Task 1: Introduction to Network Security Basics

Objective: Understand the basics of network security by learning about different types of network threats and how to implement basic security measures. This task will introduce you to the foundational concepts of securing a small network.

Skills: Basic Network Security, Threat Identification, Security Best Practices **Tools:** Firewall (Windows Defender Firewall or a basic hardware firewall), Wireshark

1. Learn Network Security Concepts:

I. Different Types of Network Threats:

Network threats can be categorized into various types based on their nature and the methods they use. Here are some common types of network threats:

1. Malware

- **Viruses**: Malicious software that attaches itself to clean files and spreads throughout a computer system.
- **Worms**: Similar to viruses but can spread independently without user intervention.
- **Trojan Horses**: Disguised as legitimate software, they can create backdoors for attackers.
- **Ransomware**: Locks users out of their data, demanding payment to restore access.

2. Phishing

- Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity, often via email.

3. Denial of Service (DoS)

- Attacks that aim to make a network service unavailable by overwhelming it with traffic or requests.

4. Man-in-the-Middle (MitM)

- Interception of communication between two parties, allowing attackers to eavesdrop or alter messages.

5. SQL Injection

- Exploiting vulnerabilities in web applications to execute arbitrary SQL code, potentially exposing sensitive data.

6. DDoS (Distributed Denial of Service)

- A more sophisticated version of DoS, where multiple compromised systems flood the target with traffic.

7. Insider Threats

- Threats originating from within the organization, often involving current or former employees who misuse their access.

8. Zero-Day Exploits

- Attacks that occur on the same day a vulnerability is discovered, before a fix is available.

9. Credential Stuffing

- Automated injection of stolen username and password pairs to gain unauthorized access to user accounts.

10. Social Engineering

- Manipulating individuals into divulging confidential information through psychological tricks.

11. Botnets

- Networks of infected devices controlled by attackers to perform coordinated attacks or send spam.

12. Advanced Persistent Threats (APTs)

- Prolonged and targeted cyberattacks where an intruder gains access to a network and remains undetected for a long time.

13. Eavesdropping

- Unauthorized interception of network traffic to access sensitive information.

14. Session Hijacking

- Exploiting a valid computer session to gain unauthorized access to the information or services.

Conclusion

II. Hardware or Network device:

Hub:

- It is uses to connect systems or nodes or networks.
- It has direct connection to a node (point to point connection).
- It suffers from high collision of data, results to data loss.
- A hub takes data from input port and retransmits the input data on output port.

Repeater:

- A repeater is a device which regenerates or amplifies the data or signal so that it can be travel to the other segment of cable.
- It is use to connect two networks that uses same technology and protocol.
- It does not filter or translate any data.
- Work in physical layer.

Bridge:

- It is used to connect two networks.
- It divides the collision domain based on number of ports or interface present in a bridge.
- It uses the packet switches that forward and filter the frames using LAN destination address.
- Bridge examines the destination address of frame and forwards it to the interface or port which leads to the destination.
- It uses the routing table for routing frame from one node to other using MAC address.

- It works in Data Link Layer.

Switch:

- It is similar to bridge. It has more number of interfaces as compared to bridge.
- It allows direct communication between the nodes.
- It works in Data Link Layer.
- It uses MAC address for data transmission and communication.

Router:

- It is used to connect different types of network (types- architecture/ Protocol).
- It work similar to bridge but it uses IP address for routing data.
- Router can't be used for connecting Systems.
- It works in Network Layer.

Gateways:

Gateways make communication possible between systems that use different communication protocols, data formatting structures, languages and architectures. Gateways repackage data going from one system to another. Gateways are usually dedicated servers on a network and are task-specific

III. Basic security concepts:

Understanding basic security concepts is essential for protecting information and systems. Here are some key concepts:

1. Confidentiality

- Ensuring that sensitive information is accessible only to authorized individuals. This often involves encryption and access controls.

2. Integrity

- Maintaining the accuracy and completeness of data. This can be achieved through checksums, hashing, and version control.

3. Availability

- Ensuring that information and resources are accessible to authorized users when needed. This includes redundancy, backups, and disaster recovery plans.

4. Authentication

- Verifying the identity of users, devices, or systems before granting access. Common methods include passwords, biometrics, and multi-factor authentication (MFA).

5. Authorization

- Granting access rights to authenticated users based on their roles and permissions. This determines what resources a user can access and what actions they can perform.

6. Non-repudiation

- Ensuring that a party in a transaction cannot deny the authenticity of their signature or the sending of a message. This often involves digital signatures and logs.

7. Risk Management

- Identifying, assessing, and prioritizing risks to minimize their impact on an organization. This includes risk assessment, mitigation strategies, and regular reviews.

8. Firewalls

- Security devices or software that monitor and control incoming and outgoing network traffic based on predetermined security rules.

9. Intrusion Detection and Prevention Systems (IDPS)

- Tools that monitor network or system activities for malicious activities or policy violations, and can take action to prevent breaches.

10. Encryption

- The process of converting information into a code to prevent unauthorized access. This is crucial for protecting data in transit and at rest.

11. Security Policies

- Formalized rules and procedures that govern the protection of information and technology assets. These policies guide user behavior and response to security incidents.

12. Patch Management

- The process of regularly updating software and systems to fix vulnerabilities and improve security.

13. Backup and Recovery

- Strategies for creating copies of data to protect against loss due to disasters, cyberattacks, or hardware failures. Recovery plans ensure business continuity.

14. Social Engineering Awareness

- Educating users about the tactics used by attackers to manipulate individuals into divulging confidential information.

IV. Secure Network Configurations

Implementing secure network configurations is crucial for protecting sensitive data and ensuring the integrity and availability of network resources. Here are some key practices for achieving secure network configurations:

1. Network Segmentation

- Divide the network into segments or zones (e.g., DMZ, internal, guest) to limit access and reduce the spread of threats.

2. Firewalls

- Utilize hardware and software firewalls to control incoming and outgoing traffic based on predefined security rules.

3. Access Control Lists (ACLs)

- Implement ACLs on routers and switches to restrict access to network resources based on user roles or IP addresses.

4. Strong Password Policies

- Enforce strong password requirements (length, complexity) and regular password changes for all network devices and user accounts.

5. Secure Protocols

- Use secure protocols for data transmission, such as HTTPS, SSH, and SFTP, instead of their insecure counterparts (HTTP, Telnet, FTP).

6. Network Address Translation (NAT)

- Use NAT to hide internal IP addresses from external networks, adding an additional layer of security.

7. Intrusion Detection and Prevention Systems (IDPS)

- Deploy IDPS to monitor network traffic for suspicious activity and take action to block potential threats.

8. Regular Software Updates and Patching

- Ensure that all network devices, including routers, switches, and firewalls, are regularly updated and patched to fix vulnerabilities.

9. Disable Unused Services and Ports

- Turn off unnecessary services and close unused ports on network devices to reduce the attack surface.

10. Virtual Private Networks (VPNs)

- Implement VPNs for secure remote access to the network, ensuring that data transmitted over the internet is encrypted.

11. Logging and Monitoring

- Enable logging on network devices and monitor logs for unusual activities or potential security breaches.

12. User Education and Training

- Provide regular training for users on security best practices, including recognizing phishing attempts and using secure passwords.

13. Network Access Control (NAC)

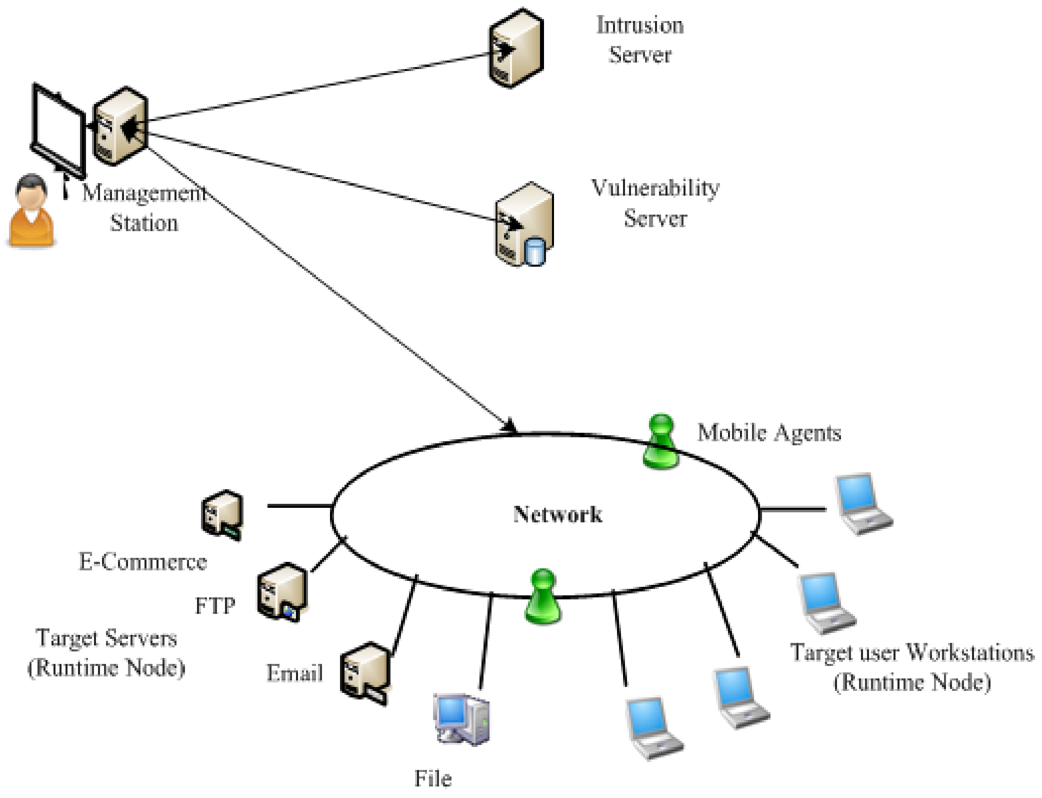
- Implement NAC solutions to enforce security policies on devices attempting to access the network, ensuring compliance with security standards.

14. Backup Configurations

- Regularly back up the configurations of network devices to ensure quick recovery in case of a failure or breach.

15. Physical Security

- Ensure that physical access to network devices is restricted to authorized personnel only, preventing tampering or unauthorized access.



2. Implement Basic Security Measures

Aim:

Configuration of computer lab set up Using cisco packet tracer

Objectives:

Creating a computer lab setup using Cisco Packet Tracer involves several key objectives. Firstly, designing and configuring a Local Area Network (LAN) infrastructure with switches and routers, ensuring seamless connectivity among lab computers. Secondly, implementing VLANs for network segmentation, allowing efficient resource allocation and management. Thirdly, establishing secure wireless access points with encryption and authentication mechanisms. Fourthly, configuring DHCP and DNS services for automatic IP assignment and name resolution. Fifthly, setting up a server for centralized file storage, user authentication, and printer sharing. Lastly, practicing network monitoring, troubleshooting, and documentation to enhance technical skills and knowledge in a simulated environment.

Theory:

Cisco Packet Tracer is a tool built by Cisco and it provides network simulation to practice simple and complex networks. A DHCP Server is a network server that automatically assigns IP addresses, default gateways, and other network parameters to client devices.

Setting up a computer lab using Cisco Packet Tracer involves designing and configuring a network environment to accommodate multiple computers. This entails interconnecting devices through switches and routers, establishing VLANs for efficient traffic management, and ensuring secure wireless access with encryption methods. Additionally, DHCP and DNS services facilitate automatic IP allocation and name resolution, while centralized servers support file storage, user authentication, and printer sharing, creating a comprehensive and functional simulated lab environment.

Procedure:

Step 1:

Open the Cisco Packet Tracer.

Step 2:

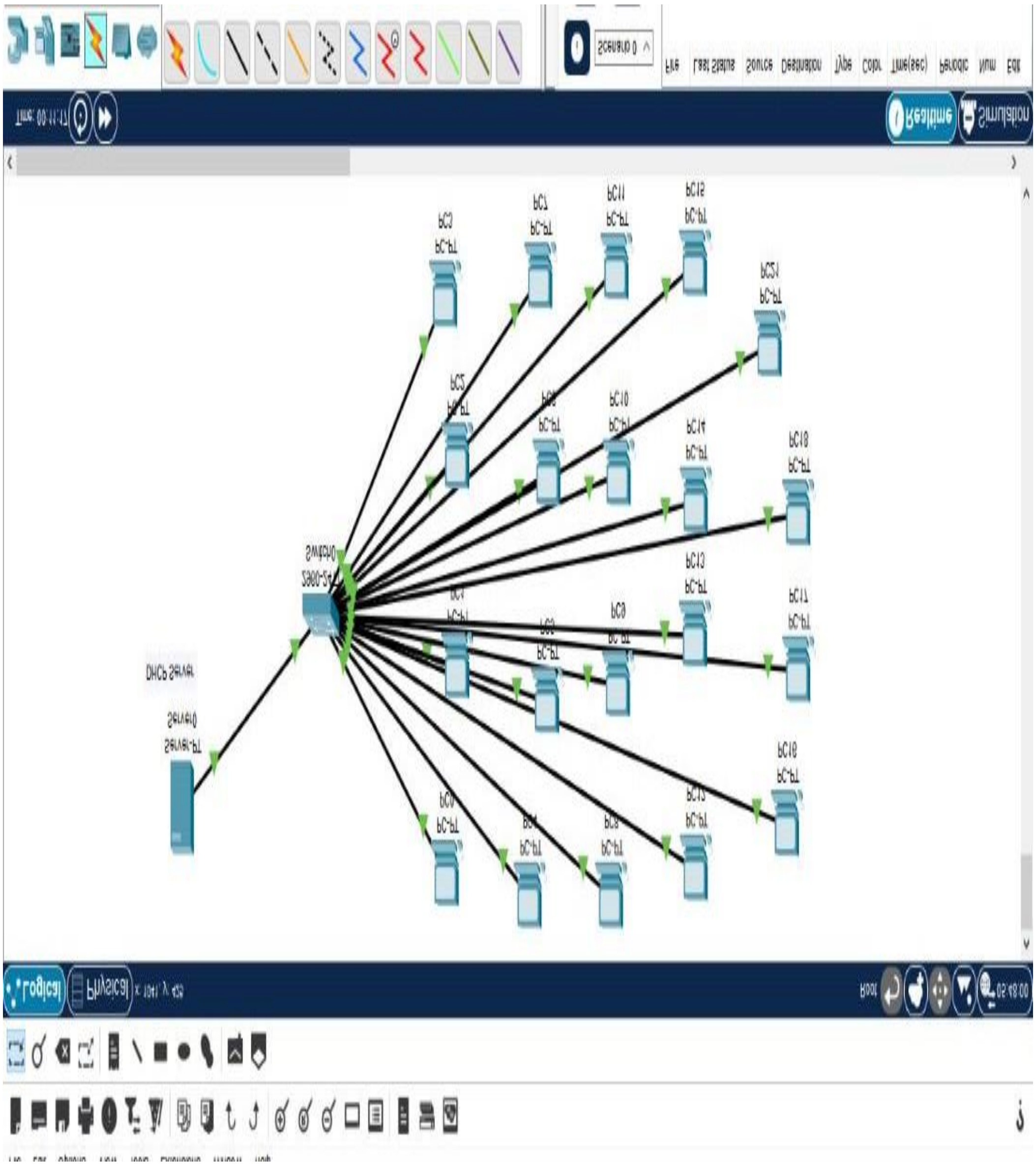
After opening the CISCO packet tracer, add a switch, a server, and 20 PCs to the screen from the bottom left section for this project.

Note: One can add any number of PCs but here we're considering 20 PCs in a lab.

Switch	**1**
Server	**1**
PC's	**20**

Step 3:

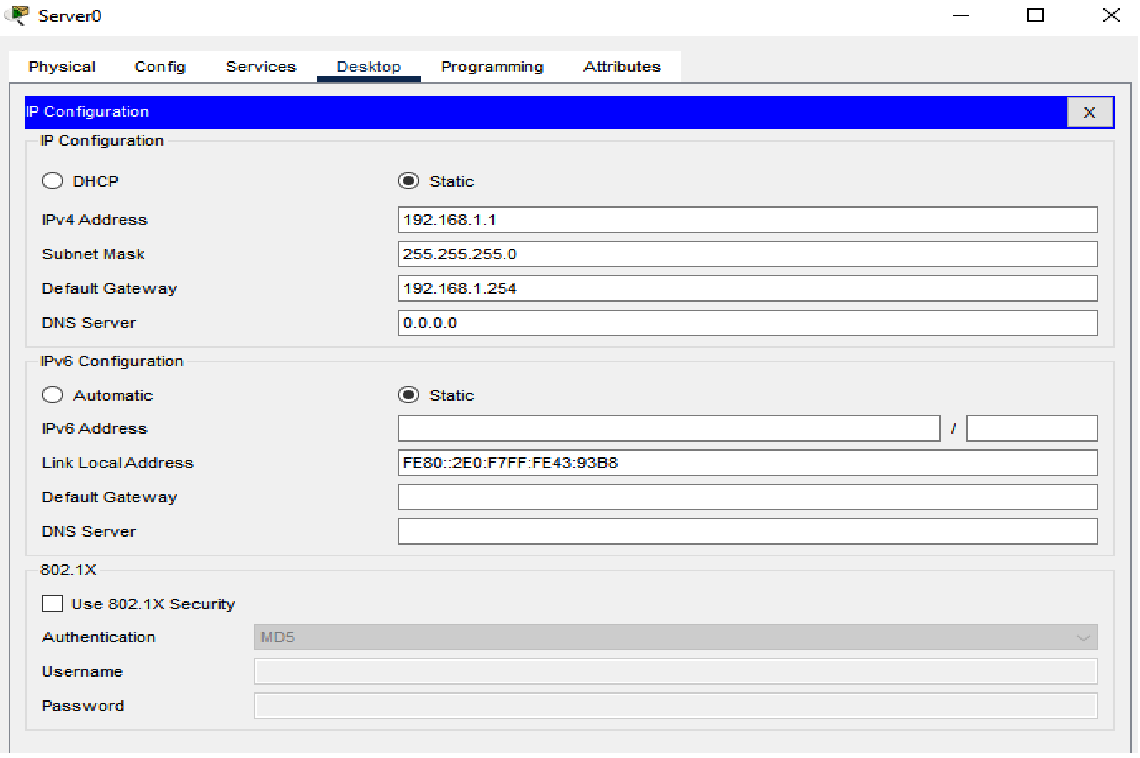
Connect all PCs and the server with a switch by using a cable from the cable section.



Step 4:

We’re considering the server as a DHCP server. Click on server, go to Desktop, and then click on IP configuration. Give an IP address, subnet mask, and default gateway to the server.

IP Address	**192.168.1.1**
Subnet Mask	**255.255.255.0**
Default Gateway	**192.168.1.254**



IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /
Link Local Address: FE80::2E0:F7FF:FE43:93B8
Default Gateway:
DNS Server:

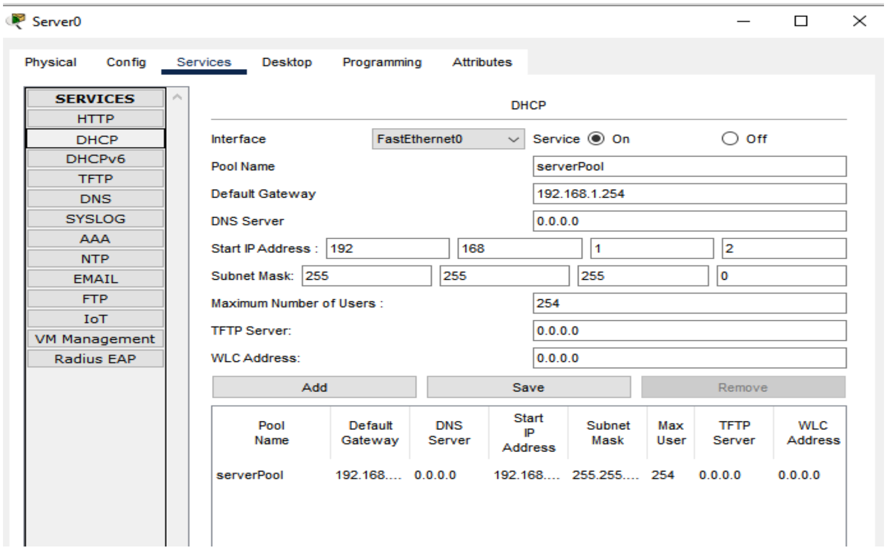
802.1X

□ Use 802.1X Security
Authentication: MD5
Username:
Password:

Step 5:

Click again on the server, click on the services section, and then go to DHCP. Turn on the DHCP services and then enter the default gateway, starting IP address, subnet mask,

and a number of devices, and then SAVE it. Now, the DHCP server will automatically assign IP, subnet mask, etc. to the PCs.



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.1.254

DNS Server: 0.0.0.0

Start IP Address : 192 168 1 2

Subnet Mask: 255 255 255 0

Maximum Number of Users : 254

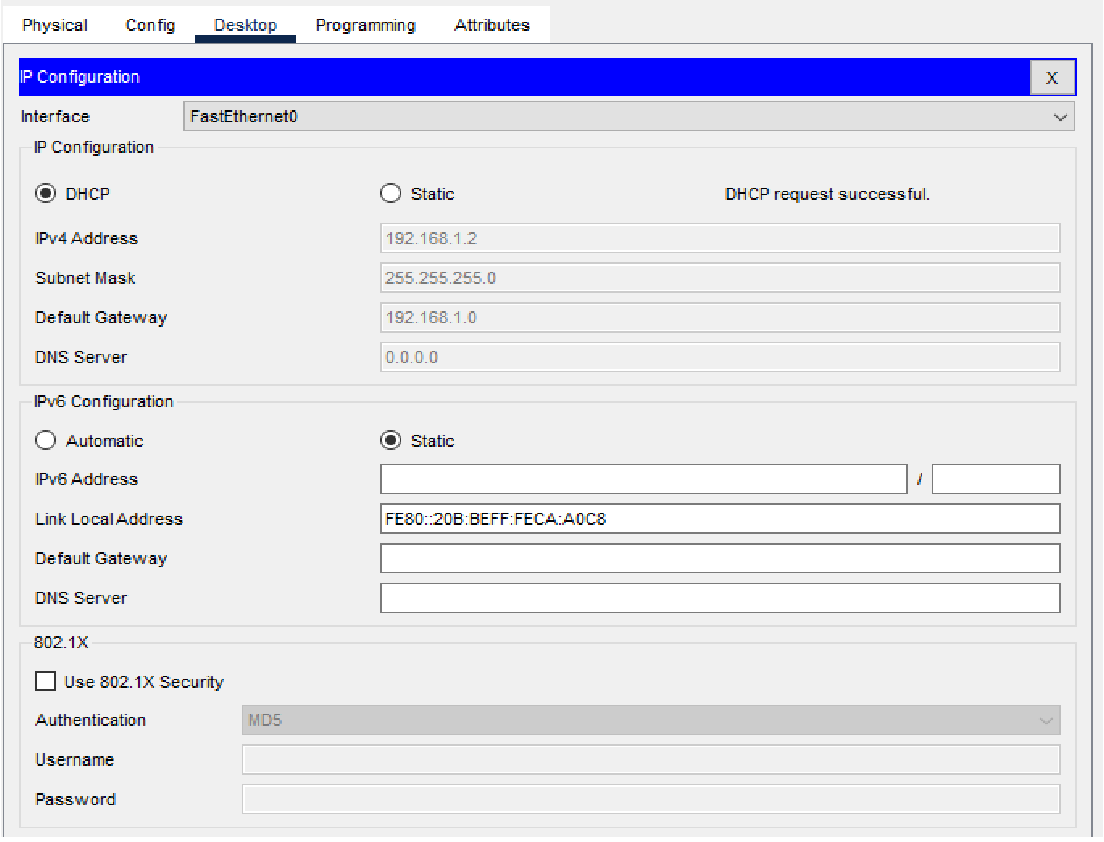
TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	0.0.0.0	192.168....	255.255....	254	0.0.0.0	0.0.0.0

Step 6:

Click on any PC, go to Desktop, and then click on the IP configuration section. Click on DHCP and it will request the IP address, subnet mask, etc. from the DHCP server and it will automatically assign all these to the PC.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20B:BEFF:FECA:A0C8

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Step 7:

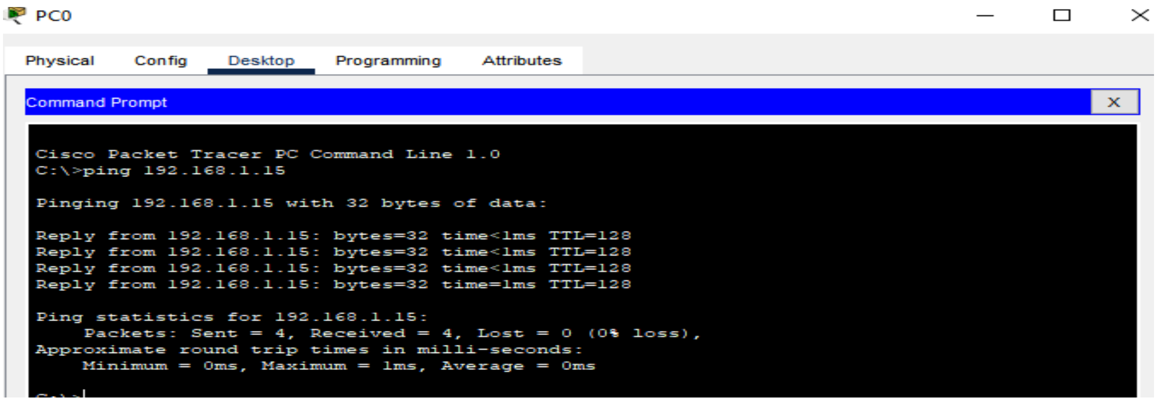
Do this for all the PCs. One can also use the ping command to check the communication between all PCs.

For example,

From PC0

ping

192.168.1.5



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.15

Pinging 192.168.1.15 with 32 bytes of data:

Reply from 192.168.1.15: bytes=32 time<1ms TTL=128
Reply from 192.168.1.15: bytes=32 time<1ms TTL=128
Reply from 192.168.1.15: bytes=32 time<1ms TTL=128
Reply from 192.168.1.15: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Results:

The result of a computer lab setup using Cisco Packet Tracer is a fully operational network environment with interconnected computers, switches, and routers. This lab facilitates hands-on learning of networking concepts, VLAN segmentation, secure wireless access, DHCP/DNS services, and centralized server functionalities within a simulated setting.

3. Monitor Network Traffic

Introduction

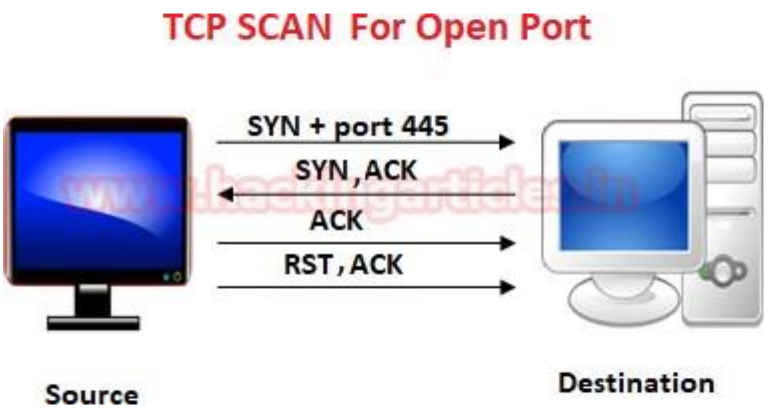
In this post, you will learn how to capture network packets using Wireshark when an attacker is scanning a target using the NMAP port scanning method. Here you will notice how Wireshark captured different network traffic packets for open and closed ports.

Note: The below practical is performed with the same IP address (192.168.1.102), which you will notice is common for our Windows and Linux machines. You may differentiate them by their MAC addresses in this case.

Let's start!!!

TCP Scan

TCP Scan will scan for TCP ports like port 22, 21, 23, 445, etc. and ensure the listening port is open through a 3-way handshake connection between the source and destination port. If the port is open, the source sent an **SYN** packet, the response destination sent an **SYN** packet, the source sent **ACK** packets, and the source sent **RST** and **ACK** packets again.



Type the following NMAP command for TCP scan as well as start Wireshark on the other hand to capture the sent packet.

```
nmap -sT -p 445 192.168.1.102
```

4. Reflecting on Security Best Practices

I. Reflecting on Security Best Practices

Security best practices are the bedrock of modern digital life. They ensure the safety of our personal information, protect our online transactions, and safeguard critical infrastructure. Here are some key reflections on these practices:

The Evolving Threat Landscape

- **Constant Evolution:** The threat landscape is continually evolving, with new vulnerabilities and attack vectors emerging regularly. This necessitates a proactive approach to security, adapting to the latest trends and techniques.
- **Sophisticated Attacks:** Cyberattacks are becoming increasingly sophisticated, often targeting specific individuals or organizations. This underscores the need for robust security measures that can withstand advanced threats.

The Importance of Human Factors

- **User Awareness:** Human error remains a significant factor in security breaches. Educating users about best practices, such as strong password hygiene, phishing awareness, and secure browsing habits, is crucial.
- **Social Engineering:** Social engineering attacks, which exploit human psychology, continue to be effective. Organizations must implement robust security awareness programs to mitigate these risks.

The Role of Technology

- **Advanced Tools:** Technology plays a vital role in enhancing security. Tools like firewalls, intrusion detection systems, and encryption software can significantly strengthen defenses.
- **AI and Machine Learning:** Artificial intelligence and machine learning are revolutionizing cybersecurity by enabling automated threat detection and response.
- **Zero-Trust Security:** This security model assumes that no one or nothing can be trusted, requiring strict verification and authorization for every access attempt.

Key Security Best Practices

- **Strong Password Hygiene:** Use complex, unique passwords for each account and enable multi-factor authentication.
- **Software Updates:** Keep software and operating systems up-to-date to address vulnerabilities.
- **Phishing Awareness:** Be cautious of suspicious emails and avoid clicking on links or downloading attachments from unknown sources.
- **Secure Browsing:** Use reputable browsers with strong security features and avoid visiting untrusted websites.
- **Data Privacy:** Be mindful of personal information shared online and use privacy settings to limit exposure.
- **Regular Backups:** Create regular backups of important data to protect against data loss.
- **Endpoint Security:** Protect devices like laptops and smartphones with antivirus software, firewalls, and encryption.

II. Educating Others on the Importance of Network Security in Everyday Use

Network security is crucial for everyone in today's digitally connected world, as it safeguards personal and organizational information from cyber threats and attacks. Educating others about network security begins with explaining the risks associated with insecure networks, such as identity theft, data breaches, and financial fraud. Simple actions, like using strong passwords, avoiding suspicious links, and enabling multi-factor authentication, can significantly reduce vulnerabilities. By raising awareness of these practical steps and promoting responsible online behaviour, we can help individuals protect their devices and data, contributing to a safer, more secure online environment for all.