Set Up a Backup Server for WebGoat

Step 1: Get the WebGoat VM online

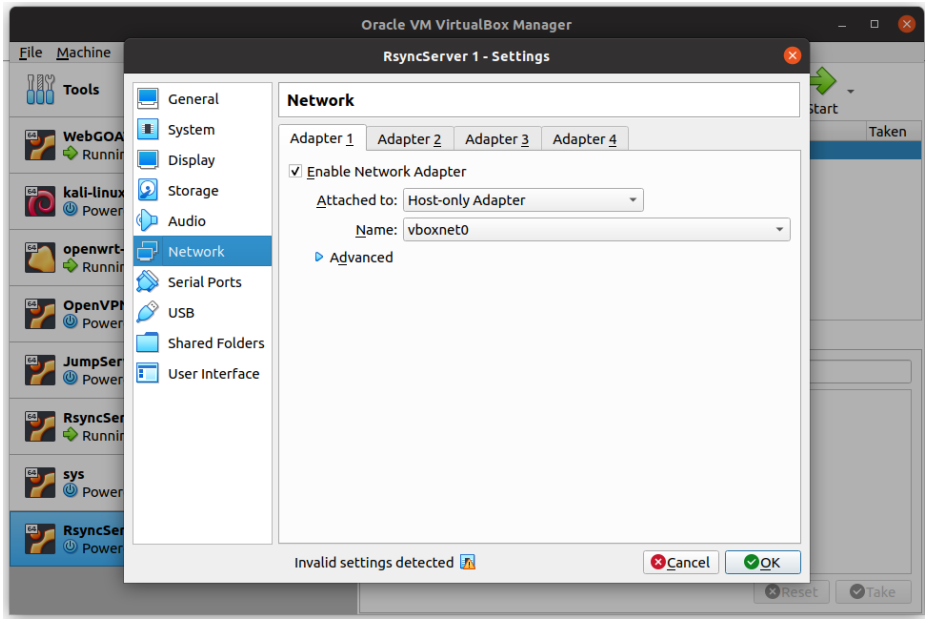
– If your VM has been shot down, simply turn it on.

– If your VM is already on, restart it (if you have multiple screenshots, try to restart the first screenshot where no iptables rules are in effect).

Step 2: Set up a backup server in the LAN

– Download the VM image from and import it to VirtualBox:
https://drive.google.com/file/d/1vqsB7RhLkMroJpUwm3EVrjEkOnlqZuVr/view?usp=sharing

– Attach the VM to the Host-only Adapter so that it will be connected to the LAN



– Start the backup server and log into it with [Username: ubuntu] and [Password: ubuntu]

Test 1: In the terminal of the backup server, run "ip a"
Requirement: Screenshot the result
Expected results: The backup server should have an IP address in the form of "192.168.56.*"

Step 3: Grant WebGoat SSH access to the backup server

– In the terminal of the backup server, run “ssh-keygen”; Type "enter" multiple times until the command finishes execution

Test 2: In the terminal of the backup server, run “cat ~/.ssh/id_rsa.pub”
Requirement: Screenshot the result
Expected results: You should see something similar to the following

```
ubuntu@rsyncserver:~$ cat ~/.ssh/id_rsa.pub

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDEXGzjwXUqeCeie/4ugI2X92XXQ9sRm5LCgdl
Dbfoy96OgoadN/7x2rQdDS+GBMsw3wX99YyuGfoCdPSEVT7N9O0WfNKjGVOdj5EnwF
ihHp+9wt9aKR3ACimcOMOPXK7JtAxFIuA9HOLx3foTlo1WE52ki+OosobSKzGx9sVKoq
oaU1RFoDsajG+HxpGJHox3aSwtBqiblq92XlMcd44SGCk2OkjiwoUt9gNZQh1or/8KEph
N+4YFQBF1NqXUOcUestvMTcxMnoiF/VcRSAwCqqmlRshx5HlZZYu8jI2vI0YTCoriNHxp
F+qnbK3lH4nHUJeMJUPbp5IFQ/Ik2FXp2+JrDF9DLbDqUL+ce7JfFtj+57SaJGqr2EcgBA
EhJfPhju+ccRnfjBmy9QDve+i7Iz7kCaSDog7gbYzHFhWtrWXkNtGCJO/gkrNAs7PQsJd3
900qVoUvRMZnN8ZZxpZBXUYuQQ31USxOB4x1qZj71WAeM3KNrZ866HXXuD2hmJss=
ubuntu@rsyncserver
```

– Add the public key of the backup server to the WebGoat server by running “ssh-copy-id webgoat@192.168.56.101” in the terminal of the backup server. This way, ssh access to the WebGoat server will be granted to the backup server.

Note:

- Please replace 192.168.56.101 with the IP address of your WebGoat VM (if different)
- When you are asked about “Yes/No”, say “Yes”
- When you are asked for a password, say “webgoat”

Test 3: In the terminal of the backup server, run “ssh webgoat@192.168.56.101”
Requirement: Screenshot the result
Expected results: You should be able to ssh into WebGoat **without** giving the password

Note: exit “ssh” from WebGoat after you are done with the above test

Step 3: Back up the files on WebGoat on the backup server

– Run the following command in the terminal of the backup server:

```
rsync -a --delete -e ssh webgoat@192.168.56.101:/home/webgoat    /opt/backup/webgoat
```

Note:

- Please replace 192.168.56.101 with the IP address of your WebGoat VM (if different)

Test 4: In the terminal of the backup server, run “ls /opt/backup/webgoat”

Requirement: Screenshot the result
Expected results:

- The same set of sub-folders and files as the “home” of “webgoat” in the WebGoat VM should show up

Step 4: Take a snapshot of your WebGoat VM

– Suggestion: name the screenshot to “cleanWebGoat”

Step 5: Run a ransomware on your WebGoat VM

– Download the package of a ransomware on your host machine:
https://drive.google.com/file/d/1j1c6Yya-bURee6SRYYypK2LsRmODMR3M/view?usp=sharing

– Upload the ransomware package to your WebGoat VM

- Put the package in the home folder of the WebGoat VM (i.e., under “/home/webgoat”)
- Tips on how to do this: try to “scp” from your host to the WebGoat VM

– In the terminal of your WebGoat VM, run:

- “cd /home/webgoat”
- “sudo apt install unzip”
- “unzip ransomware.zip”

Test 5: In the terminal of the WebGoat server, run “ls /home/webgoat/c99”
Requirement: Screenshot the result
Expected results:

- You are going to see
  - build.txt
  - main.c
  - src/

– Run the following command again:

```
rsync -a --delete -e ssh webgoat@192.168.56.101:/home/webgoat    /opt/backup/webgoat
```

– In the terminal of your WebGoat VM, run:

- “sudo apt install libssl-dev”
- “cd /home/webgoat/c99”
- “gcc main.c src/b64.h src/b64.c src/helper.h src/helper.c -lcrypto -lssl -o ransomware”

- "./ransomware" [careful: at this step: you will be running the ransomware and make sure you have done a snapshot of the WebGoat VM]
    - Type "enter" when it asks you for input and then wait

Test 6: In the terminal of the WebGoat server, run "ls /home/webgoat/c99"
Requirement: Screenshot the result
Expected results:

- You will see a file called "build.txt.itssoeasy"; and you **won't** see "build.txt" any more

Test 7: In the terminal of the WebGoat server, run "cat /home/webgoat/c99/build.txt.itssoeasy"
Requirement: Screenshot the result
Expected results:

- You will see some random bytes

Step 6: Recover the data on WebGoat

– In the terminal of the backup server, run

```
rsync -a -e "ssh" /opt/backup/webgoat webgoat@192.168.56.101:/home/
```

Test 8: In the terminal of the WebGoat server, run "ls /home/webgoat/c99" or "/home/webgoat/webgoat/c99"
Requirement: Screenshot the result
Expected results:

- You will see that "build.txt" comes back

Test 9: In the terminal of the WebGoat server, run "cat /home/webgoat/c99/build.txt"
Requirement: Screenshot the result
Expected results:

- You will see the original texts of "build.txt"

Once you are all done with the above, restore the WebGoat VM to the "cleanVM" snapshot!!!

Submission:

Please create a PDF document to include the results of **Test 1** - **Test 9**, and submit the PDF document to GradeScope:
https://www.gradescope.com/courses/411636/assignments/2324828/submissions