**Question1:**

I Created the Virtual Machines By As Follows:

For The SRV (Windows Server 2022)

1. **I Open VirtualBox** and create a new virtual machine.
2. **Name the VM**: SRV
3. **Type**: Windows
4. **Version**: Windows Server 2022
5. **Hard Drive**: I create a new virtual hard disk with a minimum size of 50GB.
6. **Network Adapter**: I set it to a Bridged Adapter.
7. I Installed the Windows Server 2022:
   * I set the computer name to **SRV** and the password to **Password123** during setup.
8. Configure TCP/IP settings:
   * I navigated to the Control Panel > Network and Internet > Network Connections.
   * Then I Right-click on the network adapter and select **Properties**.
   * And selected the **Internet Protocol Version 4 (TCP/IPv4)** and **Properties**.
     + IP Address: **192.168.10.1**
     + Subnet Mask: **255.255.255.0**
     + DNS Server: **192.168.10.1**
9. To Promote to Domain Controller, I Made the Following Changes:
   * I the Server Manager I clicked on **Add roles and features** then selected the **Active Directory Domain Services** to install.
   * Once installed, I created a new forest named **deltech.co.za**.
10. To Configure Firewall, I Had Too:
    * Open Windows Defender Firewall with Advanced Security and click on **Inbound Rules,** then Locate **File and Printer Sharing** rules and enable them for all profiles (Domain, Private, Public).

For Kali (Kali Linux)

1. I Created another VM:
   * Name: **Kali**.
   * Type: Linux
   * Version: Debian (64-bit)
   * Hard Drive: 50GB.
   * Network Adapter: "Bridged".
2. Configure TCP/IP settings:
   * **sudo nano /etc/network/interfaces**
   * **auto eth0**
   * **iface eth0 inet static**
   * **address 192.168.10.2**
   * **netmask 255.255.255.0**
3. Restart Networking

* **sudo systemctl restart networking**

Step 2: Testing the Configuration

1. Check Connectivity:

**ping 192.168.10.2**

**ping 192.168.10.1**

**Question 2:**

Step 1: Wireshark on Windows Server

1. Start Capturing Packets**:**
   * I click on the interface to start capturing packets

Step 2: Use Nmap on Kali Linux

1. Run a Ping Scan:

* **Nmap -sn 192.168.10.0/24**

1. Run an OS Discovery Scan:
   * TO perform an OS discovery scan on the Windows Server (192.168.10.1):

* **Nmap -O -Pn 192.168.10.1**

Step 3: To Analyse Captured Packets Using Wireshark

1. Stop the Packet Capture:
   * I clicked on the red square button to stop capturing packets when I completed the scans.
2. To Filter Captured Packets:
   * Use the filter bar at the top to focus on specific packets (you can apply filters later).

Step 4: List Five Captured Packets

1. Identify Packets:
   * As ICMP echo requests/responses (for the ping scan) or TCP SYN packets (for the OS scan).
2. The Documented Packets Are:
   * + Source IP:
     + Destination IP:
     + Protocol:
     + Length:
     + Info:

Step 5: Create and Save Filters in Wireshark

1. Filter for Kali Linux Address:

* **ip.addr == 192.168.10.2**

1. Filter for Destination Ports 53 and 445:

* **tcp.dstport == 53 or tcp.dstport == 445**

**Question 3:**

3.1 OpenSSH Server

1. To Install OpenSSH Server:
   * Go to Settings > Apps > Optional Features.
   * Click on Add a feature.
   * Search for OpenSSH Server, select it, and click Install.
2. I Configured the Service to Start Automatically:
   * Open PowerShell as Administrator and ran the command:

* **Set-Service -Name sshd -StartupType 'Automatic'**
* **Start-Service sshd**
  1. Tocreate an Inbound Firewall Policy for TCP Port 22

1. I Opened Windows Defender Firewall with Advanced Security and clicked on Inbound Rules > New Rule.
2. TCP and port 22.

3.3 Use ncrack on Kali

1. To Install ncrack:

* **sudo apt-get install ncrack**

1. The ncrack command with the password dictionary:

* **ncrack -p 22 -u <username> -P /usr/share/ncrack/top50000.pwd <target\_IP>**

1. Log in to the SSH server using the cracked credentials:

* **ssh <username>@<target\_IP>**

1. Display privileges:

* **whoami /priv**

1. Create the file on the Windows Server's Desktop:

* **echo "You have been PWNed!!" > "C:\Users\<username>\Desktop\Gotin.txt"**

3.4 Other Activities an Attacker Could Do with This Access

With access to the SSH server, an attacker could:

* Install malware or backdoors for persistent access.
* Exfiltrate sensitive data from the server.
* Modify system configurations to elevate privileges or create new users.
* Conduct further attacks on other machines within the same network.
* Use the server as a pivot point for attacks on other networks.

3.5 Defending Against This Type of Attack

To defend against SSH password cracking attacks, consider following measures:

1. **Use Strong Passwords:** Enforce complex password policies.
2. **Disable Password Authentication:** Use key-based authentication and disable password logins by setting Password-Authentication no in the SSH configuration.
3. **Implement Fail2Ban:** Configure Fail2Ban to block IPs after a certain number of failed login attempts.
4. **Change the Default SSH Port:** Alter the default port from 22 to a non-standard port.
5. **Limit User Access:** Use the Allow-Users directive in SSH config to restrict access to specific users.
6. **Monitor Logs:** Regularly check SSH access logs for any unusual activity.

**Question 4:**

Step 1: Create a New Policy

1. Create the Policy:
   * I added a Policy and named it First Scan.

Step 2: Run a Basic Network Scan

1. I created a New Scan:
   * I selected the First Scan
2. I Configured Scan Settings:
   * The target is Windows Server IP address 192.168.10.1.

Step 3: To Analyse the Scan Results.

1. Identified Vulnerabilities:
   * The vulnerabilities detected:
     + Missing patches
     + Default passwords
     + Unnecessary services running
     + Weak configurations
2. Remediation Steps:
   * Each vulnerability, has a remediation suggestion:
     + **Update Software:** All software and Windows are up to date with the latest patches.
     + **Change Default Passwords:** Default credentials with strong, unique passwords.
     + **Disable Unnecessary Services:** Turn off services that are not needed.
     + **Configuration Hardening:** Adjust the settings.

Step 4: Utility of Vulnerability Scans in Penetration Testing

1. Understanding the Network Environment:
   * Vulnerability scans provide an overview of the systems and services running on the network, helping pen testers to focus their efforts.
2. Identifying Weaknesses:
   * The scan identifies potential weaknesses that could be exploited, guiding penetration testers to prioritize areas of concern.
3. Assessment of Security Posture:
   * Regular vulnerability assessments can help track the security posture over time and evaluate the effectiveness of remediation efforts.
4. Informing Test Strategies:
   * Results from vulnerability scans can inform the penetration testing strategy, including choosing tools and techniques to exploit vulnerabilities.

**Question 5:**

Step 1: Configure Network Settings in snort.conf

1. Open snort.conf:
2. Edit Network Settings:
   * **ipvar HOME\_NET 192.168.10.0/24**

Step 2: Configure Local Rules

1. Open local.rules:
   * Open the **local.rules file.**
2. Create Alerts:
   * **alert tcp any any -> [YOUR\_SERVER\_IP] 22 (msg:"SSH Connectivity Detected"; sid:1000001; rev:1; threshold: type both, track by\_src, count 3, seconds 5;)**
3. For SYN Scans:
   * **alert tcp any any -> [YOUR\_SERVER\_IP] any (msg:"SYN Scan Detected"; flags:S; sid:1000002; rev:1; threshold: type both, track by\_src, count 3, seconds 5;)**

Step 3: I Ran Snort

1. To Run the Snort:
   * I Navigated to the Snort directory:
   * **cd C:\Snort\bin**
   * **snort -c C:\Snort\etc\snort.conf -i 1 -A console**

Step 4: Perform Scans from Kali Linux

1. Run Nmap TCP SYN Scan:
   * **nmap -sS -Pn 192.168.10.1**
2. Establish an SSH Session:
   * **ssh username@192.168.10.1**

Step 5: View Alerts from Snort

1. Check the Snort Console:
   * + SSH connectivity detected.
     + SYN scan detected.
2. Document Alerts: