Data Communication Lab Report



Submitted to:

Department of Computer Engineering  
  
Submitted by:  
Prajjwal Adhikari  
Roll No: 20  
  
  
Submission Date: 7/8/2024

# Lab 1: Clamping and File Sharing Between Two Computers

## Objective

The objective of this lab is to establish a physical connection between two computers using Ethernet cables and configure the necessary network settings to enable file sharing.

## Materials and Equipment

* Two computers with Ethernet ports
* Two Ethernet cables (CAT5e or CAT6 recommended)
* Network switch or hub (optional, if not using a direct connection)
* Operating systems installed on both computers (e.g., Windows, Linux, or macOS)
* Network configuration tools and administrative access on both computers

## Theory

File sharing between computers over a network allows users to access and transfer files efficiently. Establishing a direct or switched Ethernet connection and configuring appropriate network settings (such as IP addresses and file-sharing permissions) are essential steps in setting up this communication.

## Procedure

### Step 1: Physical Connection

1. **Direct Connection (without a switch or hub)**:
   * Connect one end of the Ethernet cable to the Ethernet port of the first computer.
   * Connect the other end of the Ethernet cable to the Ethernet port of the second computer.
   * For older computers, use a crossover Ethernet cable; modern computers with Gigabit Ethernet ports can use a straight-through cable as they support Auto-MDI/MDIX.
2. **Connection via Switch or Hub**:
   * Connect one end of the first Ethernet cable to the Ethernet port of the first computer.
   * Connect the other end of the first Ethernet cable to a port on the network switch or hub.
   * Connect one end of the second Ethernet cable to the Ethernet port of the second computer.
   * Connect the other end of the second Ethernet cable to another port on the network switch or hub.

### Step 2: Network Configuration

1. **Assign Static IP Addresses**:
   * On Computer 1:
     1. Open the network settings (e.g., Network and Sharing Center on Windows, Network Manager on Linux).
     2. Set the IP address to 192.168.1.1.
     3. Set the subnet mask to 255.255.255.0.
   * On Computer 2:
     1. Open the network settings.
     2. Set the IP address to 192.168.1.2.
     3. Set the subnet mask to 255.255.255.0.
2. **Verify Connectivity**:
   * Open a command prompt or terminal on Computer 1.
   * Ping Computer 2 using the command: ping 192.168.1.2.
   * Check for successful ping replies.
   * Repeat the ping test from Computer 2 to Computer 1 using the command: ping 192.168.1.1.

### Step 3: File Sharing Configuration

1. **Enable File Sharing**:
   * On both computers, enable file sharing settings:
     + Windows: Go to Control Panel > Network and Sharing Center > Advanced sharing settings. Turn on file and printer sharing.
     + Linux: Use tools like Samba to configure shared folders.
     + macOS: Go to System Preferences > Sharing, and enable File Sharing.
2. **Create Shared Folders**:
   * On Computer 1:
     + Create a new folder (e.g., SharedFolder).
     + Right-click the folder, go to Properties, and set sharing permissions.
     + Share the folder on the network.
   * On Computer 2:
     + Create a new folder (e.g., SharedFolder).
     + Set sharing permissions similarly.
     + Share the folder on the network.
3. **Access Shared Folders**:
   * On Computer 1:
     + Open File Explorer.
     + In the address bar, type \\192.168.1.2 and press Enter.
     + Access the shared folder from Computer 2.
   * On Computer 2:
     + Open File Explorer.
     + In the address bar, type \\192.168.1.1 and press Enter.
     + Access the shared folder from Computer 1.

## Results

After completing the steps above, the two computers should be successfully connected via Ethernet and configured for file sharing. Each computer should be able to access the shared folders of the other, allowing for the transfer of files between them.

## Discussion

The success of this lab demonstrates the importance of proper network configuration and file-sharing permissions in establishing a functional network for file sharing. Ensuring both computers are on the same subnet and properly configured for file sharing are crucial steps in this process.

## Conclusion

By following the outlined procedure, we established a physical connection and configured network settings to enable file sharing between two computers. This setup allows efficient file transfer and showcases fundamental networking and file-sharing principles.

# Lab 2: Generating Waves Using MATLAB

## Objective

Generating and Analyzing Waves Using MATLAB

## Materials and Equipment

* MATLAB software installed on a computer
* MATLAB code for wave generation
* MATLAB simulation environment
* Screenshots of generated waves

## Theory

MATLAB (Matrix Laboratory) is a powerful computational tool used extensively for engineering and scientific calculations. It is particularly effective in signal processing and wave generation due to its robust mathematical functions and versatile plotting capabilities.

Wave generation in MATLAB involves creating mathematical models of waves and visualizing them using MATLAB's plotting functions. Common types of waves include sine waves, cosine waves, and complex waveforms resulting from the superposition of multiple sine and cosine functions. The properties of these waves, such as amplitude, frequency, and phase, can be easily manipulated through code.

### Basic Wave Equations

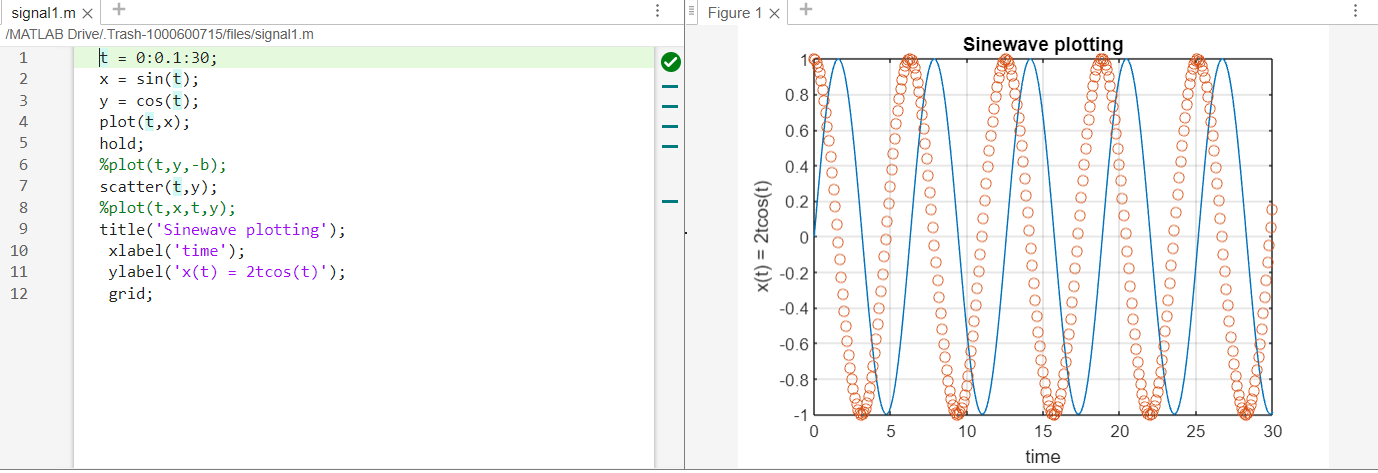
* **Sine Wave**: y(t)=Asin⁡(2πft+ϕ)y(t) = A \sin(2\pi f t + \phi)y(t)=Asin(2πft+ϕ)
* **Cosine Wave**: y(t)=Acos⁡(2πft+ϕ)y(t) = A \cos(2\pi f t + \phi)y(t)=Acos(2πft+ϕ)

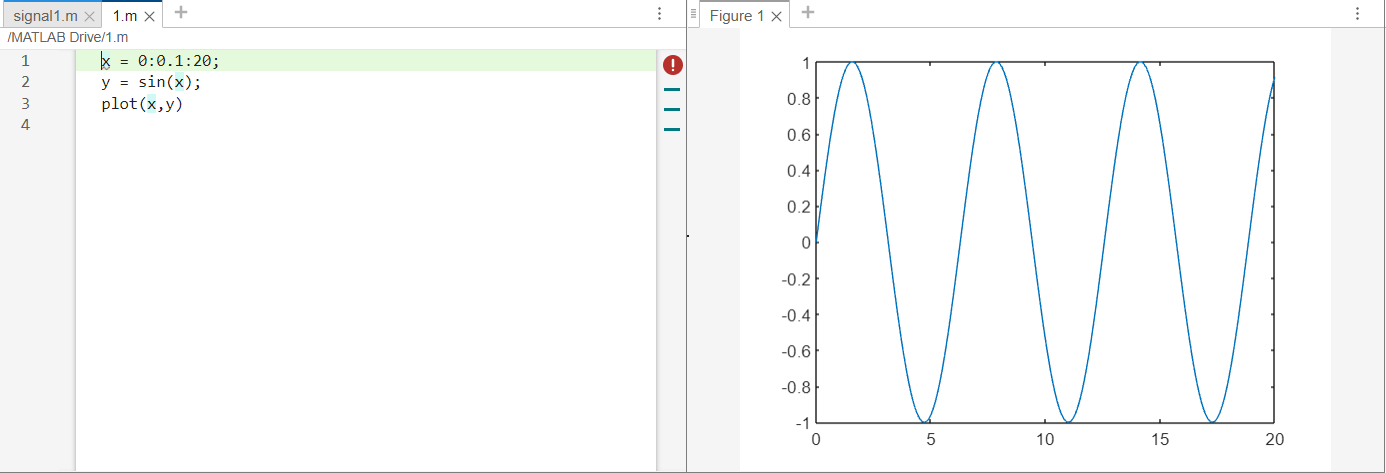
Where:

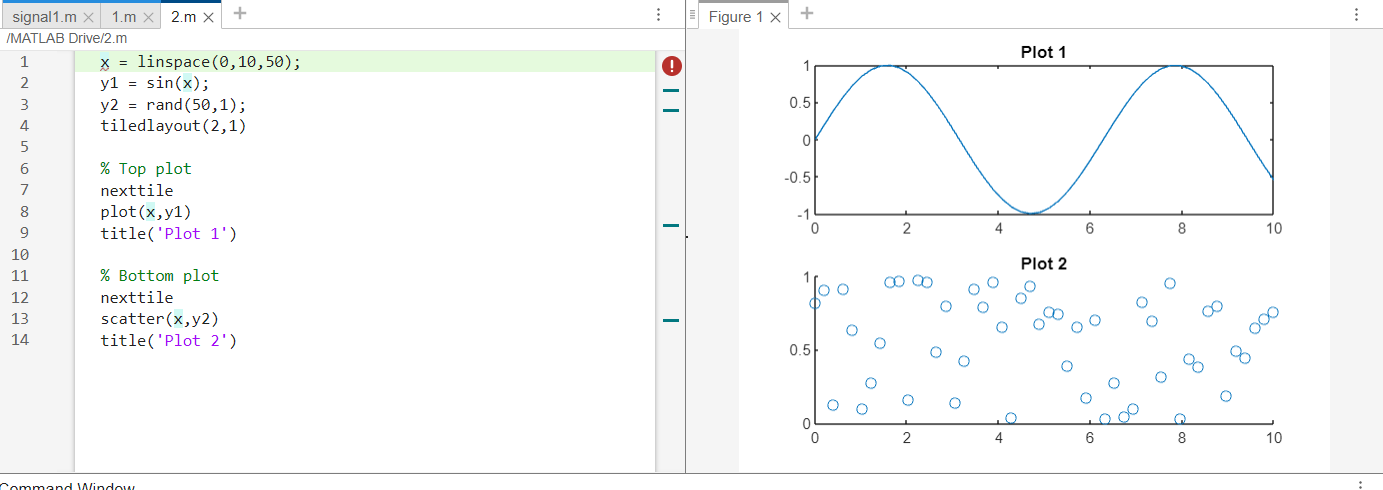
* A is the amplitude
* f is the frequency
* t is the time
* ϕ is the phase shift

## Results

The MATLAB code was used to generate and visualize different types of waves. Below are the results along with corresponding screenshots of the waves:







## Discussion

The results demonstrate MATLAB's capability in generating and visualizing different types of waves effectively. The sine was generated using their respective mathematical equations and plotted over a period of time. By adjusting parameters such as amplitude, frequency, and phase shift, various waveforms can be created and analyzed.

The complex wave, resulting from the superposition of two sine waves with different frequencies and phase shifts, illustrates how MATLAB can handle more sophisticated waveforms. This is particularly useful in signal processing and communication systems where such complex waveforms are common.

MATLAB's plotting functions provide a clear and precise visualization of these waves, which is essential for analysis and interpretation in both academic and professional settings.

## Conclusion

This lab successfully demonstrated the use of MATLAB for generating and visualizing different types of waves. The ease with which parameters can be adjusted and the clarity of the resulting plots highlight MATLAB's effectiveness as a tool for wave analysis. These skills are crucial for students and professionals working in fields related to signal processing, communication systems, and other areas requiring wave manipulation and analysis.

# Lab 3: Phishing and Profiling Using Kali Linux

## Objective

Phishing and Profiling Techniques Using Kali Linux

## Materials and Equipment

* Kali Linux operating system installed on a computer or virtual machine
* Internet connection
* Phishing tool (e.g., Social Engineering Toolkit (SET), Gophish)
* Profiling tool (e.g., Maltego, theHarvester)
* Target profiles for testing purposes

## Theory

### Phishing

Phishing is a cyber-attack technique where attackers impersonate a legitimate entity to deceive individuals into revealing sensitive information such as usernames, passwords, and credit card details. Kali Linux provides several tools to create phishing campaigns, simulate attacks, and study the effectiveness of phishing strategies.

### Profiling

Profiling involves gathering information about individuals or organizations from various sources to build a detailed profile. This information can be used for social engineering attacks, competitive analysis, or intelligence gathering. Tools like Maltego and theHarvester are commonly used for profiling as they automate the collection of data from public sources, including social media, websites, and online directories.

## Procedure

### Part 1: Conducting a Phishing Attack Using SET

1. **Launch Kali Linux** and open the terminal.
2. **Install SET** (if not already installed):

bash

Copy code

sudo apt-get update

sudo apt-get install set

1. **Start SET**:

bash

Copy code

sudo setoolkit

1. **Navigate through SET** to select a phishing attack:
   * Choose option 1: Social-Engineering Attacks.
   * Choose option 2: Website Attack Vectors.
   * Choose option 3: Credential Harvester Attack Method.
   * Choose option 2: Site Cloner.
2. **Enter the URL** of the website you wish to clone (e.g., <http://example.com>).
3. **Specify the IP address** for POST back in Harvester/Tabnabbing:

bash

Copy code

Enter the IP address for the POST back in Harvester/Tabnabbing: [Your IP Address]

1. **Monitor** the terminal for any captured credentials when the phishing page is visited.

### Part 2: Profiling Using Maltego

1. **Launch Maltego** from the applications menu or terminal:

bash

Copy code

maltego

1. **Create a new project** and add a new graph.
2. **Select an entity** to start with, such as a domain or email address.
3. **Run transforms** to gather information:
   * Right-click the entity and select "Run Transforms".
   * Choose the appropriate transforms for your investigation (e.g., DNS resolution, social media search).
4. **Analyze the results** and build a detailed profile by linking the collected data points.

### Part 3: Profiling Using theHarvester

1. **Open the terminal** in Kali Linux.
2. **Install theHarvester** (if not already installed):

bash

Copy code

sudo apt-get update

sudo apt-get install theharvester

1. **Run theHarvester** to collect information:

bash

Copy code

theharvester -d example.com -l 500 -b all

1. **Review the output**, which includes email addresses, subdomains, IP addresses, and other relevant data related to the target domain.

## Results

1. **Phishing Attack**:
   * Successfully cloned the specified website using SET.
   * Phishing page hosted and operational.
   * Credentials entered on the phishing page were captured and displayed in the SET terminal.
2. **Profiling with Maltego**:
   * Created a detailed profile of the target entity.
   * Identified various links between data points, such as email addresses, social media profiles, and associated domains.
3. **Profiling with theHarvester**:
   * Collected extensive information about the target domain.
   * Identified multiple email addresses, subdomains, and IP addresses.

## Discussion

The lab demonstrated the effectiveness of Kali Linux tools for phishing and profiling. SET proved to be a powerful tool for creating realistic phishing pages, enabling the capture of sensitive information. Maltego and theHarvester provided comprehensive profiling capabilities, allowing for the collection and analysis of data from various public sources.

Ethical considerations are paramount when using these tools. They should only be used for authorized testing, educational purposes, and improving security measures. Unauthorized use can lead to legal consequences and ethical violations.

## Conclusion

This lab successfully illustrated the use of Kali Linux for phishing and profiling activities. The tools provided by Kali Linux, such as SET, Maltego, and theHarvester, are effective for simulating phishing attacks and gathering detailed profiles from public sources. These techniques are valuable for understanding the mechanisms of cyber-attacks and enhancing cybersecurity defenses