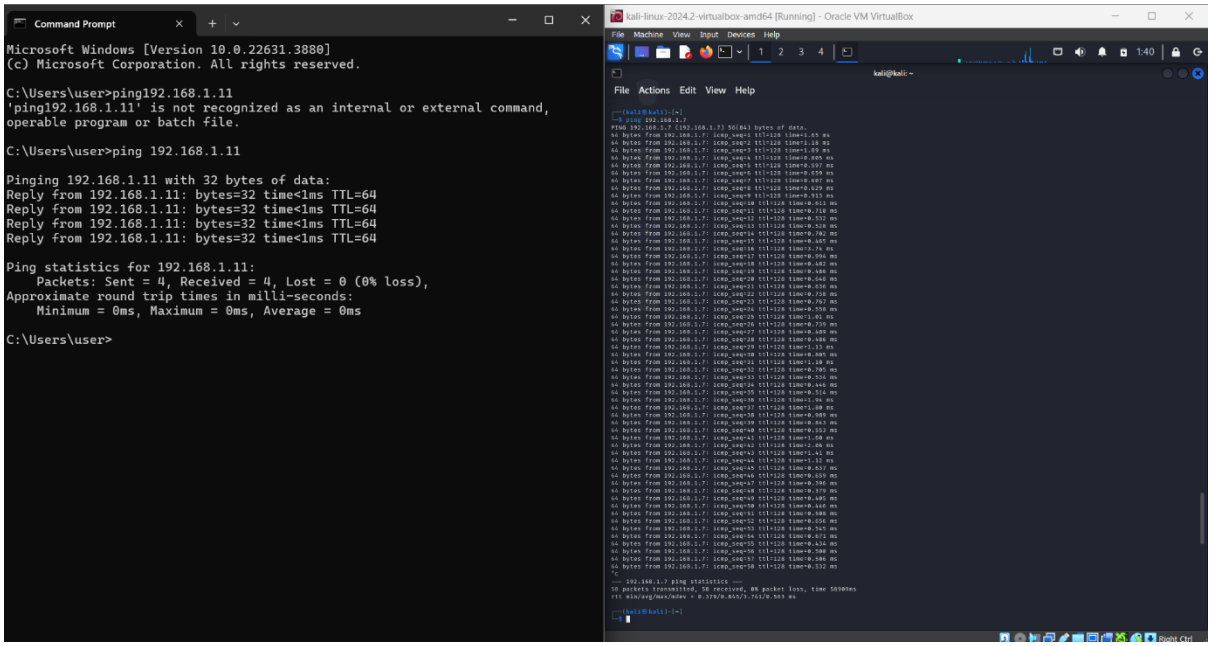
PRACTICAL ASSIGNMENT

JAIDEEP SINGH

Question 1

Set up a network in which we have at least 2 devices like – one can be a virtual machine and another can be our host machine

now using ping command on virtual machine on its terminal ping the ip of host machine and vice versa on host machine also.

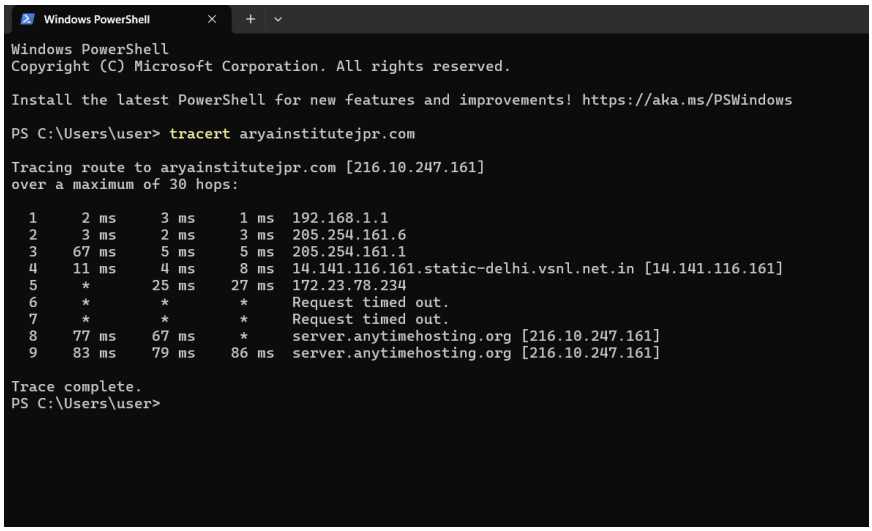


Question2

The tracert command is used to trace the path that a packet takes from your computer to a specified destination on a network. It helps diagnose network routing issues and understand the path packets travel across the Internet or within a network.

Significance of tracert:-

Path Verification , Diagnose Network Issues , Network Topology Insights , Troubleshoot Connectivity



Question3

Monitoring Network

Active Connections: Identify which applications or services are using network connections.

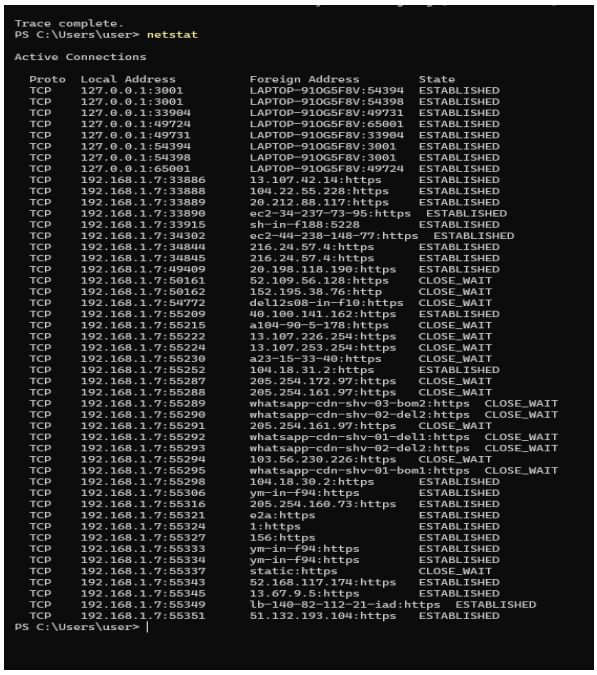
Listening Ports: Check which ports are open and listening for incoming connections

Troubleshooting

Detecting Open Ports: Identify if a specific port is open or closed, which is useful for diagnosing connectivity issues with services or applications.

Connection States: Determine the state of TCP connections to troubleshoot issues related to connectivity or network services.

Process Identification: Use netstat -o (Windows) or netstat -p (Linux) to find out which process is using a specific port, aiding in troubleshooting process-related network issues.



```
Trace complete.
PS C:\Users\user> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:3001         LAPTOP-91OG5F8V:54394  ESTABLISHED
  TCP    127.0.0.1:3001         LAPTOP-91OG5F8V:54398  ESTABLISHED
  TCP    127.0.0.1:33904        LAPTOP-91OG5F8V:49731  ESTABLISHED
  TCP    127.0.0.1:49724        LAPTOP-91OG5F8V:65001  ESTABLISHED
  TCP    127.0.0.1:49731        LAPTOP-91OG5F8V:33904  ESTABLISHED
  TCP    127.0.0.1:54394        LAPTOP-91OG5F8V:3001   ESTABLISHED
  TCP    127.0.0.1:54398        LAPTOP-91OG5F8V:3001   ESTABLISHED
  TCP    127.0.0.1:65001        LAPTOP-91OG5F8V:49724  ESTABLISHED
  TCP    192.168.1.7:33886      13.107.42.14:https     ESTABLISHED
  TCP    192.168.1.7:33888      104.22.55.228:https    ESTABLISHED
  TCP    192.168.1.7:33889      20.212.88.117:https    ESTABLISHED
  TCP    192.168.1.7:33890      ec2-34-237-73-95:https  ESTABLISHED
  TCP    192.168.1.7:33915      sh-in-f188:5228        ESTABLISHED
  TCP    192.168.1.7:34302      ec2-44-238-148-77:https  ESTABLISHED
  TCP    192.168.1.7:34844      216.24.57.4:https      ESTABLISHED
  TCP    192.168.1.7:34845      216.24.57.4:https      ESTABLISHED
  TCP    192.168.1.7:49409      20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.7:50161      52.109.56.128:https    CLOSE_WAIT
  TCP    192.168.1.7:50162      152.195.38.76:http     CLOSE_WAIT
  TCP    192.168.1.7:54772      del12s08-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.7:55209      40.100.141.162:https   ESTABLISHED
  TCP    192.168.1.7:55215      a104-90-5-178:https    CLOSE_WAIT
  TCP    192.168.1.7:55222      13.107.226.254:https   CLOSE_WAIT
  TCP    192.168.1.7:55224      13.107.253.254:https   CLOSE_WAIT
  TCP    192.168.1.7:55230      a23-15-33-40:https     CLOSE_WAIT
  TCP    192.168.1.7:55252      104.18.31.2:https      ESTABLISHED
  TCP    192.168.1.7:55287      205.254.172.97:https   CLOSE_WAIT
  TCP    192.168.1.7:55288      205.254.161.97:https   CLOSE_WAIT
  TCP    192.168.1.7:55289      whatsapp-cdn-shv-03-bom2:https   CLOSE_WAIT
  TCP    192.168.1.7:55290      whatsapp-cdn-shv-02-del2:https  CLOSE_WAIT
  TCP    192.168.1.7:55291      205.254.161.97:https   CLOSE_WAIT
  TCP    192.168.1.7:55292      whatsapp-cdn-shv-01-del1:https  CLOSE_WAIT
  TCP    192.168.1.7:55293      whatsapp-cdn-shv-02-del2:https  CLOSE_WAIT
  TCP    192.168.1.7:55294      103.56.230.226:https   CLOSE_WAIT
  TCP    192.168.1.7:55295      whatsapp-cdn-shv-01-bom1:https  CLOSE_WAIT
  TCP    192.168.1.7:55298      104.18.30.2:https      ESTABLISHED
  TCP    192.168.1.7:55306      ym-in-f94:https        ESTABLISHED
  TCP    192.168.1.7:55316      205.254.160.73:https   ESTABLISHED
  TCP    192.168.1.7:55321      e2a:https              ESTABLISHED
  TCP    192.168.1.7:55324      1:https                ESTABLISHED
  TCP    192.168.1.7:55327      156:https              ESTABLISHED
  TCP    192.168.1.7:55333      ym-in-f94:https        ESTABLISHED
  TCP    192.168.1.7:55334      ym-in-f94:https        ESTABLISHED
  TCP    192.168.1.7:55337      static:https           CLOSE_WAIT
  TCP    192.168.1.7:55343      52.168.117.174:https   ESTABLISHED
  TCP    192.168.1.7:55345      13.67.9.5:https        ESTABLISHED
  TCP    192.168.1.7:55349      lb-140-82-112-21-iad:https  ESTABLISHED
  TCP    192.168.1.7:55351      51.132.193.104:https   ESTABLISHED
PS C:\Users\user>
```

Question4

The legislative framework concerning Cyber Law in India comprises the Information Technology Act, 2000 (hereinafter referred to as the "**IT Act**") and the Rules made thereunder. The IT Act is the parent legislation that provides for various forms of Cyber Crimes, punishments to be inflicted thereby, compliances for intermediaries, and so on.

We should be aware of some basic laws like-

Section 65 – Tampering with computer Source Documents

Section 66 - Using password of another person

Section 66D - Cheating Using computer resource

Section 66E - Publishing private Images of Others

Section 66F - Acts of cyber Terrorism

Section 67 - Publishing Child Porn or predating children online

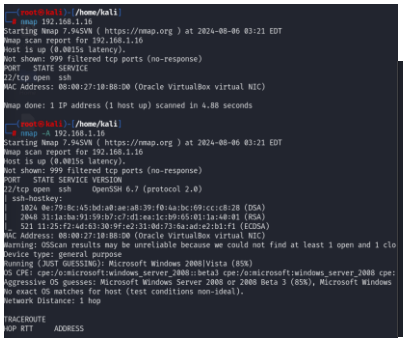
Section 69 - Govt.'s Power to block websites

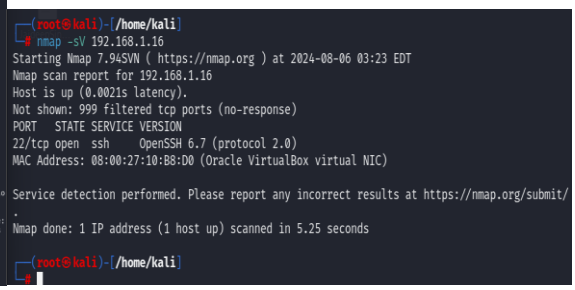
Section 43A - Data protection at Corporate level

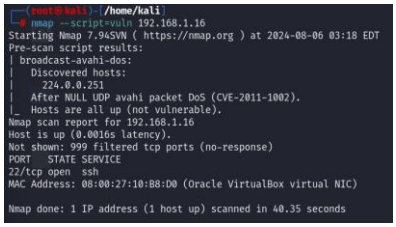
Question 5

Steps for nmap scanning:-

1. Install nmap- sudo apt-get install nmap
2. Determine the target ip like – nmap 192.168.1.1
3. If you want to scan a range of ip address then – nmap 192.168.1.1/24
4. To perform detail scan – nmap -A 192.168.1.1
5. To run a service scan – nmap -sV 192.168.1.1







Findings

1. Services
2. Service version
3. Open ports
4. Operating system of the target
5. Mac address

Potential vulnerability

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.7 (protocol 2.0)

Question 7

Installing kali linux in virtualbox

1. Downloaded and installed VirtualBox.
2. Created a new VM with specified settings.
3. Installed Linux OS from ISO or we can use vm image .
4. Installed VirtualBox Guest Additions for enhanced performance.
5. Performed system updates and optimizations.

To optimize the performance :-

1. Update the kali linux
2. Update its packages
3. Adjust vm for better performance
4. Provide storage as mentioned in documentation

Question 8

Methods Used to gather information

1. Search Engines (Google)
2. Company Profiles on Business Information Platforms
3. Official Website and Corporate Filings
4. News Articles
5. Social Media Profiles
6. Professional Networking Sites (LinkedIn)
7. WHOIS -it provide us the information about the web application
8. Subdomain finder-it is used to find the sub domain for the target website
9. Mxtoolbox.com-it diagnosis services which are integrated in web application
10. Builtwith.com-to find the technologies which are used to made the website

If our target is aryainstitutejpr.com then the gathered information from WHOIS for this web application will be-

1. Domain: aryainstitutejpr.com
2. Registrar:eNom, LLC
3. Registered On:2006-04-26
4. Expires On:2025-04-26
5. Updated On:2024-04-29
6. Status:clientTransferProhibited
7. Name Servers: (ns1.anytimehosting.org) (ns2.anytimehosting.org)

From search engine and social media plateform :-

Arya Institute of Engineering & Technology is a well-established institution offering a variety of engineering and management courses with robust infrastructure and active campus life. For more details, you can visit their official website and CollegeDunia profile.

Question 9

We are taking the following domain to perform the question

- aryainstitutejpr.com
  information gathered by WHOIS –
  1. Domain: aryainstitutejpr.com
  2. Registrar: eNom, LLC
  3. Registered On:2006-04-26
  4. Expires On:2025-04-26
  5. Updated On:2024-04-29
  6. Status: clientTransferProhibited
  7. Name Servers: (ns1.anytimehosting.org) (ns2.anytimehosting.org)

Question 10

Steps to setup a vpn connection

1. Open the VPN Application: Launch the VPN client after installation.
2. Login: Enter your VPN account credentials (username and password).
3. Select a Server: Choose a VPN server location from the list provided by the VPN client. Usually, you can select a server based on your needs (e.g., the nearest server for better speed, or a server in a specific country for content access).
4. Connect: Click on the “Connect” button to establish a VPN connection

Advantages –

1. Enhanced Security
2. Privacy Protection
3. Access Restricted Content
4. Secure Remote Access

Disadvantages –

1. Reduced Speed
2. Cost
3. Potential for Blocking
4. Security Risks with Free VPNs

Question 11

Steps to perform Ddos attack –

1. Install the hping3 – sudo apt-get install hping3
2. Simulation of DoS Attack- sudo hping3 -S --flood -V 192.168.1.16

Impact-

1. Network Congestion: Increased latency and packet loss.
2. Resource Exhaustion: High CPU and memory usage on the target machine.
3. Service Disruption: Essential services might become unresponsive or crash due to the inability to handle the excessive load

Mitigation Strategies-

Rate Limiting- Implement rate limiting on network devices to limit the number of incoming packets from a single source

Traffic Filtering- Use firewalls and intrusion detection/prevention systems (IDS/IPS) to filter out malicious traffic.

Resource Management: Optimize server configurations to handle high traffic more efficiently.

Service Hardening: Ensure that services are configured securely to withstand higher loads.

Question 12

Steps –

To perform the scan one should type the following syntax-

Wpscan --url cybervajra.com:-to scan the web application which the made by wordpress only.

Question 13

Steps and Tools for Detection

1.Check the HTML Source Code

Steps:

Right-click on the webpage and select "View Page Source" or press Ctrl+U.

Look for common WordPress markers like:

- wp-content
- wp-includes
- wp-admin
- meta name="generator" content="WordPress"

2.Use Online Detection Tools-

- Builtwith.com
- Wappalyzer
- IsItWP

3. Append /wp-admin or /wp-login.php to the website URL.

If you are redirected to a login page, the site is likely using WordPress.

Question 14

Steps to from a html form –

1. Create HTML Form: Write HTML code for the form and include it in index.html. This form will collect user data and send it to a PHP script using POST method.
2. Write PHP Script: Create save_data.php to handle the form data, sanitize it, and save it to form_data.txt.
3. Deploy: Upload files to a web server with PHP support. Ensure file permissions allow writing to form_data.txt.
4. Testing: Verify the form submission and data saving process by testing the form in a browser and checking the output file

Purpose of the Form in Phishing Attacks –

1. attackers can create a form that looks like a legitimate login page (e.g., for a bank or email service) and deceive users into entering their credentials.
2. The collected data (usernames, passwords, email addresses, etc.) can be stored in a file or database for malicious use, such as unauthorized access to accounts or identity theft
3. Forms can be used to collect email addresses that are then targeted with phishing emails containing malware.

Question 15

To crack the wifi network we will use fern wifi cracker , steps to use fern wifi cracker to crack wifi network are –

1. Install Fern WiFi Cracker
2. Launch Fern WiFi Cracker
3. Start the Tool
4. Scan for Networks: In the Fern WiFi Cracker GUI, go to "Wireless Interface" and select your wireless adapter.
5. Capture Handshake: Select the target network and click on "Start Capture" to capture the WPA/WPA2 handshake.
6. Crack the Password:After capturing the handshake, use the "WPA Cracker" feature to attempt to crack the password.
7. You can use a pre-configured wordlist or load your own custom wordlist.we can made our own wordlist by crunch command
8. Check Results: If the password is cracked, it will be displayed in the Fern WiFi Cracker interface.

Measures to Improve Wireless Security

1. Always use WPA3 if available. If not, use WPA2. Avoid WEP as it is outdated and vulnerable.
2. Use a complex password with a mix of letters, numbers, and special characters. The longer, the better.
3. WPS (Wi-Fi Protected Setup) can be vulnerable to attacks. Disable it in your router settings.
4. Check for and apply firmware updates regularly to protect against known vulnerabilities
5. Restrict network access to known devices by filtering MAC addresses
6. Ensure that all communications over the network are encrypted.

Question 16

Steps included in development process are as follows –

Create a Project Directory

Create a html file :-this file will contain the structure of our webpage.

```html
login.html > ...
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>IP Information</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body>
    <div class="container">
        <h1>IP Information</h1>
        <input type="text" id="ipInput" placeholder="Enter IP address or leave empty to get your IP">
        <button id="searchButton">Get Information</button>
        <div id="ipInfo">
            <!-- IP information will be displayed here -->
        </div>
    </div>
    <script src="script.js"></script>
</body>
</html>
```

Create css file:- This file contains styles for your web page to make it look nice.

```css
styles.css > ...
body {
    background-color: #f0f0f0;
}

.container {
    text-align: center;
    background-color: white;
    padding: 20px;
    border-radius: 8px;
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
}

input[type="text"] {
    padding: 10px;
    margin: 10px 0;
    width: 300px;
    border: 1px solid #ccc;
    border-radius: 4px;
}

button {
    padding: 10px 20px;
    background-color: #007bff;
    color: white;
    border: none;
    border-radius: 4px;
    cursor: pointer;
}

button:hover {
    background-color: #0056b3;
}

#ipInfo {
    margin-top: 20px;
}
```

Create java script file :- this file will handle the interaction with api and will update the html

```javascript
JS script.js > addEventListener('click') callback > then() callback
document.getElementById('searchButton').addEventListener('click', function() {
    const ipInput = document.getElementById('ipInput').value;
    const ip = ipInput.trim() === '' ? '' : ipInput;
    const apiUrl = ip ? `http://ip-api.com/json/${ip}` : 'http://ip-api.com/json/';

    fetch(apiUrl)
        .then(response => response.json())
        .then(data => {
            if (data.status === 'fail') {
                document.getElementById('ipInfo').innerHTML = `<p>Error: ${data.message}</p>`;
            } else {
                const info = `
                    <h2>IP Information</h2>
                    <p><strong>IP:</strong> ${data.query}</p>
                    <p><strong>City:</strong> ${data.city}</p>
                    <p><strong>Region:</strong> ${data.regionName}</p>
                    <p><strong>Country:</strong> ${data.country}</p>
                    <p><strong>ZIP:</strong> ${data.zip}</p>
                    <p><strong>ISP:</strong> ${data.isp}</p>
                    <p><strong>Organization:</strong> ${data.org}</p>
                    <p><strong>AS:</strong> ${data.as}</p>
                `;
                document.getElementById('ipInfo').innerHTML = info;
            }
        })
        .catch(error => {
            document.getElementById('ipInfo').innerHTML = `<p>Error: ${error.message}</p>`;
        });
});
```

Testing :- Open index.html in a browser to see your web page in action.