University of Utah
School of Computing
CS 6967: Security Operations

Lab 8 Response Outline

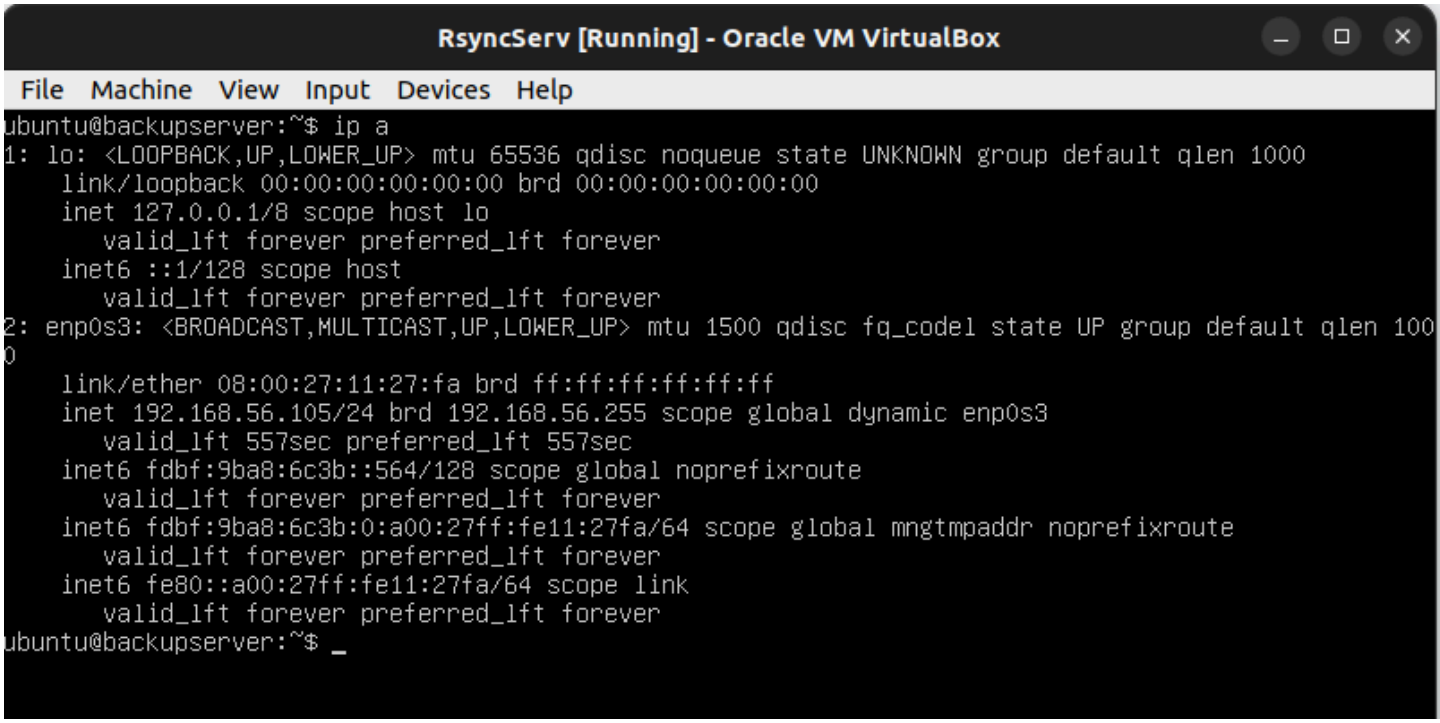
Lab 8:

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:



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

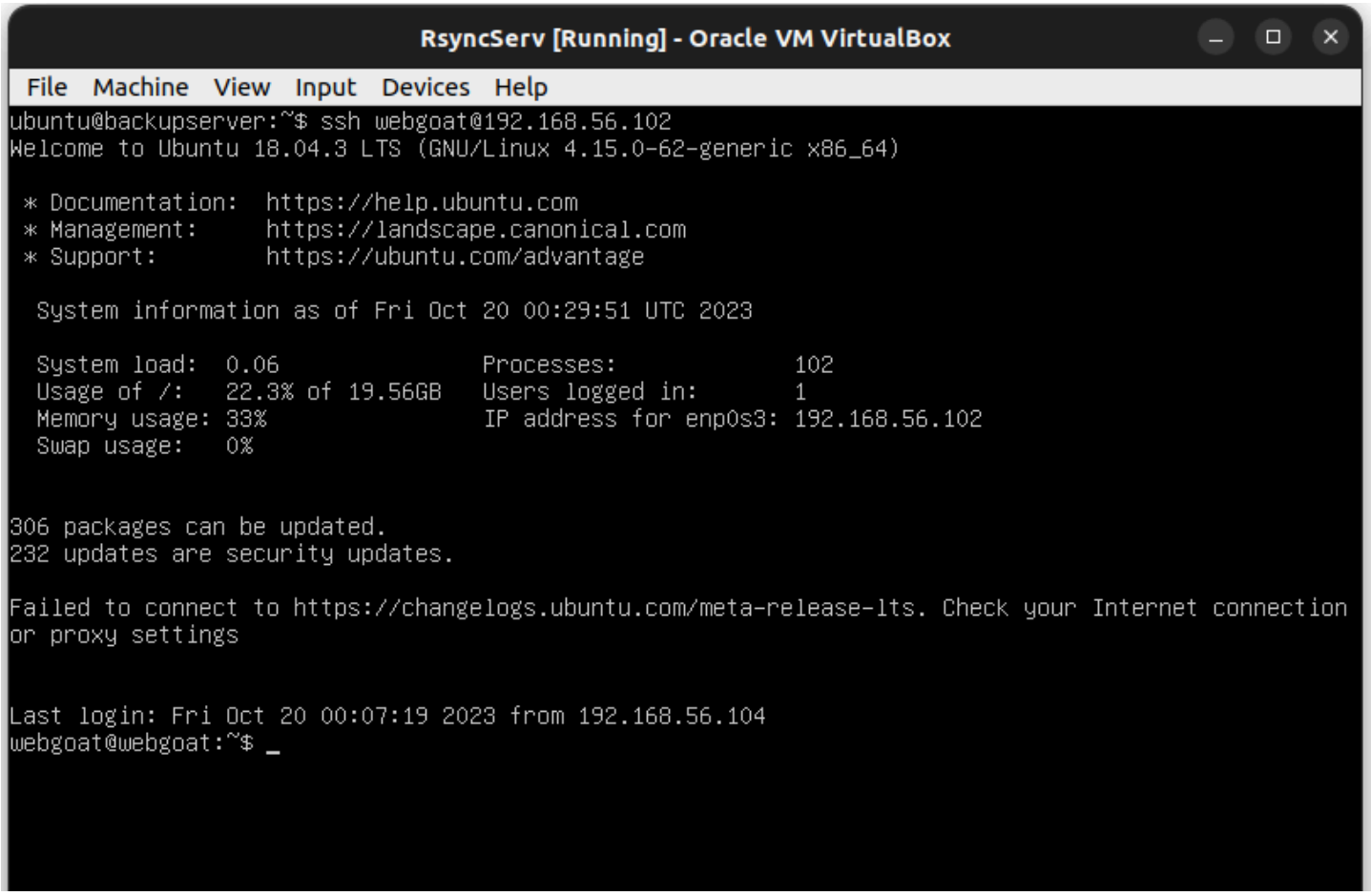
From the above screenshot, it can be seen that the IP address of the backup server is 192.168.56.105/24, meaning it's running inside the LAN we initially created.

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:



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.

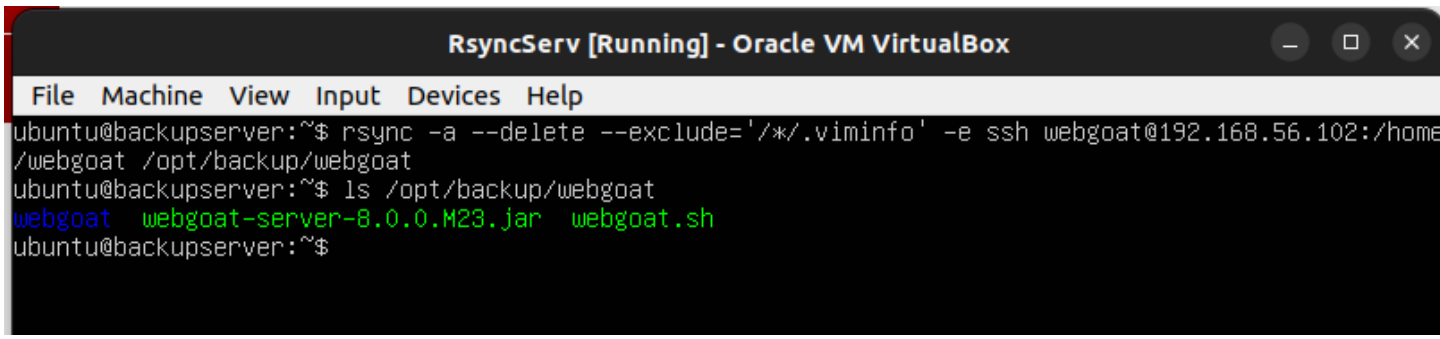
Test 3: Check Files on WebGoat Server

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:



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

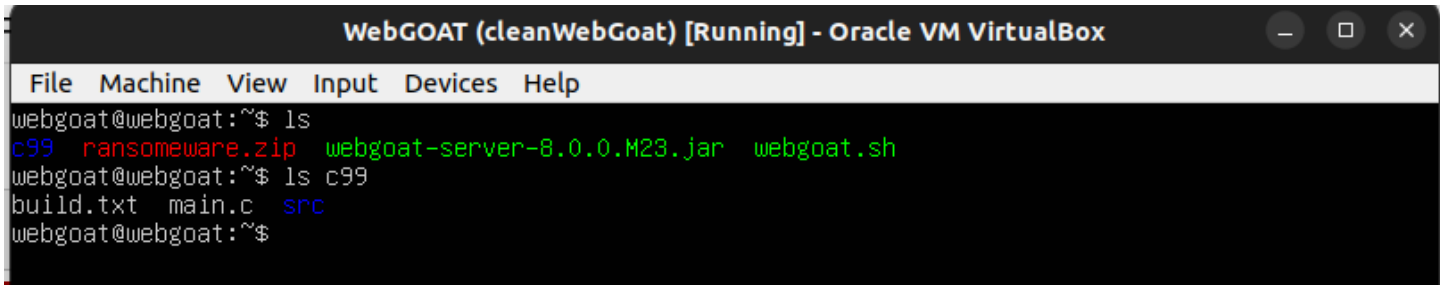
The above screenshot shows that we can view on the backup server the contents of the home directory of the WebGoat.

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:



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

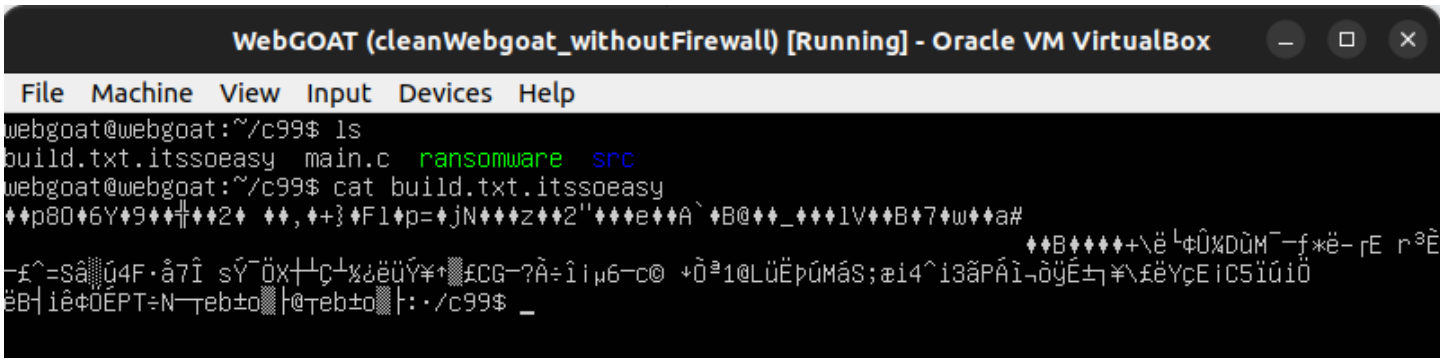
The above screenshot shows that the required files to campaign the ransomware attack are on the WebGoat server.

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:



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

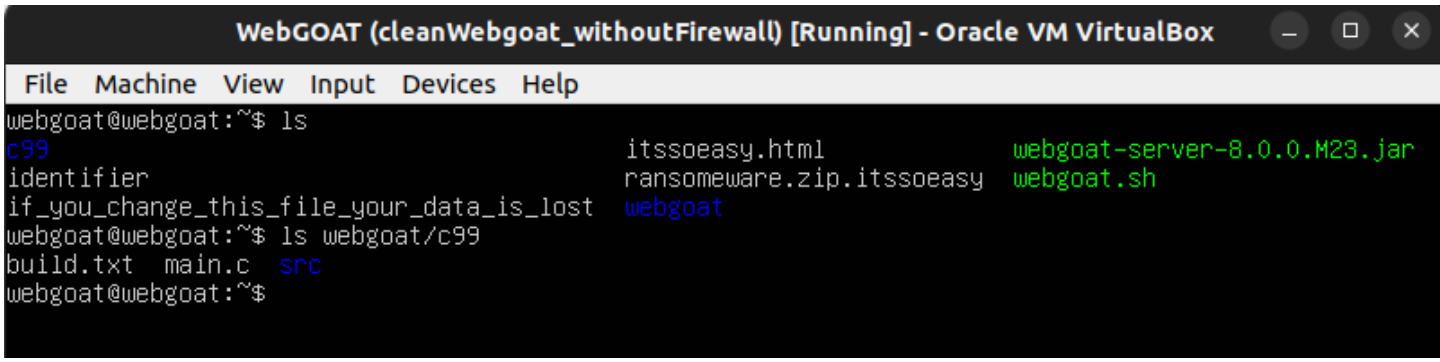
The above image shows that the ransomware attachment was successful, and the ransomware program encrypts the files, indicating the completeness of the task.

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:



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.