

Lab 4 - Linux Firewall

- This is an individual assignment and worth 5 points.
- The due is on Saturday at midnight.
- Submit the outcome file. Follow the naming convention.

Prep

- This lab requires **Kali** running on **VMware Player**. Mac users can run it on **VMware Fusion Player**. Kali is set up in the NAT network setting and can easily ping the host and vice versa.
- Kali can be run on VirtualBox as well. But you need to change the network setting of Kali to *bridged*. In that network setting, the Kali and host machines can easily ping each other. If you cannot ping the Kali from the host, you cannot do this lab using VirtualBox.

Background on IPTABLES

- Overview of IPTABLES (read this before the lab)
 - <https://www.booleanworld.com/depth-guide-iptables-linux-firewall/>
- IPTABLES manual
 - <https://linux.die.net/man/8/iptables>

Tutorials on IPTABLES

- Tutorial 1 (view these before the lab)
 - https://www.youtube.com/watch?v=vbhr4csDeI4&t=83s&ab_channel=XPSTECH
 - https://www.youtube.com/watch?v=H1WPwAjMXRo&t=474s&ab_channel=XPSTECH
- Tutorial 2
 - https://www.youtube.com/watch?v=eC8scXX1_1M

Basic Commands

- Basic commands to manage rules
- | | |
|-----------------------|---|
| # iptables -A | Append to chain |
| # iptables -D | Delete rule |
| # iptables -I | Insert in chain |
| # iptables -F | Delete all rules in chain or all chains |
| # iptables -L | List the rules in a chain or all chains |
| # iptables -X [chain] | Delete a user-defined chain |

Managing IPTABLES

- a) Find the IP address of the host.
- b) Find the IP address of the Kali.
- c) On the Kali, check existing firewall rules. Use “iptables -L” command.
- d) To clean up the rules, execute:
 - a. “iptables -F” and
 - b. “Iptables -X”

- To facilitate the execution of tasks, switch into a superuser.

```
(kali㉿kali)-[~]  
$ sudo su  
[sudo] password for kali:  
(root㉿kali)-[/home/kali]  
#
```

Task 1

- On Kali, create a rule that blocks ping requests to the Kali machine.
- Go to the host machine and ping the Kali. [Take a screenshot of the output on the host machine.](#)
- On Kali, display the rule you created. [Take a screenshot of the output.](#)

Task 2

- On Kali, launch Firefox and visit hurmfamilydentistry.com. Make sure the website is displayed properly.
- Create a rule that blocks access to this site. On a separate tab of the browser, visit the site again and [show in a screenshot that the site now is not accessible.](#)
- Display the rule you created. [Take a screenshot of the output.](#)
(Hint: watch the 2nd video in Tutorial 1).