SECURE NETWORK DESIGN, FIREWALL CONFIGURATION, AND ATTACK SIMULATION IN GNS3 GROUP 11 – NETWORK DESIGN IMPLEMENTATION PROJECT

INTRODUCTION

The purpose of the project is to organize and introduce a secure segmented network based on the GNS3, FortiGate firewall, Cisco router, and several virtual machines in the form of Kali Linux, Windows 10, and Ubuntu. The main idea is to establish complete isolated cyber-range where internal attacks like port scans and DoS-type traffic can be safely modeled and studied.

It is made deliberately unreachable (not connected to the internet) to ensure all data within the lab is kept within the lab environment. This allows a secure practical introduction of various heavy-lifting offensive tools (nmap and hping3, etc.), and also to examine a range of defensive features including firewall policy, segmentation, logs and packet capture.

NETWORK TOPOLOGY OVERVIEW

The ultimate topology will be composed of the following components:

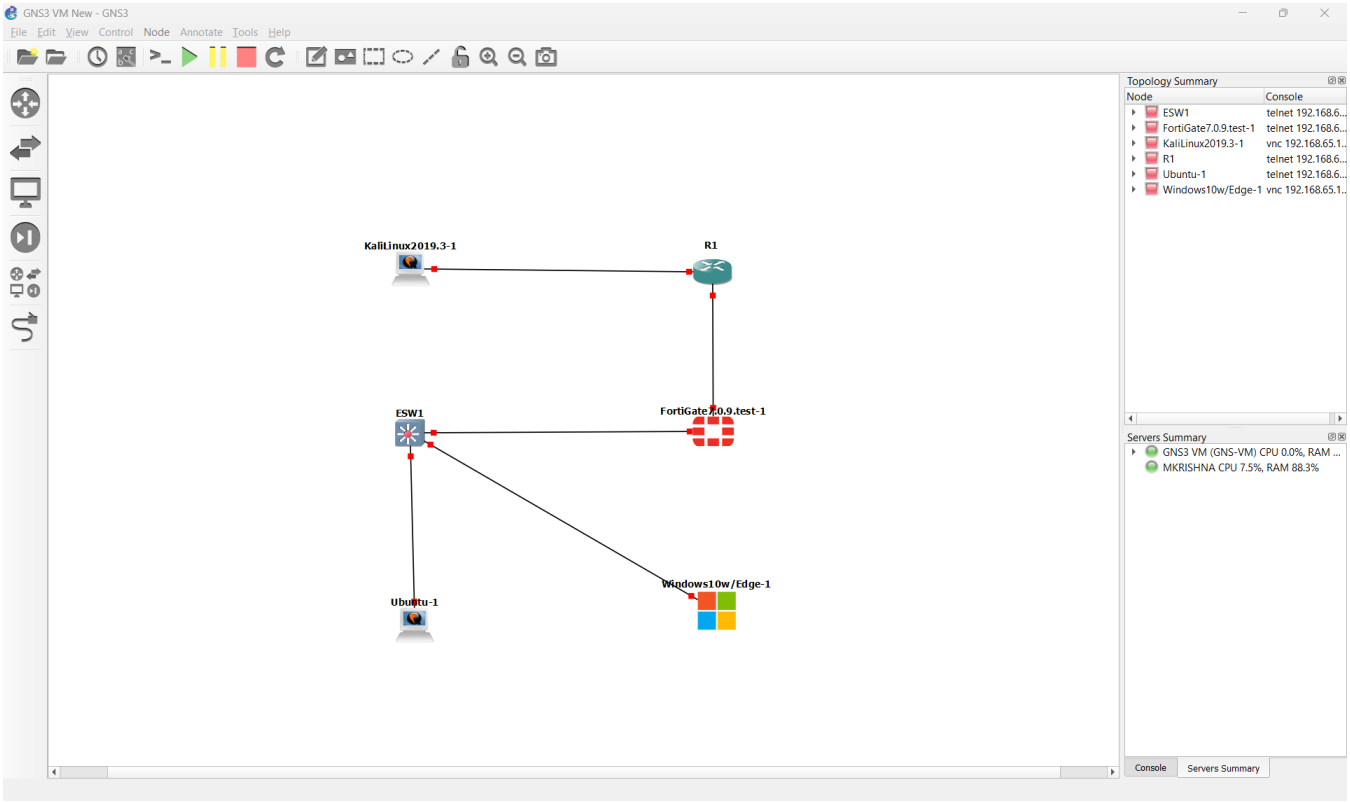
- Kali Linux – attacker machine.
- Windows 10 – victim workstation.
- Ubuntu -internal server/ normal host.
- FortiGate firewall- principal safety and observatory.
- Cisco R1 router- routing LAN segments to LAN segments.
- ESW1 switch - LAN predictable distribution switch.

Kali machine exists within a single subnet and windows and Ubuntu also exist within a subnet behind the firewall. The router links the attacker network to a firewall through a transit network. This is a segmented design that enables us to have control and monitoring of all cross-LAN traffic using the firewall.

IP ADDRESSING AND DEVICE ROLES

The addressing scheme is organized into three main networks:

Windows/Ubuntu LAN: 192.168.10.0/24



Kali, Windows, Ubuntu, FortiGate, R1, and ESW1 make up the GNS3 network topology

Windows 10: 192.168.10.30;

Ubuntu: 192.168.10.40;

default gateway: 192.168.10.1 (FortiGate port3)

Kali LAN: 192.168.20.0/24

-Gateway: 192.168.20.1 (R1 Fa0/1)

10.0.0.0/24 is the router-firewall transit network.

-FortiGate port 2: 10.0.0.2;

-R1 Fa0/0: 10.0.0.1

The FortiGate firewall therefore has:

port3 – inside LAN (192.168.10.1/24), connecting to Windows and Ubuntu via ESW1.

port2 – outside/transit (10.0.0.2/24), connected to R1.

port1 – disabled (no internet access by design).

This setup will guarantee that any traffic between Kali (attacker network) and Windows (victim) will go through the router and the firewall and it will be visible to security controls and logs.

CONFIGURATION STEPS

Router R1:

The Cisco R1 router will have two interfaces and a static route:

FastEthernet0/0 = 10.0.0.1 (toward FortiGate)

FastEthernet0/1 = 192.168.20.1 (toward Kali)

A static route was used to reach the Windows/Ubuntu LAN:

ip route 192.168.10.0 255.255.255.0 10.0.0.2

The NAT is switched off in such a way that all the environment is internal and offline.

FortiGate Firewall:

On the FortiGate, interfaces were configured as:

port3: 192.168.10.1/24 (inside LAN for Windows and Ubuntu).

port2: 10.0.0.2/24 (connected to R1).

The fundamental IPv4 policy is developed to permit the LAN-to-LAN communication using the firewall.

Source: all internal networks (e.g., 192.168.20.0/24, 192.168.10.0/24).

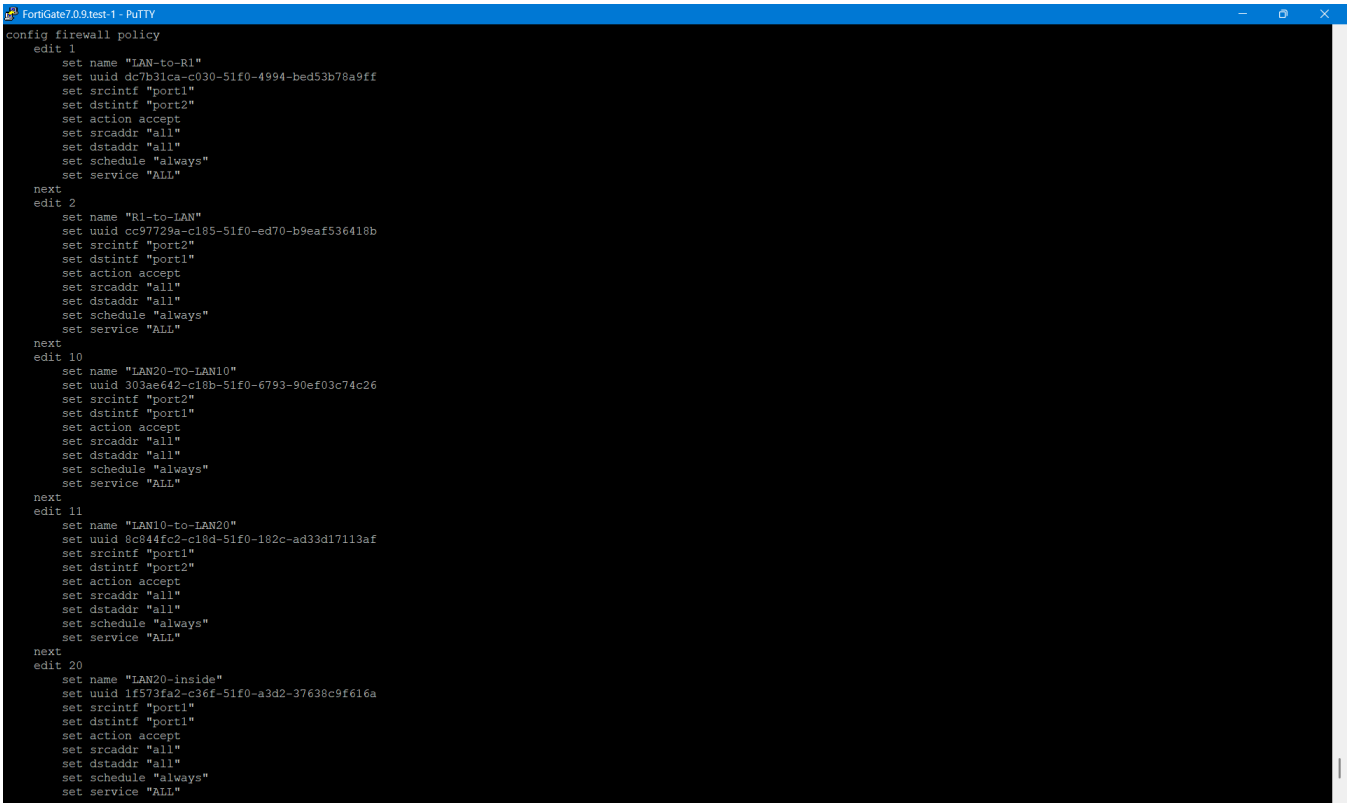
Destination: all internal networks.

Action: ACCEPT.

NAT: Disabled.

Logging: Enabled for all sessions.

This policy may also have optional DoS protection or IPS profiles in order to record high traffic patterns or suspicious traffic patterns.



FortiGate IPv4 policy allowing LAN-to-LAN traffic with logging enabled.

Switch ESW1

ESW1 switch works at Layer 2 and contains local connections in the LAN:

- Dynamic ports to windows and Ubuntu hosts associated with VLAN 10.
- Port3 of FortiGate linked to uplink port.

This basic switch setup will guarantee that anything attempting to traverse windows/ubuntu would be aggregated and sent to the firewall to be examined.

Host Configuration

The Windows and Ubuntu hosts are given the hostname: 192.168.10.1 and 192.168.10.1 respectively and with 192.168.10.1 as default gateway. The Kali machine has been set with the router as its gateway and the 192.168.20.0/24 IP address set.

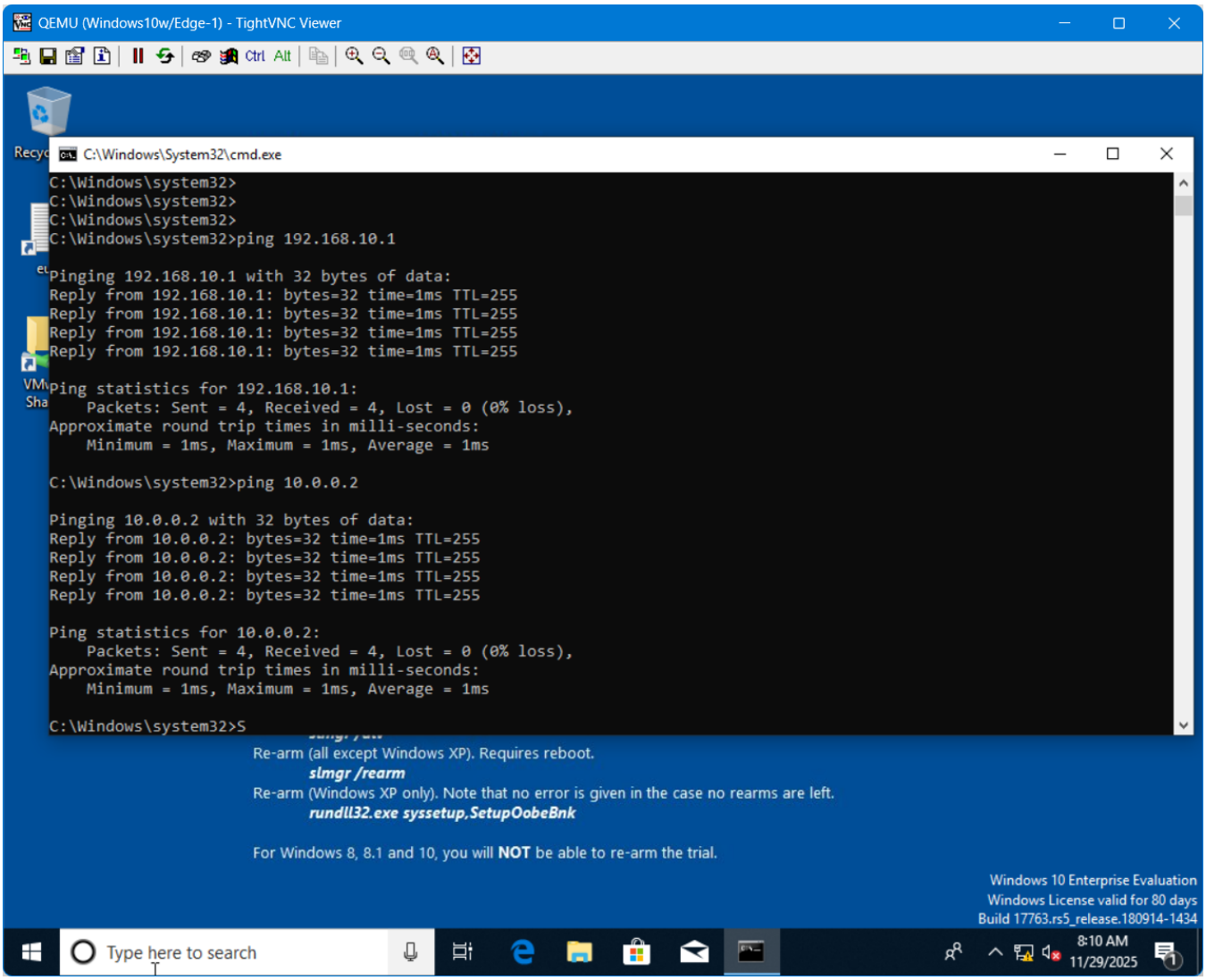
Basic connectivity testing is performed using ping:

Windows → FortiGate (192.168.10.1)

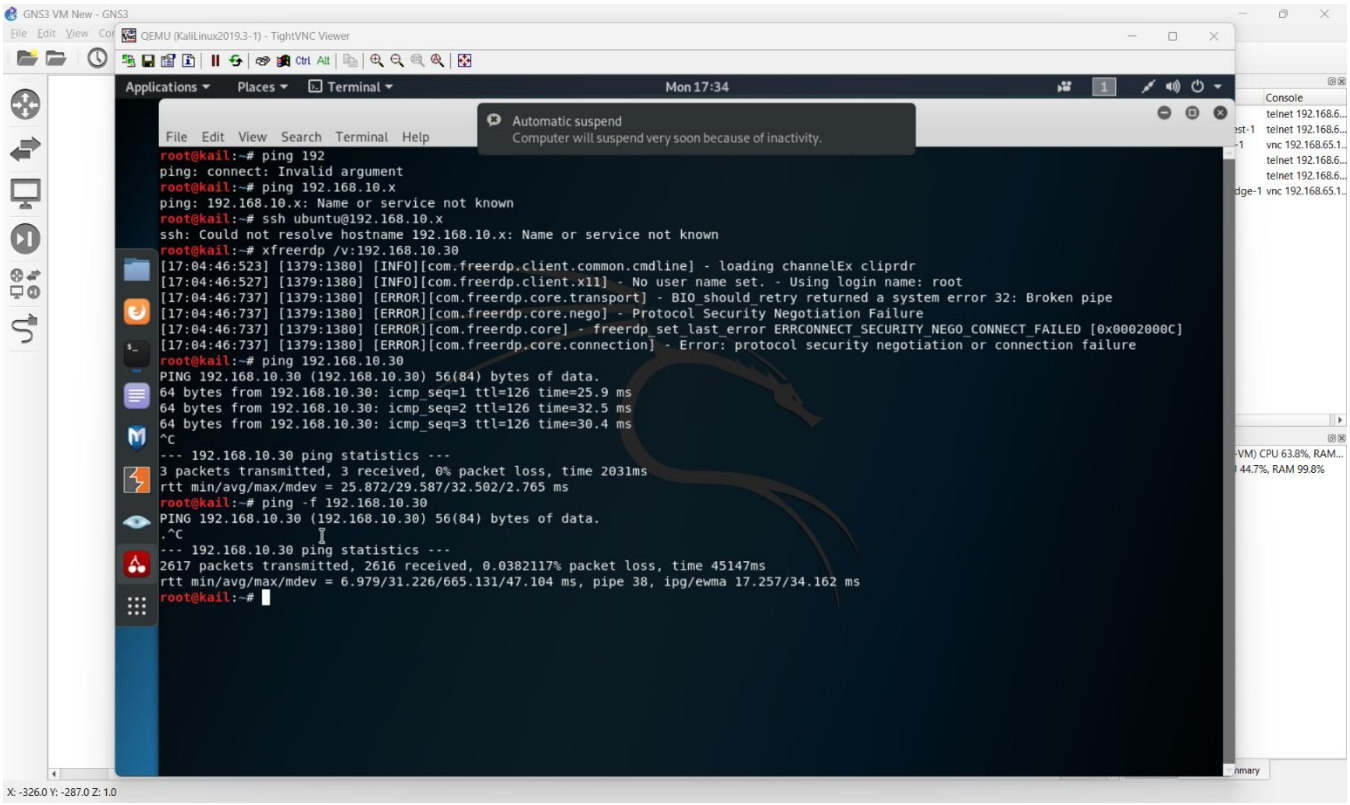
Kali → R1 (192.168.20.1)

Ubuntu → Windows and FortiGate

These tests have ensured that routing and firewall policies are also operating.



Basic connectivity testing is performed using ping from the Windows to other Appliances in the GNS3

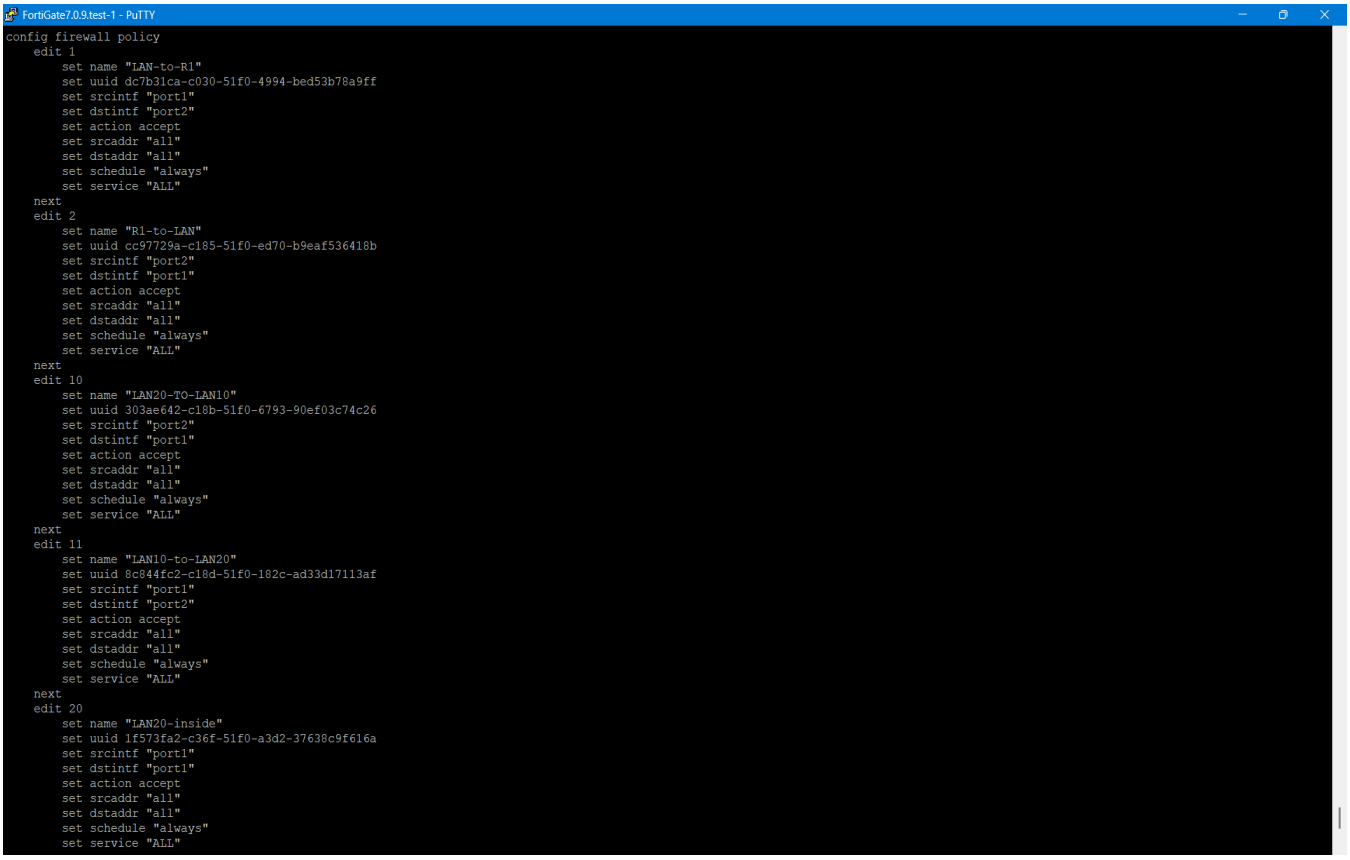


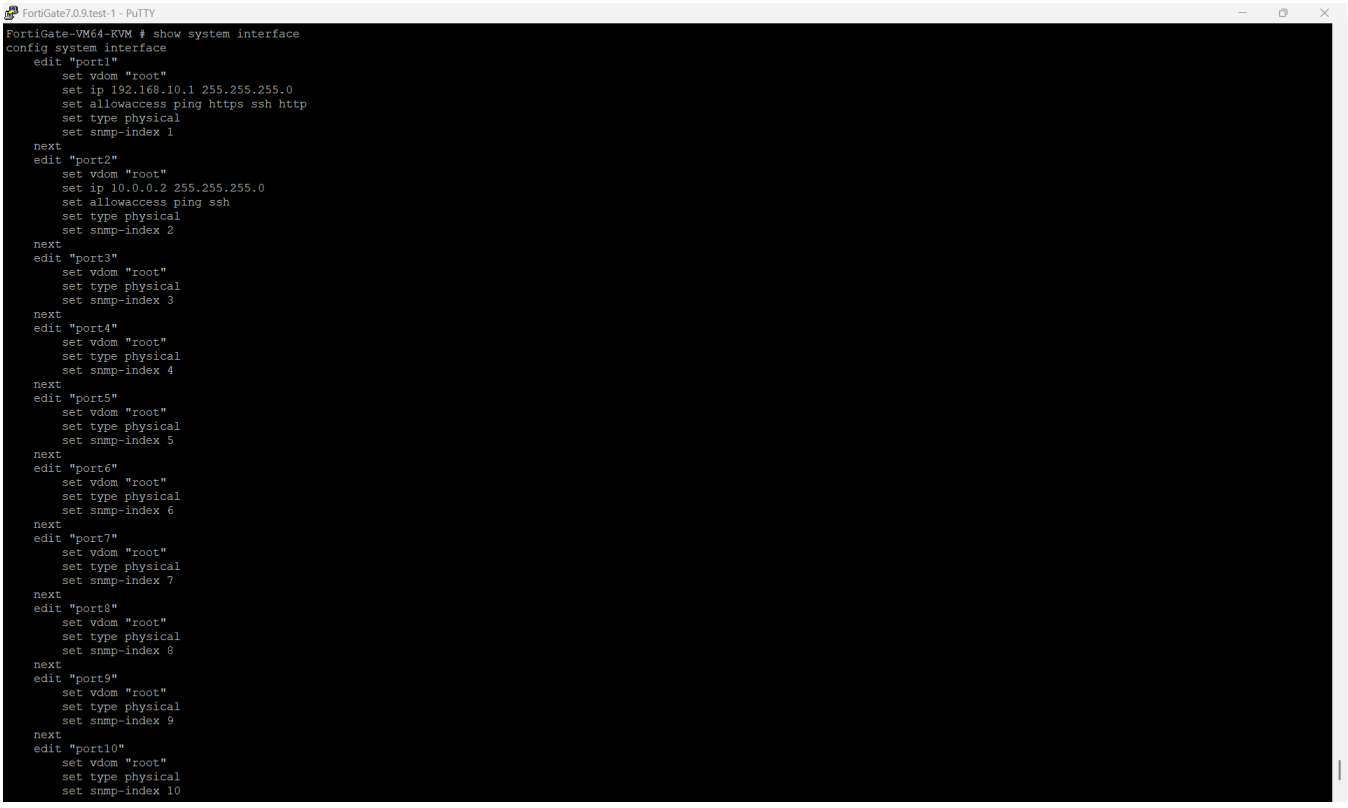
Basic connectivity testing is performed using ping from the Kail Linux to other Appliances in the GNS3

Security Controls and Attack Simulation

Firewall Policy and Logging:

The FortiGate firewall offers the primary security enforcement in this topology. With the logging on the LAN-to-LAN policy, all traffic between Kali and Windows is logged, protocol, ports, and timestamps. This plays a critical role in the analysis of normal and malicious behavior. However, we cannot get the firewall logs since the License of the appliances that have been used by us has expired.

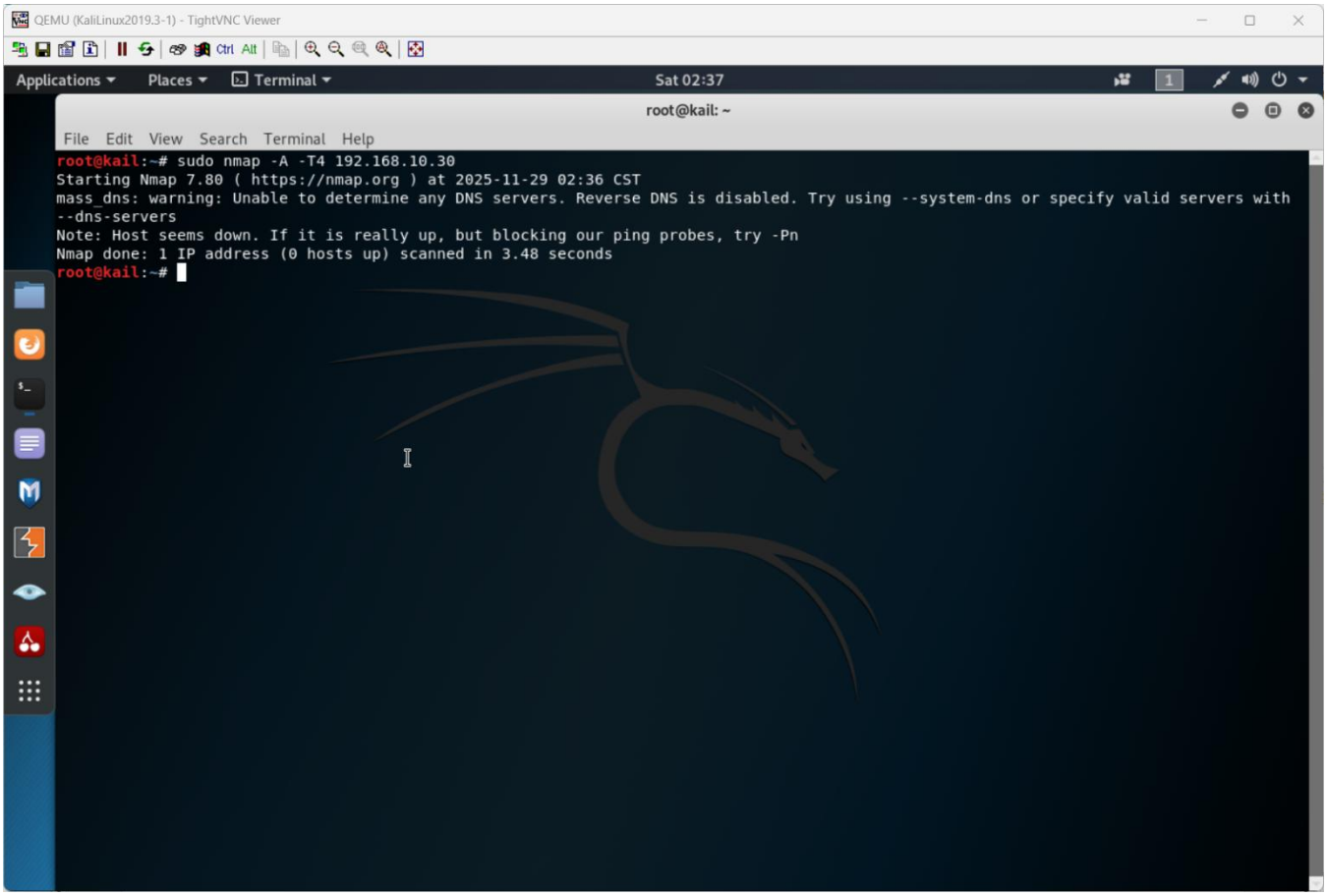




Firewall Policy and PORT Connections

Port Scan Simulation with nmap

A nmap reconnaissance attack is simulated to Kali against the windows host: nmap -A 192.168.10.30 This scan tries to uncover the open ports, running services and the OS information of the windows machine. During the running of the scan, the firewall records several connection requests, made by the Kali IP, to different windows ports in the TCP connection.



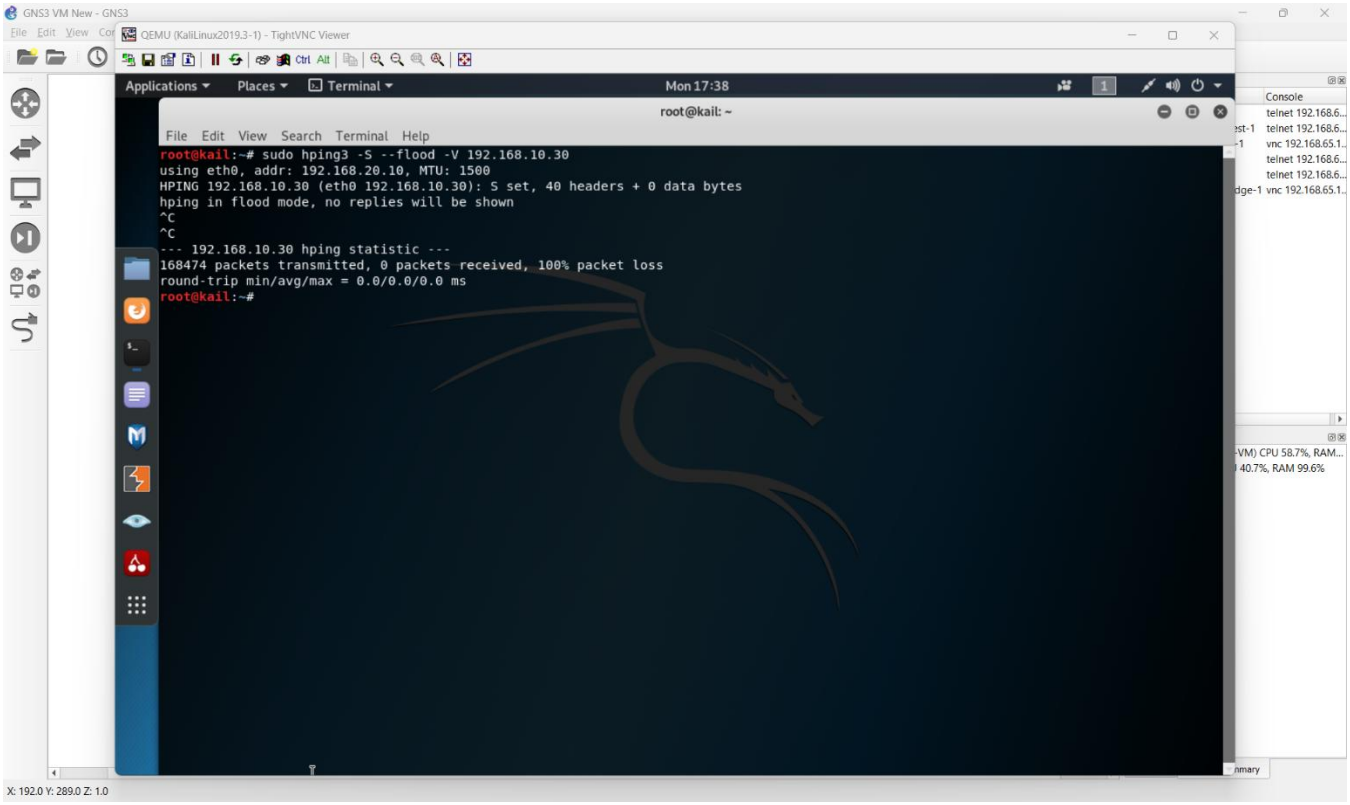
Port Scan Simulation with nmap in the Kail Linux in the GNS3

DoS-Style Traffic Simulation with hping3

Hping3 is used to do a safe DoS-type simulation, which sends a large number of SYN packets of Kali to Windows:

sudo hping3 -S --flood -V 192.168.10.30

This causes a SYN flood pattern to the isolated lab. Windows system could be delayed and the firewall logs indicates a peak in the connections made by the Kali host.



DoS-style SYN flood simulation from Kali to Windows using hping3.

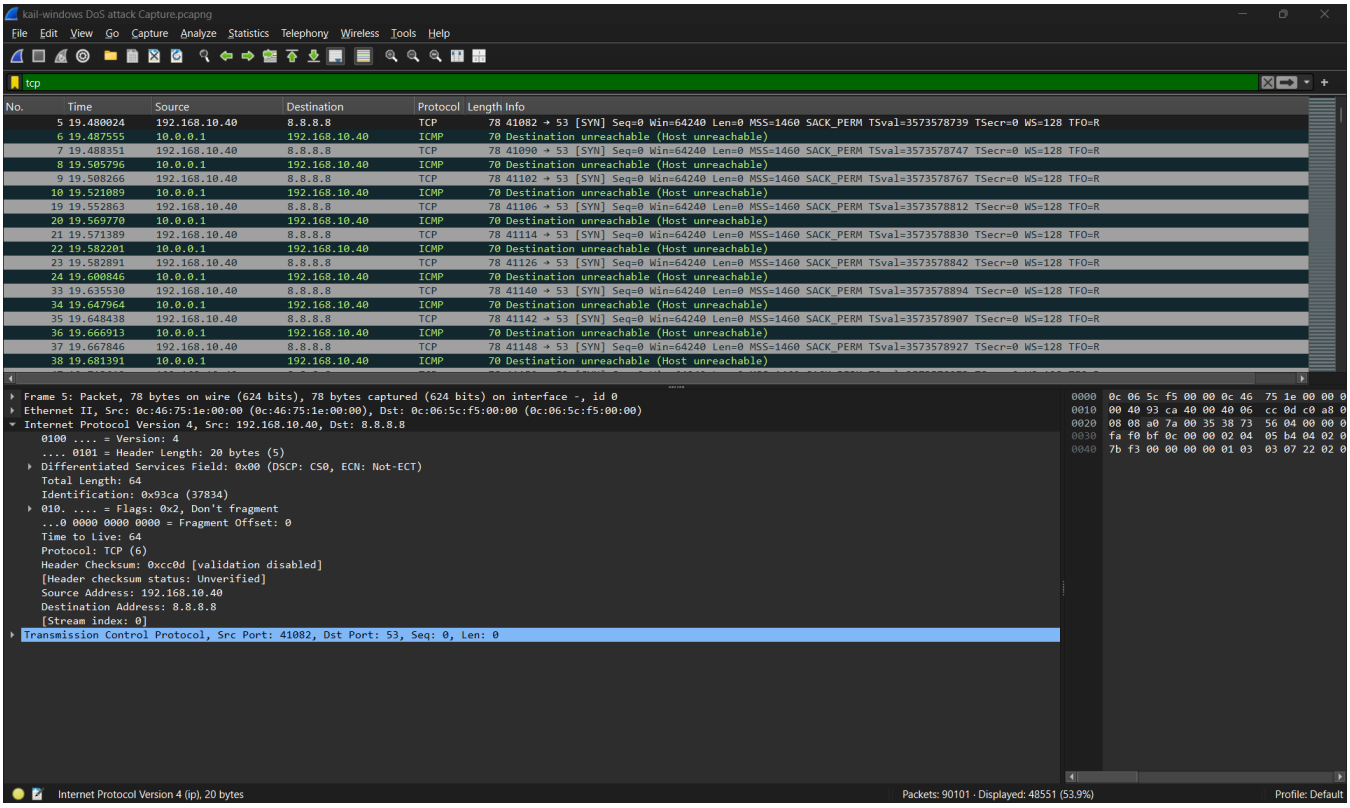
Packet Capture and Analysis

Packet capture is carried over within the GNS3 in tools like wireshark. Captured traffic includes:

- ICMP echo interacting with connectivity tests.
- TCP SYN packets in DoS style attack.

ARP broadcasting and responding inside of LAN.

The packet capture analysis is useful to visualize the way in which attacks spread across the network and ensures that all harmful traffic is redirected across the firewall to be inspected



Packet Capture and Analysis Using the Wireshark

CONCLUSION

This project shows that a segmented network with a central firewall is applicable in studying internal attacks within a safe, controlled environment. The design achieves this by ensuring that reconnaissance and DoS-type activities are not only visible but also restricted in scope by isolating Kali (attacker) and Windows and Ubuntu (victims) on different subnets and restricting all cross-LAN traffic to the FortiGate firewall.

The recorded topology, configuration procedures and security measures demonstrate that:

- Segmentation minimizes the number of targets to attack.
- Firewall policy gives necessary insight into bad traffic.
- Packet captures and logs are effective tools in reporting and comprehending attacks.

Overall, the offline GNS3-based lab provides a reusable platform for future experiments in network security, intrusion detection, and defensive configuration testing.