University of Utah
School of Computing
CS 6967: Security Operations

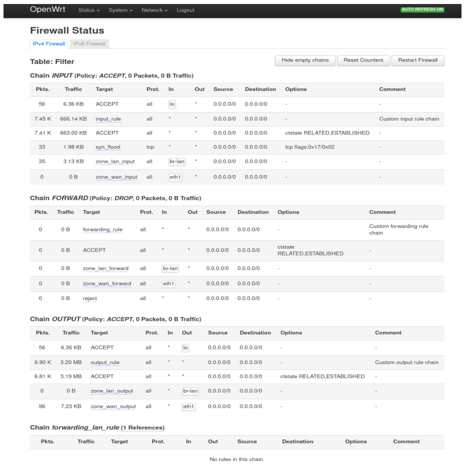
Lab 1 Response Outline

Test 1: Start the VM and Test Whether It Works as Expected

Summary of test experience:

Installation of the VM was a bit tricky as I had to configure UEFI secure boot on my working machine. This test requires setting up a router VM file and binding it to a host-only LAN network of the virtual machine. After this, we can visit the router's website to see if it's alive and its various stats regarding its activity.

Screenshot of test results:



Firewall Status

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
56	6.36 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
7.45 K	666.14 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
7.41 K	663.00 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
33	1.98 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
35	3.13 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *FORWARD* (Policy: *DROP*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
0	0 B	zone_lan_forward	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_forward	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	reject	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

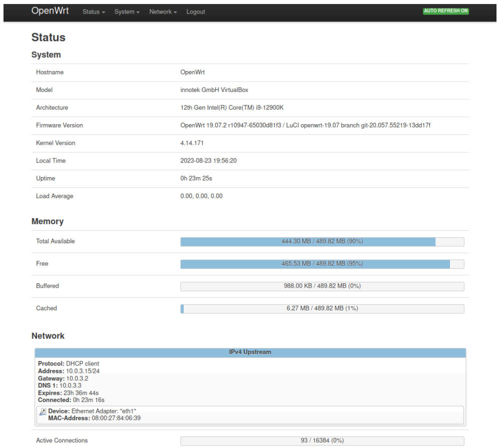
Chain *OUTPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
56	6.36 KB	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	-	-
6.90 K	3.20 MB	output_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom output rule chain
6.81 K	3.19 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
0	0 B	zone_lan_output	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	-	-
96	7.23 KB	zone_wan_output	all	*	eth1	0.0.0.0/0	0.0.0.0/0	-	-

Chain *forwarding_lan_rule* (1 References)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment

No rules in this chain.



Status

System

Hostname	OpenWrt
Model	innotek GmbH VirtualBox
Architecture	12th Gen Intel(R) Core(TM) i9-12900K
Firmware Version	OpenWrt 19.07.2 r10947-65030d81f3 / LuCI openwrt-19.07 branch git-20.057.55219-13dd17f
Kernel Version	4.14.171
Local Time	2023-08-23 19:56:20
Uptime	0h 23m 25s
Load Average	0.00, 0.00, 0.00

Memory

Total Available	444.30 MB / 489.82 MB (90%)
Free	465.53 MB / 489.82 MB (95%)
Buffered	988.00 KB / 489.82 MB (0%)
Cached	6.27 MB / 489.82 MB (1%)

Network

IPv4 Upstream

Protocol: DHCP client
Address: 10.0.3.15/24
Gateway: 10.0.3.2
DNS 1: 10.0.3.3
Expires: 23h 36m 44s
Connected: 0h 23m 16s
Device: Ethernet Adapter: "eth1"
MAC-Address: 08:00:27:84:06:39

Active Connections	93 / 16384 (0%)

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

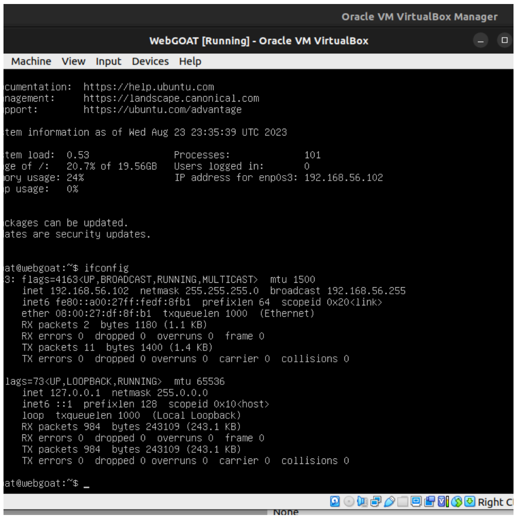
The left one describes Firewall Status, keeping the active network connections to explain input/output traffic, whereas the right one delineates the System, Network, and Memory details of the router. The uptime is 23 mins, meaning the router has been running for 23 mins. Also, you can know that the available memory of this router is 444.30 MB.

Test 2: Start the VM for the OpenWrt Router

Summary of test experience:

This started with knowing the OWASP WebGoat, which is an intentionally-made vulnerable web server for learning purposes of hacking. Later, I configured the WebGoat server to the LAN connection.

Screenshot of test results:



Oracle VM VirtualBox Manager
WebGOAT [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Right C
None

```
cumentation:  https://help.ubuntu.com
nagement:     https://landscape.canonical.com
pport:        https://ubuntu.com/advantage

tem information as of Wed Aug 23 23:35:39 UTC 2023

tem load:  0.53              Processes:            101
ge of /:   20.7% of 19.56GB   Users logged in:       0
ory usage: 24%               IP address for enp0s3: 192.168.56.102
p usage:   0%


ckages can be updated.
ates are security updates.


at@webgoat:~$ ifconfig
3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
   inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
   inet6 fe80::a00:27ff:fedf:8fb1  prefixlen 64  scopeid 0x20<link>
   ether 08:00:27:df:8f:b1  txqueuelen 1000  (Ethernet)
   RX packets 2  bytes 1180 (1.1 KB)
   RX errors 0  dropped 0  overruns 0  frame 0
   TX packets 11  bytes 1400 (1.4 KB)
   TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lags=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 984  bytes 243109 (243.1 KB)
   RX errors 0  dropped 0  overruns 0  frame 0
   TX packets 984  bytes 243109 (243.1 KB)
   TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

at@webgoat:~$ _
```

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

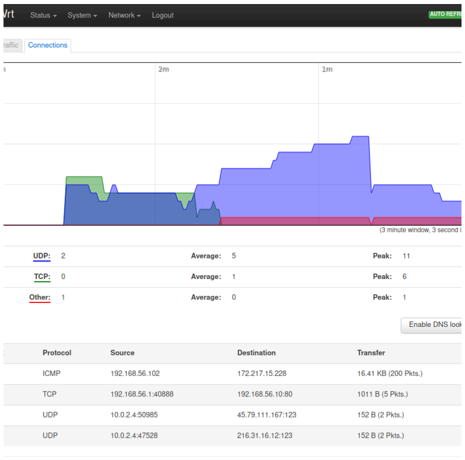
The above screenshot says that the IP address of the WebGoat server is 192.168.56.102, indicating the completeness of the test.

Test 3: Check Whether the VM Has an IP Address

Summary of test experience:

It's time for the connection between the WebGoat VM and the router by adding a default route ip on the terminal of the WebGoat server. I missed this and got a temporary failure message in reply to my ping to www.google.com until I fixed that. After successful setup, I saw the server's presence on the router's website.

Screenshot of test results:



UDP:	2	Average:	5	Peak:	11
TCP:	0	Average:	1	Peak:	6
Other:	1	Average:	0	Peak:	1

Protocol	Source	Destination	Transfer
ICMP	192.168.56.102	172.217.15.228	16.41 KB (200 Pkts.)
TCP	192.168.56.1:40888	192.168.56.10:80	1011 B (5 Pkts.)
UDP	10.0.2.4:50985	45.79.111.167:123	152 B (2 Pkts.)
UDP	10.0.2.4:47528	216.31.16.12:123	152 B (2 Pkts.)

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

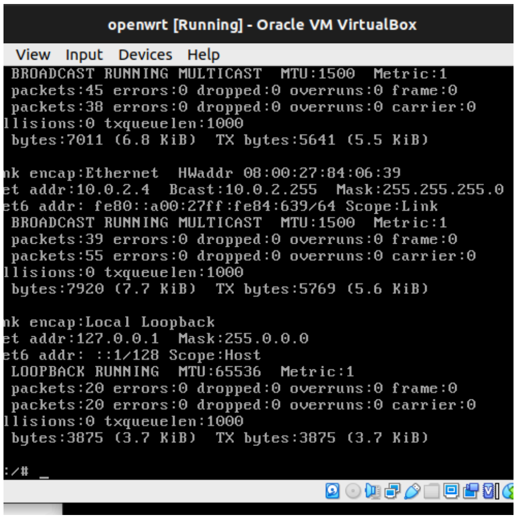
From the image, we can see that the IP address connected to the router’s traffic here is 192.168.56.102, which we saw earlier was the IP address of the WebGoat server.

Test 4: Check Whether You Get an IP Address

Summary of test experience:

Now we need to connect the router to a WAN connection. So, I created a NAT connection on the VM and got the router connected to that using another adapter. Then, I ran the ifconfig command on the terminal of the router to get the connection IP.

Screenshot of test results:



```
 BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
 packets:45 errors:0 dropped:0 overruns:0 frame:0
 packets:38 errors:0 dropped:0 overruns:0 carrier:0
llisions:0 txqueuelen:1000
 bytes:7011 (6.8 KiB)  TX bytes:5641 (5.5 KiB)

nk encap:Ethernet  HWaddr 08:00:27:84:06:39
et addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
et6 addr: fe80::a00:27ff:fe84:639/64 Scope:Link
 BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
 packets:39 errors:0 dropped:0 overruns:0 frame:0
 packets:55 errors:0 dropped:0 overruns:0 carrier:0
llisions:0 txqueuelen:1000
 bytes:7920 (7.7 KiB)  TX bytes:5769 (5.6 KiB)

nk encap:Local Loopback
et addr:127.0.0.1  Mask:255.0.0.0
et6 addr: ::1/128 Scope:Host
 LOOPBACK RUNNING  MTU:65536  Metric:1
 packets:20 errors:0 dropped:0 overruns:0 frame:0
 packets:20 errors:0 dropped:0 overruns:0 carrier:0
llisions:0 txqueuelen:1000
 bytes:3875 (3.7 KiB)  TX bytes:3875 (3.7 KiB)

:/# _
```

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

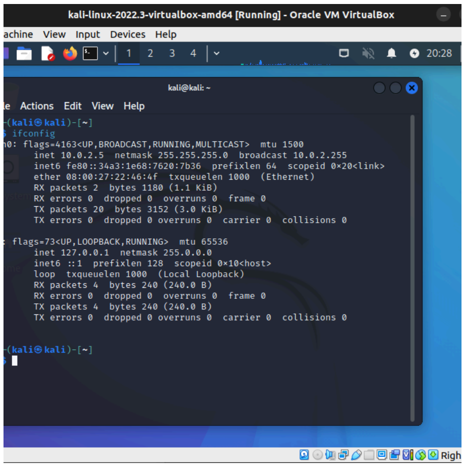
What I can infer from the above image is that OpenWrt has an IP address of 10.0.2.4 in WAN connection.

Test 5: Home Page of the Web Server Running in the LAN

Summary of test experience:

In this test, I connected the VM image of Kali Linux to the WAN. Then, I logged in to the Kali Linux machine and ran the ifconfig command to get the IP address of the Kali.

Screenshot of test results:



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
achine View Input Devices Help
1 2 3 4
20:28
kali@kali: ~
le Actions Edit View Help
Righ

```
-(kali㉿kali)-[~]
$ ifconfig
h0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::34a3:1e68:7620:7b36  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 1180 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 3152 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

: 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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


-(kali㉿kali)-[~]
$ 
```

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

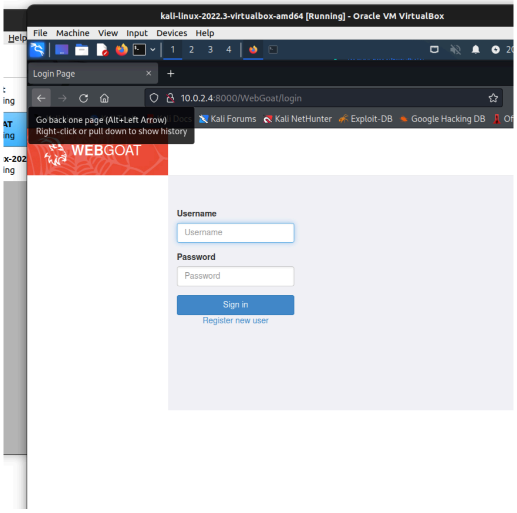
We see that the Kali Linux has an IP address of the Kali Linux VM is 10.0.2.5.

Test 6: Connect to SSH in the Web Server

Summary of test experience:

In this test, the target is to get the WebGoat server running on the web browser of Kali Linux. But this requires permission from the firewall of the router. So we can just have that by just port forwarding in the router. Then, going to **10.0.2.4:8000/WebGoat** on the web browser of Kali should be enough to see the server.

Screenshot of test results:


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Login Page
10.0.2.4:8000/WebGoat/login
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
WEBGOAT
Username
Password
Sign in
Register new user

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

This clearly shows that the Kali Linux is getting on its web browser the WebGoat server, which is connected to the LAN connection of the VM.