Quality of service and security of computer networks

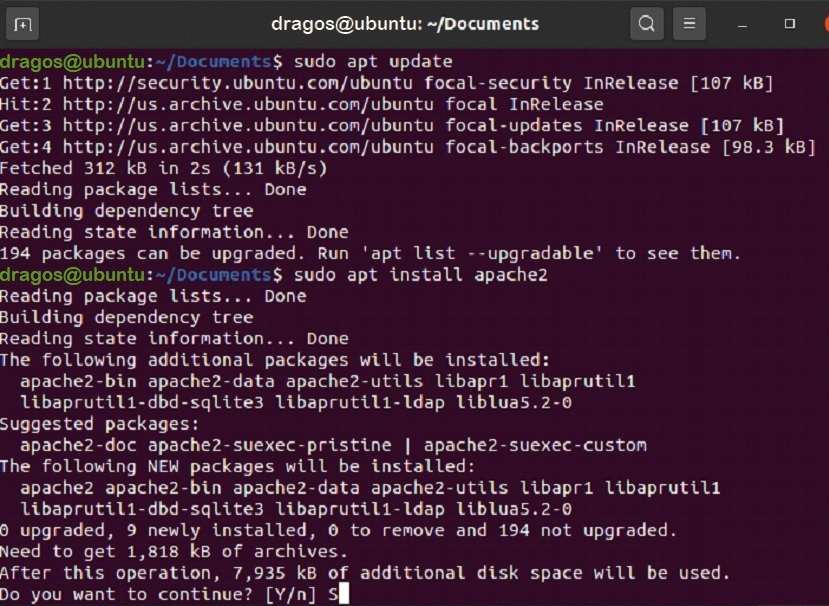
Step 1. System configuration

# VMware Workstation is used as virtualisation environment, running: Kali-Linux and Ubuntu, configured via NAT (Network Address Translation).

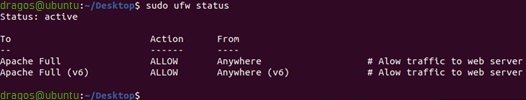
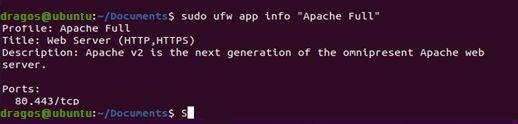
Step 2. Connectivity testing

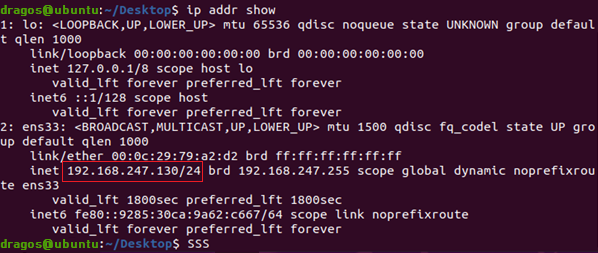
Connectivity testing is done by accessing from Kali Linux the address: https://192.168.247.130

1.Configuration / installation of Apache server (WEB server):



1. Firewall configuration to allow HTTP/HTTPS traffic to the server:

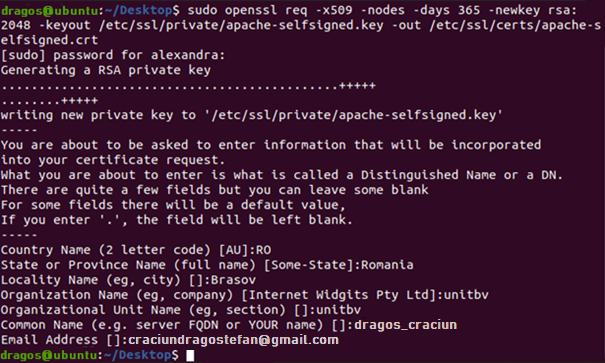


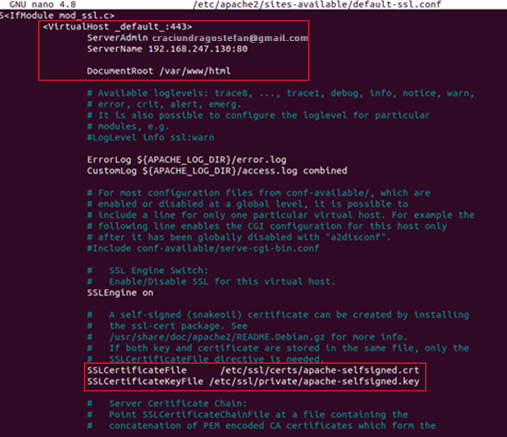
IP address for the server (local address):

SSL key generation:

A self-signed certificate will encrypt the communication between server and client. However, because it is not signed by any of the trusted certificate authorities included in web browsers, users cannot use the certificate to validate the server's identity.

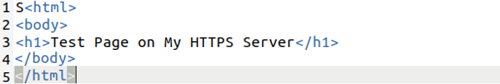
SSL works using a combination of a public certificate and a private key. The SSL key is kept secret on the server. It is used to encrypt content sent to clients. The SSL certificate is publicly distributed to anyone who requests the content. It can be used to decrypt content signed by the associated SSL key.



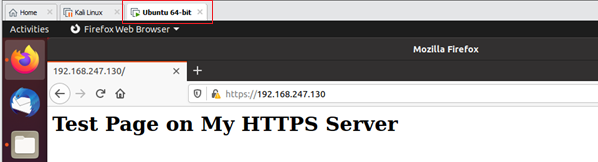
1. Change virtual SSL host:

1. Automatic HTTP HTTPS redirection: 

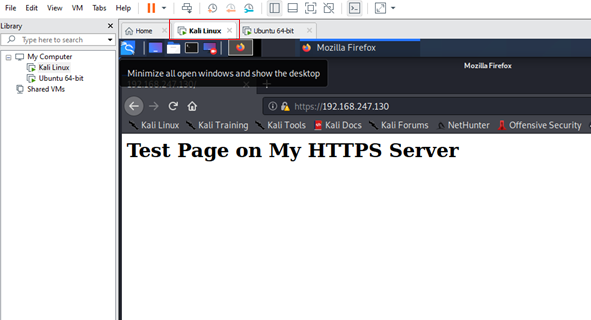
Create WEB page



Test local web page (on Ubuntu):

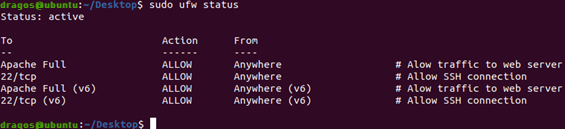


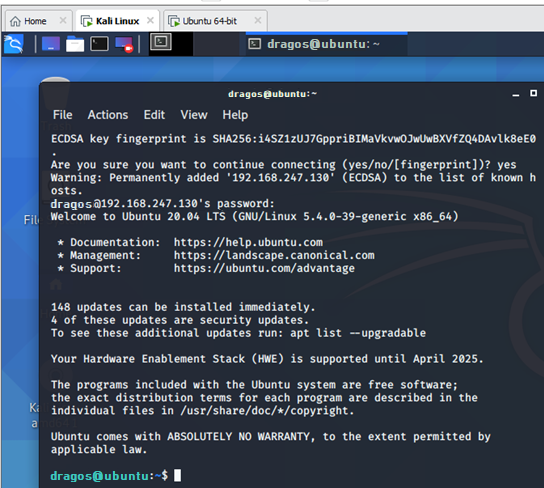
Connectivity testing - accessing the WEB page from Kali-Linux:



Connectivity testing - SSH connection initiation

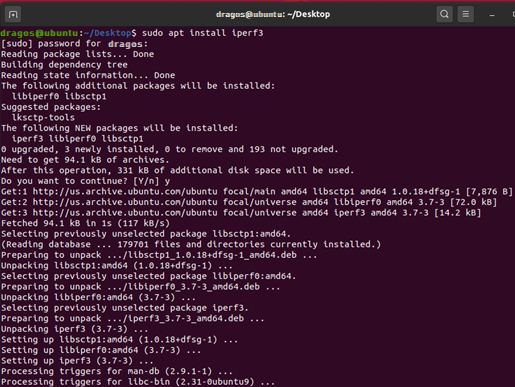
- Change Firewall to allow SSH connections:

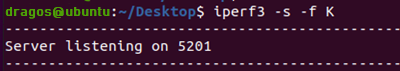


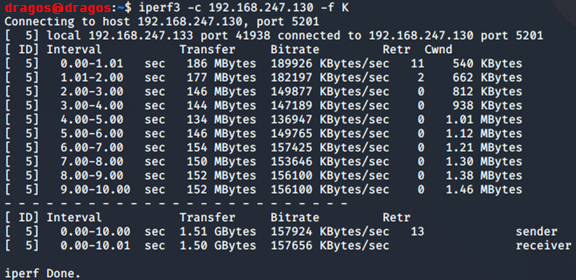
- Kali Linux connectivity check:

Step 3. Bandwidth measurement with iperf3

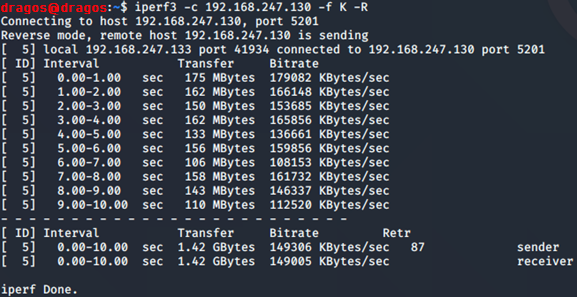
*iPerf3 requires two systems because one system must act as a server while the other acts as a client. The client connects to the server where the speed is being tested.*

*- Install iperf3 on both Ubuntu and Kali Linux:* 

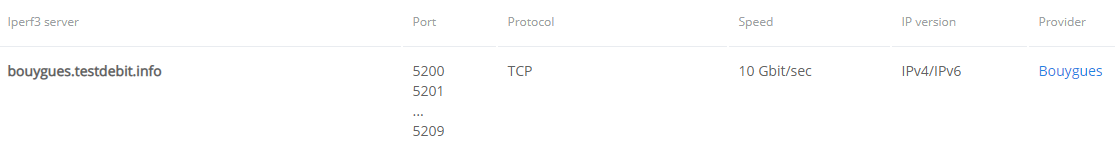
- Scenario 1: Ubuntu - server (receives packages from client), Kali Linux (sends packages to serve

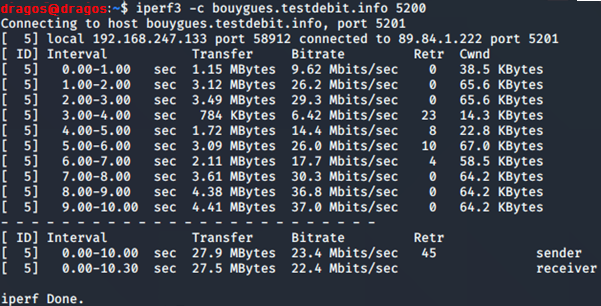


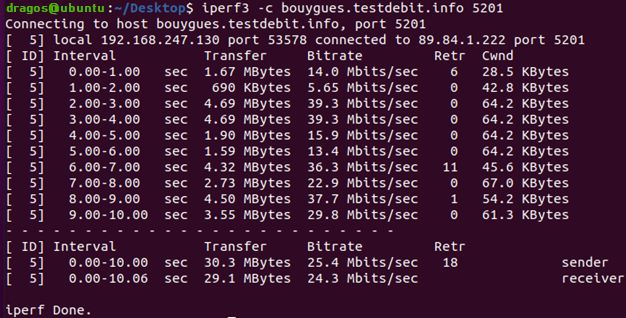
- Scenario 2: Ubuntu - server (sends packages to client), Kali Linux (receives packages from server):

):

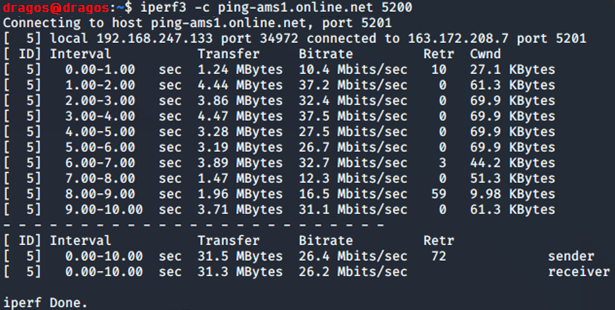
- Scenario 3: Bandwidth to an external service:Server TCP:

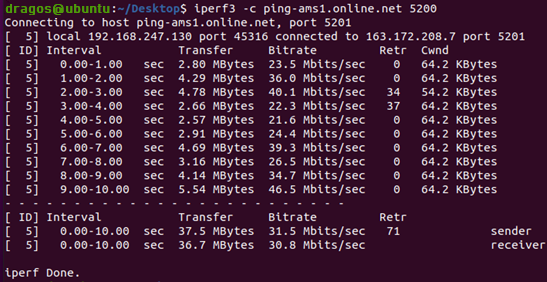


Running iperf3 on Kali Linux:

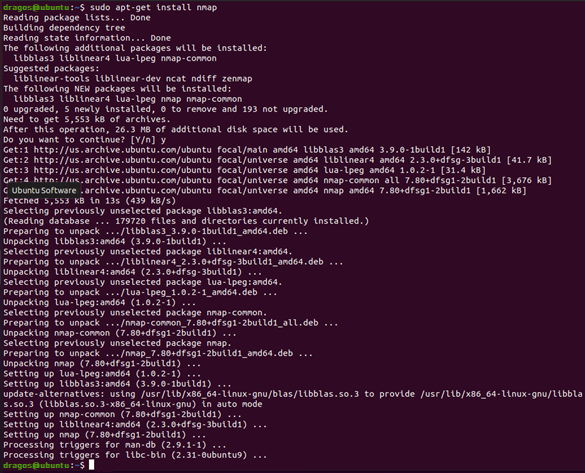
Running iperf3 on Ubuntu:

TCP/UDP server:

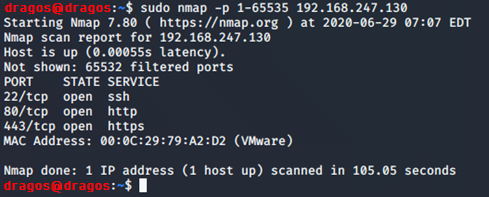
- Running iperf3 on Kali Linux:

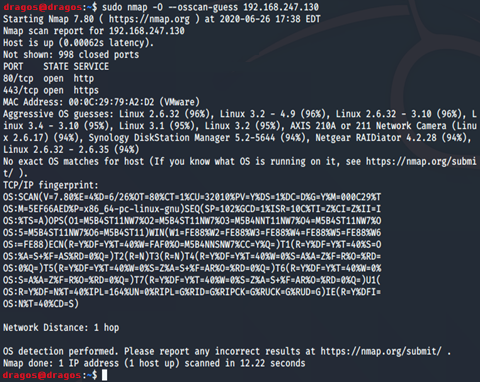
- Running iperf3 on Ubuntu:

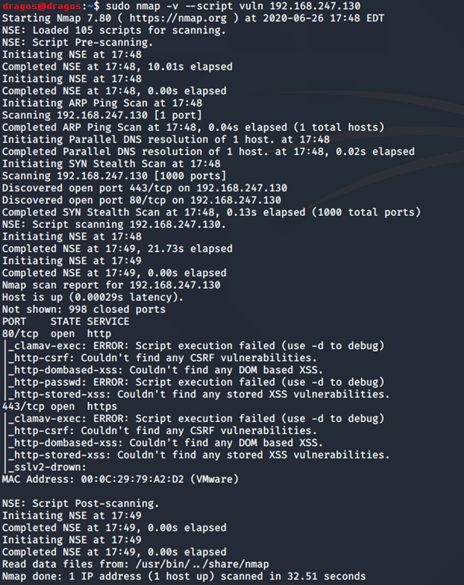
* Step 4. Scanning ports with nmap

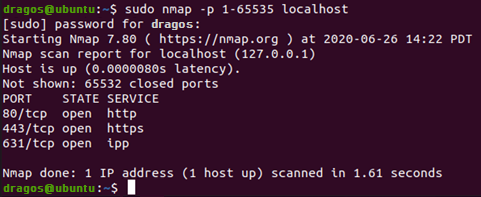
nmap installation (similar for Kali)

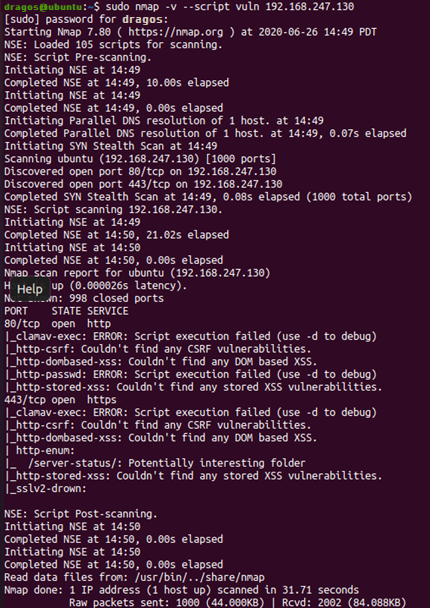
- Scenario : Running nmap on Kali-Linux for port and vulnerability discovery on Ubuntu.



Use nmap to find out the operating system:****

Scanning for vulnerabilities:

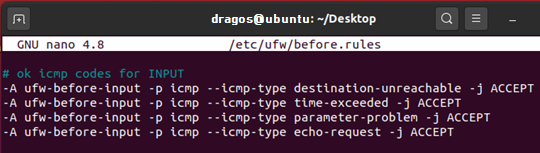
- Scenario: Running nmap on Ubuntu for discovering ports and vulnerabilities locally.

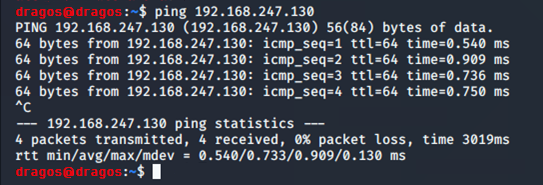
Scanning for vulnerabilities on localhost

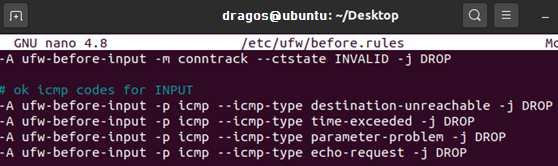
Step 5. Implement Firewall

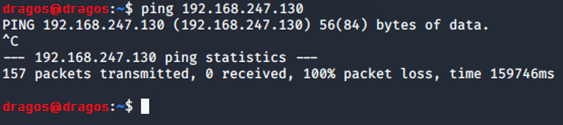
* UFW (Uncomplicated Firewall) is an interface to iptables that is geared towards simplifying the process of configuring a firewall. While iptables is a solid and flexible tool, it can be difficult for beginners to learn how to use it to properly configure a firewall.

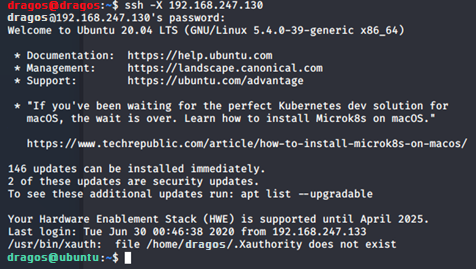
Server connectivity (192.168.247.130) before the firewall.

- iptables content:

- Initiate icmp connection:

- Change rules for icmp packages:

- Initiate ping command to Ubuntu after changing Firewall rules:

- SSH connection before firewall application:

- Connection to WEB Server after Firewall change: