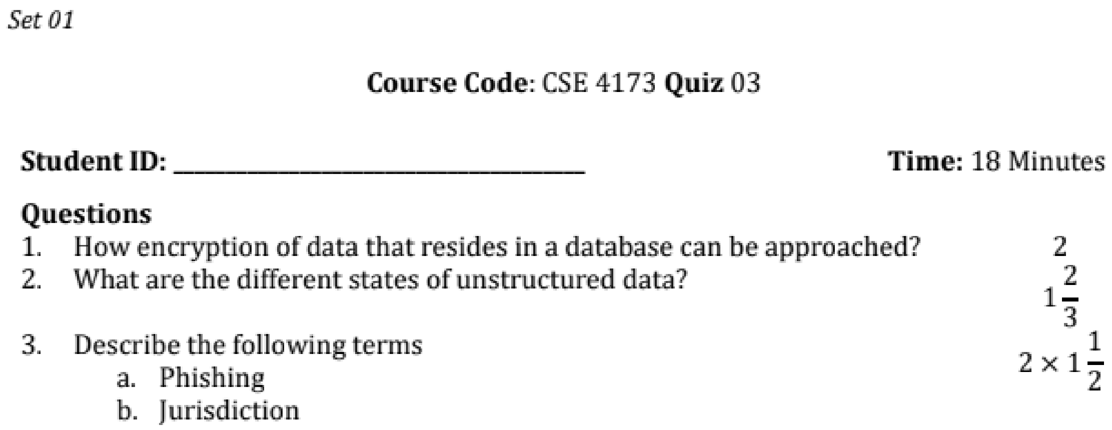
SET-01



Set 01

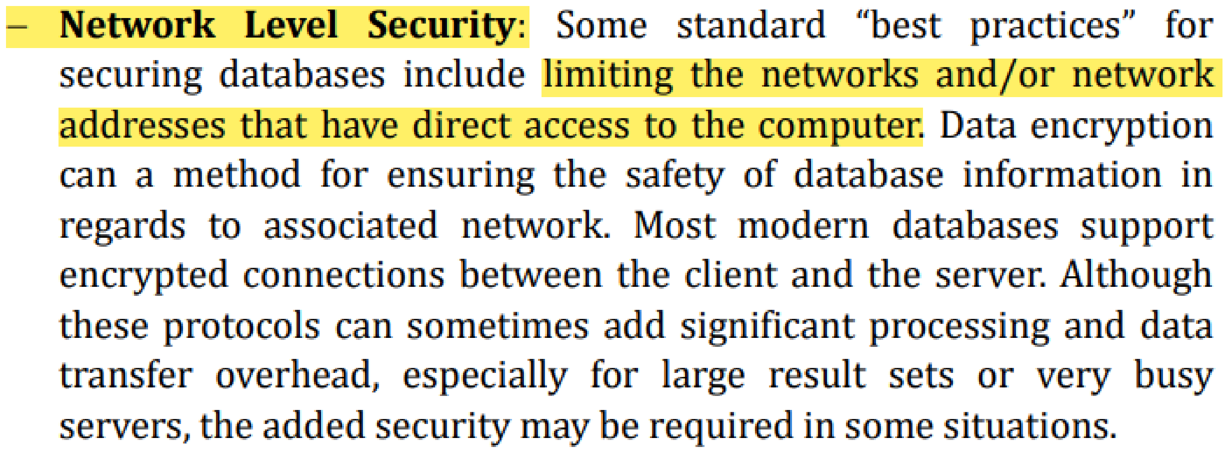
Course Code: CSE 4173 **Quiz** 03

Student ID: __________________________________ **Time:** 18 Minutes

Questions

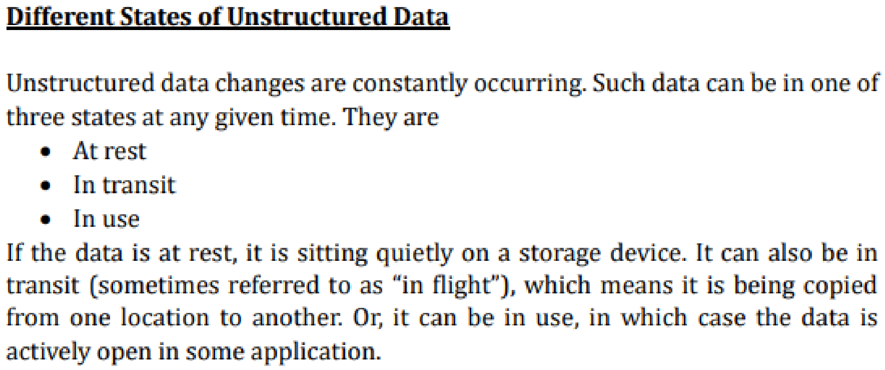
1. How encryption of data that resides in a database can be approached? 2
2. What are the different states of unstructured data? $1\frac{2}{3}$
3. Describe the following terms $2 \times 1\frac{1}{2}$
   a. Phishing
   b. Jurisdiction

1)



– **Network Level Security**: Some standard "best practices" for securing databases include limiting the networks and/or network addresses that have direct access to the computer. Data encryption can a method for ensuring the safety of database information in regards to associated network. Most modern databases support encrypted connections between the client and the server. Although these protocols can sometimes add significant processing and data transfer overhead, especially for large result sets or very busy servers, the added security may be required in some situations.

2)



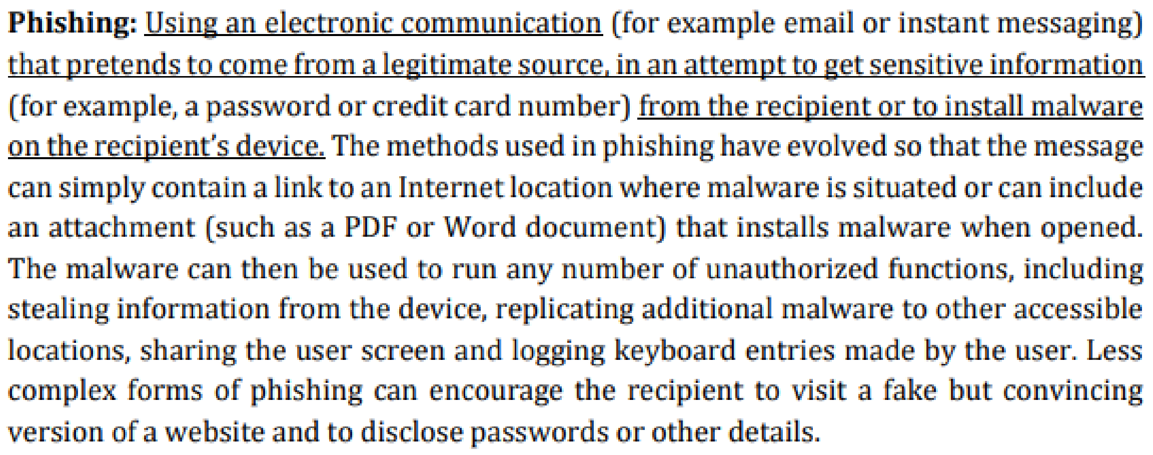
Different States of Unstructured Data

Unstructured data changes are constantly occurring. Such data can be in one of three states at any given time. They are

- At rest
- In transit
- In use

If the data is at rest, it is sitting quietly on a storage device. It can also be in transit (sometimes referred to as "in flight"), which means it is being copied from one location to another. Or, it can be in use, in which case the data is actively open in some application.

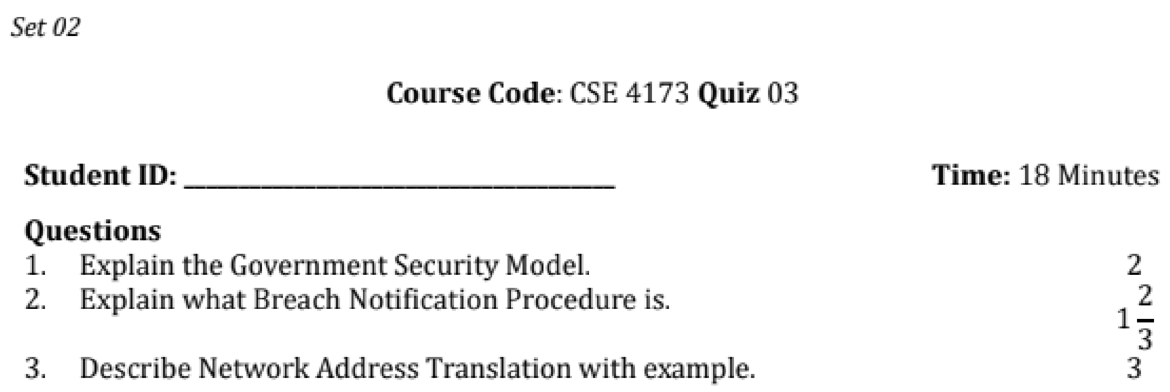
3)



Phishing: Using an electronic communication (for example email or instant messaging) that pretends to come from a legitimate source, in an attempt to get sensitive information (for example, a password or credit card number) from the recipient or to install malware on the recipient's device. The methods used in phishing have evolved so that the message can simply contain a link to an Internet location where malware is situated or can include an attachment (such as a PDF or Word document) that installs malware when opened. The malware can then be used to run any number of unauthorized functions, including stealing information from the device, replicating additional malware to other accessible locations, sharing the user screen and logging keyboard entries made by the user. Less complex forms of phishing can encourage the recipient to visit a fake but convincing version of a website and to disclose passwords or other details.

Jurisdiction is like the authority or power a court or government agency has to handle certain cases and make decisions. It's about where they have the right to operate. Think of it as their turf or territory. They can only make decisions and enforce laws within the boundaries of their jurisdiction. So, if a court has jurisdiction over a certain area, it means it has the power to hear cases and make rulings there.

SET-02



Set 02

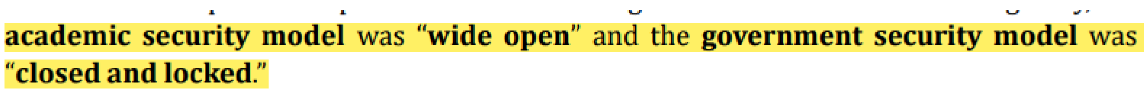
Course Code: CSE 4173 **Quiz** 03

Student ID: ________________________________ **Time:** 18 Minutes

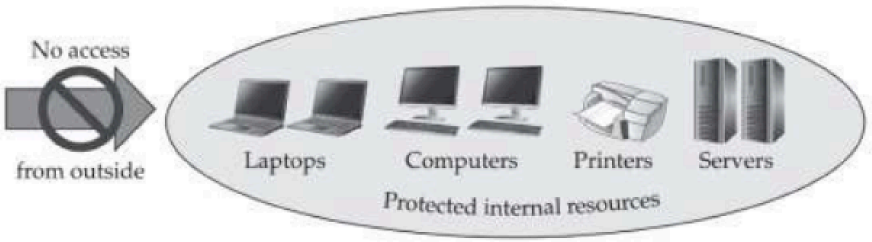
Questions

1. Explain the Government Security Model. 2
2. Explain what Breach Notification Procedure is. $1\frac{2}{3}$
3. Describe Network Address Translation with example. 3

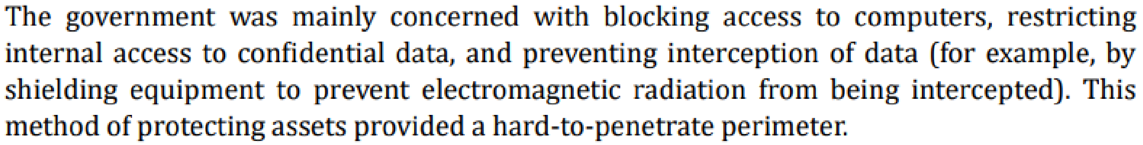
1)



academic security model was "**wide open**" and the **government security model** was "**closed and locked**."



Original government perimeter blockade model



The government was mainly concerned with blocking access to computers, restricting internal access to confidential data, and preventing interception of data (for example, by shielding equipment to prevent electromagnetic radiation from being intercepted). This method of protecting assets provided a hard-to-penetrate perimeter.

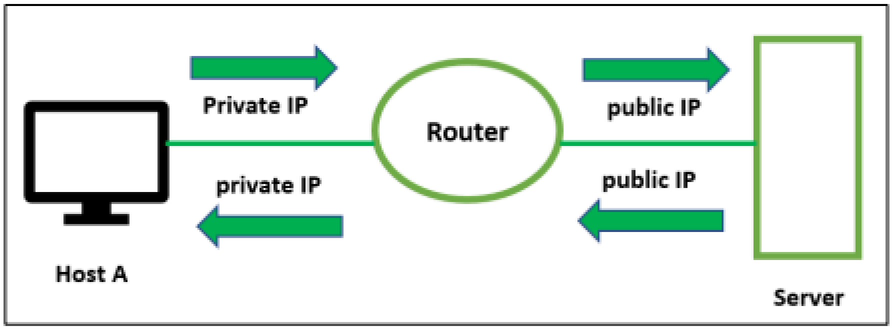
2)**Breach Notification Procedure**: When certain types of information are lost or stolen, companies are legally required to report it to authorities within a specific timeframe, often within 24 hours. This includes telling the people affected by the breach what happened. Larger companies typically have a plan in place for this, called a breach notification procedure, to make sure they meet these legal requirements on time. They also have to investigate why the breach happened and show how they've fixed the problem. Depending on how well they handle the situation, the fines they face for the breach can be higher or lower.

3)

- **Network Address Translation (NAT):** The primary version of TCP/IP used on the Internet is version 4 (IPv4). Version 4 of TCP/IP was created with an address space of 32 bits divided into four octets, mathematically providing approximately four billion addresses. Strangely enough, this is not sufficient. A newer version of IP, called IPv6, has been developed to overcome this address-space limitation, but it is not yet in widespread deployment.

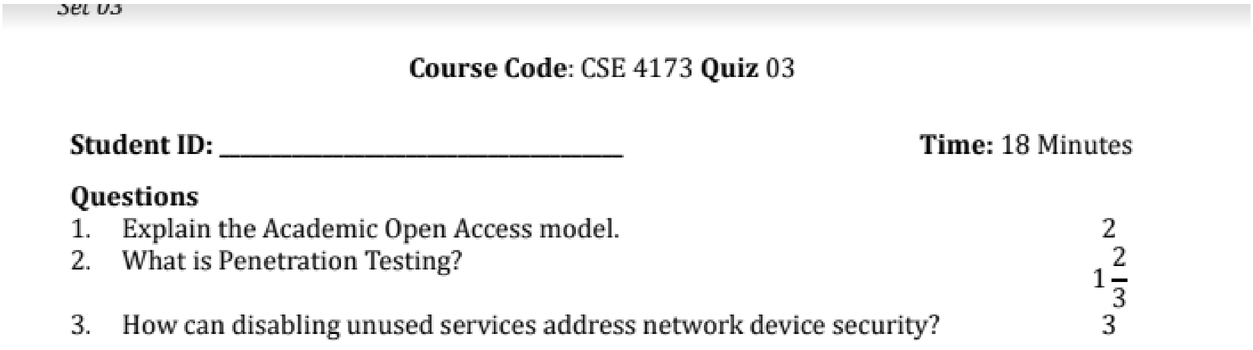
  In order to conserve IPv4 addresses, blocks of addresses have been specified that will never be used on the Internet. These network ranges are referred to as "private" networks.

  This allows organizations to use these blocks for their own corporate networks without worrying about conflicting with an Internet network. However, when these networks are connected to the Internet, they must translate their private IP network addresses into public IP addresses (NAT) in order to be routable. By doing this, a large number of hosts behind a firewall can take turns or share a few public addresses when accessing the Internet.



Network Address Translation

SET-03



Set 03

Course Code: CSE 4173 **Quiz** 03

Student ID: ______________________________ **Time:** 18 Minutes

Questions

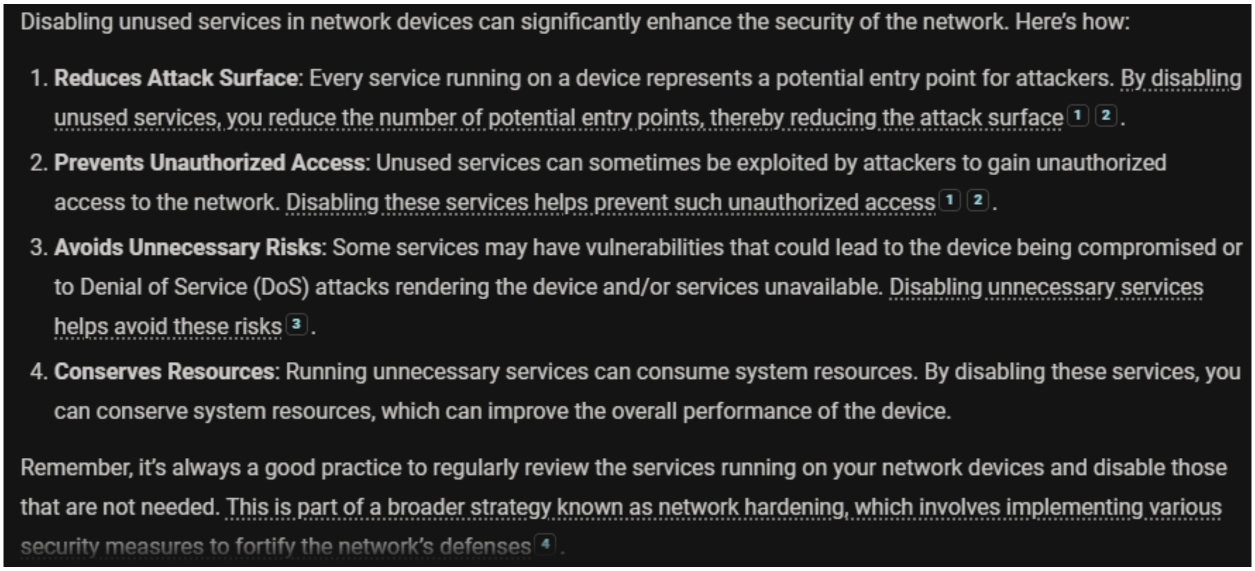
1. Explain the Academic Open Access model. 2
2. What is Penetration Testing? $1\frac{2}{3}$
3. How can disabling unused services address network device security? 3

1) The **academic open access model** refers to the approach to networking and information sharing in academic environments during the early days of networking. In this model, individual computers were initially connected within academic settings. The focus was on fostering open communication and sharing of information among academic institutions.

During this period, the academic security model was characterized as "wide open." This meant that there were minimal restrictions or security controls on accessing and sharing information. The primary goal was to facilitate the open exchange of knowledge and data within academic circles. Security measures were primarily directed towards accounting functions, such as tracking and charging for the use of computer resources, rather than restricting access to information.

2)A **penetration test** is like a security checkup for applications, systems, or websites. It looks for any weak spots or vulnerabilities that could be used by hackers. It's done in a controlled environment to avoid causing any real harm. The test tries to see how serious the vulnerabilities are and if they could lead to a successful attack. It's usually done before using a new application or site and regularly afterwards, like every 6 months or when updates are made. Any serious issues found need to be fixed within a reasonable timeframe. The person who does this testing is called a penetration tester, and they try to simulate real hacking attempts on behalf of the organization that owns the system.

3)

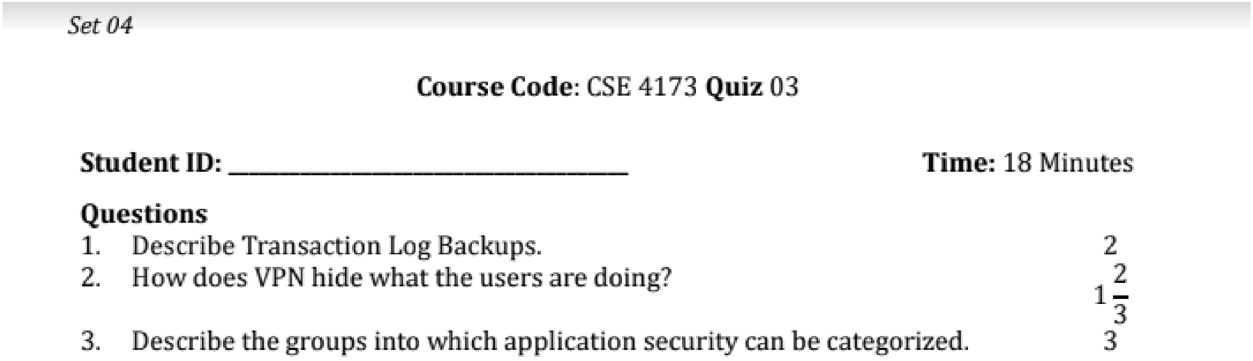


Disabling unused services in network devices can significantly enhance the security of the network. Here's how:

1. **Reduces Attack Surface**: Every service running on a device represents a potential entry point for attackers. By disabling unused services, you reduce the number of potential entry points, thereby reducing the attack surface[1] [2].
2. **Prevents Unauthorized Access**: Unused services can sometimes be exploited by attackers to gain unauthorized access to the network. Disabling these services helps prevent such unauthorized access[1] [2].
3. **Avoids Unnecessary Risks**: Some services may have vulnerabilities that could lead to the device being compromised or to Denial of Service (DoS) attacks rendering the device and/or services unavailable. Disabling unnecessary services helps avoid these risks[3].
4. **Conserves Resources**: Running unnecessary services can consume system resources. By disabling these services, you can conserve system resources, which can improve the overall performance of the device.

Remember, it's always a good practice to regularly review the services running on your network devices and disable those that are not needed. This is part of a broader strategy known as network hardening, which involves implementing various security measures to fortify the network's defenses[4].

SET-04



Set 04

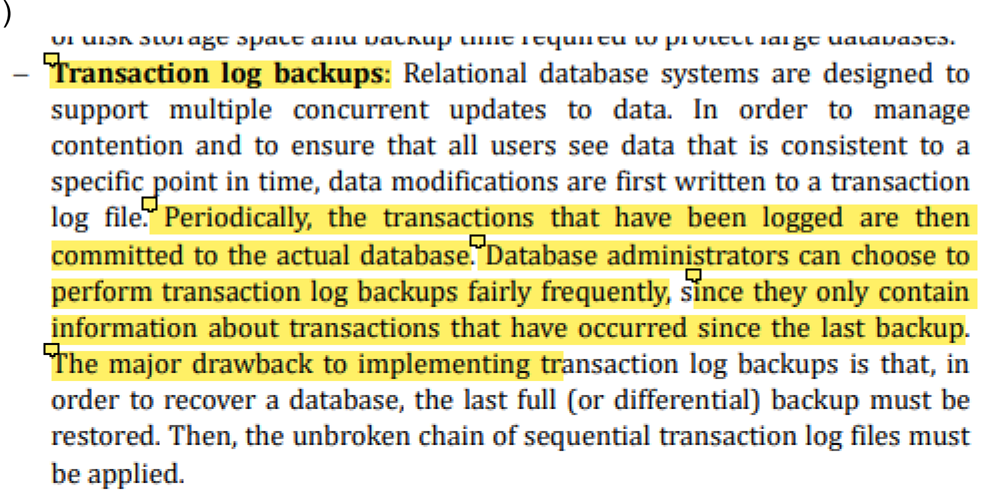
Course Code: CSE 4173 **Quiz** 03

Student ID: ______________________________ **Time:** 18 Minutes

Questions

1. Describe Transaction Log Backups. 2
2. How does VPN hide what the users are doing? $1\frac{2}{3}$
3. Describe the groups into which application security can be categorized. 3

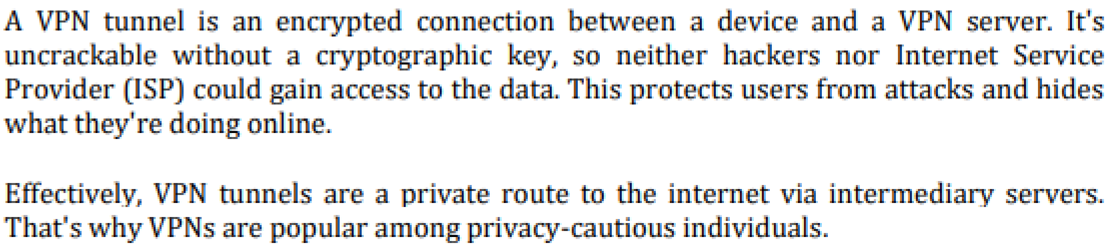
1)



of disk storage space and backup time required to protect large databases.

- **Transaction log backups**: Relational database systems are designed to support multiple concurrent updates to data. In order to manage contention and to ensure that all users see data that is consistent to a specific point in time, data modifications are first written to a transaction log file. Periodically, the transactions that have been logged are then committed to the actual database. Database administrators can choose to perform transaction log backups fairly frequently, since they only contain information about transactions that have occurred since the last backup. The major drawback to implementing transaction log backups is that, in order to recover a database, the last full (or differential) backup must be restored. Then, the unbroken chain of sequential transaction log files must be applied.

2)



A VPN tunnel is an encrypted connection between a device and a VPN server. It's uncrackable without a cryptographic key, so neither hackers nor Internet Service Provider (ISP) could gain access to the data. This protects users from attacks and hides what they're doing online.

Effectively, VPN tunnels are a private route to the internet via intermediary servers. That's why VPNs are popular among privacy-cautious individuals.

3)

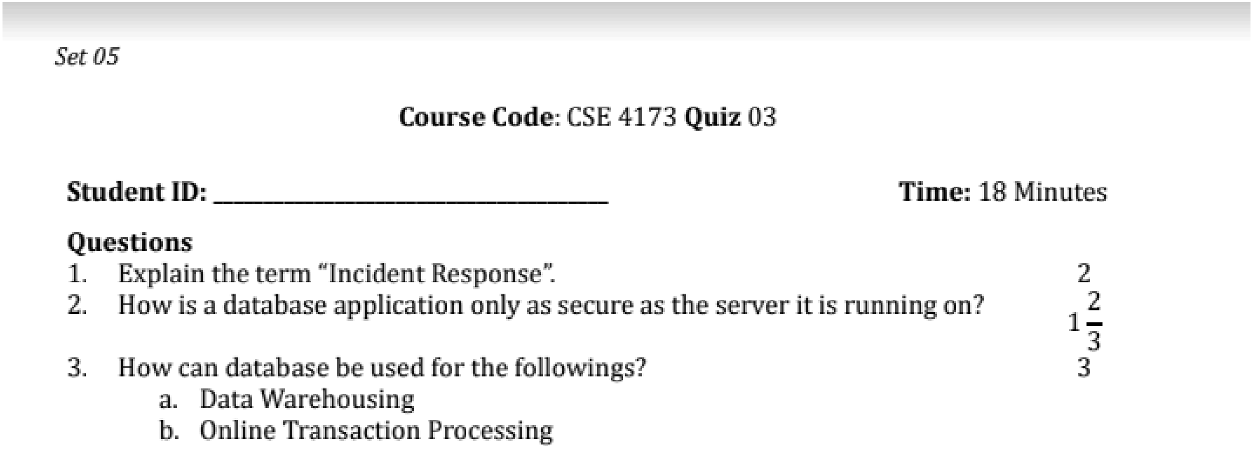
- **Applications**: Unstructured data is typically created in either of two ways: through user activity on their workstations, or as applications access and manipulate structured data and reformat it into a document, e-mail, or image.

  Securing applications is one of the most important ways to protect data, because applications are the interface between the end user and the data. As a result, a great deal of the security investment is devoted to the development of the application.

  Application security can be categorized into the following groups:

  - Application access controls that ensure an identity is authenticated and authorized to view the protected data, to which that identity is authorized, via the application
  - Network and session security to ensure the connection between the database, application, and user is secure
  - Auditing and logging of activity to provide reporting of valid and invalid application activity
  - Application code and configuration management that ensure code and changes to the application configuration are secure

SET-05



Set 05

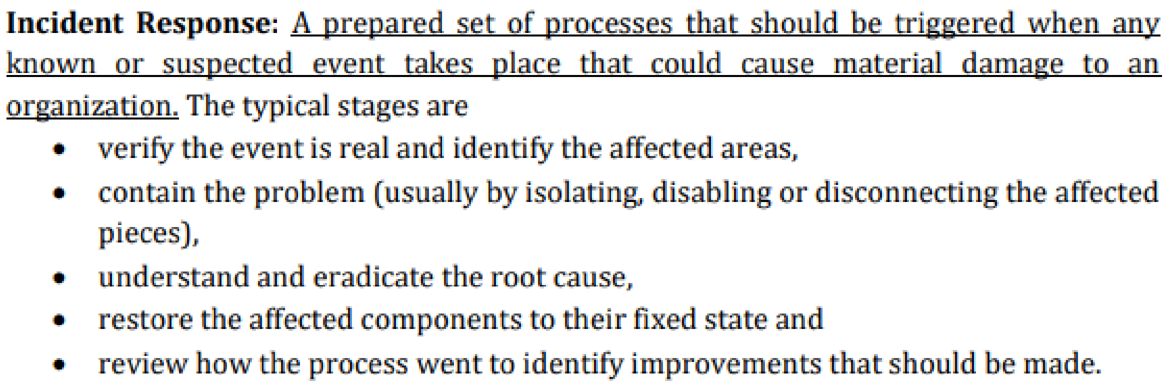
Course Code: CSE 4173 **Quiz** 03

Student ID: ______________________________ **Time:** 18 Minutes

Questions

1. Explain the term “Incident Response”. 2
2. How is a database application only as secure as the server it is running on? $1\frac{2}{3}$
3. How can database be used for the followings? 3
   a. Data Warehousing
   b. Online Transaction Processing

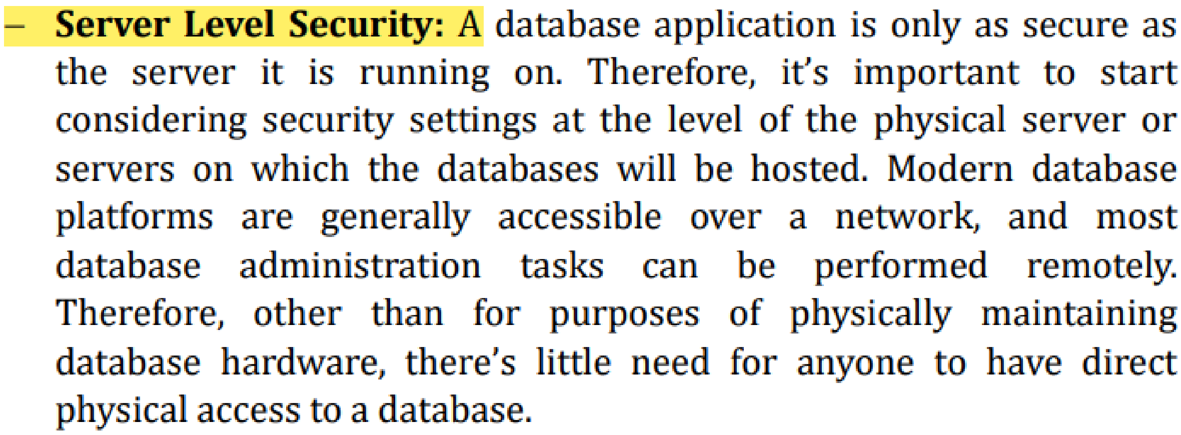
1)



Incident Response: A prepared set of processes that should be triggered when any known or suspected event takes place that could cause material damage to an organization. The typical stages are

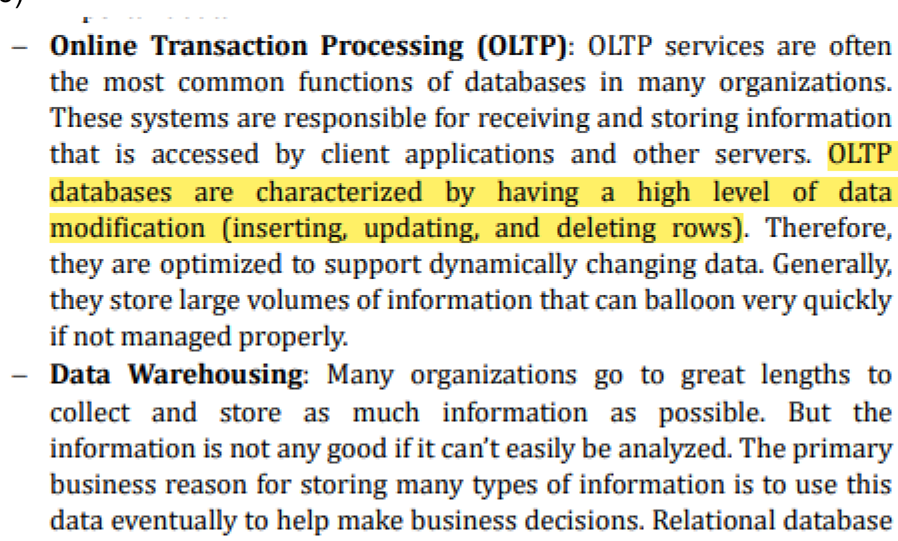
- verify the event is real and identify the affected areas,
- contain the problem (usually by isolating, disabling or disconnecting the affected pieces),
- understand and eradicate the root cause,
- restore the affected components to their fixed state and
- review how the process went to identify improvements that should be made.

2)

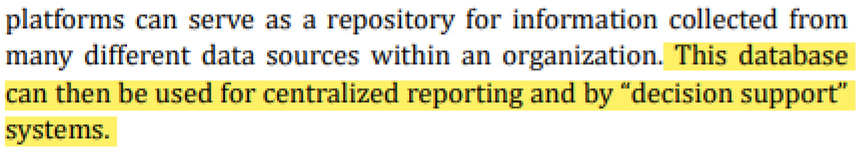


- **Server Level Security:** A database application is only as secure as the server it is running on. Therefore, it's important to start considering security settings at the level of the physical server or servers on which the databases will be hosted. Modern database platforms are generally accessible over a network, and most database administration tasks can be performed remotely. Therefore, other than for purposes of physically maintaining database hardware, there's little need for anyone to have direct physical access to a database.

3)

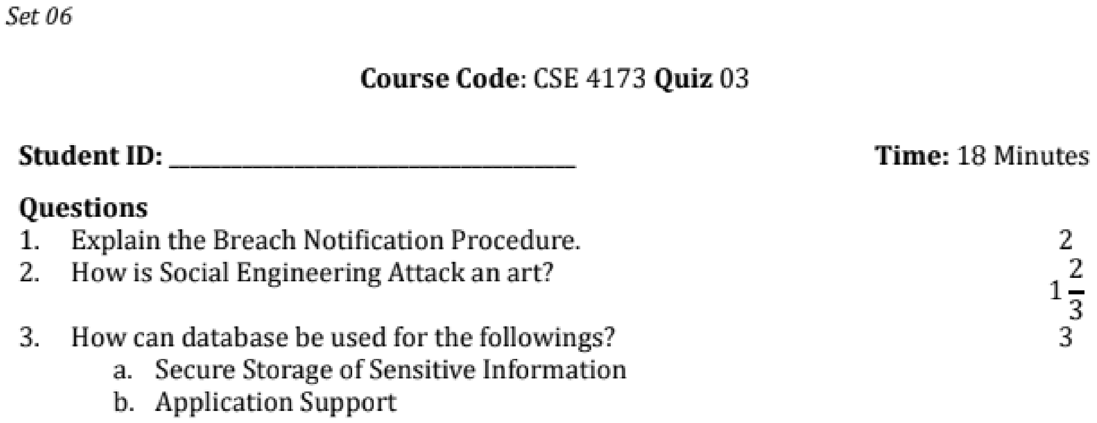


- **Online Transaction Processing (OLTP)**: OLTP services are often the most common functions of databases in many organizations. These systems are responsible for receiving and storing information that is accessed by client applications and other servers. OLTP databases are characterized by having a high level of data modification (inserting, updating, and deleting rows). Therefore, they are optimized to support dynamically changing data. Generally, they store large volumes of information that can balloon very quickly if not managed properly.
- **Data Warehousing**: Many organizations go to great lengths to collect and store as much information as possible. But the information is not any good if it can't easily be analyzed. The primary business reason for storing many types of information is to use this data eventually to help make business decisions. Relational database



platforms can serve as a repository for information collected from many different data sources within an organization. This database can then be used for centralized reporting and by "decision support" systems.

SET-06



Set 06

Course Code: CSE 4173 **Quiz** 03

Student ID: ________________________________ **Time:** 18 Minutes

Questions

1. Explain the Breach Notification Procedure. 2
2. How is Social Engineering Attack an art? $1\frac{2}{3}$
3. How can database be used for the followings? 3
   a. Secure Storage of Sensitive Information
   b. Application Support

1)set2-2
2)

social engineering like a sneaky trick or a con game. It's all about fooling people into doing things they shouldn't, like giving away passwords or clicking on harmful links.

Here's how it's like an art:

1. **Understanding People**: Social engineers need to know how people think and behave to trick them effectively.

2. **Being Creative**: They have to come up with clever ways to trick people, like making up believable stories or pretending to be someone they're not.

3. **Good Communication**: Social engineers are great at talking to people and making them trust them, even when they shouldn't.

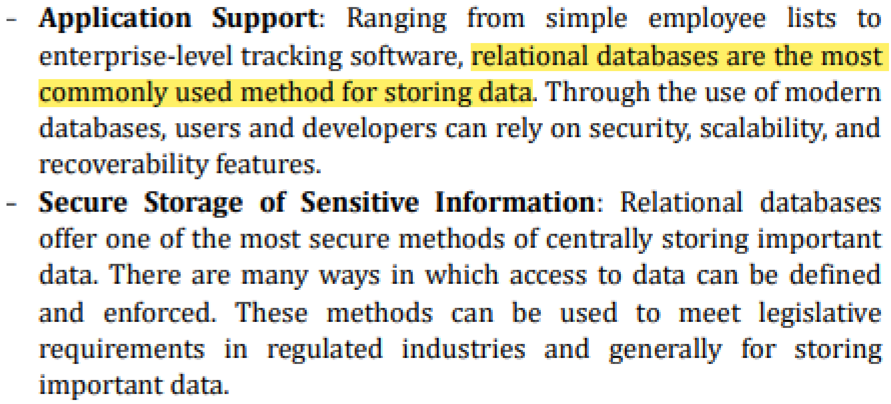
4. **Being Patient**: Sometimes, they have to wait a long time and slowly gain someone's trust before they can pull off their trick.

5. **Tricking People**: Just like an artist uses brushes and paint, social engineers use lies and manipulation to achieve their goals.

6. **Learning from Mistakes**: They learn from their successes and failures, just like an artist learns from their paintings.

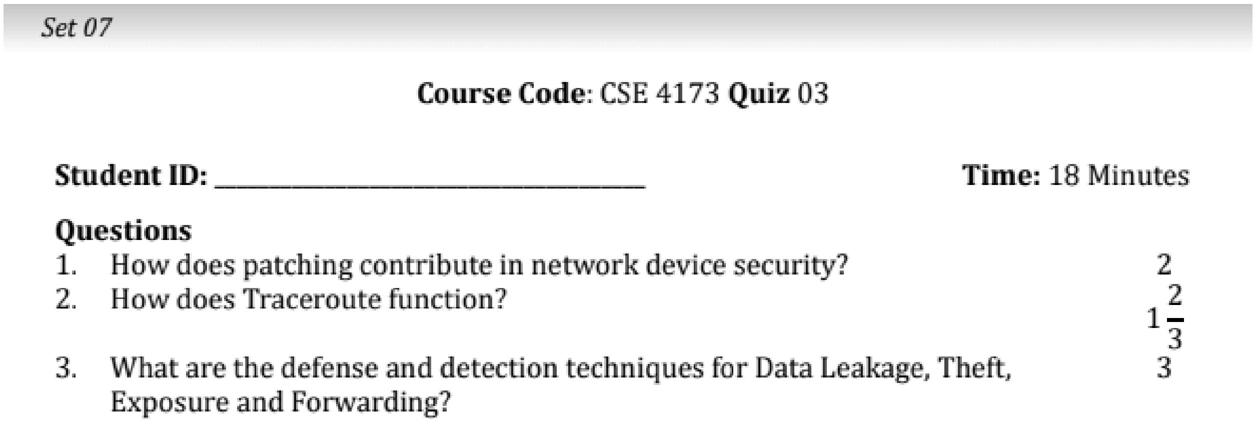
So, social engineering is like a sneaky art form where the "artist" tricks people into doing things they shouldn't.

3)



- **Application Support**: Ranging from simple employee lists to enterprise-level tracking software, relational databases are the most commonly used method for storing data. Through the use of modern databases, users and developers can rely on security, scalability, and recoverability features.
- **Secure Storage of Sensitive Information**: Relational databases offer one of the most secure methods of centrally storing important data. There are many ways in which access to data can be defined and enforced. These methods can be used to meet legislative requirements in regulated industries and generally for storing important data.

SET-07



Set 07

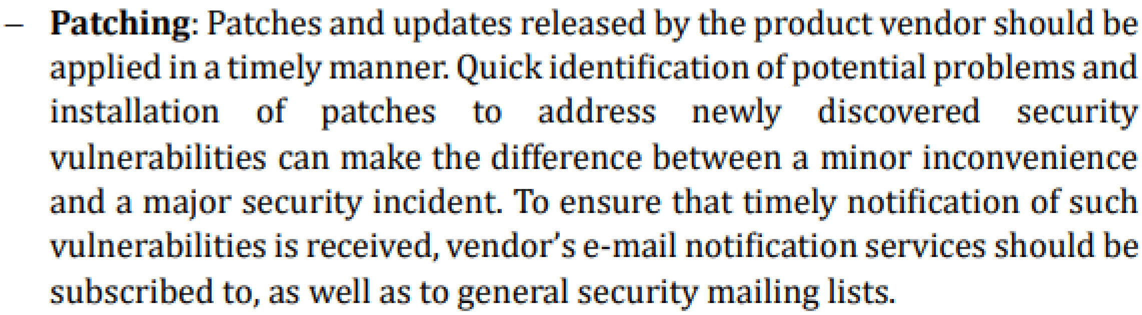
Course Code: CSE 4173 **Quiz** 03

Student ID: ______________________________ **Time:** 18 Minutes

Questions

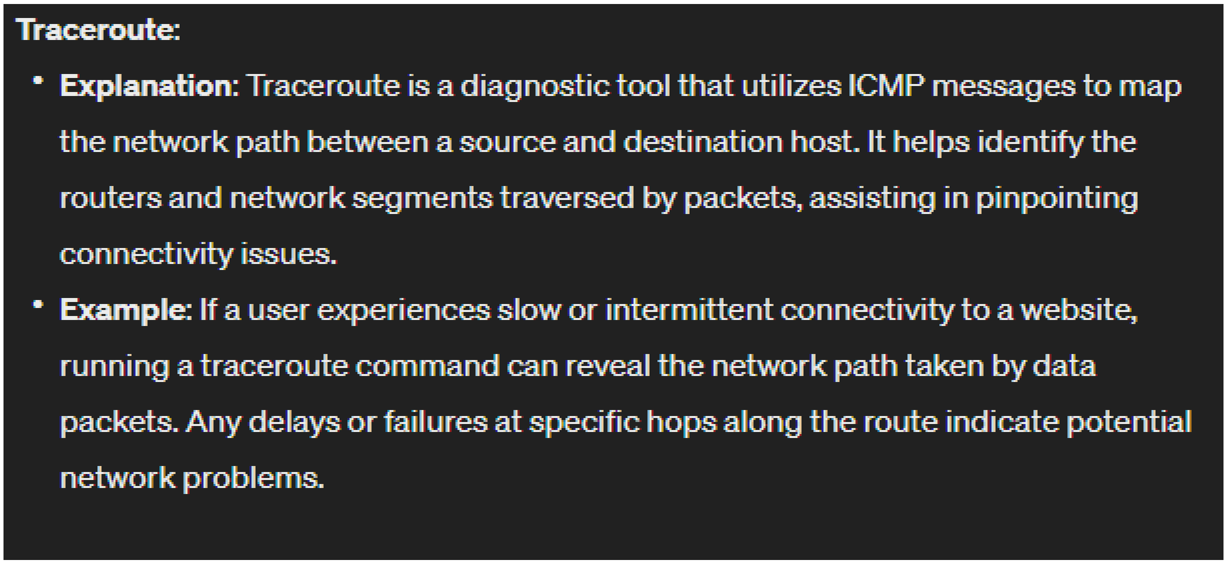
1. How does patching contribute in network device security? 2
2. How does Traceroute function? $1\frac{2}{3}$
3. What are the defense and detection techniques for Data Leakage, Theft, Exposure and Forwarding? 3

1)



– **Patching**: Patches and updates released by the product vendor should be applied in a timely manner. Quick identification of potential problems and installation of patches to address newly discovered security vulnerabilities can make the difference between a minor inconvenience and a major security incident. To ensure that timely notification of such vulnerabilities is received, vendor's e-mail notification services should be subscribed to, as well as to general security mailing lists.

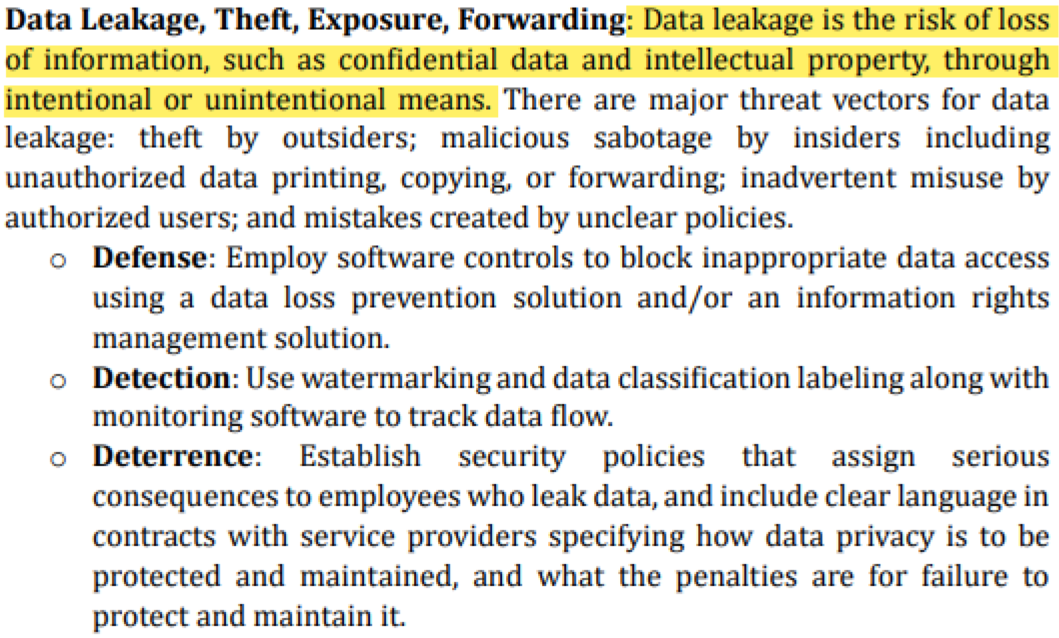
2)



Traceroute:

- **Explanation:** Traceroute is a diagnostic tool that utilizes ICMP messages to map the network path between a source and destination host. It helps identify the routers and network segments traversed by packets, assisting in pinpointing connectivity issues.
- **Example:** If a user experiences slow or intermittent connectivity to a website, running a traceroute command can reveal the network path taken by data packets. Any delays or failures at specific hops along the route indicate potential network problems.

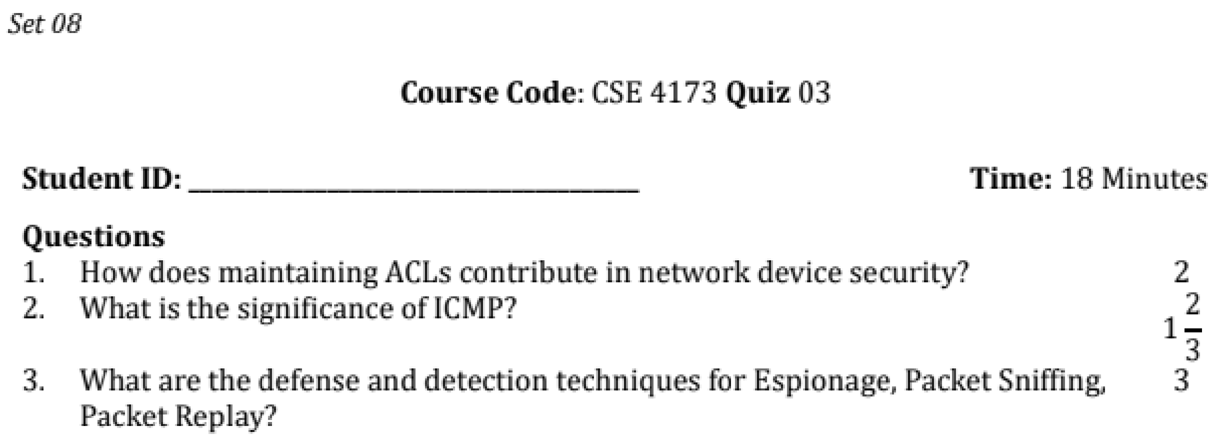
3)



Data Leakage, Theft, Exposure, Forwarding: Data leakage is the risk of loss of information, such as confidential data and intellectual property, through intentional or unintentional means. There are major threat vectors for data leakage: theft by outsiders; malicious sabotage by insiders including unauthorized data printing, copying, or forwarding; inadvertent misuse by authorized users; and mistakes created by unclear policies.

- **Defense**: Employ software controls to block inappropriate data access using a data loss prevention solution and/or an information rights management solution.
- **Detection**: Use watermarking and data classification labeling along with monitoring software to track data flow.
- **Deterrence**: Establish security policies that assign serious consequences to employees who leak data, and include clear language in contracts with service providers specifying how data privacy is to be protected and maintained, and what the penalties are for failure to protect and maintain it.

SET-08



Set 08

Course Code: CSE 4173 **Quiz** 03

Student ID: ______________________________ **Time:** 18 Minutes

Questions

1. How does maintaining ACLs contribute in network device security? 2
2. What is the significance of ICMP? $1\frac{2}{3}$
3. What are the defense and detection techniques for Espionage, Packet Sniffing, Packet Replay? 3

1)

Maintaining Access Control Lists (ACLs) on routers contributes significantly to network device security in several ways:

1. **Traffic Filtering**: ACLs allow routers to filter incoming and outgoing traffic based on specific criteria, such as source and destination IP addresses, protocol types (TCP, UDP), and port numbers. By carefully configuring ACLs, administrators can control which types of traffic are allowed or denied, thus reducing the attack surface and minimizing the risk of unauthorized access or malicious activities.

2. **Protection Against Denial-of-Service (DoS) Attacks**: ACLs can be used to block or limit traffic from known malicious sources or to restrict access to vulnerable services. This helps prevent bandwidth saturation and resource exhaustion caused by DoS attacks, improving the overall availability and performance of the network.

3. **Enforcement of Security Policies**: ACLs enable organizations to enforce security policies by specifying which network resources are accessible to different users or devices. For example, ACLs can be used to restrict access to sensitive servers or applications only to authorized personnel, ensuring that critical data remains protected from unauthorized access or tampering.

4. **Segmentation and Isolation**: ACLs facilitate network segmentation and isolation by controlling the flow of traffic between different network segments or zones. By implementing

ACLs at strategic points in the network architecture, organizations can create secure boundaries between internal networks, DMZs (Demilitarized Zones), and the internet, preventing lateral movement of threats and containing potential security breaches.

5. **Complementary Security Measures**: While firewalls offer more advanced inspection capabilities, ACLs complement firewall functionalities by providing an additional layer of defense at the network perimeter. By combining ACLs with other security measures such as intrusion detection/prevention systems (IDS/IPS) and endpoint protection, organizations can establish a multi-layered security posture that enhances overall resilience against cyber threats.

Overall, maintaining ACLs on routers is essential for controlling network traffic, enforcing security policies, and mitigating various security risks. By effectively managing ACL configurations, organizations can strengthen their network defenses and minimize the likelihood of security incidents and breaches.

2)

ICMP stands for Internet Control Message Protocol. It is a fundamental part of the Internet Protocol Suite (TCP/IP) and is used for diagnostic and error-reporting purposes in computer networks. ICMP messages are typically carried within IP packets and are used by network devices to communicate information about network conditions, troubleshoot connectivity issues, and exchange error messages.

Here are some key aspects of ICMP:

1. **Diagnostic Tool**: ICMP provides tools for network diagnostics, allowing devices to communicate information about network connectivity and conditions. For example, ICMP echo requests and replies, commonly known as "pings," are used to determine if a host is reachable and responsive on the network.

2. **Error Reporting**: ICMP is used to report errors that occur during the transmission of IP packets. When a network device encounters an issue, such as a packet being unable to reach its destination or a router encountering a problem forwarding a packet, it may generate an ICMP error message to inform the sender of the issue.

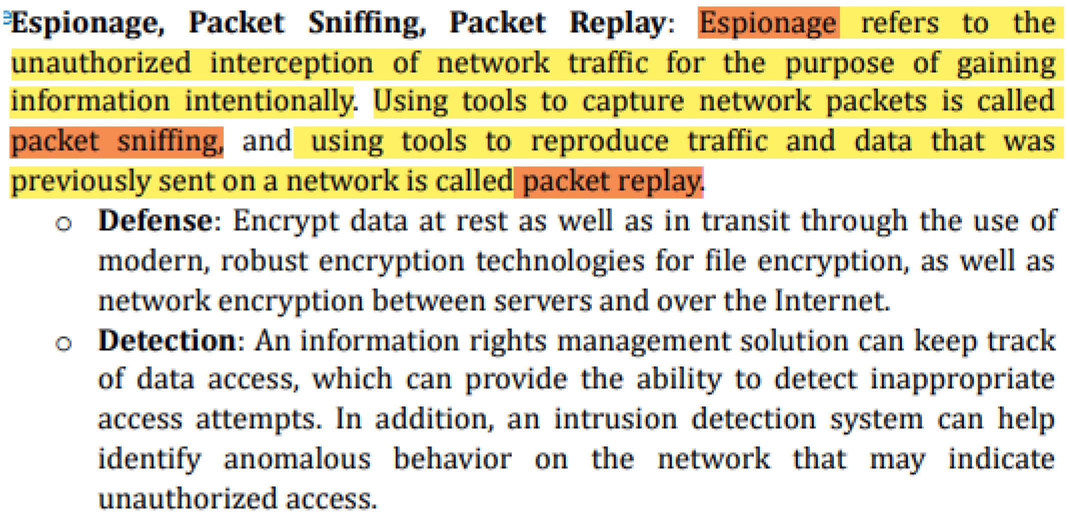
3. **Message Types**: ICMP includes various message types, each serving a specific purpose. Some common ICMP message types include:

- Echo Request and Reply: Used for ping tests to check network reachability.
- Destination Unreachable: Sent by routers to indicate that a packet cannot be delivered to its destination.
- Time Exceeded: Indicates that a packet's time-to-live (TTL) value has expired.
- Redirect: Used by routers to inform hosts of a better route to a particular destination.

4. **Routing Information**: ICMP can also be used to exchange routing information between routers. For example, ICMP Router Discovery messages can be used by hosts to learn about available routers on a network.

Overall, ICMP plays a crucial role in network troubleshooting, error reporting, and communication between network devices. It provides essential functionality for maintaining and diagnosing network connectivity and conditions.

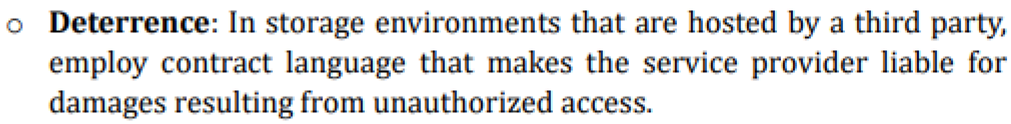
3)



Espionage, Packet Sniffing, Packet Replay: Espionage refers to the unauthorized interception of network traffic for the purpose of gaining information intentionally. Using tools to capture network packets is called packet sniffing, and using tools to reproduce traffic and data that was previously sent on a network is called packet replay.

- **Defense**: Encrypt data at rest as well as in transit through the use of modern, robust encryption technologies for file encryption, as well as network encryption between servers and over the Internet.
- **Detection**: An information rights management solution can keep track of data access, which can provide the ability to detect inappropriate access attempts. In addition, an intrusion detection system can help identify anomalous behavior on the network that may indicate unauthorized access.

[redacted]



- **Deterrence**: In storage environments that are hosted by a third party, employ contract language that makes the service provider liable for damages resulting from unauthorized access.