University of Utah
School of Computing
CS 6967: Security Operations

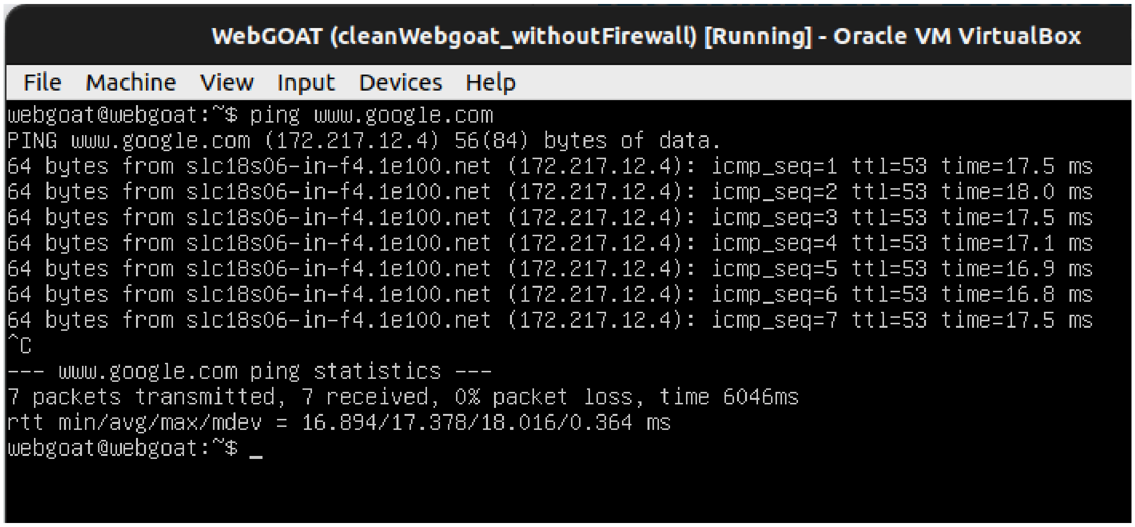
Assignment 2 Response Outline

Task 1: Set Up the LAN and WebGoat Server

Summary of task experience:

The task here is to set up the LAN and run the WebGoat Server inside the LAN. Then, we must check whether we can access the WebGoat server from our host machine. First, I added a host-only virtual network to the VirtualBox based on the DHCP protocol for the LAN. Second, I added an OpenWrt-based router for the LAN so that any server connected to the LAN can communicate with the internet through the router. Then, I added the VBox image of the WebGoat Server to the LAN and configured the WebGoat server by adding the router's IP as the default IP route for the WebGoat. Finally, I opened the terminal of the WebGoat server and ran "ping www.google.com.

Screenshot of task results:


WebGOAT (cleanWebgoat_withoutFirewall) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help

```
webgoat@webgoat:~$ ping www.google.com
PING www.google.com (172.217.12.4) 56(84) bytes of data.
64 bytes from slc18s06-in-f4.1e100.net (172.217.12.4): icmp_seq=1 ttl=53 time=17.5 ms
64 bytes from slc18s06-in-f4.1e100.net (172.217.12.4): icmp_seq=2 ttl=53 time=18.0 ms
64 bytes from slc18s06-in-f4.1e100.net (172.217.12.4): icmp_seq=3 ttl=53 time=17.5 ms
64 bytes from slc18s06-in-f4.1e100.net (172.217.12.4): icmp_seq=4 ttl=53 time=17.1 ms
64 bytes from slc18s06-in-f4.1e100.net (172.217.12.4): icmp_seq=5 ttl=53 time=16.9 ms
64 bytes from slc18s06-in-f4.1e100.net (172.217.12.4): icmp_seq=6 ttl=53 time=16.8 ms
64 bytes from slc18s06-in-f4.1e100.net (172.217.12.4): icmp_seq=7 ttl=53 time=17.5 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6046ms
rtt min/avg/max/mdev = 16.894/17.378/18.016/0.364 ms
webgoat@webgoat:~$ _
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the task?

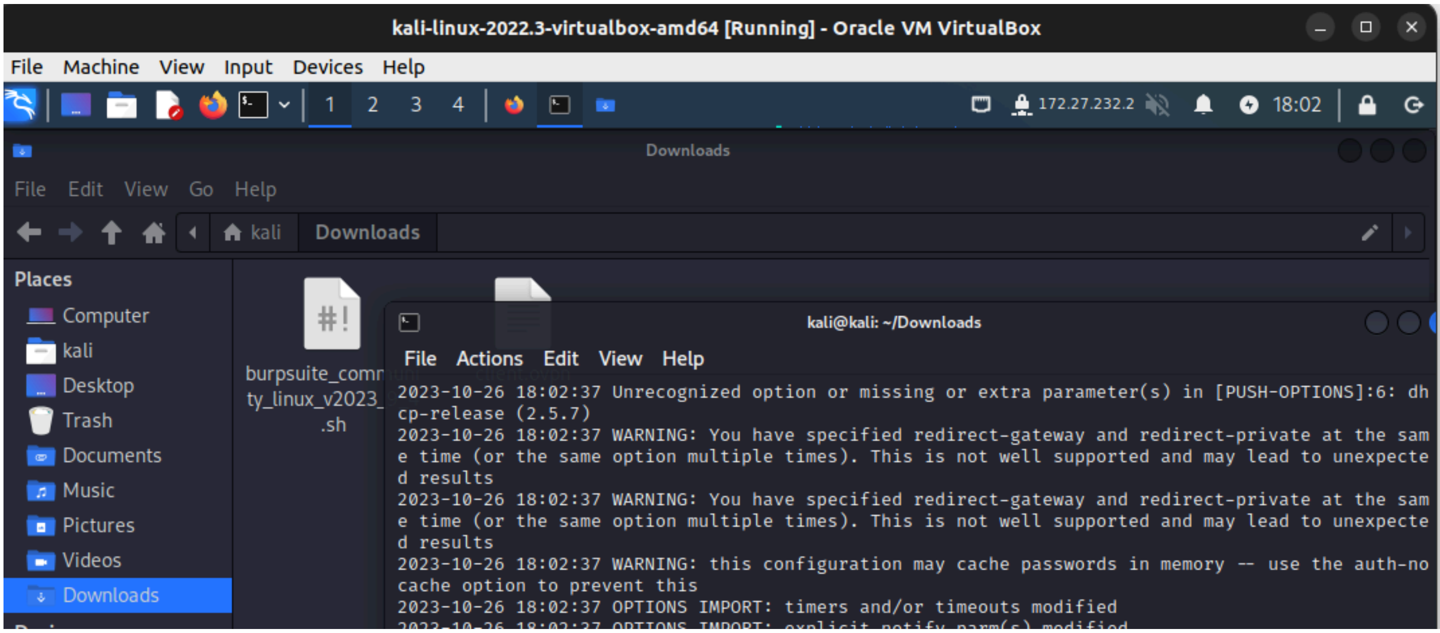
From the above screenshot, it can be seen that the WebGoat server can connect itself to the internet through the router.

Task 2: Set Up the VPN Server

Summary of task experience:

Task 2 focuses on establishing a connection between Kali and a VPN server for internet communication. I arranged an OpenVPN virtual machine and implemented port forwarding rules on the Openwrt router to facilitate VPN connectivity. Subsequently, I configured an OpenVPN client file, allowing the Kali machine to utilize the OpenVPN server.

Screenshot of task results:


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
172.27.232.2
18:02
Downloads
File Edit View Go Help
kali
Downloads
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
burpsuite_community_linux_v2023_.sh
kali@kali: ~/Downloads
File Actions Edit View Help

```
2023-10-26 18:02:37 Unrecognized option or missing or extra parameter(s) in [PUSH-OPTIONS]:6: dh
cp-release (2.5.7)
2023-10-26 18:02:37 WARNING: You have specified redirect-gateway and redirect-private at the sam
e time (or the same option multiple times). This is not well supported and may lead to unexpecte
d results
2023-10-26 18:02:37 WARNING: You have specified redirect-gateway and redirect-private at the sam
e time (or the same option multiple times). This is not well supported and may lead to unexpecte
d results
2023-10-26 18:02:37 WARNING: this configuration may cache passwords in memory -- use the auth-no
cache option to prevent this
2023-10-26 18:02:37 OPTIONS IMPORT: timers and/or timeouts modified
2023-10-26 18:02:37 OPTIONS IMPORT: explicit notify parm(s) modified
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the task?

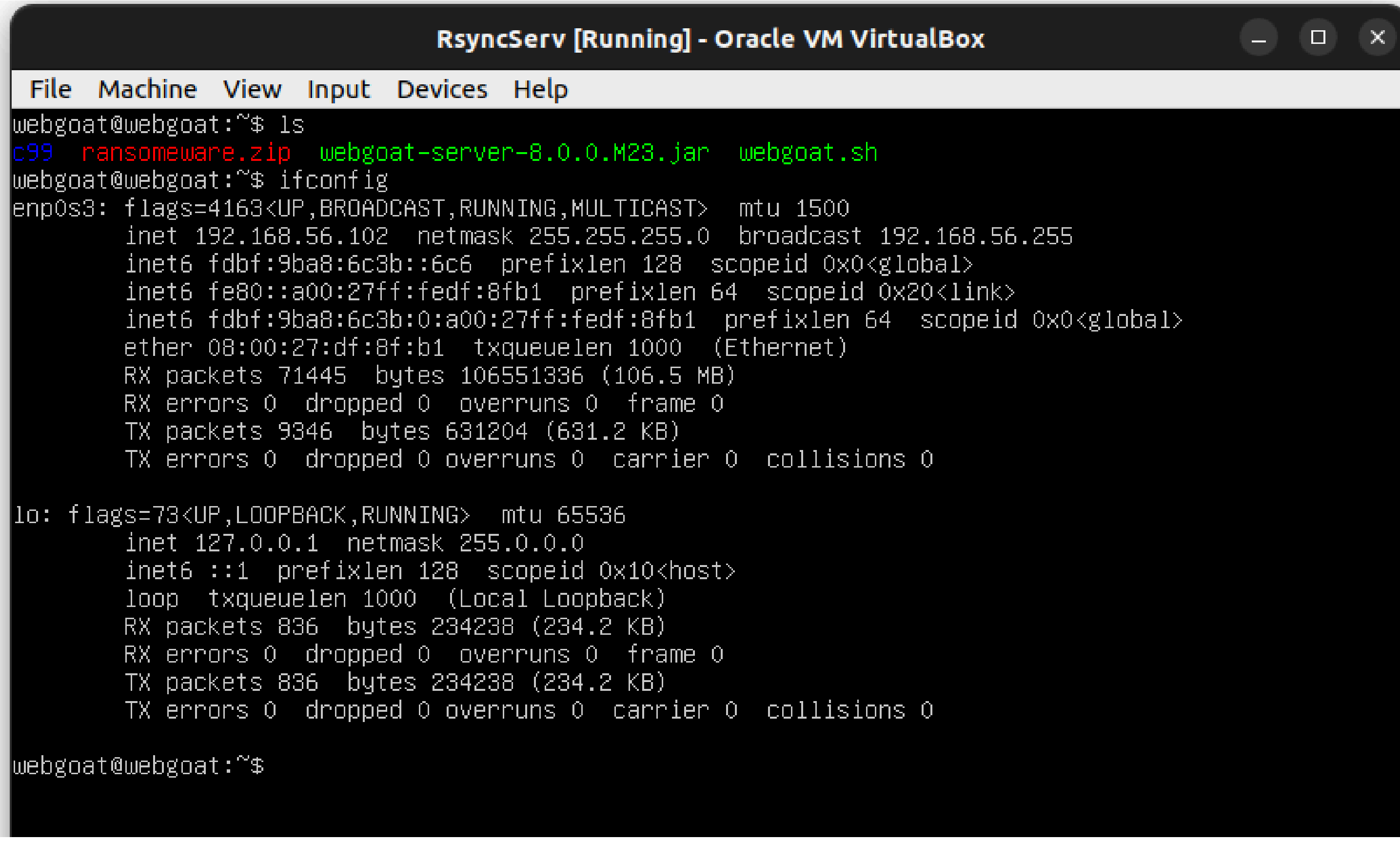
The above image shows that Kali is using the OpenVPN server, and the IP address is 172.27.232.2.

Task 3: Setup Rsync Server

Summary of task experience:

In this task, we are required to set up the Rsync server as a backup server. First, I set up a Rsync VB image. Then, I granted WebGoat SSH access to the backup server.

Screenshot of task results:



RsyncServ [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
webgoat@webgoat:~$ ls
c99  ransomeware.zip  webgoat-server-8.0.0.M23.jar  webgoat.sh
webgoat@webgoat:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fdbf:9ba8:6c3b::6c6  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fedf:8fb1  prefixlen 64  scopeid 0x20<link>
        inet6 fdbf:9ba8:6c3b:0:a00:27ff:fedf:8fb1  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:df:8f:b1  txqueuelen 1000  (Ethernet)
        RX packets 71445  bytes 106551336 (106.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9346  bytes 631204 (631.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 836  bytes 234238 (234.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 836  bytes 234238 (234.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

webgoat@webgoat:~$
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the task?

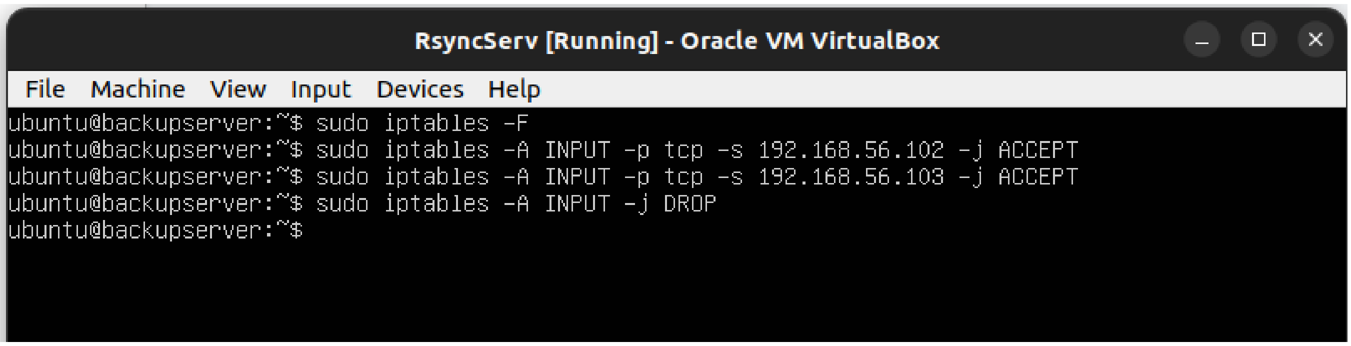
From the image provided, it's evident that the backup server is operational and successfully linked to the WebGoat server.

Task 4: Configure the Iptables

Summary of task experience:

Task 4 involves setting up iptables on the rsync server to restrict incoming TCP traffic. Specifically, the objective is to block incoming TCP traffic from all machines except the WebGoat and VPN servers. In other words, the backup server should only allow TCP traffic from the WebGoat and VPN servers.

Screenshot of task results:


RsyncServ [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
ubuntu@backupserver:~$ sudo iptables -F
ubuntu@backupserver:~$ sudo iptables -A INPUT -p tcp -s 192.168.56.102 -j ACCEPT
ubuntu@backupserver:~$ sudo iptables -A INPUT -p tcp -s 192.168.56.103 -j ACCEPT
ubuntu@backupserver:~$ sudo iptables -A INPUT -j DROP
ubuntu@backupserver:~$
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the task?

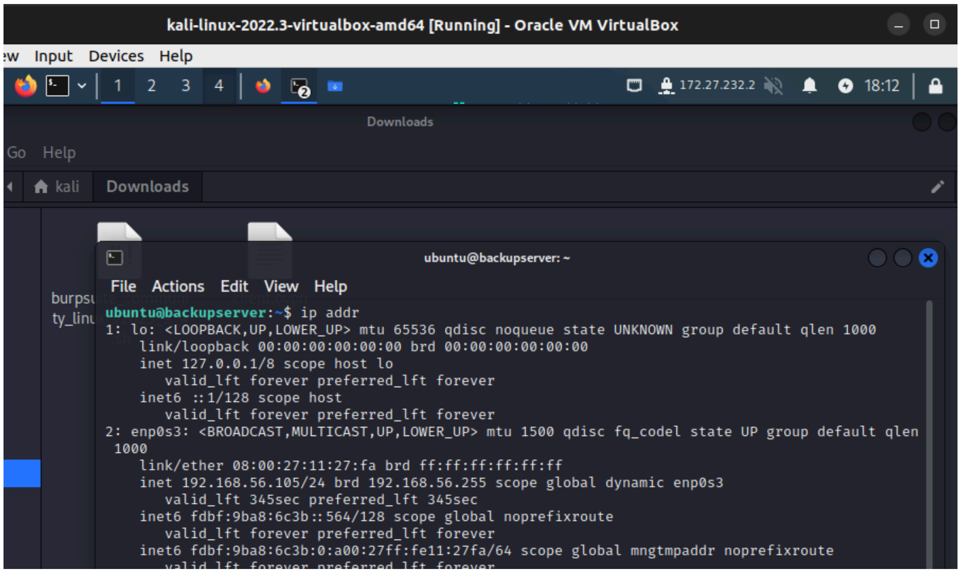
In the provided screenshot, the initial command removed all existing rules from the iptables firewall on the Rsync server. The second command allows all incoming TCP requests from the WebGoat server, the third permits TCP requests from the VPN server, and the last one denies any other incoming requests.

Task 5: Connect Kali Linux to the VPN Server

Summary of task experience:

In Task 5, we need to connect the Kali machine to the VPN server and make an SSH connection to the backup server.

Screenshot of task results:



```
ubuntu@backupserver:~$ ip addr
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 345sec preferred_lft 345sec
    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
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the task?

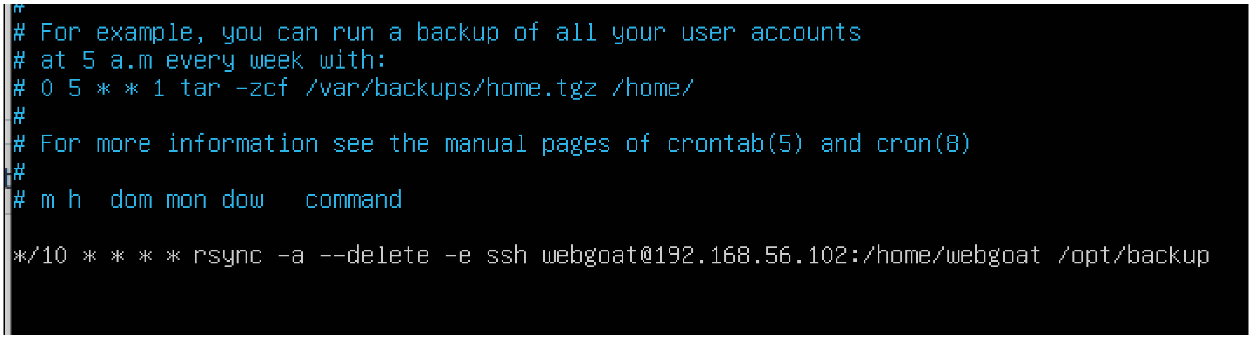
The provided screenshot shows that Kali uses a VPN and is connected to the Rsync backup server.

Task 6: Set up the Rsync Server to Make a Backup of the Home Folder

Summary of task experience:

The focus of Task 6 is to set up the RSync backup server so it can do a backup of the home folder on the WebGoat Server. As the backup server is Linux-based, I used the Cron system to schedule the full backup of the WebGoat's home server every ten minutes. Then, I searched the system log for the CRON job to check whether the backup command had run every 10 minutes.

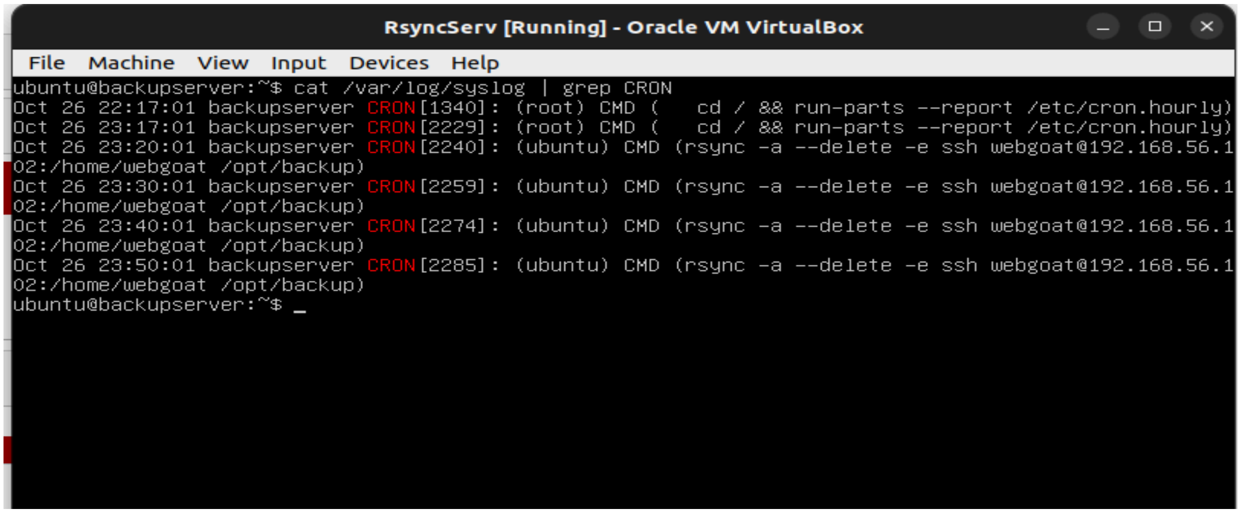
Screenshot of task results:



```
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

*/10 * * * * rsync -a --delete -e ssh webgoat@192.168.56.102:/home/webgoat /opt/backup
```

Fig 1



RsyncServ [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
ubuntu@backupserver:~$ cat /var/log/syslog | grep CRON
Oct 26 22:17:01 backupserver CRON[1340]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Oct 26 23:17:01 backupserver CRON[2229]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Oct 26 23:20:01 backupserver CRON[2240]: (ubuntu) CMD (rsync -a --delete -e ssh webgoat@192.168.56.1
02:/home/webgoat /opt/backup)
Oct 26 23:30:01 backupserver CRON[2259]: (ubuntu) CMD (rsync -a --delete -e ssh webgoat@192.168.56.1
02:/home/webgoat /opt/backup)
Oct 26 23:40:01 backupserver CRON[2274]: (ubuntu) CMD (rsync -a --delete -e ssh webgoat@192.168.56.1
02:/home/webgoat /opt/backup)
Oct 26 23:50:01 backupserver CRON[2285]: (ubuntu) CMD (rsync -a --delete -e ssh webgoat@192.168.56.1
02:/home/webgoat /opt/backup)
ubuntu@backupserver:~$ _
```

Fig 2

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the task?

Fig 1 shows a corn job command to fully back up the WebGoat's home directory every ten minutes. From Fig 2, it can be seen that the first backup happened at 23:20:01, the second one at 23:30:01, and the fourth one at 23:50:01, fulfilling the completeness of the test.