CEGEP VANIER COLLEGE
CENTRE FOR CONTINUING EDUCATION
Cybersecurity
420- 950-VA

Teacher: Samir Chebbine **Lab 5** **Mar 12, 2025**

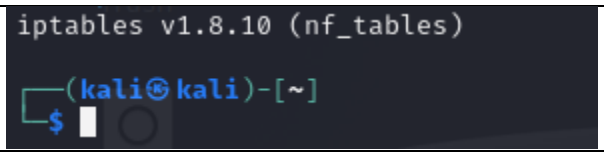
Lab 5: Firewall Technologies and Administration & SQL Injection UNION Attacks (Cont)

Complete all these following sections as explained in **class.** All *steps* were presented during class time.

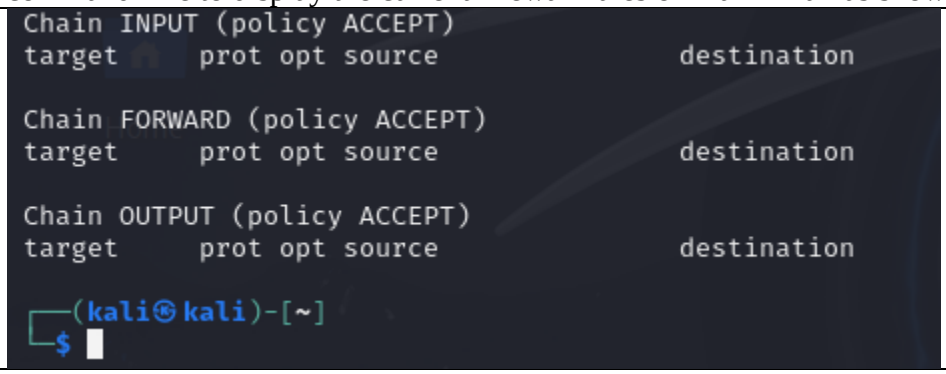
Create and Submit a Word file ***Lab5CybersecurityYourName.doc*** which contains answers of Book Exercises and output screenshots for every project. Submit all Python scripts.

1. Kali-Linux command-line utility as a firewall:

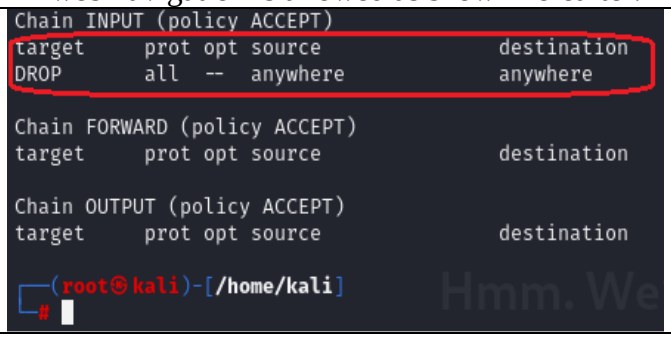
a) Show command-line utility that acts as a firewall, allowing system administrators to control incoming and outgoing network traffic by defining rules that filter packets as shown hereafter.

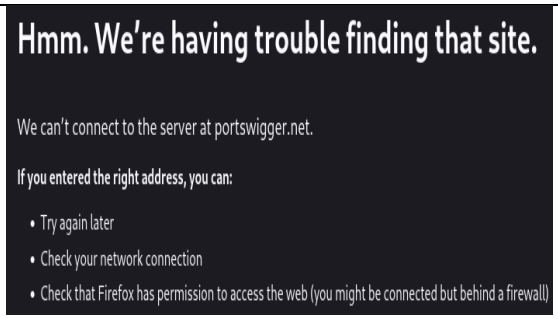


b) Execute command-line to display the current firewall rules on Kali Linux as shown hereafter.



c) Execute command-line to drop all the traffic coming on any port and check your browser if web navigation is allowed as shown hereafter.





d) Execute command-line to display the following firewall rule that configures the built-in chain OUTPUT on Kali Linux as shown hereafter.

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

┌──(root㉿kali)-[/home/kali]
└─#
```

e) Execute command-line to display the following firewall rule that configures the built-in chain FORWARD on Kali Linux as shown hereafter.

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
```

f) Execute command-line to ping traffic to web site (in the case google.com) to check if incoming traffic is allowed as shown hereafter.

```
ping: google.com: Temporary failure in name resolution

┌──(root㉿kali)-[/home/kali]
└─#
```

g) Execute command-line to delete all previous firewall rules on Kali Linux as shown hereafter.

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

h) Execute command-line to display the following firewall rule that blocks incoming traffic from a given web site (in this case google.com) on Kali Linux as shown hereafter. Check in your browser that all web navigation is allowed except google.com as shown hereafter

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  qro02s19-in-f4.1e100.net  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

i) Execute command-line to display the following firewall rule that blocks incoming traffic from a given web site (in this wikipedia.org) on Kali Linux as shown hereafter. Check in your browser that all web navigation is allowed except google.com and wikipedia.org as shown hereafter

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  qro02s19-in-f4.1e100.net  anywhere
DROP       all  --  text-lb.eqiad.wikimedia.org  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

┌──(root㉿kali)-[/home/kali]
└─#
```

j) Execute command-line to restore incoming traffic from wikipedia.org on Kali Linux as shown hereafter. Check in your browser that all web navigation is allowed except google.com as shown hereafter

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  qro02s19-in-f4.1e100.net  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

┌──(root㉿kali)-[/home/kali]
└─#
```

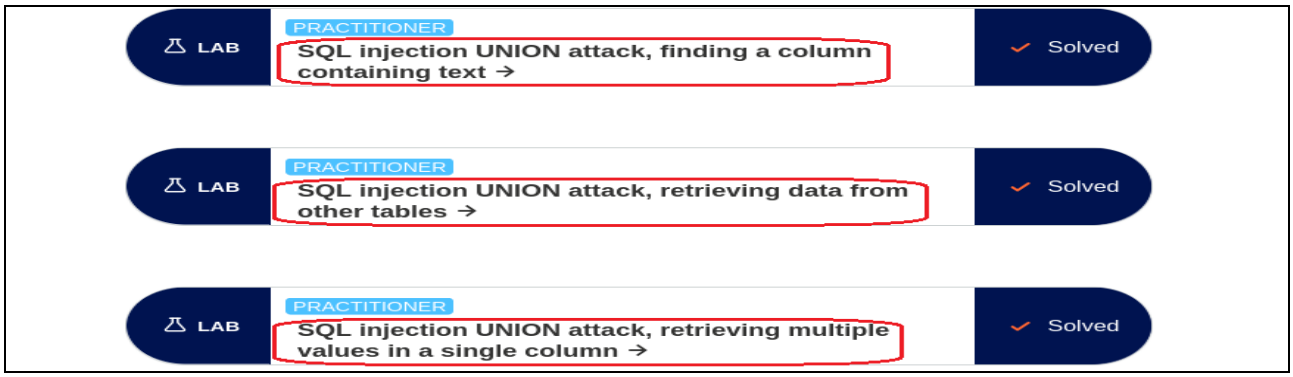
k) Execute command-line to drop all ICMP traffic to firewall on Kali Linux as shown hereafter. Check that ping taraffic to ang web site (in the case google.com) is not allowed as shown hereafter. Do research on how to block icmp traffic.

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  qro02s19-in-f4.1e100.net  anywhere
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(root㉿kali)-[/home/kali]
└─# ping google.com
PING google.com (142.250.69.142) 56(84) bytes of data.
^C
--- google.com ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5119ms
```

2. PortSwigger Web Security:

a) Navigate to https://portswigger.net/ and select the following SQL injection labs to test different web application vulnerabilities.



b) Create a text file explaining all steps toward solving above listed labs using SQL Injection UNION attacks in Web shopping application following the format shown in class.

Describe the problem:
Highlight the end goal:
Lay down the analysis:

c) Provide Python scripting attacks for each SQL injection listed above. Using Burp Suite proxy, you need to script the above attack using Python by sending appropriate http request and parsing the http response to display requested data if the SQL Injection attack is successful.

LAB | PRACTITIONER | SQL injection UNION attack, finding a column containing text → | Solved

```
┌──(kali㉿kali)-[~/CybersecurityProjects]
└─$ python3 Lab4Swigger.py "https://0a5100fa036acb56d4fbc4e200ab0013.web-security-academy.net/"
[+] Figuring out the number of columns...
[+] The number of columns is 3.
Figuring out which column has string data type
[+] The column that has string data type is 2.
```

LAB | PRACTITIONER | SQL injection UNION attack, retrieving data from other tables → | Solved

```
┌──(kali㉿kali)-[~/CybersecurityProjects]
└─$ python3 Lab5Swigger.py "https://0a9f001a047bcc5e8280020100000099.web-security-academy.net/"
[+] Dumping the list of username and password...
[+] Found the administrator password
[+] The administrator password wh9py3czyfpgaqnlb18m
```

LAB | PRACTITIONER | SQL injection UNION attack, retrieving multiple values in a single column → | Solved

Retrieve administrator password by parsing the http response based on the delimeter used in retrieving multiple values in a single column.

```
┌──(kali㉿kali)-[~/PycharmProjects/Lab1PortSwigger]
└─$ python3 Lab6Swigger.py "https://0a22006a04dd4795ecc2c36500870037.web-security-academy.net/"
[+] Dumping the list of username and password...
[+] Found the administrator password
[+] The administrator password l9zfbx62yy2lyeq0dt4k
```