

Lab 8 Response Outline

Lab 8:

Test 1: Backup Server Running Inside the LAN

Summary of test experience:

In Test 1, we have to configure the Rsync as a backup server running inside the LAN. I downloaded the vbox instance of the Rsync server and configured its network to Host-only-network so that it could be running inside the LAN.

Screenshot of test results:



```
RsyncServ [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ubuntu@backupserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:11:27:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.105/24 brd 192.168.56.255 scope global dynamic enp0s3
        valid_lft 557sec preferred_lft 557sec
    inet6 fdbf:9ba8:6c3b::564/128 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fdbf:9ba8:6c3b:0:a00:27ff:fe11:27fa/64 scope global mngtmpaddr noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe11:27fa/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@backupserver:~$ _
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

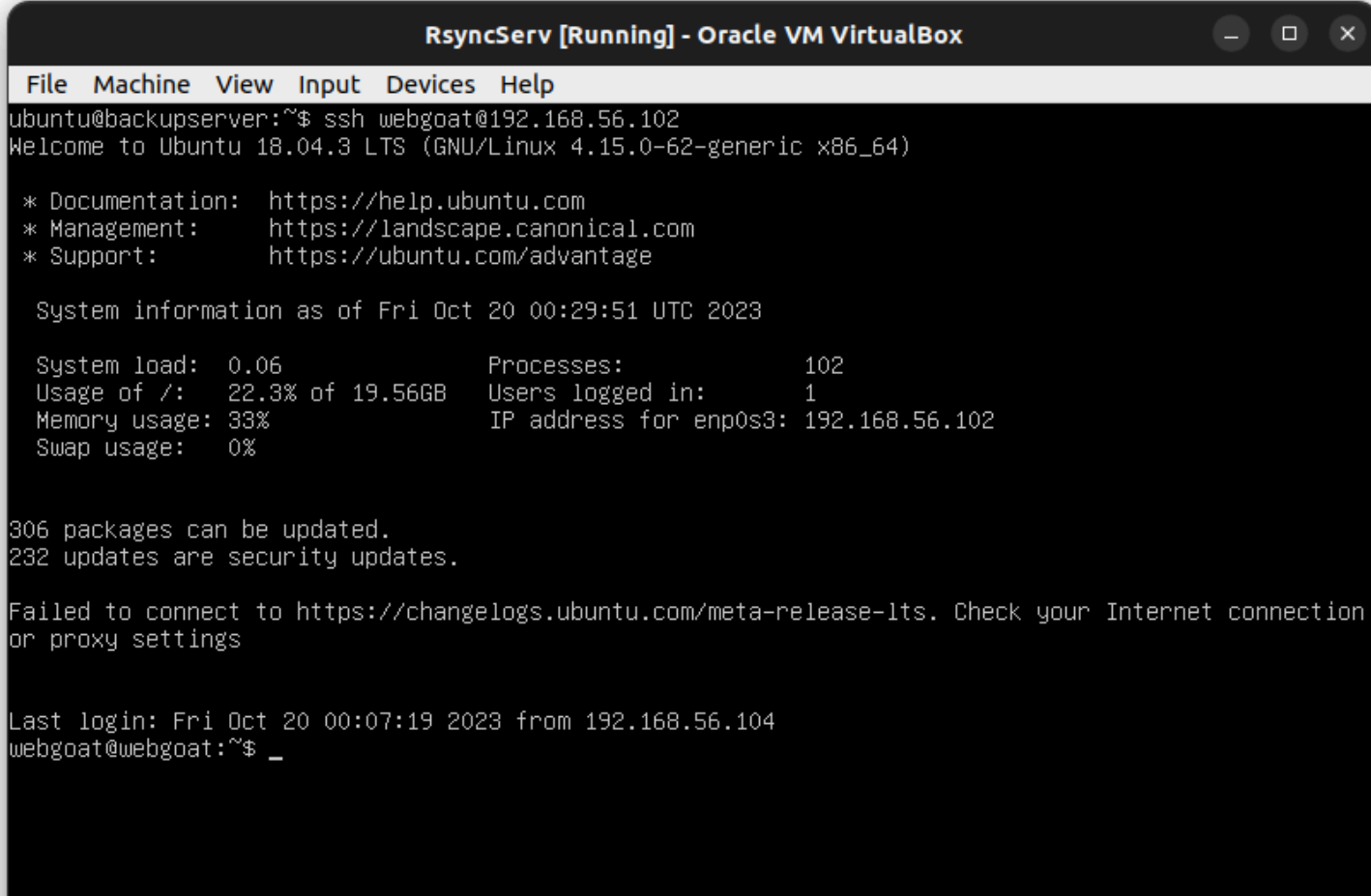
From the above screenshot, it can be seen that the IP address of the backup server is 192.168.56.105/24, meaning it's running inside the LAN we initially created.

Test 2: Backup Server Has SSH Access to the WebGoat Server

Summary of test experience:

In this test, we must ensure the WebGoat server can be accessible from the backup server we just configured. Here, I first created for the backup server a public key-private key pair for ssh-authentication. Then, I added the public key of the backup server to the WebGoat server. After that, a successful ssh-authentication can be made from the backup server to the WebGoat server.

Screenshot of test results:



```
RsyncServ [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ubuntu@backupserver:~$ ssh webgoat@192.168.56.102
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-62-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Fri Oct 20 00:29:51 UTC 2023

System load:  0.06               Processes:            102
Usage of /:   22.3% of 19.56GB    Users logged in:     1
Memory usage: 33%               IP address for enp0s3: 192.168.56.102
Swap usage:   0%

306 packages can be updated.
232 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

Last login: Fri Oct 20 00:07:19 2023 from 192.168.56.104
webgoat@webgoat:~$ _
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

The above screenshot shows that the backup server successfully accessed the WebGoat server, fulfilling the completeness of this task.

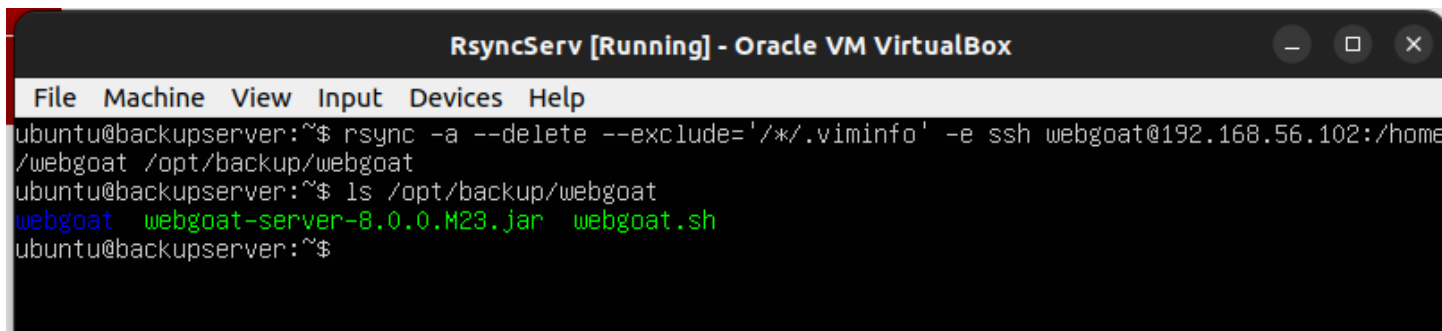
Test 3: Check Files on WebGoat Server

Summary of test experience:

Test 3 requires us to make a backup of the home directory of the WebGoat server. As an SSH-connection has been established from the backup server to the WebGoat server, the rsync

command can be used to make the required backup. The rsync command is syncing the contents of the /home/webgoat directory on the WebGoat to the local directory /opt/backup/. The options -a ensure the preservation of file attributes, --delete removes files in the destination not present in the source, and --exclude='*/.viminfo' skips syncing the .viminfo file in any subdirectory. The -e ssh flag specifies the use of SSH for the remote connection, and the username for the connection is webgoat. It essentially creates a replica of the remote directory on the local machine, excluding specific files and leveraging SSH for secure communication.

Screenshot of test results:



```
RsyncServ [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ubuntu@backupserver:~$ rsync -a --delete --exclude='*/.viminfo' -e ssh webgoat@192.168.56.102:/home/webgoat /opt/backup/webgoat
ubuntu@backupserver:~$ ls /opt/backup/webgoat
webgoat webgoat-server-8.0.0.M23.jar webgoat.sh
ubuntu@backupserver:~$
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

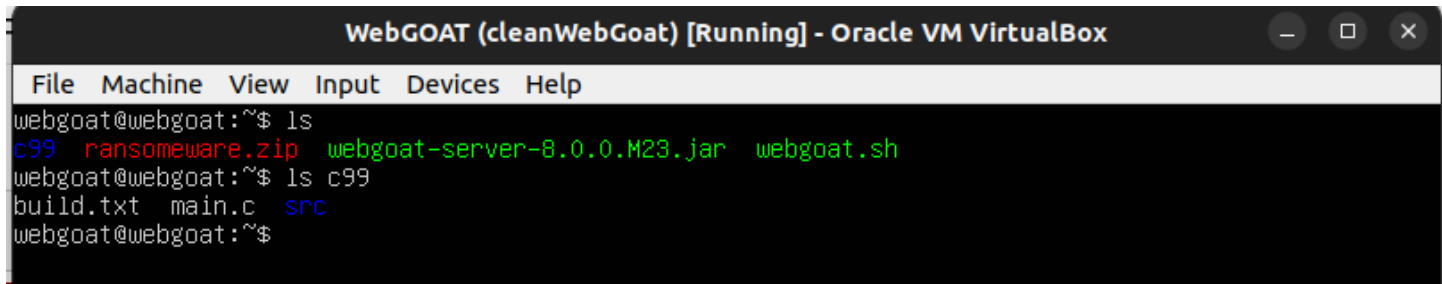
The above screenshot shows that we can view on the backup server the contents of the home directory of the WebGoat.

Test 4: Decompressed Files From the Ransomware

Summary of test experience:

In this test, we are required to get the files for the Ransomware from the host machine into the webgoat server. We can use Linux's secure copy feature to transfer the zip file. Initially, it was not working on my host machine due to the iptables rules from the previous module. Once the rules were removed, the scp command worked.

Screenshot of test results:



```
WebGOAT (cleanWebGoat) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
webgoat@webgoat:~$ ls
c99  ransomware.zip  webgoat-server-8.0.0.M23.jar  webgoat.sh
webgoat@webgoat:~$ ls c99
build.txt  main.c  src
webgoat@webgoat:~$
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

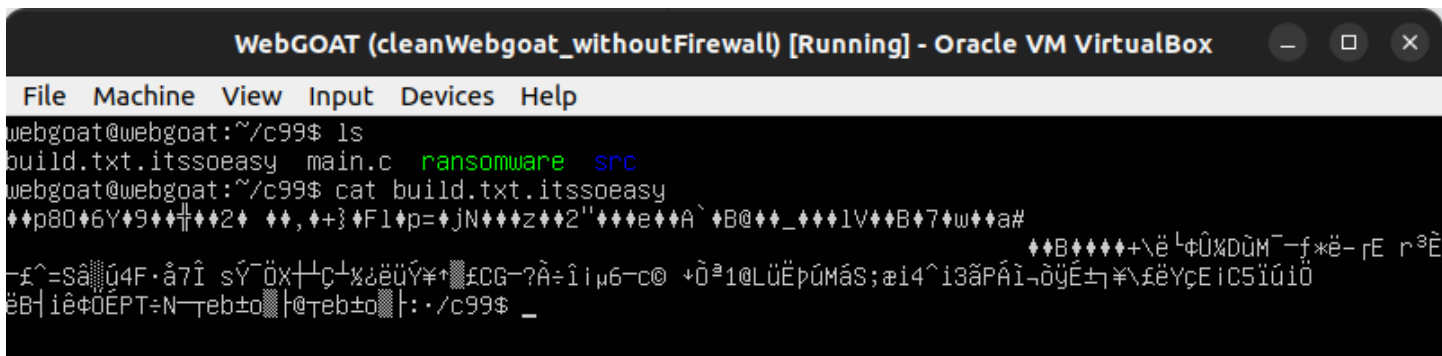
The above screenshot shows that the required files to campaign the ransomware attack are on the WebGoat server.

Test 5: Attach Ransomware to the WebGoat Server

Summary of test experience:

In this test, we must campaign a self-ransomware attack on the WebGoat server. This gcc command is compiling the program named "ransomware" from source files. It includes the main program file "main.c" and additional source files "b64.h," "b64.c," "helper.h," and "helper.c" from the "src" directory. The options specified include -lcrypto and -lssl, indicating the linkage of the OpenSSL library for cryptographic functions. The -o ransomware flag specifies the output file's name as "ransomware."

Screenshot of test results:



```
WebGOAT (cleanWebgoat_withoutFirewall) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
webgoat@webgoat:~/c99$ ls
build.txt  itssoeasy  main.c  ransomware  src
webgoat@webgoat:~/c99$ cat build.txt.itssoeasy
p80+6Y+9+2+ +,++ F1+p=jN++z+2"++e+A`+B@+_++1V+B+7+w+a#
++B+++++\\e Lf0xDUM-f*ë-rE r³Ë
-f^=Sâ||û4F-â7Î sÿ-Öx+|c¹%jEÜÿ+ fCG-?Ã÷îµ6-c@ +0³1@LÜËpÜMâS;æi4^i3âPÁî-ôÿË±¶\fëYçE iC5iûi0
EB|iê#0EPT÷N-Tebo|@Tebo|:./c99$ _
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

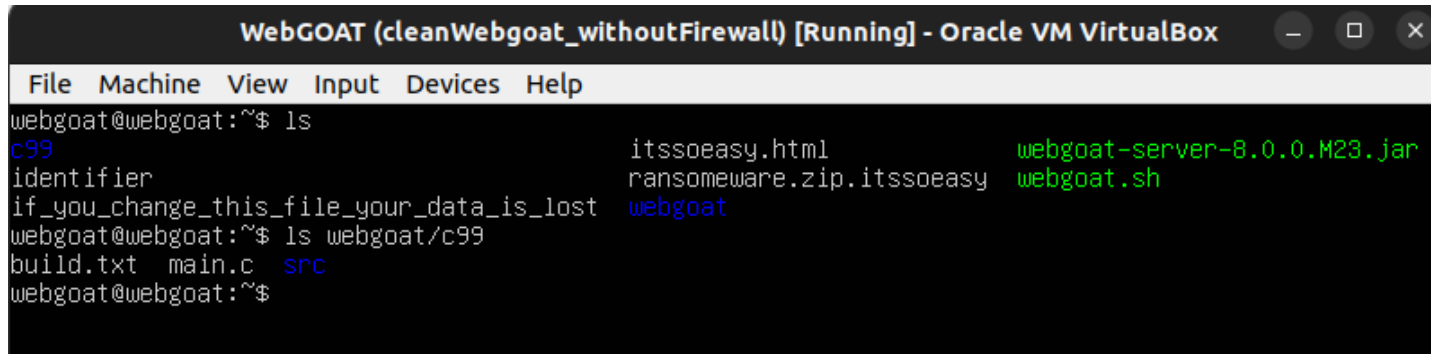
The above image shows that the ransomware attachment was successful, and the ransomware program encrypts the files, indicating the completeness of the task.

Test 6: Rsync Recovers Data on WebGoat

Summary of test experience:

In this test, we must recover the data from the last backup. It shouldn't be done on the WebGoat server as it is unsafe due to the ransomware attack. So, on the backup server, with the help of the rsync command, I was successfully able to restore the last data I backed up.

Screenshot of test results:

A screenshot of a terminal window titled "WebGOAT (cleanWebgoat_withoutFirewall) [Running] - Oracle VM VirtualBox". The terminal shows a user at the "webgoat@webgoat:~" prompt. They run "ls" and see a list of files: "c99", "identifier", "if_you_change_this_file_your_data_is_lost", "build.txt", "main.c", "src", "itssoeasy.html", "ransomeware.zip", "itssoeasy", "webgoat-server-8.0.0.M23.jar", and "webgoat.sh". Then they run "ls webgoat/c99" and see the output "build.txt main.c src", indicating that the files have been successfully restored to their original format.

```
WebGOAT (cleanWebgoat_withoutFirewall) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
webgoat@webgoat:~$ ls
c99                                itssoeasy.html                webgoat-server-8.0.0.M23.jar
identifier                        ransomeware.zip.itssoeasy     webgoat.sh
if_you_change_this_file_your_data_is_lost  webgoat
webgoat@webgoat:~$ ls webgoat/c99
build.txt main.c src
webgoat@webgoat:~$
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

From the above screenshot, we can see that the original form of the build file has successfully been restored to its original txt format.