Cybersecurity lab

2023-2024

Configuration of iptables firewall

Baptiste HAMON – Copy forbidden without prior authorization

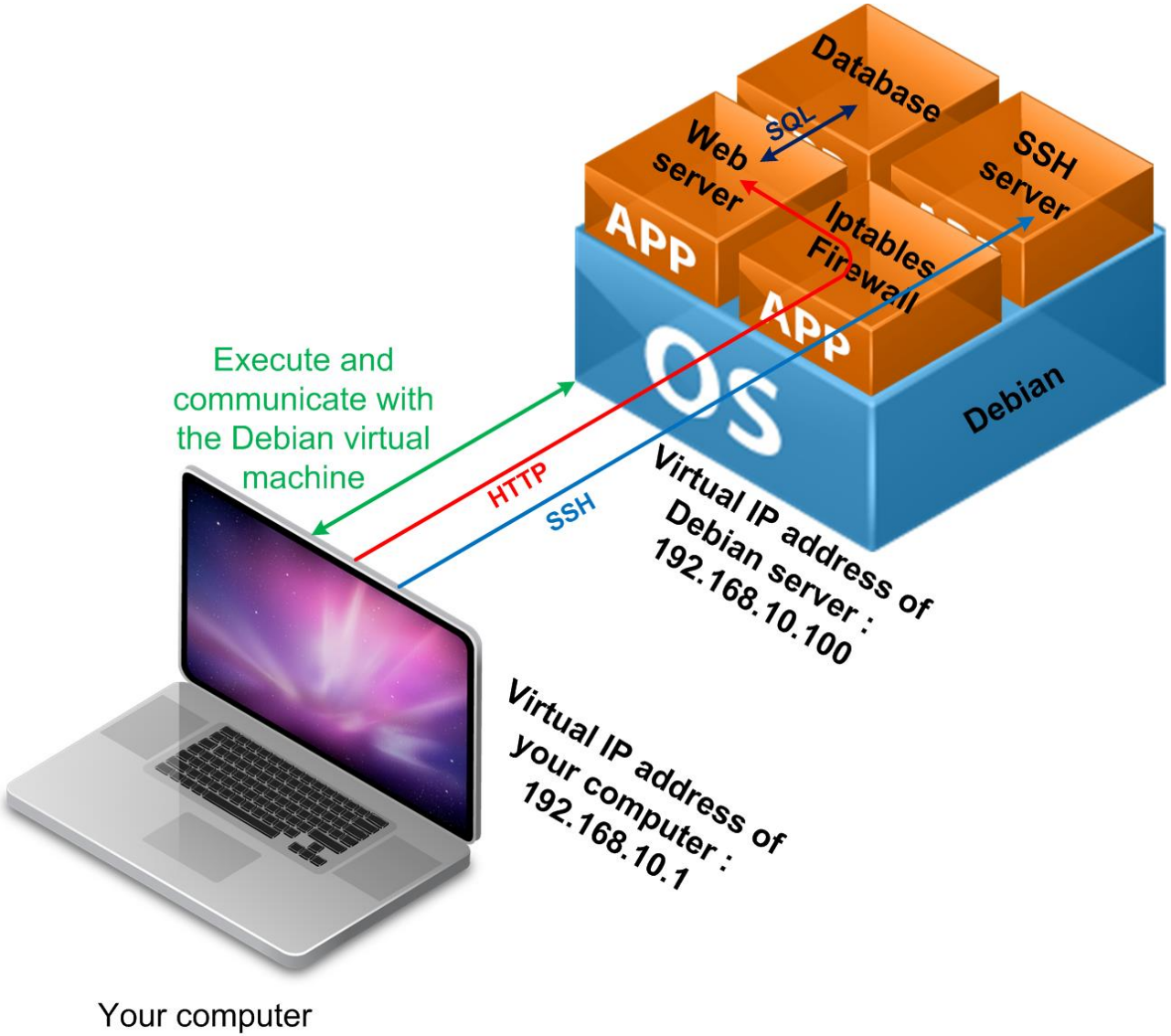
Summary

- Lab objective
- Architecture
- Flow matrix
- Iptables configuration
- Configuration test
- Persistence
- Connections logs

Lab objective

- The purpose of this lab is to understand the interest of setting up a local firewall and to learn how to configure a firewall in Linux
  - The chosen firewall is iptables because it is present by default in Linux distributions
- The configuration of a firewall systematically consists of analyzing which flows will pass through the machine and ensure that they are necessary and sufficient
  - For this purpose, a flow matrix is created indicating the source, the destination, the service and the functional description of the flow
- Once this pre-study is done, you can configure the firewall on the machine

Architecture



Baptiste HAMON – Copy forbidden without prior authorization

Flow matrix

- The server on which you will configure a firewall contains several applications:
  - An SSH server that receives SSH requests only from the administrator's computer
  - A web server that receives HTTP requests from any client in the network
  - A database that sends / receives MySQL requests only from the local web server (on the same machine)

1. Write the flow matrix for this server :

Source IP	Source port	Destination IP	Destination port	Action	Description
10.10.10.1	*>1024*	*10.10.10.2*	*TCP/21*	*Allow*	*FTP connection to Debian*

  - Be careful, only write the connection from the client to the server (do not write the response flow)

Iptables configuration

- Start Linux and use the virtual machine "VM Debian vulnerable"
- Once the virtual machine has started, authenticate to the server:
  - Login : security
  - Password : security
- Use the command "sudo iptables [...]" with the same password to configure iptables
- Use the iptables manual to find the right arguments for your needs (man iptables)

Iptables configuration

2. Iptables configuration :
   - Allow SSH only from the administration workstation (your PC)
   - Allow HTTP access for everyone (Any)
   - Allow the bidirectional flow between the database and the web server (localhost)
   - Change the default policy to deny all connections
3. Configure iptables to automatically accept all response streams
   - For that, the firewall must analyze the state of the connection (use the module state → see the documentation "man iptables-extensions")
   - Delete all unnecessary static rules from previously configured rules

Configuration test

4. Test your configuration :
   - From an SSH client on the terminal of your computer, connect to the server in SSH
   - From a web browser on your computer, connect to the HTTP server: http://192.168.10.100
   - Ping the server from your computer : "ping 192.168.10.100"

Persistence

- Rules are cleared when you turn off or restart the web server
  - Save the firewall rules
  - Restore rules at server startup

Baptiste HAMON – Copy forbidden without prior authorization

Connection logs

5. Create a rule to trace all connections refused by your firewall
   - For this, find the information in the "TARGET EXTENSIONS" / "LOG" section in the "iptables-extensions" manual
   - In order to avoid overloading the logs of your system, you can limit the number of similar log to 2 logs per minute (use the limit module → see the documentation “man iptables-extensions”)