

Lab 4 Response Outline

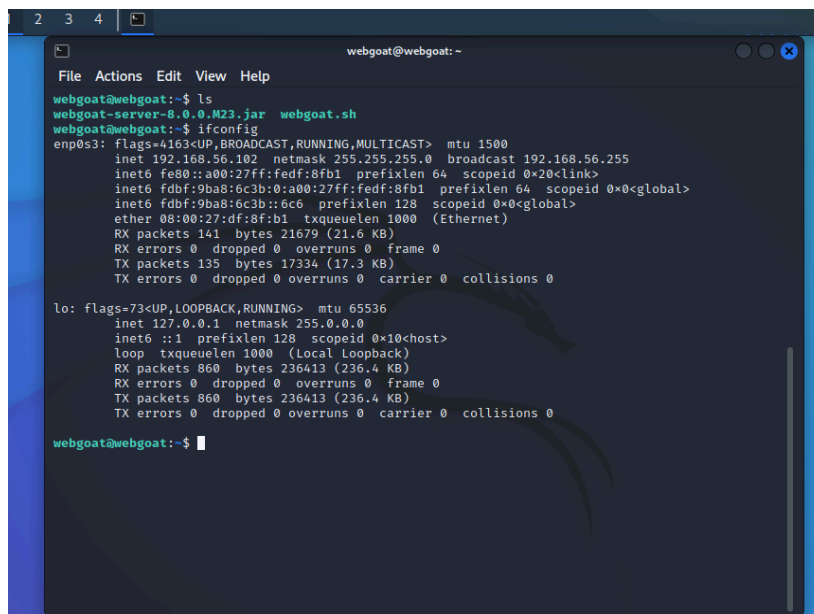
Lab 4: Firewalls

Test 1: Confirm the Traffic From the WAN to the LAN is Allowed

Summary of test experience:

This test requires connecting the Kali Linux to the WebGoat server through the secure shell protocol. As Kali Linux is using OpenWrt to make any outside connection, the router needs to have a port forwarding rule such that if the router gets any request from port 222, it will then forward the request to port 22 of the WebGoat server. It can be done using the router's Firewall. Thus, any request from port 2222 of the Kali will reach port 22 of the WebGoat. It is also essential for the server to have the sh file that describes the shell access to the client asking for access to the server.

Screenshot of test results:



```
webgoat@webgoat: ~  
File Actions Edit View Help  
webgoat@webgoat:~$ ls  
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 fe80::a00:27ff:fedf:8fb1 prefixlen 64 scopeid 0x20<link>  
    inet6 fdbf:9ba8:6c3b:0:a00:27ff:fedf:8fb1 prefixlen 64 scopeid 0x0<global>  
    inet6 fdbf:9ba8:6c3b::6c6 prefixlen 128 scopeid 0x0<global>  
    ether 08:00:27:df:8f:b1 txqueuelen 1000 (Ethernet)  
    RX packets 141 bytes 21679 (21.6 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 135 bytes 17334 (17.3 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 860 bytes 236413 (236.4 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 860 bytes 236413 (236.4 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
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?

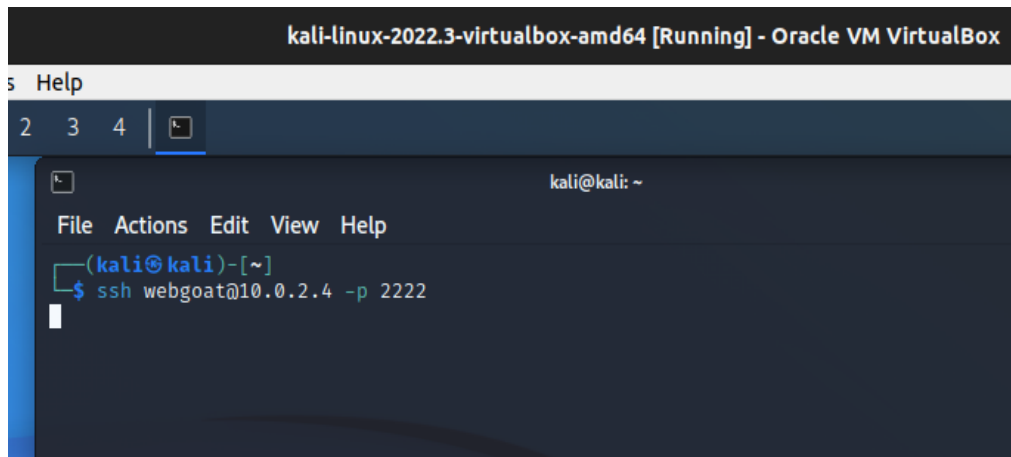
From the above image, it is evident that from the Kali Linux terminal, I got the shell access of the WebGoat server and ran the 'ls' command to list all the current files of the home location. And a sh file is also seen here.

Test 2: Confirm the Traffic From the WAN to the LAN is Disallowed

Summary of test experience:

Now, we must ensure that any request from Kali Linux gets blocked unless it's going to port 8000. Here, we can use the 'iptables' utility tool as the OpenWrt router is based on Linux. 'Iptables' works as a firewall based on the rules set on it. We need to provide the rule with the destination IP range, packet type, the port 8000 that can get passed, and the action to drop all ports' requests except 8000. As this is the only goal, we can put the rule on top of the table to avoid conflict.

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?

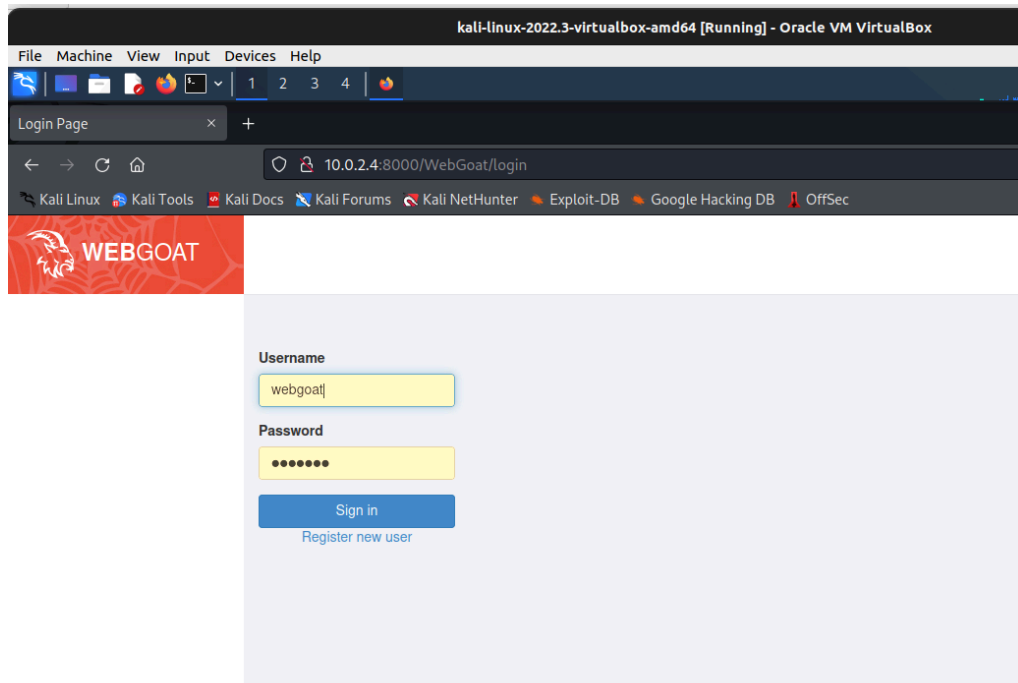
After the rule has been set, it can be seen that the request of Test 1 from Kali's terminal has got stuck. The OpenWrt router's firewall, 'iptables,' blocks the request as it's marching toward port 2222 of the WebGoat server.

Test 3: Confirm the Traffic From the WAN to the LAN is Disallowed

Summary of test experience:

In this test, we need to check whether the request to port 8000 works. If we can get the WebGoat server's login page from Kali's web browser, then it can be said that the firewall is working correctly.

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 WebGoat's login page located at port 8000, is accessible from Kali's Firefox, fulfilling the goal of this test.