Assignment 1

The Basics

# Networking Fundamentals

1. Consider the following scenario

Suppose, you are a network consultant advising a medium-sized manufacturing company with departments spread across three floors. The current network setup is becoming inefficient, and the company is looking to revamp its infrastructure. Your task is to recommend a suitable network topology (among star, bus & ring), considering factors like data transfer efficiency, fault tolerance, scalability, and ease of management. Provide a brief analysis of the chosen topology's advantages and disadvantages, along with real-world examples where this topology has been successfully implemented. Consider cost implications and potential challenges in your recommendations.

**Ans:**

The topology which I have chosen is the Star topology for the above scenario.

Starting with the advantages of star topology:

1. Transferring data is efficient within specific individual departments. In a star topology, devices do communication directly with a central switch. It reduces chances of data collisions and loss of data.
2. If a device fails in one specific department, it does not affect the whole network. So, when one device fails, other departments and devices can keep working.
3. Star topology follows centralized management. It makes managing the whole network simple and easy.
4. It is scalable. New devices can be easily added to the network without disrupting the functions of the network in any way.

Now, we discuss the disadvantages of star topology.

1. We know that star topology has a central switch. If it somehow fails then the whole network can be hard to access.
2. Installing a central switch can be really expensive where other topologies are less costly.

In the real world, many companies and industries use star topology in office environment and Local area networks use it commonly.

Challenges:

1. Since star topology has a central switch, if it fails then the whole network will fail. To prevent it from happening, we should install backup switches.

1. Research and outline three common network security threats and propose preventive measures to mitigate each threat.

**Ans:** The three common network security threats are, (1) Malware, (2) DdoS attacks, (3) phishing attacks.

1. Malware: malware is a dangerous software that harms computer systems. These include viruses, ransomware etc. Viruses make your computer applications infected and later makes the pc unusable. Ransomware locks all files the computer and later they demand money to unlock those files.

Preventive measures: We must use antivirus software and update that regularly. We should also backup all of our sensitive and important files on another device and safeguard them from hackers.

1. Ddos attacks: ddos attacks floods a network with extensive amount of traffic so it becomes overwhelmed and inaccessible to users.

Preventive measures: We should monitor the network or service regularly by experts to detect any unusual activity. Additionally, we could use ddos weakening softwares or services.

1. Phishing attacks: Phishing is the unethical practice of using emails or texts pretending to be reliable to gain sensitive information of the user.

Preventive measures: We can filter emails and block spam emails to get rid of phishing attempts. Additionally, expert users should verify if the mails or texts are actually reliable and trustworthy or not.

# Operating System Knowledge (Linux)

1. Provide a step-by-step guide on how to change file permissions on Linux.

**Ans:**

First step is opening the terminal in linux using the command: ctrl+alt+t

Secondly, use the ‘cd’ command to locate the file we want to change the permission for.

After that, we can use the ‘ls -l’ command to check the current permissions.

And then, use the ‘chmod’ command to change permissions. ‘chmod permission filename’ where permission means the desired permission and filename is the name of the file.

1. Imagine a Linux server experiencing high CPU usage. Research and outline the commands and techniques used for monitoring and managing processes on Linux. Provide a detailed explanation of how to identify and terminate processes consuming excessive system resources.

**Ans:**

The “htop” command gives visual representation of cpu and memory usage.

The “ps” command displays information about processes currently running.

Here, using “-e” means all processes, “-o” user defined output format.

The “kill” command terminates processes. The “pkill” command terminates processes based on their names. “pgrep” is used to find processes by their names and get their process ids.

The “killall” command terminates processes with a specific name.

The explanation of how to identify and terminate processes consuming excessive system resources is given below: The “strace” shows system calls made by a single process. It helps to diagnose issues. “lsof” command lists open files associated with a process. Additionally, the “vmstat” command gives information about system memory, processes and cpu activity. The “sar” command collects and saves system activity information.

1. Provide a step-by-step guide on how to install, update, and remove software packages using the package manager relevant to a chosen Linux distribution.

**Ans:** The chosen linux distribution is ubuntu.

To install a package, we follow these commands:

sudo apt update

sudo apt install package\_name

To update all packages:

sudo apt update

sudo apt upgrade

To remove packages:

sudo apt remove package\_name

1. Provide examples of common log files, their locations, and the information they contain.

**Ans:** Common system logs for ubuntu are:

1. System log:

Location: /var/log/syslog

Information they contain: Contains general system messages, kernel messages, startup and shutdown events.

1. Authentication log:

Location: /var/log/auth.log

Information they contain: contains login attempts, authentication events etc.

1. Kernel log:

Location: /var/log/kern.log

Information: contains messages related to kernel, error and warnings.

1. Package management log:

Location: /var/log/dpkg.log

Information: contains information about package installation, removal and upgrade events.

1. Syslog:

Location: /var/log/syslog

Information: contains logs from different services on the server.

1. A system administrator needs to manage user accounts on a Linux server. Research on the internet and explain the commands and procedures for creating, modifying, and deleting user accounts and groups.

**Ans:**

Creating user accounts: The “useradd” command is used to add a new user.

sudo useradd -m -s /bin/bash username

“-m” creates the users home directory and “-s /bin/bash username” sets the default shell to bash.

Setting password: The “passwd” command is used.

sudo password username

modify user properties: The “usermod” command is used.

sudo usermod -aG groupname username

“-aG” adds the user to another group.

Deleting user: The “userdel” command is used to delete a user.

sudo userdel -r username

“-r” removes the users home directory.

Creating a new group: the “groupadd” command is used.

Sudo groupadd groupname

Adding user to a group: “usermod” command is used.

sudo usermod -aG groupname username

Deleting a group: “groupdel” command is used.

Sudo groupdel groupname

# Basic Programming Skills

1. Implement a python script that takes a user-provided password as input and evaluates it against the following conditions -

* At least 8 characters in length.
* Should contain a mix of uppercase and lowercase letters.
* Must include at least one numeric digit
* must include at least one special character from the set: **!@#$%^&\*()-\_=+[]{}|;:'",.<>/?.**

**Ans:**

import re

def evaluate\_password(password):

conditions = [

len(password) >= 8,

any(char.isupper() for char in password),

any(char.islower() for char in password),

any(char.isdigit() for char in password),

any(char in r”!@#$%^&\*()-\_=+[]{}|;:’\”,.<>/?.” for char in password)

]

return “password is strong.” if all(conditions) else “password is weak. Kindly retry.”

user\_given\_pass= input(“Enter password: ”)

result = evaluate\_password(user\_given\_pass)

print(result)

1. Write a Python script to encrypt and decrypt files using a cryptographic algorithm (e.g., AES). Users should be able to provide a key for encryption and use the same key for decryption.

**Ans:**

# Cybersecurity Basics

1. A company has noticed an increase in phishing attempts targeting its employees. Research and outline the common techniques used in social engineering attacks.

**Ans:**

Common techniques used in social engineering attacks are given below:

1. Email phishing: Attackers send emails that are pretending to be trustworthy and later they try to trick the users into dangerous links so they accidentally provide personal information.
2. Some times these attackers leave usb drives and cd’s in public places or university labs so that naïve users can access them easily. Once they use the device in their personal computer, the malware accesses all of the user’s personal information.
3. These days surveys are prevalent in social media sites. Through these surveys the attackers try to gain personal information. This information can be later used to attack the users.
4. Call center scams are a huge issue in this subcontinent. Attackers use phone calls and pretend to be trustworthy and trick the users to provide their personal information posing as bank officers, technology officers etc.
5. Imagine a scenario where a company's computer systems have been infected with malware. Research and propose a detailed strategy for defending against malware attacks.

**Ans:**

The first person who will encounter the malware infection are the employees of the company. First of all, the company should hold meetings and seminars regularly about cybersecurity and how to avoid them.

Secondly, since it is a company then the emails are a major aspect of their business. So, they must use advanced and latest software specifically designed to filter out spam and malicious emails. It can be done if the dangerous emails display a warning in the website. The company must ensure it.

Additionally, every network must be protected at all times by latest state of the art antivirus software. We should update the antivirus regularly along with scanning for dangerous files in the system. Once a malware is detected, we should report it and block all the related files and links as soon as possible.

Finally, the company should back up all their sensitive information and files regularly. They should also do regular security check ups to find weak spots of the system.

1. A small business is concerned about the security of its network. Research and suggest basic network security measures, including the use of firewalls, intrusion detection systems, and encryption. Provide a step-by-step guide on implementing these measures and explain how they contribute to a secure network environment.

**Ans:**

The step by step guide to implementing these measures and explain how they contribute to a secure network environment is given below:

1. firewalls: Choose a firewall software. Install it and configure. Define access rules. Regularly update the software.

It serves as a barrier, keeping others from entering. Oversees and regulates network traffic.

1. Intrusion detection systems: Choose an IDS solution. Deploy ids sensors. Define detection rules. Regularly monitor alerts.

It keeps an eye out for questionable activity. Delivers notifications in real time for prompt action.

1. Encryption: Use SSL/TLS for secure communication. Set up VPNs for remote access. Encrypt sensitive data.

It keeps data safe from unwanted access. Secures routes of communication to stop spying.

# Web Technologies

1. A development team is tasked with building a data-intensive web application. Conduct an in-depth technical comparison of three web development frameworks (e.g., Django, Ruby on Rails, Express.js). Evaluate their ORM capabilities, routing mechanisms, and support for RESTful APIs. Recommend the framework that aligns best with the project's technical requirements and scalability needs.

**Ans:**

Django:

ORM: Django has a robust ORM that offers a high level abstraction for database operations. Includes capabilities including model relationships and migrations, and it supports a wide range of database backends.

Routing systems: Routes urls using a declarative method via the urls.py file. Focuses more on convention than configuration, which makes defining URL patterns simple.

Restful API support: By use of the Django REST framework, Django comes with integrated support for RESTful APIs. Offers authentication methods, views, and serializers to build reliable apis.

Ruby on rails:

ORM: ActiveRecord is the default ORM used by ruby on rails, providing a model-centric approach. Facilitates effective database interactions by supporting validations, relationships and migrations.

Routing systems: Focuses on convention over configuration when routing, which simplifies the process of defining routes in routes.rb. Promotes RESTful standards, which simplify the definition of routes and actions.

Restful API support: Actioncontroller may be used to create restful apis with built in support in rails. Enables the creation of controllers that respond to various HTTP methods by developers.

Express.js:

ORM: It does not come with an ORM. For ORM like capabilities, developers use libraries like Sequelize or mongoose.

Routing systems: Recognized for its adaptable and simple routing design. Express is used to define routes.Router which makes processing HTTP methods and arguments simple.

Restful API support: Express.js is intended to be a lightweight, neutral framework. Although it lacks built-in support, there are a number of middleware and libraries available, such as express-restify-mongoose.

The framework that aligns best with the project's technical requirements and scalability needs is the Django framework.

1. What is Content Security Policy (CSP) & Cross-Origin Resource Sharing (CORS), why do we require these?

**Ans:** The content security policy(csp) protects websites from certain types of attacks such as cross-site scripting (XSS) attacks. It tells the browser where to get scripts and helps stop harmful code. It keeps the website safe and lets developers know about any issues. It whitelists script sources, prevents inline script execution.

The CORS allows websites to share certain things with other websites. It enables servers to specify allowed origins. It is implemented through HTTP headers. Additionally, it prevents unauthorized cross-origin requests. CORS makes sure only approved websites can use shared stuff. It is important because CORS makes sure things work securely.

We require CSP and CORS because it enhances web application security, ensures integrity of the web content and protects against unauthorized access.

1. Mention the risks (2 for each platform) while using popular CMS options - Wordpress, Joomla, Drupal

**Ans:**

Wordpress:

1. Hacking risk: many hackers target it. Old plugins can cause problems.
2. Plugin issues: some plugins or themes may not be safe.

Joomla:

1. Security problems: needs regular updates to stay safe.
2. Hard to learn: can be tricky for beginners. It might also lead to mistakes.

Drupal:

1. Complicated and needs power: A bit hard for new users. Uses a lot of computer power or computational memory.
2. Smaller plugin ecosystem: Doesn’t have as many added features as some others.

# Database Management

1. Research and outline best practices for securing a database, covering topics such as authentication, authorization, encryption, and auditing.

**Ans:**

The best practices are given below:

Authentication: Use strong passwords and update regularly, enable multi-factor authentication and limit login attempts and review user access regularly.

Authorization: Follow the principle of least privilege, implement role-based access control and perform regular access reviews and log access attempts.

Encryption: Encrypt stored data and transmissions. Implement transparent data encryption and secure key management.

Auditing: Enable and review audit logs and set alerts for unsual activities.

1. A data-intensive application is being developed to handle large volumes of unstructured data. Which NoSQL database options would be more suitable among - MongoDB, Cassandra, Redis in this situation?

**Ans:**

MongoDB is good for flexible, unstructured data and it is document-oriented along with scalable with sharding. Cassandra handles large unstructured data and is distributed. The advantage of it is it can store in wide column and has high scalability. Lastly, Redis is suitable for semi-structured data and it has fast read access. The NoSQL database option which would be more suitable is Cassandra.

# Cryptography

1. What is PKI? Describe how PKI can enhance the confidentiality and integrity of communication in the financial sector.

**Ans:** Public key infrastructure or pki is a system for managing digital keys and certificates to enable safe network communication.

Pki protects transactions with digital signatures, encrypts sensitive data during transmission, and offers strong authentication methods for clients and servers. It improves confidentiality and integrity in the financial industry.

By guaranteeing the confidentiality of financial data and ensuring the integrity of digital transactions, this framework helps to build trust.

1. A security analyst needs to recommend an encryption method for securing communication between two systems. Research and compare symmetric and asymmetric encryption methods. Discuss the strengths and weaknesses of each approach, considering factors such as key management, speed, and suitability for different use cases.

**Ans:**

Symmetric encryption: Key management is straight-forward (one key), but safely sharing the key might be difficult. It has quicker speed which is appropriate for apps where speed is crucial. Excellent for situations when speed is essential, such as encryption of real time data.

Asymmetric encryption: Key management uses two keys, which makes distribution easier but requires a lot of processing power. In comparison to symmetric encryption, the speed is reduced. It is suitable for safe key distribution, frequently employed in situations where security takes precedence above speed.

1. Research and explain how digital signatures can be used for authentication. Provide a step-by-step guide on how digital signatures work

**Ans:** Digital signatures for authentication are given below:

Key pair generation: users create a private-public key pair.

Message hashing: sender hashes the message content.

Signing: Sender encrypts the hash with their private key.

Attaching signature: Digital signature is attached to the message.

Transmission: Signed messages is sent to the recipient.

Verification: Recipient hashes the received message.

Decryption: Recipient decrypts the senders signature with their public key.

Comparison: If hashes match, the message is authentic and unedited.

Digital signatures ensures senders identity. Sender cant deny sending. Detects message tampering and finally assures senders identity over untrusted networks.

# Familiarity with Security Tools and Software

1. What kind of tasks can be performed using tools like - Snort or Suricata? Describe a scenario where these can be used.

**Ans:** Open source network intrusion detection and prevention systems like suricata and snort examine network data to find dangerous activity. Both programs have the ability to record packet level information, giving forensic records of network activity. The investigation of security issues can benefit from this knowledge.

1. List 3 vulnerability scanning tools and compare based on - features, price, and popularity.

**Ans:** 3 vulnerability scanning tools are Nessus, OpenVAS, Qualys.

Nessus: It is thorough, forms policy and does compliance audits. It has a range of plans, some are free. Nessus is quite well liked among the cybersecurity community.

OpenVAS: OpenVAS is scalable, configurable and open-source. Since it is open-source, it is free of cost. This is liked by people who are looking for open-source remedies.

Qualys: This prioritizes assets, is cloud based and goes through ongoing monitoring. The cost of this one depends on subscriptions. Qualys is widely used in the business community.

1. What kind of tool is Autopsy? What can be done using this software?

**Ans:** Autopsy is a digital forensics platform. Forensic examiners may analyze and look at digital evidence from computers and storage devices with the help of autopsy. Comprehensive digital investigations, such as file system analysis, keyword searches, and artifact inspection are done by autopsy.