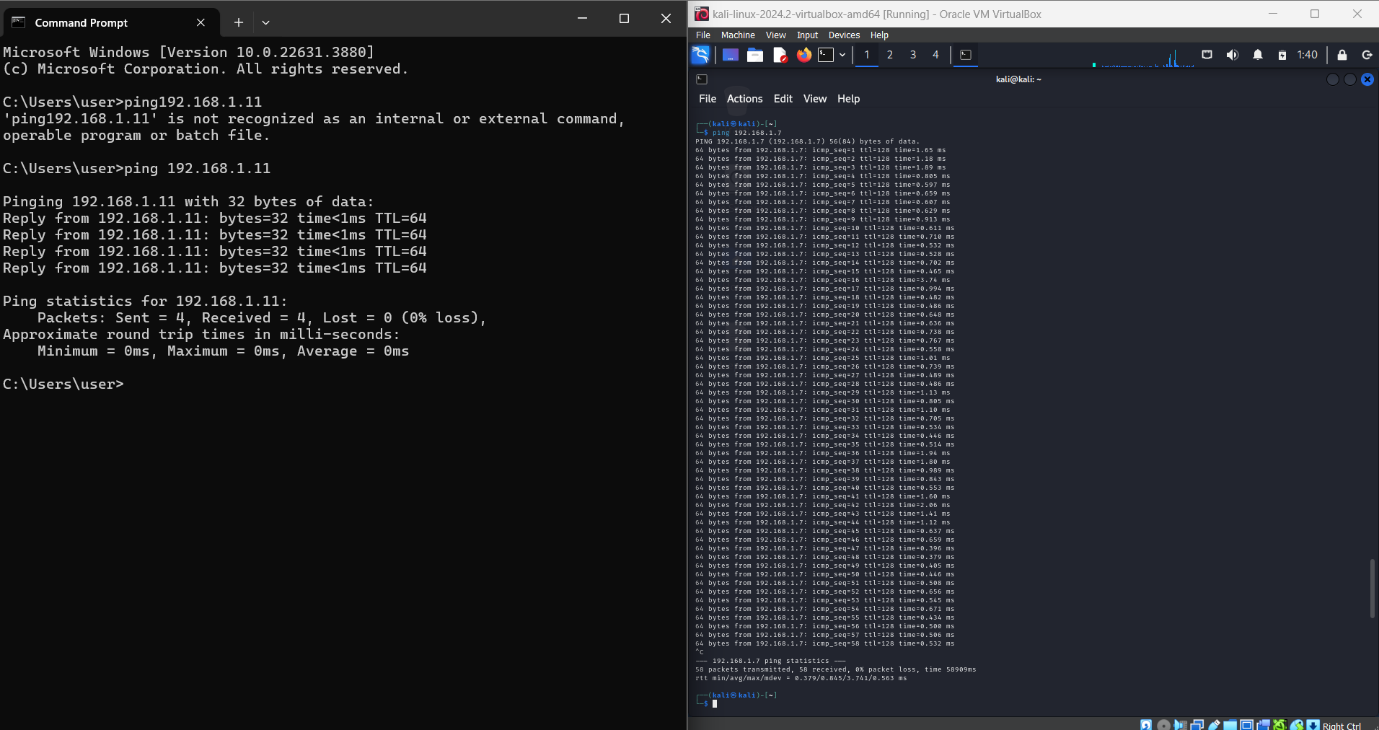
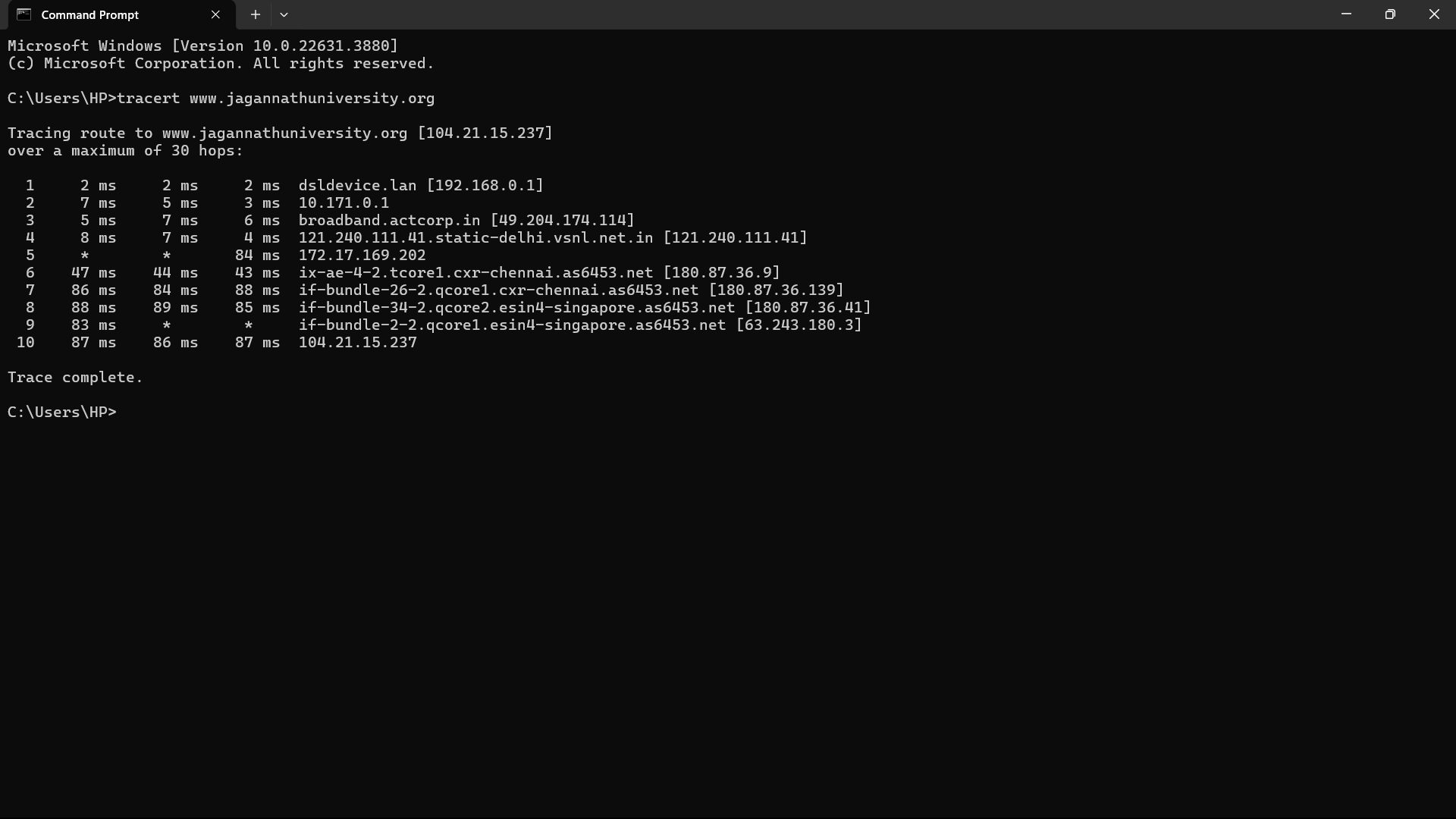
**Q1.**  **Set up a small network using at least two devices and ping each other. Document the process and explain the results.**

**ANS.s et 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.**



**.Q2. Use the tracert command on your college website. Explain the steps and the significance of the results obtained.**

ANS. 

Traceroute is a simple yet clever command-line tool for tracing the path an IP packet takes across one or many networks. It was originally developed for UNIX-based platforms, but is now included in most operating systems, with the Windows implementation being known as “tracert”. The output of these commands is also frequently referred to as a traceroute. Ask for help with poor streaming video performance, for example, and your ISP might ask you for a traceroute.

Steps by Steps result

1. **Hop Number**

The first column just tells you which hop the trace is on. Whenever you access the Internet (or even data on an internal network), the data travels from one piece of hardware to another. These will typically be routers, but could also be switches, servers, or even computers. Each of these pieces of hardware that the data goes through is considered a hop.The total number of hops that a connection goes through will depend on many factors, the most important of which is the physical locations where you run the command and the destination.

**2.Round Trip Time (RTT) Results**

The next three columns (Table 3) show the amount of time it took data to go from the source (typically your computer) to that hop and back. This is measured in milliseconds.When running the traceroute command, you are sending data to each hop three times. The first column is the amount of time it took the first time, the second is for the second attempt, and the third is for the last attempt. When everything is running properly, the round-trip time for each attempt should be similar.

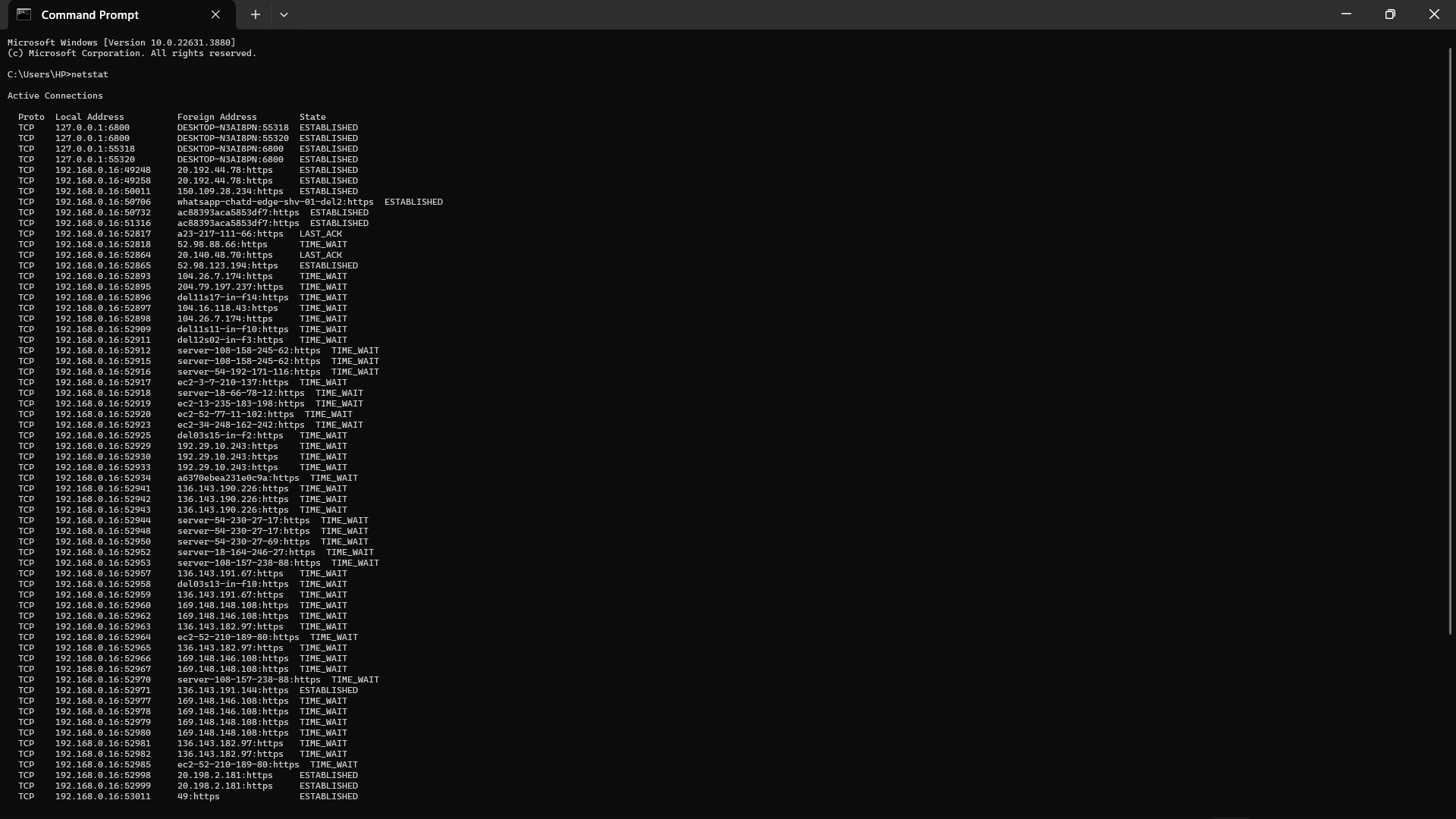
**3.Hop Name and IP Address**

The final column is where the name, IP address, or other information about the hop is displayed. The information displayed here is determined by the settings on the hop itself.Some devices are set to only display their IP addresses. Others will also display the device name or other information. In some cases, the owner of the device has set it up so that it will not reveal any information at all, in which case you will simply see an asterisk (\*) for that particular hop.

**Q3. Use the netstat command on your system. Document the output and explain its use in network monitoring and troubleshooting.**

**ANS.** The netstat command is a highly practical tool for network diagnostics, configurations, and other port-scanning activities. More specifically, system administrators use it for network troubleshooting and performance diagnostics

The netstat command works on Microsoft Windows, Linux, Unix, FreeBSD, and more



**Q4. Research and present a case study of a cyber law incident in India. Explain the laws involved and the outcome of the case**

**ANS. SONY.SAMBANDH.COM CASE**

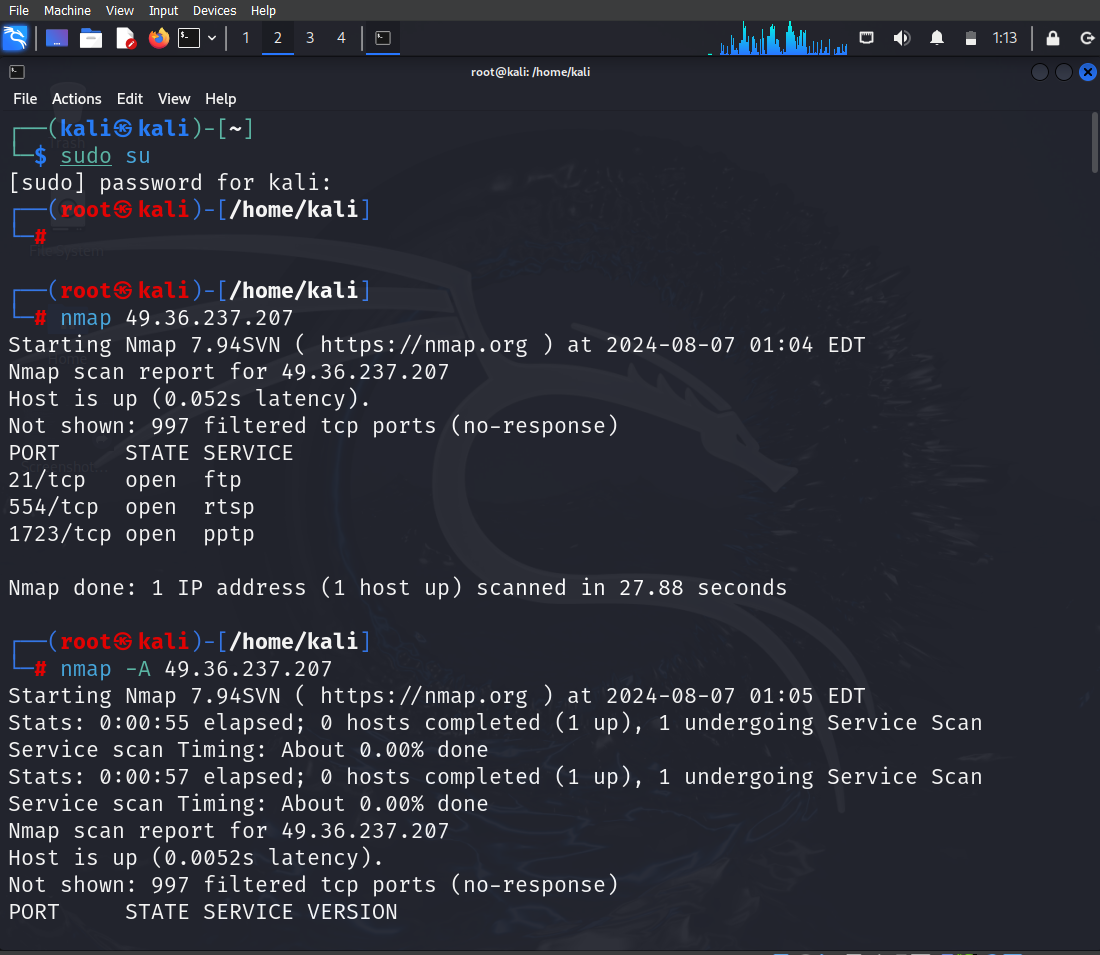
India saw its 1st cybercrime conviction. This is the case where Sony India Private Limited filed a complaint that runs a website referred to as www.sony-sambandh.com targeting the NRIs. The website allows NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the involved recipients. In May 2002, somebody logged onto the web site underneath the identity of Barbara Campa and ordered a Sony colour television set and a cordless head phone. She requested to deliver the product to Arif Azim in Noida and gave the number of her credit card for payment. The payment was accordingly cleared by the credit card agency and the transaction processed. After the related procedures of dues diligence and checking, the items were delivered to Arif Azim by the company. When the product was delivered, the company took digital pictures so as to indicate the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company had filed a complaint for online cheating at the CBI that registered a case under the Section 418, Section 419 and Section 420 of the IPC (Indian Penal Code). Arif Azim was arrested after the matter was investigated. Investigations discovered that Arif Azim, whereas acting at a call centre in Noida did gain access to the number of the credit card of an American national which he misused on the company’s site. The CBI recovered the color television along with the cordless head phone. In this matter, the CBI had proof to prove their case so the accused admitted his guilt. The court had convicted Arif Azim under the Section 418, Section 419 and Section 420 of the IPC, this being the first time that a cybercrime has been convicted. The court, felt that since the defendant was a boy of 24 years and a firsttime convict, a compassionate view needed to be taken. Thus, the court discharged the defendant on the probation for one year.

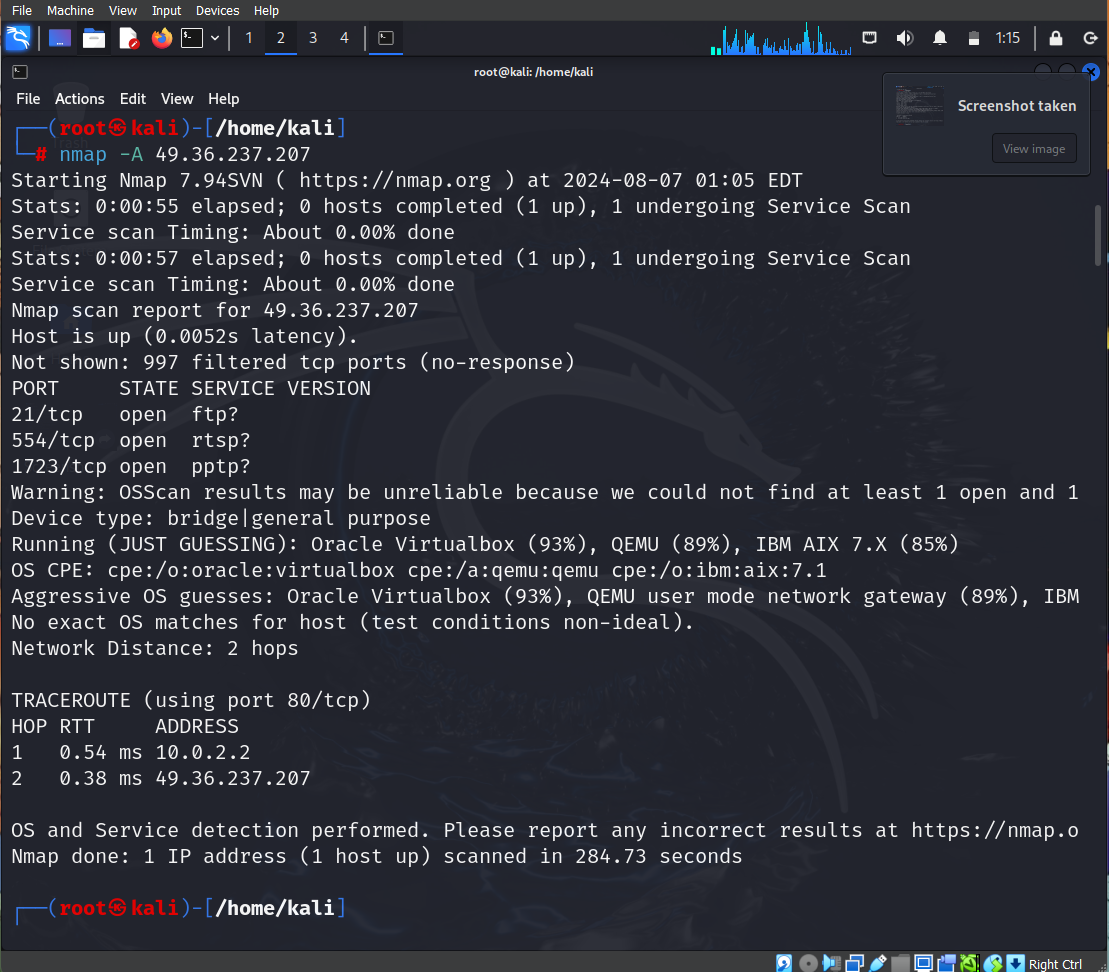
**LAW INVOLVED**

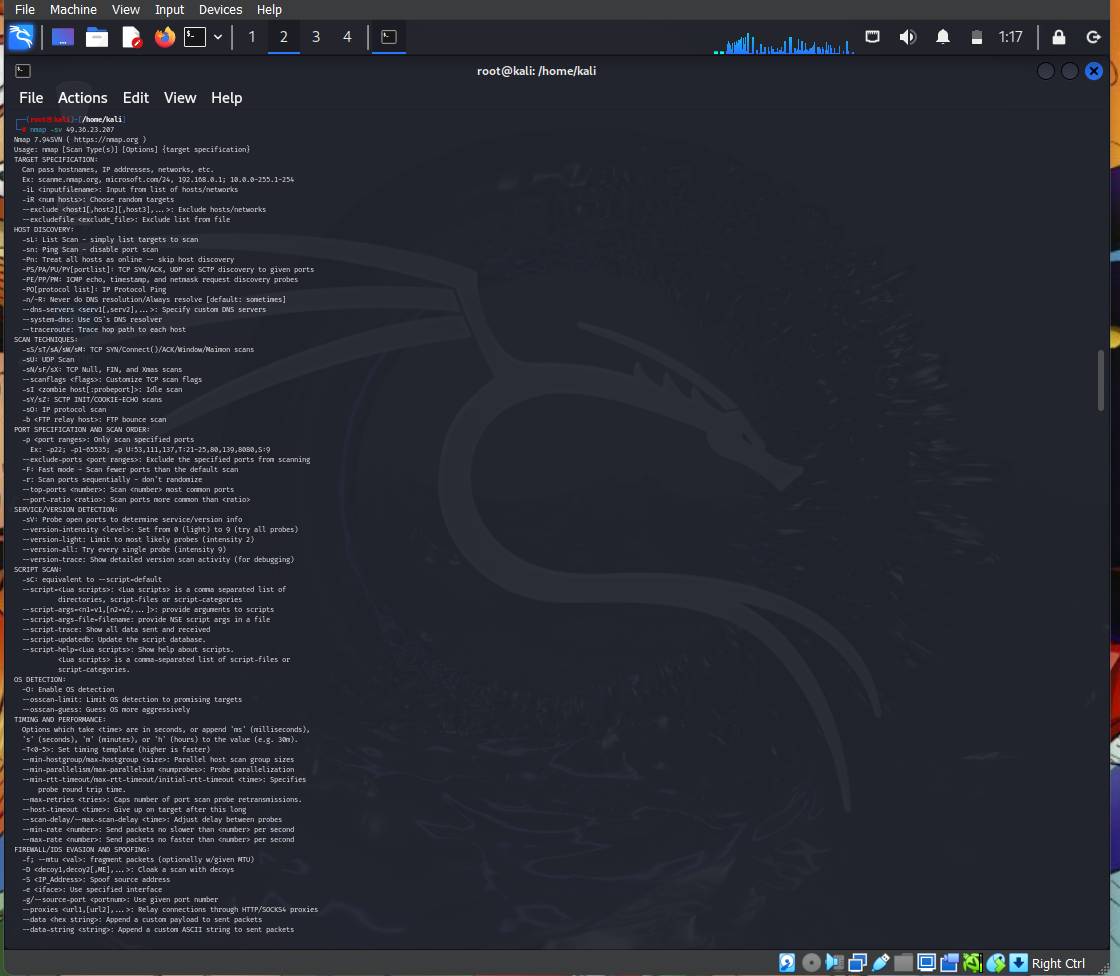
Section 67 and Section 70 of the IT Act are also applied. In this case the hackers hacks ones webpage and replace the homepage with pornographic or defamatory page.

**Q5. Use Nmap to perform a network scan. Document the steps, findings, and potential vulnerabilities identified**

**ANS.**

****

****

****

**Nmap scripts contain well over 100 specific scans for vulnerabilities that can be run against domains or against specific host IP addresses.**

**Application Scans: Run Nmap against a target domain (ex: esecurityplanet.com)  to check websites for vulnerabilities such as:**

* **http-csrf: Detect Cross-Site Request Forgery (CSRF) vulnerabilities by entering the command: Nmap -sV –script http-csrf <target domain>**
* **http-sherlock: Check if the “shellshock” vulnerability can be exploited in web applications by entering the command: Nmap -sV –script http-sherlock <target domain>**

**Q7 .Set up a virtual machine using a hypervisor (e.g., VirtualBox or VMware). Install a Linux operating system on the VM and optimize its performance. Document the process.**

**ANS. 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**

**Q8. Use search engines and online tools to gather information about a specific target (ensure it is a legal and ethical target). Document the methods used and the information found.**

**ANS .** **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: Jagannathuniversity.org**

**2. Registrar: eNom, LLC**

**3. Registered On:** **2008-04-20**

**4. Expires On:** **2027-04-20**

**5. Updated On:** **2022-05-17**

**6. Status: clientTransferProhibited**

**7. Name Servers: kai.ns.cloudflare.com and malavika.ns.cloudflare.com**

**From search engine and social media plateform :-**

**Jagannath university 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.**

**Q9 .** **Perform a WHOIS lookup on a domain name and interpret the results. Provide details on the domain’s ownership, registration, and expiration.**

**ANS. We are taking the following domain to perform the question**

* **Jagannathuniversity.org**

**information gathered by WHOIS –**

**1. Domain: Jagannathuniversity.org**

**2. Registrar: eNom, LLC**

**3. Registered On:** **2008-04-20**

**4. Expires On:** **2027-04-20**

**5. Updated On:** **2022-05-17**

**6. Status: clientTransferProhibited**

**7. Name Servers: kai.ns.cloudflare.com and malavika.ns.cloudflare.com**

**Q10. Set up a VPN connection on your system. Document the steps and explain the advantages and disadvantages of using a VPN for secure communication.**

**ANS. 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 –**

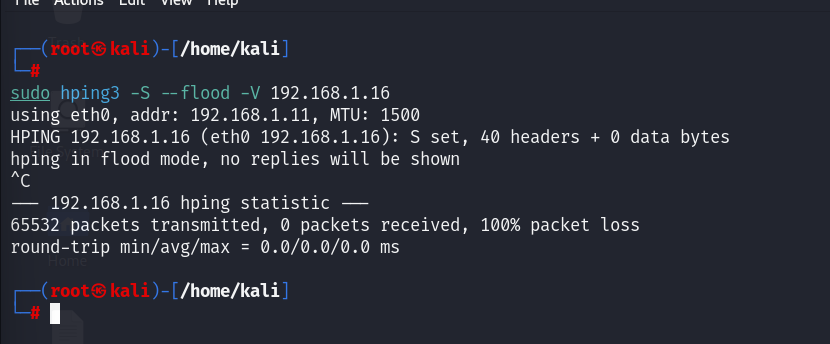
1. **Enhanced Security**
2. **Privacy Protection**
3. **Access Restricted Content**
4. **Secure Remote Access**

**Disadvantages –**

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

**Q11. Use hping3 to perform a DoS attack simulation. Document the process, the impact observed, and suggest mitigation strategies.**

**ANS.**



**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-

from a single source

Traffic FilterinRate Limiting- Implement rate limiting on network devices to limit the number of incoming packets g- Use firewalls and intrusion detection/prevention systems (IDS/IPS) to filter out malicious traffic.

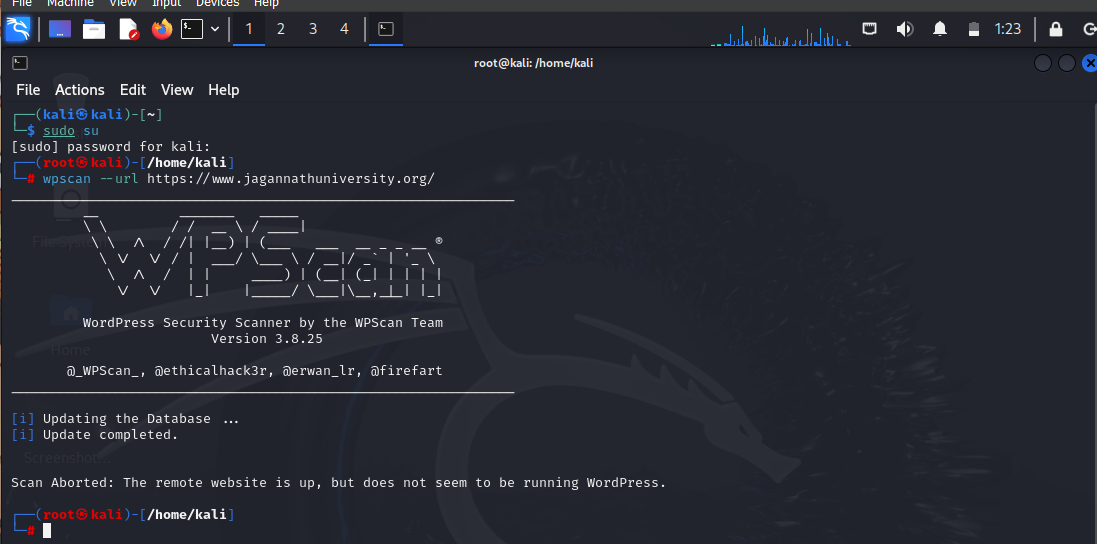
Resource Management: Optimize server configurations to handle high traffic more efficiently.

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

Q12. Perform a vulnerability scan on the WordPress website cybervajra.com using wpscan. Document the process and findings.

ANS. 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.



Q13. Explain how you would identify if a website is using WordPress. List the steps and tools used for detection

ANS. 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.

Q14. Create a simple HTML form that saves submitted data to a text file. Document the steps and the purpose of the form in phishing attacks.

ANS. 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.

Q15. Set up a wireless network and attempt to crack its security using tools .Document the process and results, and suggest measures to improve wireless security.

ANS. 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

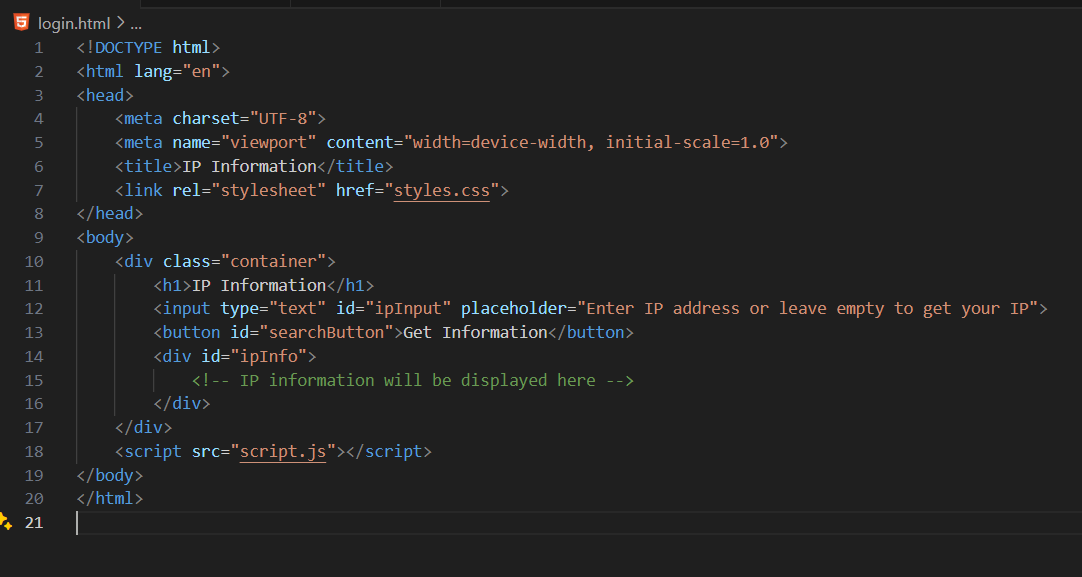
1. Always use WPA3 if available. If not, use WPA2. Avoid WEP as it is outdated and vulnerable.
2. Use a complex password with a mix of letters, numbers, and special characters. The longer, the better.
3. WPS (Wi-Fi Protected Setup) can be vulnerable to attacks. Disable it in your router settings.
4. 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.

Q16. Using the API "http://ip-api.com/json/{query}", create a web page similar to https://osint-tan.vercel.app/ that grabs your IP and shows its information. Add a search bar where users can search any IP. You are free to use any additional APIs. Document the development process and the functionality of the page.

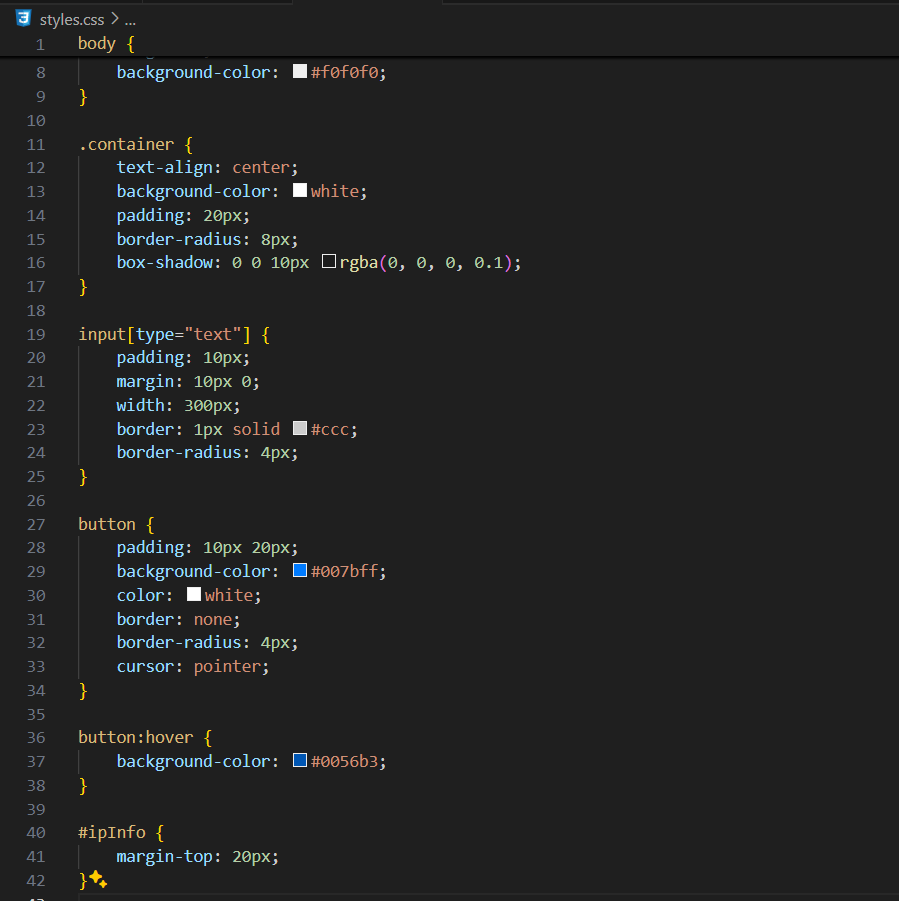
ANS. Steps included in development process are as follows –

Create a Project Directory

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



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



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



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

