimal.

GOVERNANCE, RISK AND COMPLIANCE

- A Non-Disclosure Agreement (NDA) is a legally enforceable contract that establishes confidentiality between two parties—the owner of protected information and the recipient of that information. By signing an NDA, participants agree to protect confidential information shared with them by the other party.

Practice Questions

Question 1. You have been hired by a company to identify and document all aspects of an asset's configurations in order to create a secure template against which all subsequent configurations will be measured. What type of configuration management will you implement?

(A) Standard naming conventions

(B) Internet protocol (IP) schema

(C) Configuration template

(D) Baseline configurations

Question 2. Which of the following process is designed to trigger automatic code integration in the main code base instead of developing in isolation and then integrating them at the end of the development cycle?

(A) Continuous integration

(B) Continuous delivery

(C) Continuous monitoring

(D) Continuous deployment

Question 3. Authentication, _____, and Accounting is the term for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

(A) Controlling

(B) Authorization

(C) Auditing

(D) Enforcing

Question 4. A company hired you as a security expert. You have been tasked to implement a solution to deceive and attract hackers who attempt to gain unauthorized access to their network in order to gain information about how they operate. Which of the following technique will you implement to meet this requirement as cost-effective as possible?

(A) Honeyfile

(B) Honeypots

(C) ~~DNS Sinkholing~~

(D) Honeynet

Question 5. What type of architecture developers use to build and run applications and services without having to manage infrastructure?

(A) Software-Defined Networking

(B) Serverless

(C) Software-Defined visibility

(D) Transit gateway

Question 6. Your company due to a strict budget migrating to the cloud. The primary reason is to avoid spending money on purchasing hardware and time on maintaining it. The company needs to pay only for the cloud computing resources it uses. Which of the following cloud computing architecture your company will use to deploy the cloud services?

(A) Public Cloud

(B) ~~Private Cloud~~

(C) ~~Hybrid Cloud~~

(D) ~~Community Cloud~~

Question 7. The developers of your company thinking to switch the development process to the cloud, so they don't need to start from scratch when creating applications with the purpose of saving a lot of time and money on writing code. Which of the following cloud service models developers will use to create unique, customizable software on the Cloud?

(A) PaaS

(B) ~~IaaS~~

(C) ~~XaaS~~

(D) ~~SaaS~~

Question 8. Which of the following companies is not a cloud service provider?

(A) Amazon Web Services

(B) Microsoft Azure

(C) Examsdigest

(D) Google Cloud Platform

Question 9. You are developing a new system that requires users to be authenticated using temporary passcode which is generated by an algorithm that uses the current time of day. Which of the following authentication methods will you use to authenticate the users?

(A) HOTP

(B) SMS

(C) Push notifications

(D) TOTP

Question 10. Version _____?_____ keeps track of every modification to the code in a special kind of database. If a mistake is made, you can turn back the clock and compare earlier versions of the code to help fix the mistake.

(A) Scalability

(B) Elasticity

(C) Control

(D) Compiler

Question 11. You are working for a client as a web developer and your client asked you to check the new update of the app without making the updates live for the users. In which environment will you push the update so your client can look it over in a stable format before it gets pushed to the users?

(A) ~~Development~~

(B) ~~Quality Assurance~~

(C) ~~Production~~

(D) ~~Staging~~

Question 12. The solution to the problem of how to get the software to run reliably when moved from one computing environment to another is known as:

(A) Containers

(B) Microservice

(C) API

(D) Thin Client

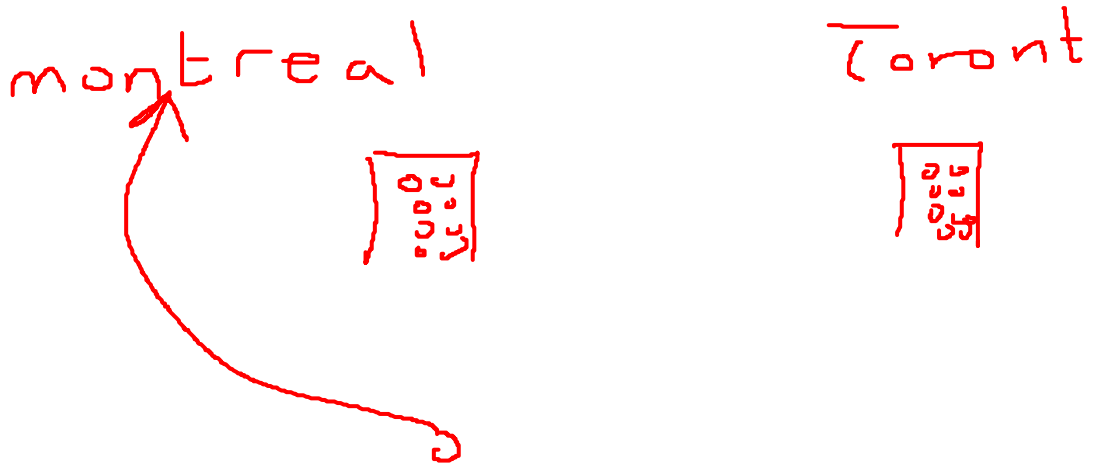
Question 13. A decentralized computing infrastructure in which data, compute, storage, and applications are located between the data source and the cloud is called _____ computing. In this environment, intelligence is at the local area network (LAN) and data is transmitted from endpoints only.

(A) Fog

(B) ~~Edge~~

(C) ~~Distributed~~

(D) ~~Cloud~~



Question 14. Which of the following types of disaster recovery sites doesn't have any pre-installed equipment and it takes a lot of time to properly set it up so as to fully resume business operations?

(A) Cold Site

(B) Hot Site

(C) ~~Normal Site~~

(D) Warm Site

Question 15. The security process that relies on the unique traits such as retinas, irises, voices, facial characteristics, and fingerprints of an individual to verify that he is who says he is, is called:

(A) Trait authentication

(B) Characteristics authentication

(C) Personalized authentication

(D) Biometric authentication

Question 16. Which of the following options is a network architecture approach that enables the network to be intelligently and centrally controlled, or programmed using software applications and helps operators manage the entire network consistently, regardless of the underlying network technology?

(A) ~~Serverless~~

(B) ~~Transit gateway~~

(C) SDN

(D) ~~SDV~~

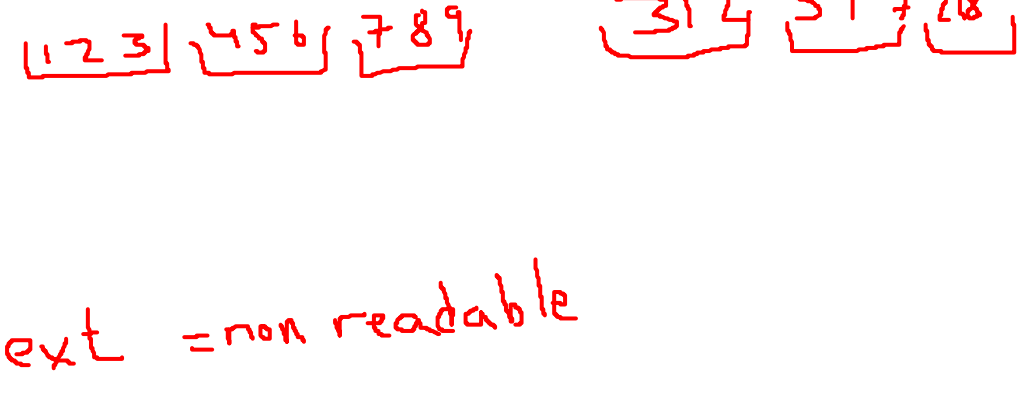
Question 17. Your organization is working with a contractor to build a database. You need to find a way to hide the actual data from being exposed to the contractor. Which of the following technique will you use in order to allow the contractor to test the database environment without having access to actual sensitive customer information?

(A) Data Masking

(B) Tokenization

(C) Encryption

(D) Data at rest



Question 18. The software that monitoring user activity and automatically preventing malware between cloud service users and cloud applications is known as:

(A) Cloud access security broker

(B) Hashing

(C) Hardware security modules

(D) SSL/TLS inspection

Question 19. A managed service provider (MSP) is a company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.

(A) TRUE

(B) FALSE

Question 20. Which of the following types of disaster recovery sites allows a company to continue normal business operations, within a very short period of time after a disaster?

(A) Warm Site

(B) Hot Site

(C) Cold Site

(D) Normal Site

Question 21. Recently the physical network adapter card from your company's server broke. As a result, your co-workers couldn't access important resources for hours. You have been instructed to implement a solution to eliminate this from happening again in the event of a network adapter failure. Which of the following solutions will you implement to meet the requirement?

(A) NIC teaming

(B) ~~UPS~~

(C) ~~PDU~~

(D) ~~Power generator~~

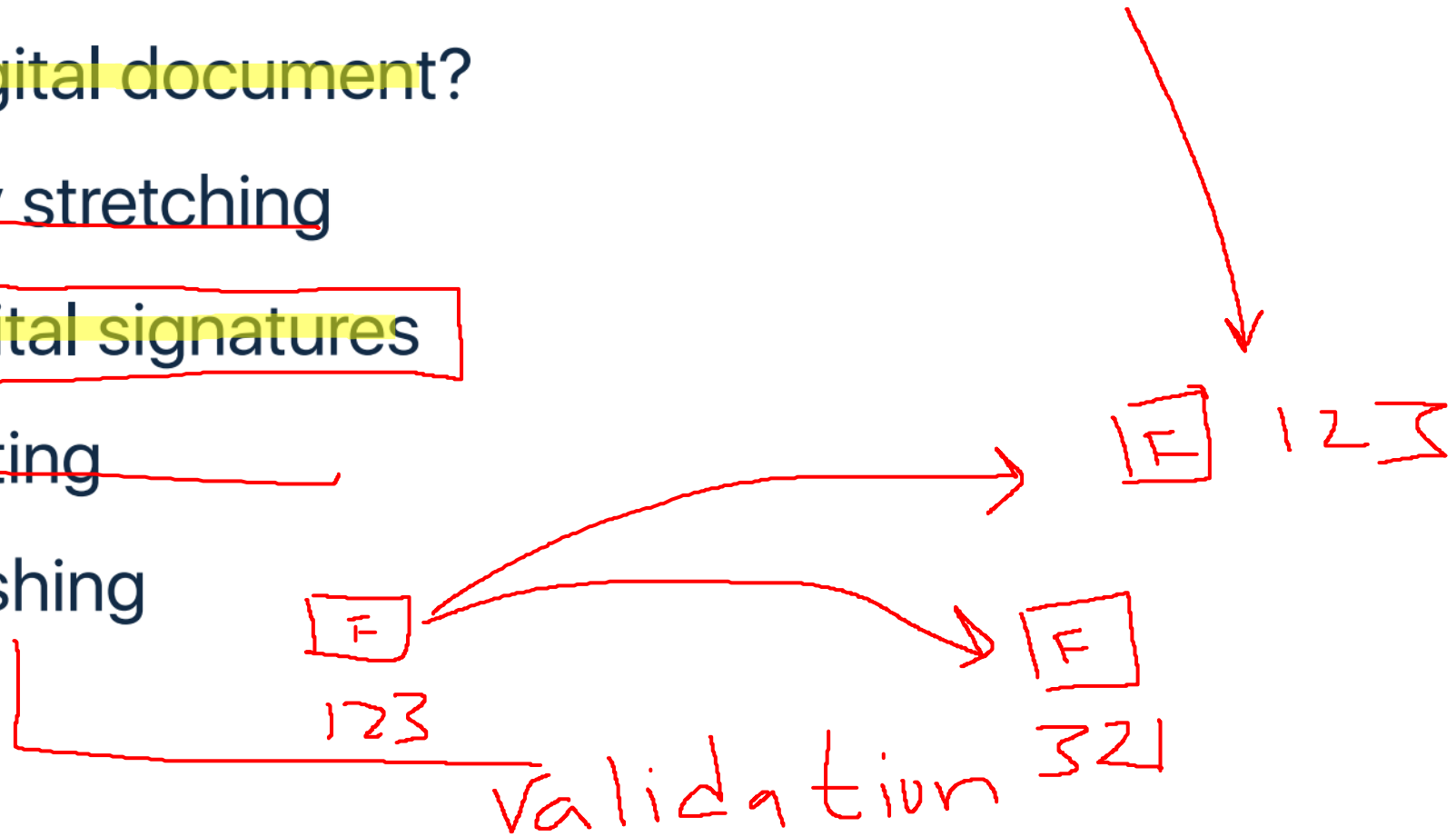
Question 22. Which of the following cryptographic technique will you use to validate the authenticity and integrity of a message or digital document?

(A) Key stretching

(B) Digital signatures

(C) Salting

(D) Hashing



Question 23. Which of the following products using Software as a Service cloud model? (Choose all the apply.)

(A) Google Apps

(B) Dropbox

(C) Google Compute Engine

(D) Mailchimp

(E) AWS EC2

(F) Slack

marketing
mass email

Question 24. You are working for a startup and recently the application you are developing experienced a large amount of traffic. As a result, the performance of the application was decreased. You have been instructed to implement a solution to efficiently distributing incoming network traffic across a group of backend servers to increase the performance of the APP.

Which of the following solutions will you implement to meet the requirement?

(A) Load balancers

(B) Network interface card teaming

(C) Multipath

(D) Redundant array of inexpensive disks

Question 25. You have been instructed to connect a storage device that allows storage and retrieval of data from a central location for authorized network users and varied clients. Which of the following storage type will you use to meet the requirement?

(A) ~~Storage area network~~

(B) ~~Tape storage~~

(C) Network-attached storage ✓

(D) ~~Disk storage~~ Local

Question 26. Continuous _____ is a software development method that releases or deploys software automatically into the production environment. In this model, no one manually checks the code and pushes it into your app.

(A) Integration

(B) Deployment

(C) Monitoring

(D) Delivery

Question 27. Which of the following options allows your application to interact with an external service using a simple set of commands rather than having to create complex processes yourself?

(A) Thin Client

(B) API

(C) Microservice

(D) Containers

Question 28. Cloud backup is a strategy for sending a copy of files or database to a secondary server which is usually hosted by a third-party service provider, for preservation in case of equipment failure or catastrophe. (True/False)

(A) TRUE

(B) ~~FALSE~~

Question 29. Asymmetrical encryption uses a single key that needs to be shared among the people who need to receive the message while symmetric encryption uses a pair of a public key and a private key to encrypt and decrypt messages when communicating. (True/False)

(A) TRUE

(B) FALSE

Question 30. Which of the following technique will you use to hide secret data within a non-secret file or message with the purpose of avoiding data detection?

(A) Elliptical curve cryptography

(B) Homomorphic encryption

(C) Lightweight cryptography

(D) Steganography

Question 31. You have been tasked to find a way to transform a plain text sensitive file into a non-readable form and send it through the web. Which of the following technique will you use to send the file through the web and only authorized parties can understand the information?

(A) Encryption

(B) Data masking

(C) Tokenization

(D) Data at rest

Question 32. Which of the following backup types only back up the data that has changed since the previous backup?

(A) ~~Full backup~~

(B) Incremental backup ✓

(C) Differential backup

(D) ~~Snapshot backup~~

Incremental backups were introduced as a way to decrease the amount of time and storage space that it takes to do a full backup. Incremental backups only back up the data that has changed since the previous backup

A differential backup is similar to an incremental backup in that it starts with a full backup and subsequent backups only contain data that has changed.

Full

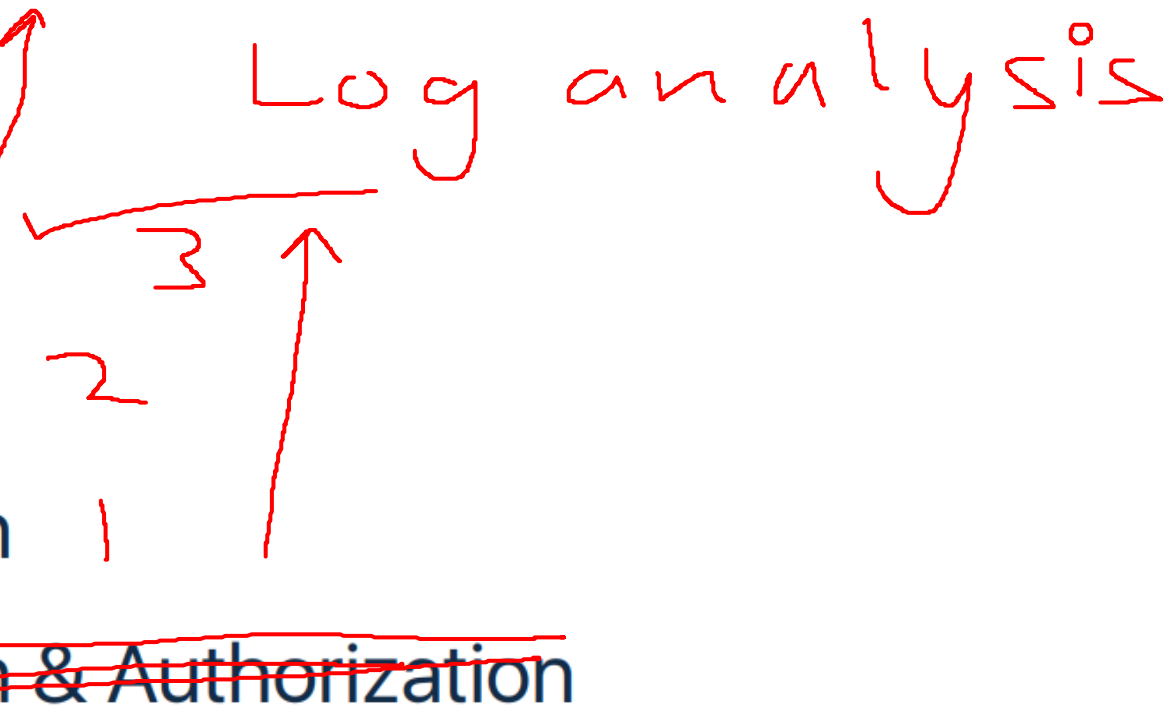
Question 33. Which of the following part(s) of the Authentication, Authorization, and Accounting (AAA) is responsible for measuring the resources a user consumes during access to a system?

(A) Accounting

(B) Authorization

(C) Authentication

(D) ~~Authentication & Authorization~~



Question 34. Which of the following actions should be taken to increase the security of SCADA networks? (Choose all that apply)

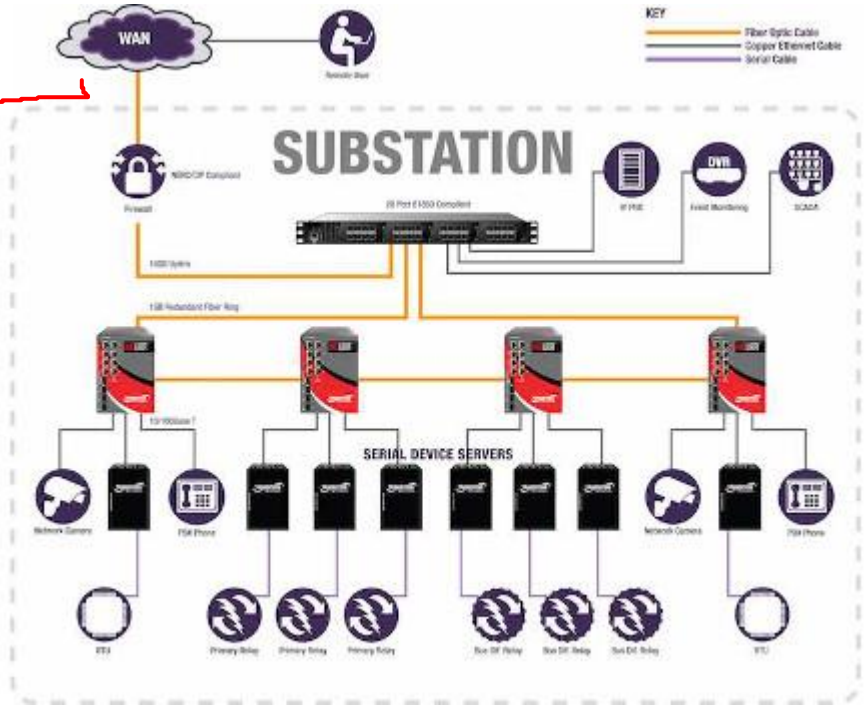
(A) Identify all connections to SCADA networks

(B) Disconnect unnecessary connections to the SCADA network

(C) Enable unnecessary services

(D) Implement internal and external intrusion detection systems

(E) Conduct physical security surveys and assess all remote sites connected to the SCADA network



Nerc CIP

Supervisory control and data acquisition (**SCADA**) is a control system architecture comprising computers, networked data communications and graphical user interfaces (GUI) for high-level process supervisory management, while also comprising other peripheral devices like programmable logic controllers (PLC)

Question 35. Your company migrates its infrastructure to the public cloud because of the advantages the cloud offers. Which of the following options are considered advantages for using public cloud services? (Choose all that apply.)

(A) Lower costs

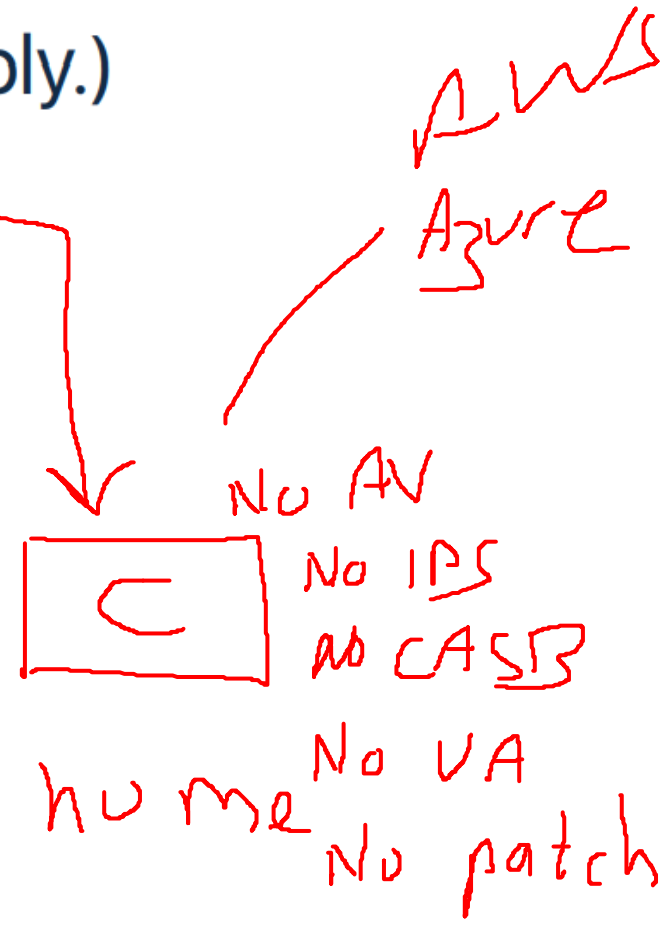
(B) No maintenance

(C) ~~Full-control~~

(D) Near-unlimited scalability

(E) High reliability

(F) ~~Secure data~~



Question 36. Given the following injection attacks, which one allows an attacker to interfere with the queries that an application makes to its database?

(A) SQL injection

(B) DLL Injection

(C) LDAP Injection

(D) XML Injection

Question 37. A member of the company asks for a financial transfer by sending an encrypted message to the financial administrator. An attacker eavesdrops on this message, captures it, and is now in a position to resend it. Because it's an authentic message that has simply been resent, the message is already correctly encrypted and looks legitimate to the financial administrator. Then the financial administrator is likely to respond to this new request, that response could include sending a large sum of money to the attacker's bank account. Which of the following type of attack does the scenario describe?

(A) Improper Input Handling

(B) Pass the hash attack

(C) Replay attack

(D) SSL Stripping

Question 38. The type of malicious code or software that looks legitimate but can take control of your computer is known as _____ . It is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network.

(A) Worm

(B) Spyware

(C) Ransomware

(D) Trojan

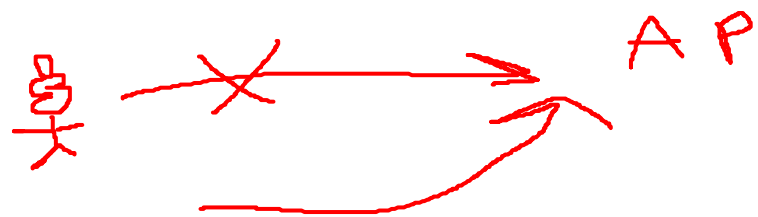
Question 39. _____ attacks are a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks.

(A) ~~Disassociation~~

(B) ~~Bluesnarfing~~

(C) ~~Bluejacking~~

(D) Jamming



Question 40. There are two main techniques for driver manipulating: Shimming and Refactoring. Shiming is the process of changing a computer program's internal structure without modifying its external functional behavior or existing functionality.

(A) ~~TRUE~~

(B) FALSE ✓

Refactoring is the process of changing a computer program's internal structure without modifying its external functional behavior or existing functionality.

Shimming is a small library that transparently intercepts API calls and changes the arguments passed. They also can be used for running programs on different software platforms than they were developed for.

Question 41. In which of the following attacks the attacker submitting many passwords or passphrases with the hope of eventually guessing correctly?

(A) Brute force attack

(B) Rainbow table attack

(C) Dictionary attack

(D) Plaintext Attack

Question 42. Which of the following attacks is a type of hacking wherein the perpetrator tries to crack the passwords stored in a database system?

(A) Brute force attack

(B) Rainbow table attack

(C) Dictionary attack

(D) Plaintext Attack

Question 43. Which of the following attack occurs when someone infiltrates a system through an outside partner or provider with access to the systems and data?

(A) Supply-chain attack — solarwinds

(B) ~~Skimming~~

(C) ~~Remote Access Trojan~~

(D) ~~Command and control~~

Question 44. Which of the following types of social engineering is a method in which the attacker seeks to compromise a specific group of end-users by infecting websites that members of that group are known to visit?

(A) Credential Harvesting

(B) Shoulder surfing

(C) Watering hole attack

(D) Dumpster diving

Question 45. In which of the following wireless network attacks the attacker set up a fraudulent Wi-Fi access point that appears to be legitimate but it is used to eavesdrop wireless communications?

(A) Rogue Access Point

(B) Evil Twin

(C) Initialization Vector

(D) Near-field Communication

Question 46. Which of the following types of social engineering techniques is the use of messaging systems to send an unsolicited message to large numbers of recipients for the purpose of commercial advertising, or for the purpose of non-commercial proselytizing?

(A) Tailgating

(B) Whaling

(C) Pharming

(D) Spamming

Question 47. Which of the following attacks is known as URL hijacking?

(A) ~~Impersonation attack~~

(B) ~~Hoax~~

(C) ~~Identity fraud~~

(D) Typosquatting attack ✓

goθgle

cyberwall.com

Question 48. Adversarial machine learning is a machine learning technique that attempts to fool models by supplying deceptive input.

(A) TRUE

(B) FALSE

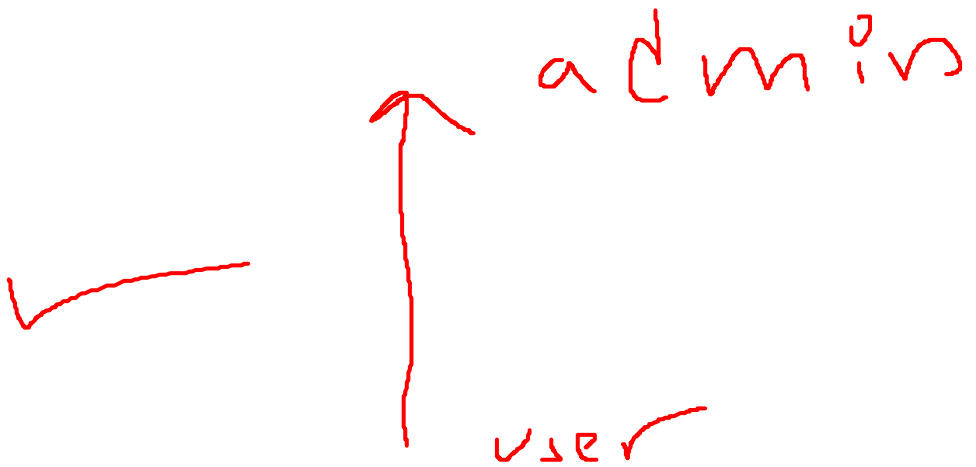
Question 49. What type of attack is when an attacker takes over a regular user account on a network and attempts to gain administrative permissions?

(A) Cross-site scripting

(B) ~~Directory traversal~~

(C) Privilege escalation

(D) ~~Buffer overflow~~



Question 50. A method by which authorized and unauthorized users are able to get around normal security measures and gain high-level user access (root access) on a computer system, network, or software application is known as:

(A) Backdoor

(B) ~~Botnet~~

(C) ~~Spraying~~

(D) ~~Pretexting~~

Question 51. In which of the following social engineering techniques the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile devices?

(A) Smishing

(B) Phising

(C) Spear phishing

(D) Vishing

Question 52. The attacker connects to a switch port and start sending a very large number of Ethernet frames with a different fake source MAC address. The switch's MAC address table becomes full and now it's not able to save more MAC address, which means it enters into a fail-open mode and starts behaving like a network Hub. Frames are flooded to all ports, similar to a broadcast type of communication. The attacker's machine will be delivered with all the frames between the victim and other machines. The attacker will be able to capture sensitive data from the network. Given the above scenario, identify the Layer 2 type of attack.

(A) ~~ARP poisoning~~

(B) MAC flooding

(C) ~~MAC cloning~~

(D) ~~Man-in-the-browser~~

Question 53. Which of the following Cryptographic attacks force victims to use older, more vulnerable versions of software in order to exploit known vulnerabilities against them?

(A) ~~Birthday~~

(B) ~~Collision~~

(C) Downgrade

(D) ~~Reconnaissance~~

Question 54. Which of the following attacks isn't intended to steal data but to remain in place for as long as possible, quietly mining in the background?

(A) Logic bomb

(B) Keylogger

(C) Rootkit

(D) Crypto-malware

Question 55. In which of the following API attacks, the attacker intercepts communications between an API endpoint and a client in order to steals and/or alters the confidential data that is passed between them?

(A) Man in the Middle

(B) Authentication Hijacking

(C) Unencrypted Communications

(D) Injection Attacks

Question 56. Which of the following options are considered as request forgery attacks? (Choose all that apply)

(A) Server-side

(B) Cross-site

(C) Forge-site

(D) Request-side

(E) Forge-side

Question 57. A hacker introduced corrupt Domain Name System (DNS) data into a DNS resolver's cache with the aim of redirecting users either to the wrong websites or to his own computer. What type of DNS attack, hacker implement in this scenario?

(A) DNS Poisoning

(B) URL redirection

(C) Domain Hijacking

(D) DNS Corruption

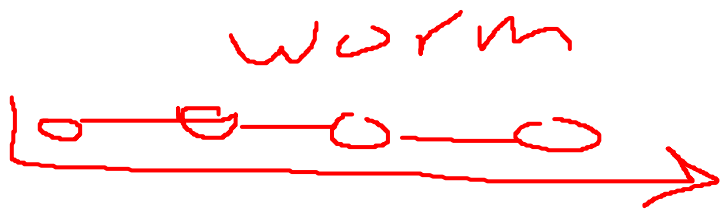
Question 58. The document that lists out the specifics of your penetration testing project to ensure that both the client and the engineers working on a project know exactly what is being tested when it's being tested, and how it's being tested is known as:

(A) ~~Lateral Movements~~

(B) Rules of Engagement

(C) ~~Pivoting~~

(D) ~~Bug Bounty~~



Question 59. Which of the following attacks is a Network Layer DDoS attack?

(A) BGP Hijacking

(B) DNS amplification

(C) HTTP Flood

(D) Slow Read

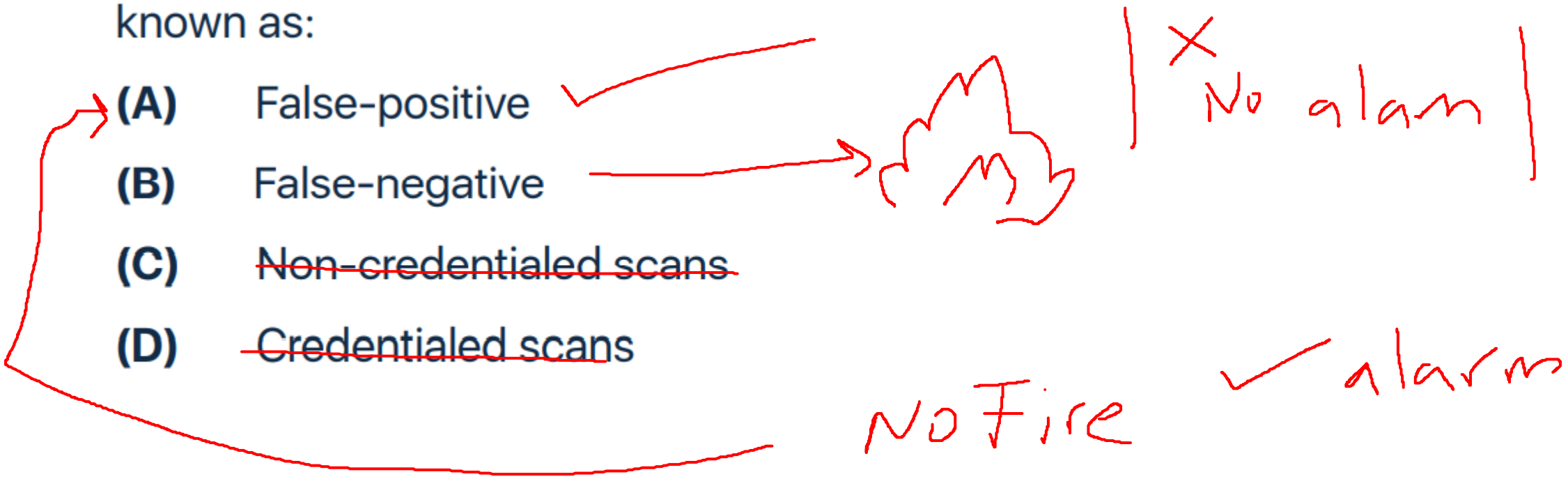
Question 60. You have set up an Intrusion detection system (IDS) and suddenly the IDS identifies an activity as an attack but the activity is acceptable behavior. The state, in this case, is known as:

(A) False-positive

(B) False-negative

(C) ~~Non-credentialed scans~~

(D) ~~Credentialed scans~~



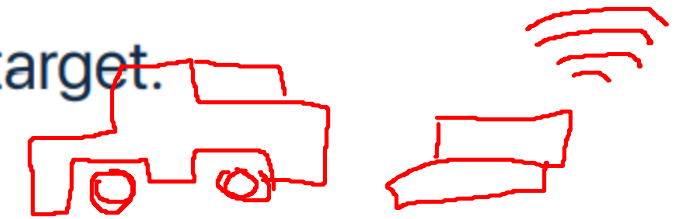
Question 61. A zero-day attack is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. (True/False)

(A) TRUE

(B) FALSE

Question 62. _____ is the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

(A) War Driving



(B) OSINT

(C) Footprinting

(D) ~~Cleanup~~

Question 63. Which of the following options is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures?

(A) ~~Log aggregation~~

(B) Common Vulnerabilities and Exposures

(C) Sentiment analysis

(D) ~~Security~~ Orchestration, Automation, and Response

Question 64. The type of hackers that violates computer security systems without permission, stealing the data inside for their own personal gain or vandalizing the system is commonly known as:

(A) Black-Hat hackers

(B) White-Hat hackers

(C) Red-Hat hackers

(D) Gray-Hat hackers

Question 65. A hacker attacks a network with the aim of maintaining ongoing access to the targeted network rather than to get in and out as quickly as possible with the ultimate goal of stealing information over a long period of time. Which type of attack a hacker used in this case?

(A) Insider threat

(B) State actors

(C) Hacktivism

(D) Advanced persistent threat (APT)

Question 66. Which of the following statements are true regarding Cloud-based security vulnerabilities? (Choose all the apply)

(A) Misconfigured Cloud Storage

(B) Poor Access Control

(C) Shared Tenancy

(D) Secure APIs

Question 67. You have been hired as a penetration tester for a company to locate and exploit vulnerabilities in its target's outward-facing services. You are not provided with any architecture diagrams or source code. This means that you are relying on dynamic analysis of currently running programs and systems within the target network. Which of the following pentesting assignments are you currently on?

(A) Gray-Box Testing

(B) White-Box Testing

(C) Black-Box Testing

(D) Open-Box Testing

Question 68. Which of the following terms refers to Information Technology (IT) applications and infrastructure that are managed and utilized without the knowledge of the enterprise's IT department?

(A) Script Kiddies

(B) Indicators of compromise

(C) Shadow IT

(D) Open-source intelligence

Question 69. Which of the following cybersecurity testing exercise team do not focus exclusively on attacking or defending, but they do both?

(A) Red team

(B) Blue team

(C) White team

(D) Purple team

Question 70. The technique of redirecting victims from a current page to a new URL which is usually a phishing page that impersonates a legitimate site and steals credentials from the victims is known as:

(A) URL redirection

(B) DNS spoofing

(C) Domain hijacking

(D) Domain redirection

Question 71. The type of hackers that are experts in compromising computer security systems and use their abilities for good, ethical, and legal purposes rather than bad, unethical, and criminal purposes is commonly known as:

(A) White-Hat hackers

(B) Black-Hat hackers

(C) Red-Hat hackers

(D) Gray-Hat hackers

Question 72. Which of the following features will you use to remotely clear your phones' data in the event of losing your phone?

(A) ~~Geofencing~~

(B) Remote wipe

(C) ~~Geolocation~~

(D) ~~Push notifications~~

Question 73. You have been tasked to access a remote computer for handling some administrative tasks over an unsecured network in a secure way. Which of the following protocols will you use to access the remote computer to handle the administrative tasks?

(A) ~~SRTP~~

(B) ~~LDAPS~~

(C) SSH

(D) ~~HTTPS~~

Question 74. As a security expert of your company you are responsible for preventing unauthorized (rogue) Dynamic Host Configuration Protocols servers offering IP addresses to the clients. Which of the following security technology will you implement to meet the requirement?

(A) DHCP snooping

(B) ~~BPDU guard~~

(C) ~~MAC filtering~~

(D) ~~Jump server~~

Question 75. You have been hired as a security expert to implement a security solution to protect an organization from external threats. The solution should provide packet filtering, VPN support, network monitoring, and deeper inspection capabilities that give the organization a superior ability to identify attacks, malware, and other threats. Which of the following security solutions will you implement to meet the requirement?

(A) Next-generation firewall (NGFW)

(B) Endpoint detection and response (EDR)

(C) Anti-malware

(D) Antivirus

Question 76. One of the features of SNMPv3 is called message integrity.

(A) TRUE

(B) FALSE

Question 77. You have been tasked to implement a solution to increase the security of your company's local area network (LAN). All of the company's external-facing servers (Web server, Mail server, FTP server) should be placed in a separate area in order to be accessible from the internet, but the rest of the internal LAN to be unreachable. Which of the following techniques will you implement to meet the requirement?

(A) DMZ

(B) ~~VLAN~~

(C) ~~VPN~~

(D) ~~DNS~~

allow

Question 78. Application whitelisting prevents undesirable programs from executing, while application blacklisting is more restrictive and allows only programs that have been explicitly permitted to run.

(A) TRUE — black

(B) FALSE ✓

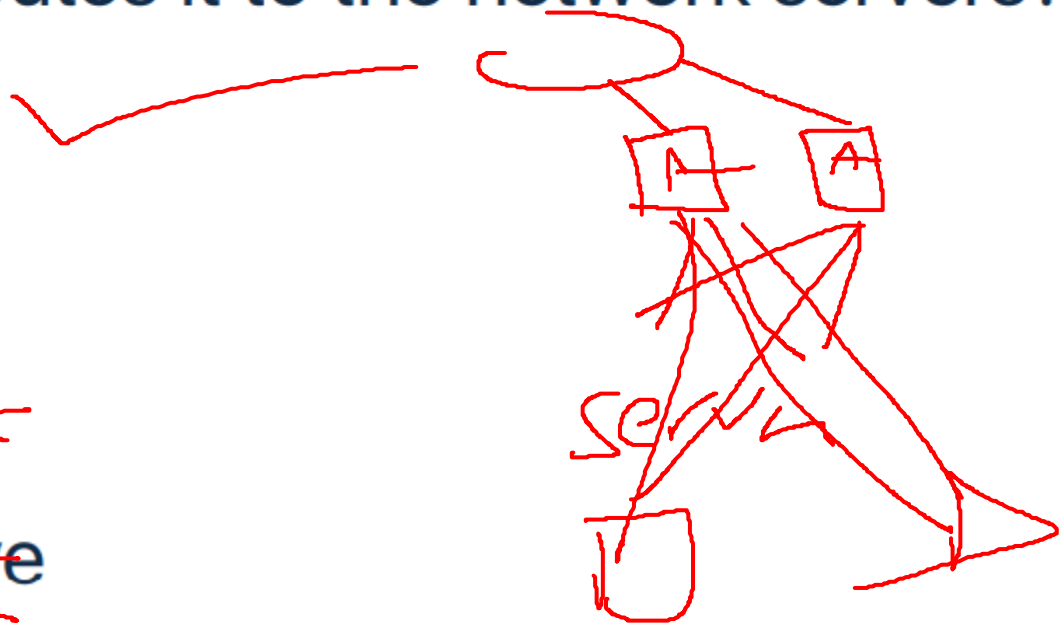
Question 79. In which of the following load balancer mode, two or more servers aggregate the network traffic load and work as a team distributes it to the network servers?

(A) Active/active

(B) Active/passive

(C) ~~Passive/active~~

(D) ~~Passive/passive~~



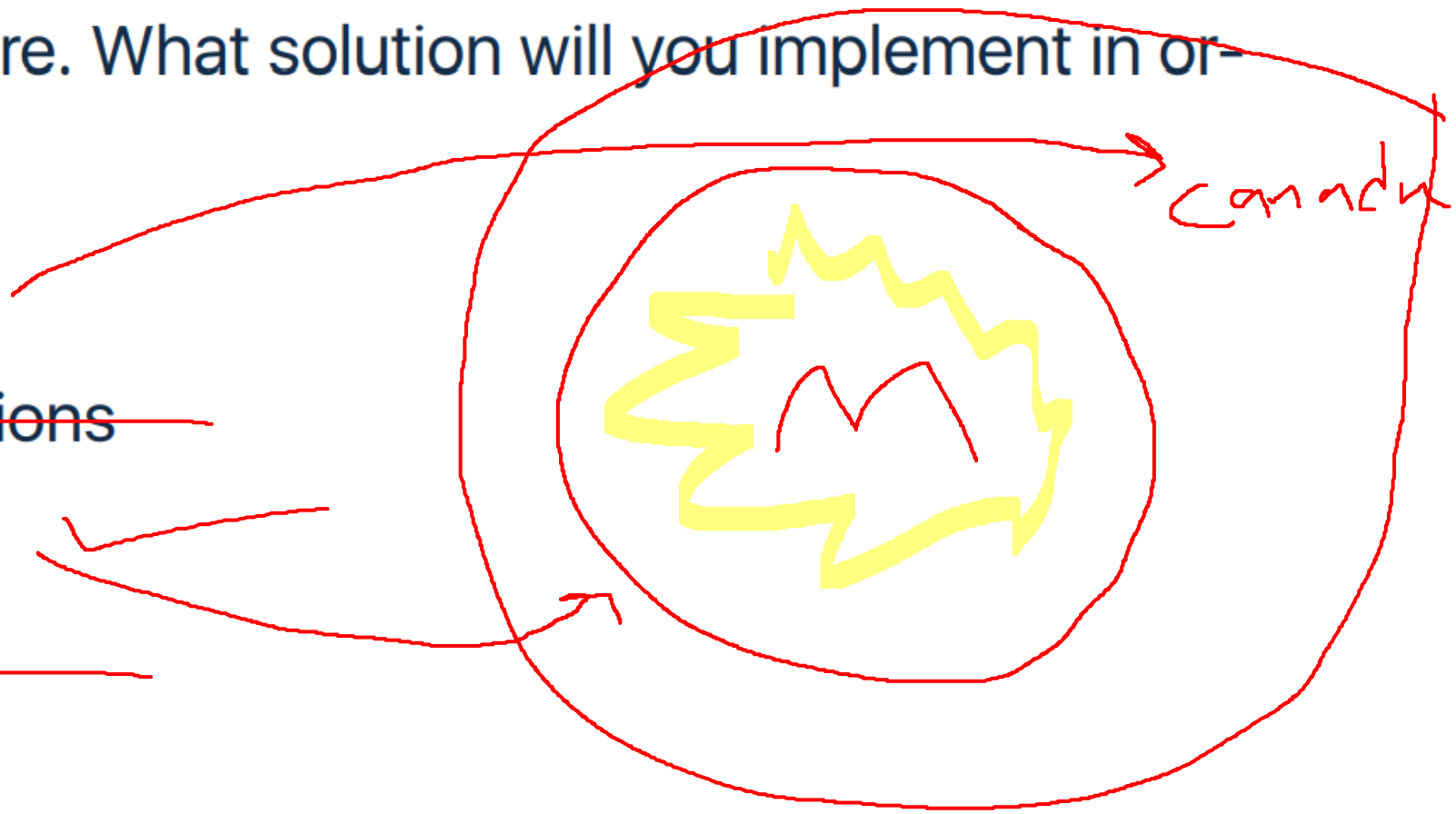
Question 80. You have been tasked to implement a solution to send product offers to consumers' smartphones when they trigger a search in a particular geographic location, enter a mall, neighborhood, or store. What solution will you implement in order to achieve that?

(A) Geolocation

(B) ~~Push notifications~~

(C) Geofencing

(D) ~~Remote wipe~~



Question 81. The type of network hardware appliance that protects networks against security threats (malware, attacks) that simultaneously target separate parts of the network by integrating multiple security services and features is known as:

(A) Network address translation (NAT)

(B) Web application firewall (WAF)

(C) Content/URL filter

(D) Unified threat management (UTM)

Question 82. For security and monitoring purposes your company instructed you to implement a solution so that all packets entering or exiting a port should be copied and then should be sent to a local interface for monitoring. Which of the following solution will you implement in order to meet the requirement?

(A) ~~Access control list (ACL)~~

(B) Port mirroring

(C) ~~Quality of service (QoS)~~

(D) ~~File Integrity Monitoring~~

Question 83. Your manager trying to understand the difference between SFTP and FTPS. So, he asked you to explain the difference between those. Which of the following statements are correct? (Choose all that apply.)

(A) SFTP, also known as SSH FTP, encrypts both commands and data while in transmission

(B) FTPS, also known as FTP Secure or FTP-SSL

(C) SFTP protocol is packet-based as opposed to text-based making file and data transfers faster

(D) FTPS authenticates your connection using a user ID and password or SSH Keys

(E) SFTP authenticates your connection using a user ID and password, a certificate, or both

Question 84. The network administrator from your company notices that the network performance has been degraded due to a broadcast storm. Which of the following techniques will you recommend to the network administrator in order to reduce broadcast storms? (Choose all that apply)

(A) Check for loops in switches

(B) Split up your broadcast domain

(C) Allow you to rate-limit broadcast packets

(D) Check how often ARP tables are emptied

(E) Split up your collision domain

(F) Check the routing tables

Question 85. Which of the following technologies will you use in order to send instant notifications to your subscribed users each time you publish a new blog post on your website?

(A) Push notifications

(B) ~~Geofencing~~

(C) ~~Geolocation~~

(D) ~~Remote wipe~~

Question 86. It has been noticed the Wi-Fi of your company is slow and sometimes not operational. After investigation, you noticed this caused by channel interference. Which of the following solutions will you implement to avoid problems such as channel interference when you build your WLAN?

(A) Heat maps

(B) WiFi Protected Setup

(C) Captive portal

(D) You can't avoid channel interference

Question 87. Which of the following options are cryptographic protocols? (Choose all the apply)

(A) WPA2

(B) WPA3

(C) CCMP

(D) SAE

(E) EAP

(F) PEAP

Question 87. Which of the following options are cryptographic protocols? (Choose all the apply)

(A) WPA2

(B) WPA3

(C) CCMP

(D) SAE

(E) EAP

(F) PEAP

Question 89. You have been tasked to implement a solution to encrypt data as it is written to the disk and decrypt data as it is read off the disk. Which of the following solution will you implement to meet the requirement?

(A) ~~Root of trust~~

(B) ~~Trusted Platform Module~~

(C) Self-encrypting drive (SED) / full-disk encryption (FDE)

(D) ~~Sandboxing~~

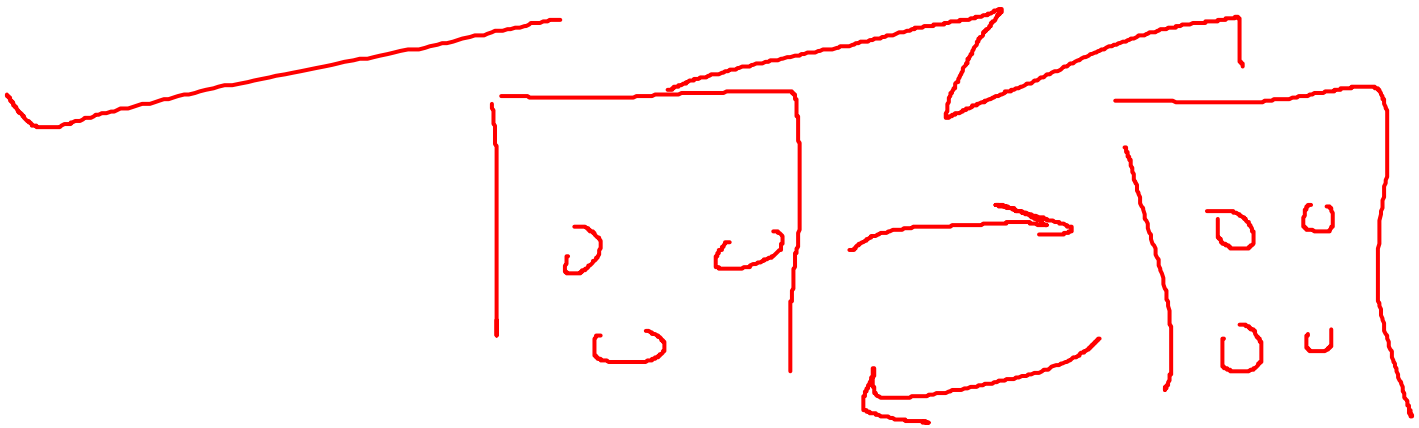
Question 90. Which of the following VPN solutions is used to connect two local area networks (LANs) utilized by businesses large and small that want to provide their employees with secure access to network resources?

(A) Remote access

(B) Site-to-site

(C) Split tunnel

(D) Proxy server



Question 91. Which of the following options are authentication protocols? (Choose all the apply)

(A) EAP

(B) PEAP

(C) ~~WPA2~~

(D) ~~WPA3~~

(E) RADIUS

Question 92. Which of the following types of certificates will you use to digitally sign your apps as a way for end-users to verify that the code they receive has not been altered or compromised by a third party?

(A) ~~Wildcard~~

(B) ~~Subject alternative~~ name

(C) Code signing certificates

(D) ~~Self-signed~~

Question 93. What technique is used for IP address conservation by making private IP addresses to connect to the Internet?

(A) NAT

(B) UTM

(C) WAF

(D) ACL

Question 94. Which of the following authentication protocols allows you to use an existing account to sign in to multiple websites, without needing to create new passwords?

(A) OpenID

(B) Kerberos

(C) TACACS+

(D) OAuth

OpenID is about authentication (ie. proving who you are), **OAuth** is about authorisation (ie. to grant access to functionality/data/etc.. without having to deal with the original authentication). **OAuth** could be used in external partner sites to allow access to protected data without them having to re-authenticate a user.

Question 95. Assuming you have the domain yourcompany.com with the following sub-domains:

www.yourcompany.com

mail.yourcompany.com

intranet.yourcompany.com

secure.yourcompany.com

me.yourcompany.com

Which of the following types of certificates will you choose to secure all the first-level sub-domains on a single domain name?

(A) Subject alternative name

(B) Code signing certificates

(C) Wildcard

(D) Self-signed

Question 96. A _____ certificate is a digital certificate that's not signed by a publicly trusted certificate authority (CA). These certificates are created, issued, and signed by the company or developer who is responsible for the website or software being signed.

(A) Self-signed

(B) Wildcard

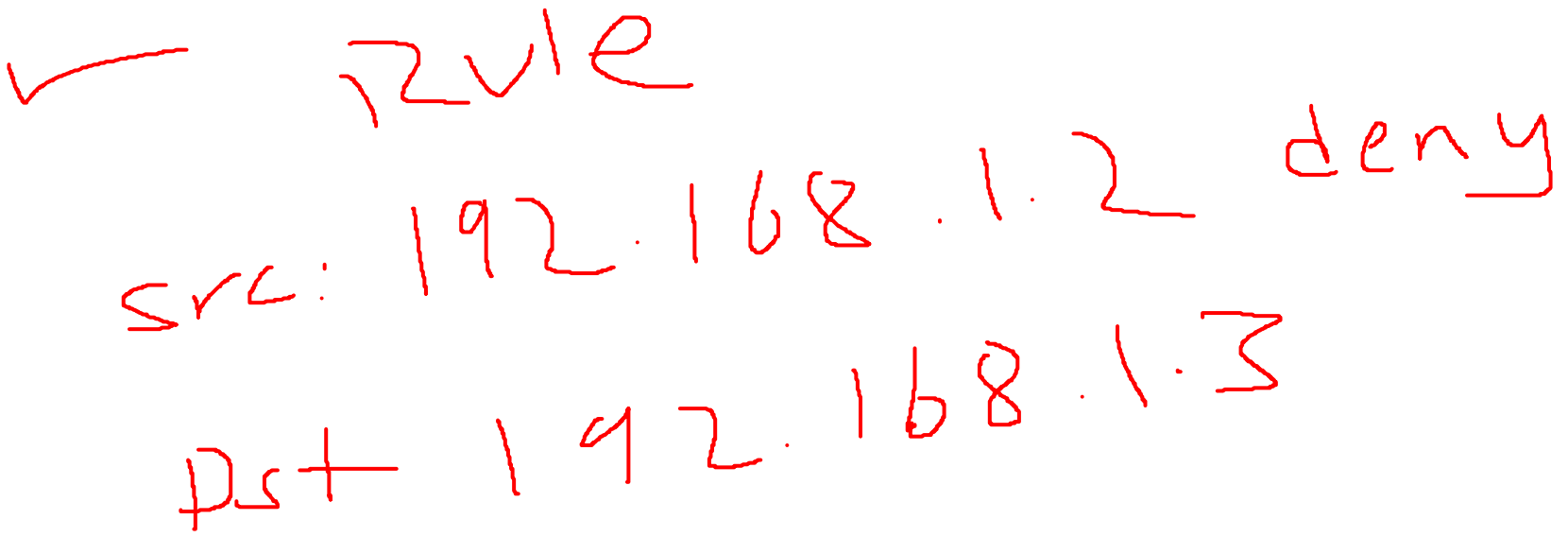
(C) Subject alternative name

(D) Code signing certificates

Question 97. In the form of Rule-Based Access Control, data are accessible or not accessible based on the user's IP address.

(A) TRUE

(B) FALSE



Question 98. WiFi _____ Setup is a wireless network security standard that tries to make connections between a router and wireless devices faster, easier, and more secure.

(A) Faster

(B) Easier

(C) Protected

(D) Secured

Question 99. Which of the following Public key infrastructure (PKI) terms is known as an organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates?

(A) Certificate authority (CA)

(B) Registration authority (RA)

(C) Online Certificate Status Protocol (OCSP)

(D) Certificate signing request (CSR)

Question 100. You have been tasked to implement a security solution so all the network events from your company should be recorded in a central database for further analysis. Which of the following security solutions will you implement to meet the requirement?

(A) Next-generation firewall (NGFW)

(B) Endpoint detection and response (EDR) — network

(C) Anti-malware

(D) Antivirus

Question 101. Access _____ List is a network traffic filter that controls incoming or outgoing traffic. It works on a set of rules that define how to forward or block a packet at the router's interface.

(A) Security

(B) Filter

(C) Control

(D) Service

Question 102. Which of the following VPN solutions is used to connect a personal user device to a remote server on a private network?

(A) Remote Access

(B) Site-to-site

(C) Split tunnel

(D) Proxy server

Question 103. In the form of Role-Based Access Control, data are accessible or not accessible based on the user's IP address.

(A) TRUE

(B) FALSE ✓

Question 104. In cloud computing, the ability to scale up and down resources based on the user's needs is known as:

(A) Virtual private cloud

(B) Network segmentation

(C) Dynamic resource allocation

(D) Public subnet

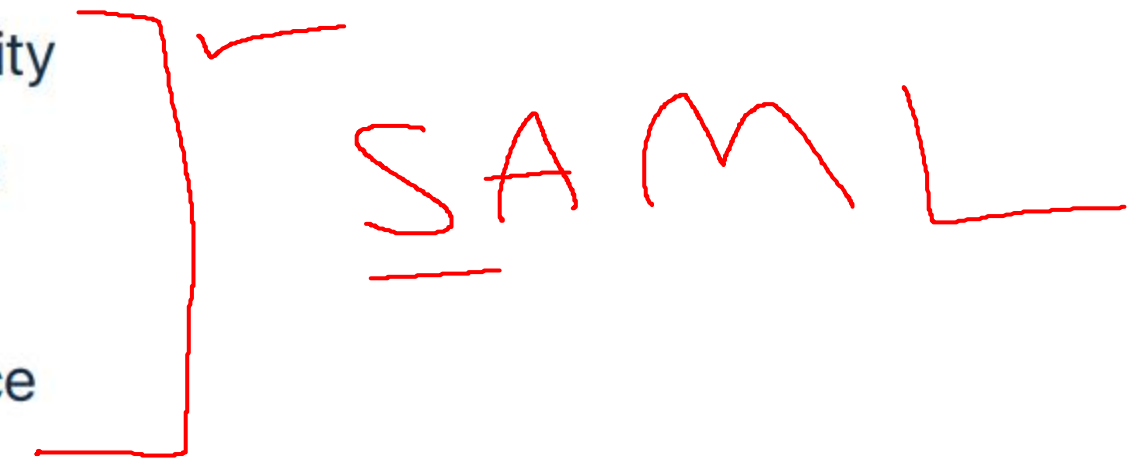
Question 105. _____ Assertions Markup Language is an important component of many SSO systems that allow users to access multiple applications, services, or websites from a single login process. It is used to share security credentials across one or more networked systems.

(A) Security

(B) Single

(C) Sign

(D) Service



Question 106. You have been tasked to configure the Wi-Fi of your company's LAN to allow certain computers to have access to the Internet and the rest computers need to be blocked.

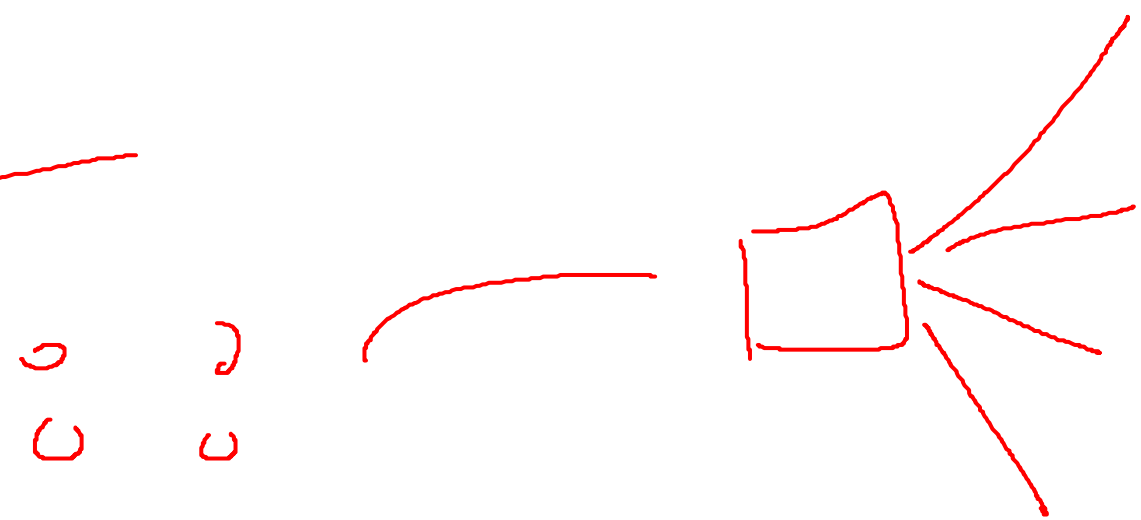
Which of the following security technology will you implement to meet the requirement?

(A) ~~DHCP snooping~~

(B) ~~BPDU guard~~

(C) MAC filtering

(D) ~~Jump server~~



Question 107. You have been noticed that the email server doesn't work. Your manager said that someone from the company changed the DNS records (MX) of the email server. Which of the following commands will you type to find the new MX records of the server?

(A) ~~tracert~~

(B) ~~ipconfig~~

(C) ~~ping~~

(D) nslookup — -query =mx yourdomain.com

Question 108. Assuming you are working on a Windows environment. What command will you type to identify the number of hops and the time it takes for a packet to travel between your local computer and your web server?

(A) tracert

(B) ~~ipconfig~~

(C) ~~ping~~

(D) ~~nslookup~~

Question 109. Wireshark is a command-line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.

(A) TRUE

(B) FALSE

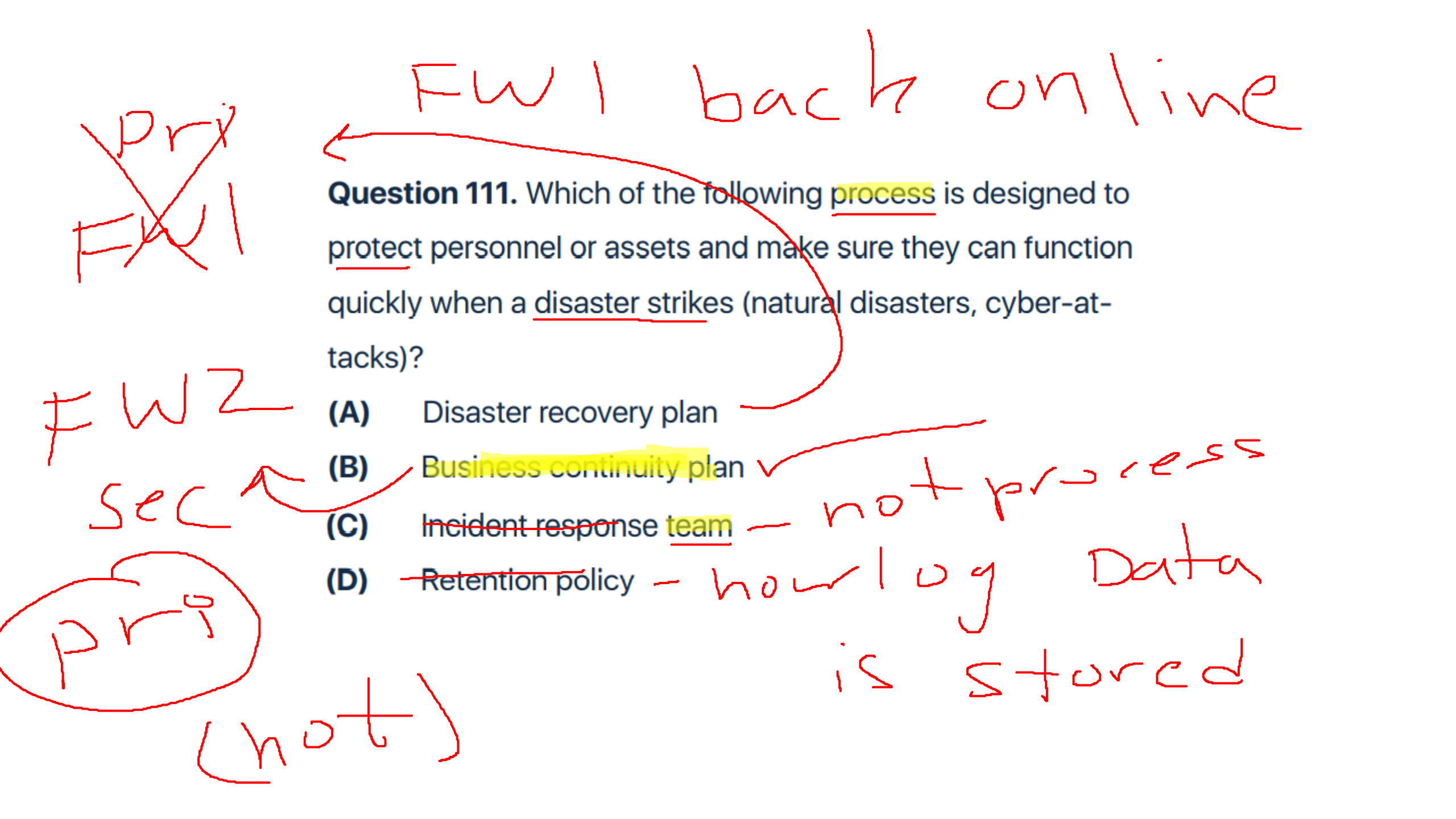
Question 110. PC1 can ping the printer device on the Marketing team network but can't ping the printer on the Sales team network. Assuming you are working on a Linux environment, which of the following commands will you type to get details about the route that packets go through from the PC1 to the printer on the Sales team network?

(A) traceroute

(B) ~~ifconfig~~

(C) ~~dig~~

(D) tracert



Question 111. Which of the following process is designed to protect personnel or assets and make sure they can function quickly when a disaster strikes (natural disasters, cyber-attacks)?

(A) Disaster recovery plan

(B) Business continuity plan

(C) ~~Incident response~~ team

(D) ~~Retention~~ policy

Question 112. You need to mitigate all the networking attacks that exploit open unused TCP ports on your system. Which of the following command displays active TCP connections and ports on which the computer is listening?

(A) netstat

(B) arp

(C) route

(D) sniper

Question 113. The log file of your company's network status is updated frequently, and the most critical information is on the first five lines. You want to avoid opening the entire file each time, only to view the first five lines. What command will you use to view only the first five lines of the log file?

(A) head

(B) tail

(C) cat

(D) chmod

Question 114. Assuming you are working on a Windows environment. For troubleshooting reasons, you need to discover your IP information, including DHCP and DNS server addresses from your current workstation. Which of the following commands will help you to troubleshoot the network?

(A) tracert

(B) ipconfig

(C) nslookup

(D) ping

Question 115. Which of the following tools can you use to perform manual DNS lookups? Assuming you are working on a Linux environment. (Choose all that apply)

(A) route

(B) pathping

(C) nslookup

(D) dig

(E) ifconfig

(Linux)

Question 116. Which of the following process describes how long businesses need to keep a piece of information (a record), where it's stored, and how to dispose of the record when its time?

(A) Disaster recovery plan

(B) Business continuity plan

(C) Incident response team

(D) Retention policy

Question 117. _____ measures the predicted time that passes between one previous failure of a mechanical/electrical system to the next failure during normal operation. In simpler terms, it helps you predict how long an asset can run before the next unplanned breakdown happens.

(A) Recovery point objective (RPO)

(B) Mean time to repair (MTTR)

(C) Recovery Time Objective (RTO)

(D) Mean time between failures (MTBF)

Question 118. _____ is a set of rules designed to give EU citizens more control over their personal data.

(A) General Data Protection Regulation (GDPR)

(B) Payment Card Industry Data Security Standard (PCI DSS)

(C) National Institute of Standards and Technology (NIST)

(D) International Organization for Standardization (ISO)

Question 119. The _____ is described as an estimated frequency of the threat occurring in one year.

(A) Single loss expectancy (SLE)

(B) Annualized loss expectancy (ALE)

(C) Annualized rate of occurrence (ARO)

(D) Business continuity plan

Question 121. A _____ is an agreement between two or more parties outlined in a formal document. It is not legally binding but signals the willingness of the parties to move forward with a contract.

(A) Service level agreement (SLA)

(B) End of life (EOL)

(C) Memorandum of understanding (MOU)

(D) Non-Disclosure Agreement (NDA)

Question 122. A _____ is a legally enforceable contract that establishes confidentiality between two parties—the owner of protected information and the recipient of that information.

(A) Non-Disclosure Agreement (NDA)

(B) Memorandum of understanding (MOU)

(C) Service-level agreement (SLA)

(D) End of life (EOL)

Question 123. _____ describes a period of time in which an enterprise's operations must be restored following a disruptive event, e.g., a cyberattack, natural disaster, or communications failure.

(A) Recovery point objective (RPO)

(B) Mean time to repair (MTTR)

(C) Recovery Time Objective (RTO)

(D) Mean time between failures (MTBF)

Question 124. The _____ is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

(A) Recovery point objective (RPO)

(B) Mean time to repair (MTTR)

(C) Recovery Time Objective (RTO)

(D) Mean time between failures (MTBF)

Question 125. _____ is a strategy that ensures continuity of operations with minimal service outage or downtime. It is designed to protect personnel or assets and make sure they can function quickly when a disaster strikes such as natural disasters or cyber-attacks.

(A) Single loss expectancy (SLE)

(B) Annualized loss expectancy (ALE)

(C) Annualized rate of occurrence (ARO)

(D) Business continuity plan

Practice TEST

1. Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow

B. Zero-day

C. End of life

D. Race condition

2. A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

A. Due to foreign travel, the user's laptop was isolated from the network.

B. The user's laptop was quarantined because it missed the latest path update.

C. The VPN client was blacklisted.

D. The user's account was put on a legal hold.

3. A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.

B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.

C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.

D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

4. A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location

B. Impossible travel time

C. Geolocation

D. Geofencing

5. A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

A. Option A

B. Option B

C. Option C

D. Option D

6. A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

7. An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?

A. Zero-day

B. Default permissions

C. Weak encryption

D. Unsecure root accounts

8. A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

A. FDE

B. NIDS

C. EDR

D. DLP

9. A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

A. AH
B. ESP

C. SRTP

D. LDAP

10. A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

A. Trusted Platform Module

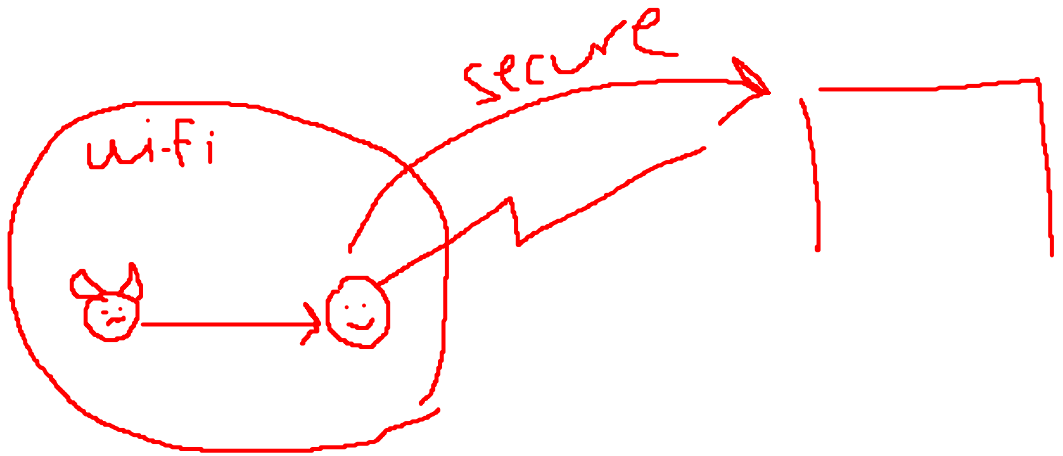
B. A host-based firewall

C. A DLP solution

D. Full disk encryption

E. A VPN

F. Antivirus software



11. Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

A. An ARO

B. An MOU

C. An SLA

D. A BPA

12. Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer

B. The data processor

C. The data owner

D. The data controller

13. Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log m to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

A. COPE

B. VDI

C. GPS

D. TOTP

E. RFID

F. BYOD

14. The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

A. Geolocation

B. Time-of-day restrictions

C. Certificates

D. Tokens

E. Geotagging

F. Role-based access controls

15. Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

A. Cross-site scripting

B. Data exfiltration

C. Poor system logging

D. Weak encryption

E. SQL injection

F. Server-side request forgery

16. A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management

B. Full-device encryption

C. Remote wipe

D. Biometrics

17. A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN?

A. AH

B. EDR

C. ESP

D. DNSSEC

18. The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed.

Which of the following is the MOST likely cause of the CRO's concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.

B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.

C. SSO would reduce the password complexity for frontline staff.

D. D. SSO would reduce the resilience and availability of system if the provider goes offline.

19. A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

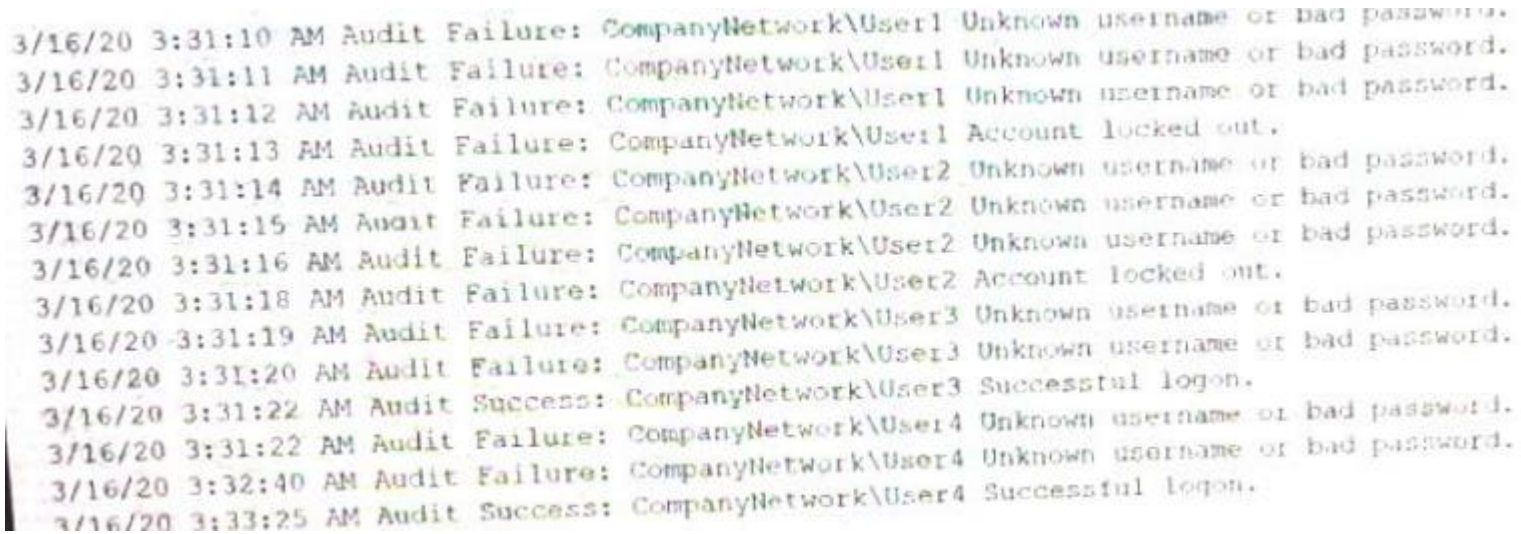
A. Automated information sharing

B. Open-source intelligence

C. The dark web

D. Vulnerability databases

20. A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:



Which of the following attacks MOST likely occurred?

A. Dictionary

B. Credential-stuffing

C. Password-spraying

D. Brute-force

21. Which of the following will provide the BEST physical security countermeasures to stop intruders?

(Select TWO.)

A. Alarms

B. Signage

C. Lighting

D. Mantraps

E. Fencing

F. Sensors

22. In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference

B. Avoidance

C. Acceptance

D. Mitigation

23. A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

A. MAC Flooding

B. DNS poisoning

C. MAC cloning

D. ARP poisoning

24. An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

A. Date of birth

B. Fingerprints

C. PIN

D. TPM

25. A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

A. Configuring signature-based antivirus io update every 30 minutes

B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.

C. Implementing application execution in a sandbox for unknown software.

D. Fuzzing new files for vulnerabilities if they are not digitally signed

26. Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.

B. Implement an IDS/IPS

C. Implement a heuristic behavior-detection solution.

D. Implement CASB to protect the network shares.

27. A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.

B. Segment the network into trusted and untrusted zones.

C. Enforce application whitelisting.

D. Implement DLP at the network boundary.

28. A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

A. Session replay

B. Evil twin

C. Bluejacking

D. ARP poisoning

29. A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

A. Hard token

B. Retina scan

C. SMS text

D. Keypad PIN

are: Bio
know: pin
have: card

30. A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE

B. SIEM

C. SOAR

D. CVSS

31. Which of the following algorithms has the SMALLEST key size?

A. DES

B. Twofish

C. RSA

D. AES

32. The process of passively gathering information poor to launching a cyberattack is called:

A. tailgating

B. reconnaissance

C. pharming

D. prepending

34. An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

A. business continuity plan

~~B. communications plan.~~

C. disaster recovery plan.

~~D. continuity of operations plan~~

35. Which of the following relets to applications and systems that are used within an organization without consent or approval?

A. Shadow IT

B. OSINT

C. Dark web

D. Insider threats

The difference between MFA and 2FA is simple. **Two-factor** authentication (2FA) always utilizes **two** of these **factors** to verify the user's identity. **Multi-factor** authentication (MFA) could involve **two** of the **factors** or it could involve all three. "**Multi-factor**" just means any number of **factors** greater than one.

36. A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

A. VPN

B. Drive encryption

C. Network firewall

D. File level encryption

E. USB blocker

F. MFA

37. After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

A. Multifactor authentication

B. Something you can do

C. Biometric

D. Two-factor authentication

38. A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

A. DoS

B. SSL stripping

C. Memory leak

D. Race condition

E. Shimming

F. Refactoring

A **race condition** is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time. It becomes a bug when one or more of the possible behaviors is undesirable.

39. A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).

A. Password and security question

B. Password and CAPTCHA

C. Password and smart card

D. Password and fingerprint

E. Password and one-time token

F. Password and voice

40. An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility

B. Data recovery

C. Chain of custody

D. Non-repudiation

41. An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

A. Shadow IT

B. An insider threat

C. A hacktivist

D. An advanced persistent threat

42. An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

A. MTBF

B. RPO

C. MTTR

D. RTO

43. In which of the following common use cases would steganography be employed?

A. Obfuscation

B. Integrity

C. Non-repudiation

D. Blockchain

44. An analyst has determined that a server was not patched and an external actor exfiltrated data on port

139. Which of the following sources should the analyst review to BEST ascertain how the Incident could have been prevented?

A. ~~The vulnerability scan output~~

B. The security logs — raw event logs

C. ~~The baseline report~~

D. The correlation of events → something happened

45. A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting

B. Keylogger

C. Brute-force

D. Spraying

46. Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before

sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing

B. Whaling

C. Phishing

D. Vishing

47. A security analyst is configuring a large number of new company-issued laptops. The analyst received

the following requirements:

• The devices will be used internationally by staff who travel extensively.

• Occasional personal use is acceptable due to the travel requirements.

• Users must be able to install and configure sanctioned programs and productivity suites.

• The devices must be encrypted

• The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

A. Configuring an always-on VPN

B. Implementing application whitelisting

C. Requiring web traffic to pass through the on-premises content filter

D. Setting the antivirus DAT update schedule to weekly

48. The website http://companywebsite.com requires users to provide personal Information, Including security question responses, for registration. Which of the following would MOST likely cause a data breach?

A. Lack of input validation

B. Open permissions

C. Unsecure protocol

D. Missing patches

49. A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

A. DNSSEC

B. Reverse proxy

C. VPN concentrator

D. PKI

E. Active Directory

F. RADIUS

50. A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk.

Which of the following should the administrator use?

A. dd

B. chmod

C. dnsenum

D. logger

51. A company uses wireless tor all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

A. A BPDU guard

B. WPA-EAP

C. IP filtering

D. A WIDS

52. The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

A. Updating the playbooks with better decision points

B. Dividing the network into trusted and untrusted zones

C. Providing additional end-user training on acceptable use

D. Implementing manual quarantining of infected hosts

53. A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A. An air gap

B. A Faraday cage

C. A shielded cable

D. A demilitarized zone

54. A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords

B. Email tokens

C. Push notifications

D. Hardware authentication

55. The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.

B. Segment the network with firewalls.

C. Update all antivirus signatures daily.

D. Implement application blacklisting.

56. A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

A. An NGFW

B. A CASB

C. Application whitelisting

D. An NG-SWG

58. A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network

B. Implement salting and hashing

C. Configure the web content filter to block access to the forum.

D. Increase password complexity requirements

59. Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS

B. PaaS

C. IaaS

D. DaaS

60. A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

A. Man-in- the middle

B. Spear-phishing

C. Evil twin

D. DNS poising

61. A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers Which of the following tools should the analyst use?

A. netstat

B. net share

C. netcat

D. nbtstat

E. net session