**CMSC 491/691 Active Cyber Defense Lab 1**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assigned: 9/8/2021

Due: 9/15/2021 by 7:00pm

Part 1: Virtual Machine Setup

A virtual machine (VM) is an emulation of a computer system and provides the functionality of a physical computer. They allow us to test configurations and exploits with less risk of harming physical devices. Setting up a VM requires a computer with at least 4 GB of RAM. If you have not done so already, follow these instructions to set up your Kali Linux VM:

* Download Virtualbox (you don’t need the Extensions pack) from: <https://www.virtualbox.org/wiki/Downloads>

Download ActiveCyberKaliLinux.ova from <https://drive.google.com/file/d/1IDknBGd3j-CwxOc18Hiw-ZFem4UA5Ow3/view?usp=sharing>. This is a large download and you will need a UMBC email to access it.

* In VirtualBox, select File -> Import Appliance and choose ActiveCyberKaliLinux.ova. Click “Next” and then “Install”. The import process may take several minutes.
* The username to the Kali VM is activecyber and the password is Sqordfish0!
* Take a snapshot of the Kali VM after it is installed.

Part 2: Linux System Administration (70 points)

During this section of the lab, you are allowed to receive assistance from other students in the class / CyberDawgs. You must complete this section on **your** Kali VM.

This lab will familiarize you with concepts needed for performing system administration on Linux. During this lab, you will configure an SSH server on your Kali VM so that your host can connect to it.

First, we will create a user on the Kali Linux VM. Later in the lab we will configure the SSH service so that this is the only user to which other SSH clients will be able to connect.

* Use the adduser command to add a new user to your Kali VM. You may name the new user anything you wish, subject to bounds of good taste.
* Add your new user to the sudo group.
* Use the su command to switch to your new user.

**1**. What command did you use to add your user to the sudo group? (4 pts) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2**. What is the UID of your new user? (4 pts) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3**. What is the GID of the sudo group? (4 pts) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4**. What is the default shell of your new user? How did you find this information? (6 pts) \_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Next, we will configure the network settings on VirtualBox so that your host is able to connect to your VM. Answer the following questions:

**5**. What is the IP address of the eth0 interface on your Kali VM? How did you find this information? (6 pts) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6**. What is the loopback IP address of your host? How did you find this information? (6 pts) \_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* In VirtualBox, open the settings of your Kali VM and select Network -> Advanced -> Port Forwarding.
* Add a port forwarding rule so that Port 3022 of your host is forwarded to Port 22 of your Kali VM. Provide the loopback IP address of your host as the Host IP and the eth0 IP address of your Kali VM as the Guest IP.

**7**. Provide a screenshot of this port forwarding rule below. (6 pts)

Now that we have configured the port forwarding in VirtualBox, we will start the SSH server on your Kali VM and then test that it is working properly under default settings.

* The openssh-server package should already be installed on your Kali VM. Start it using the following command: sudo systemctl start ssh
* If you are on a Windows host, download PuTTY from the following link: <https://the.earth.li/~sgtatham/putty/latest/w64/putty-64bit-0.74-installer.msi>.
* If you are on a Linux or Mac host, you can use the ssh command on the terminal.
* SSH from your host to the Kali VM, providing the new user you created, the loopback IP address of your host, and port 3022. Since you have added a port forwarding rule to VirtualBox, connecting to this IP address and port will forward you to the IP address of your Kali VM at port 22.

**8.** Provide a screenshot showing a successful SSH connection from your host to your Kali VM. Make sure to SSH to the new user you created and port 3022. (10 pts)

Next, we will generate an SSH keypair on your host machine.

* If you are on a Windows host, use PuTTYgen to generate an RSA keypair. PuTTYgen is included as a separate program when PuTTY is installed. Hit “Generate”. Save the private key as a .ppk file. Copy the full contents of the text box labeled “Public key for pasting into OpenSSH authorized\_keys file”. We will need this later.
* In PuTTY, load the session for your Kali VM. Navigate to Connection -> SSH -> Auth. Hit “Browse” and select the private key file. You will also want to edit the session so that you connect to your new user. Then, save the session for your Kali VM.
* If you are on a Linux or Mac host, use the command ssh-keygen -t rsa to generate an RSA keypair. Save the key to the default location and provide a passphrase. Open the saved public key file and copy the full contents of it.

Once the keypair is generated, we need to configure the Kali VM so that our host is allowed to authenticate to it.

* If it does not already exist, create a directory called .ssh/ inside of the home directory of your new user. Inside of the .ssh/ directory, create a file named authorized\_keys and paste the contents of the RSA public key into it.

**9**. Provide a screenshot showing a successful SSH connection from your host to your Kali VM with public key authentication. Make sure to SSH to the new user you created. (10 pts)

The last step of the lab will be configuring the SSH server on the Kali VM. First, we will disable password authentication so that only public key authentication can be used.

* Edit the file /etc/ssh/sshd\_config so that password authentication is disabled.
* Run the command sudo systemctl restart ssh. You can check the status of the SSH server using sudo systemctl status ssh.

**10**. What line of /etc/ssh/sshd\_config did you edit to accomplish this? (4 pts) \_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Finally, we will configure the SSH server so that only your new user is allowed to connect.

* Edit the file /etc/ssh/sshd\_config so that only your new user is allowed to log in
* Run sudo systemctl restart ssh to restart the SSH server.

**11**. What line of /etc/ssh/sshd\_config did you add to accomplish this? (4 pts) \_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**12**. Provide a screenshot showing that an SSH connection from your host to the activecyber user on the Kali VM using public key authentication is refused. (6 pts)

Part 3: Short Answer (30 points)

Please answer these questions **individually and in your own words**. We recommend searching for online resources about the RSA algorithm!

**13**. In a few sentences, describe how an RSA keypair is generated. Make sure to describe which values are part of the public key and which values are part of the private key. (10 pts) \_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**14**. Suppose that you want to authenticate to an SSH server using RSA public key authentication. The SSH server randomly generates a number, encrypts it using your public key, and sends the encrypted number to you. Then, the SSH server challenges you to tell it what number it generated. If you tell it the correct number, the server authenticates you. Describe, using the mathematical properties of RSA, how you would find this number. (10 pts) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**15**. Suppose that you generate your own RSA keypair with a key size of only 32 bits. Why is this insecure? Describe how would an attacker with only your public key could find out what your private key is. (10 pts) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_