National College of Ireland

# Configuration Manual

MSc Research Project
MSc Cybersecurity (MSCCYB)

Rohan Yele
Student ID: X21203971

School of Computing
National College of Ireland

Supervisor: Prof. Mr. Michael Pantridge

**National College of Ireland**

**MSc Project Submission Sheet**

**School of Computing**

**Student Name:** Rohan Yele

**Student ID:** X21203971

**Programme:** MSc Cybersecurity (MSCCYB1) **Year:** 2023

**Module:** Research Project

**Lecturer:** Prof. Mr. Michael Pantridge

**Submission Due Date:** 18/09/2023

**Project Title:** Using Redundancy of Perimeter Firewall to Increase the Availability of Business Resources

**Word Count:** 1101 **Page Count:** 7

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** Rohan Yele

**Date:** 18/09/2023

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

| | |
|---|---|
| Attach a completed copy of this sheet to each project (including multiple copies) | □ |
| **Attach a Moodle submission receipt of the online project submission,** to each project (including multiple copies). | □ |
| **You must ensure that you retain a HARD COPY of the project**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | □ |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| **Office Use Only** | |
|---|---|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

# Configuration Manual

Rohan Yele
Student ID: x21203971

## 1 Overview

Reliability, security and availability of the networking devices is extremely important for the continuity of the services provided by a business organisation. In this report, we have proposed the usage of variable software tool and devices such as firewalls used for providing defence mechanism to safeguard the internal devices of the organisation from different attack vectors.

The Effectiveness of the proposed fabric was evaluated using some well-known attacks such as SYN flood and HTTP flood and also redundancy mechanism is proven in case of hardware failure to achieve service continuity for an organisation. The septs used to deploy the network fabric are detailed in the following sections.

## 2 Tools Used

The Following tools were used to implement the research project,

(1) VMware Workstation Pro 16.0.0[1]:
Download and install VMware Workstation Pro from its official website[1]. VMware Workstation is used to deploy Emulated Virtual Environment where GNS3 server version image and kali Linux image will be run on it.

(2) GNS3 2.2.21 tool[2]:
Download and install GNS3 from its official website, it alco contains console software packet capture software's and GNS3 server image.

(3) GNS3 2.2.21 Server Image[3]:
Download and install GNS3 image from its official website and then load it into the VMware environment. Both the GNS3 image and tool must be of same versions.

(4) Putty 0.73[4]:
Putty will be used to take the ssh access of the devices which will be implemented in GNS3.

(5) Python Scripts- GoldenEye[5]:
Download and install the python script from GitHub official website, it will be used to attack from Linux environment to Firewall.

[1] https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html
[2] https://www.gns3.com/software/download
[3] https://www.gns3.com/software/download-vm
[4] https://www.putty.org/
[5] https://www.geeksforgeeks.org/goldeneye-ddos-tool-in-kali-linux/

# 3 GNS3 Lab Setup

The hardware requirements include windows 11 machine with minimum 16 GB ram and 1 TB SSD with intel core i5 7th generation.

VMware workstation was used to upload and install GNS3 server image and was given 9GB ram, 100 GB SCSI storage with two network interface host –only to connect with the devices inside the GNS3 environment and to bridge network adapter to ensure the connectivity to the internet.

(Stoitsov & Shotlekov, 2016), (Sararwat, 2022) and (D. T. Vojnak, 2019) recommended the basic deployment of networking images and devices using VMware due to its better compatibility as compare to Virtualbox and HyperV

# 4 Preparation Of Images

(1) Cisco Router[6]:
Cisco router 3725 images were downloaded from a website with image name c3725-adventerprisek9-mz.124-15.T14.image.

(2) Cisco ASAv 992 firewall[7]:
The Asav992 firewall was downoaded online and uploaded to the GNS3 enviornment. Qcow image asav992-N.qcow2 was uploaded to GNS3.

(3) Kali Linux[8]:
Download and install kali linux 2021.3 version image from the officical website of linux and after integrating GNS3 with VMware, Kali can be seen in side window pane.

(4) Docker Images[9]:
Images of Docker can be directly installed in GNS3. The GNS3 will pull the specified imaged from the docker container, here images such as DNS server turnkeylinux/worpress:latest and ubuntu server ubuntu image were pulled from the docker container.

# 5 Load Images on GNS3 Enviornment

Downlaod all the images and sav them in appliance folder so that it is easier for the user as wel as the software to do some inclusion or exclusion of images.

[6] https//networkrare.com/free-download-cisco-ios-images-for-gns3-and-eve-ng/
[7] https://upw.io/5Ga/asav992.qcow2
[8] https://www.kali.org/
[9] https://hub.docker.com/

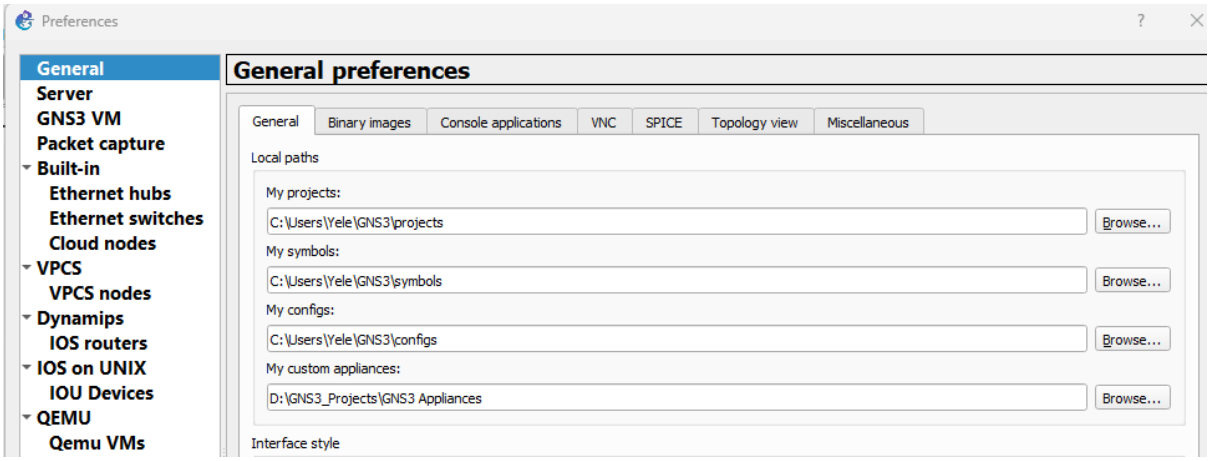


**Figure 1:GNS3VM Integration**

# 6 Lab Setup

The GNS3 VM should be imported in VMware and then it should be called from GNS3 tool by enabling the GNS3 VM and selecting the appropritae image from the drop down menu as shown below,

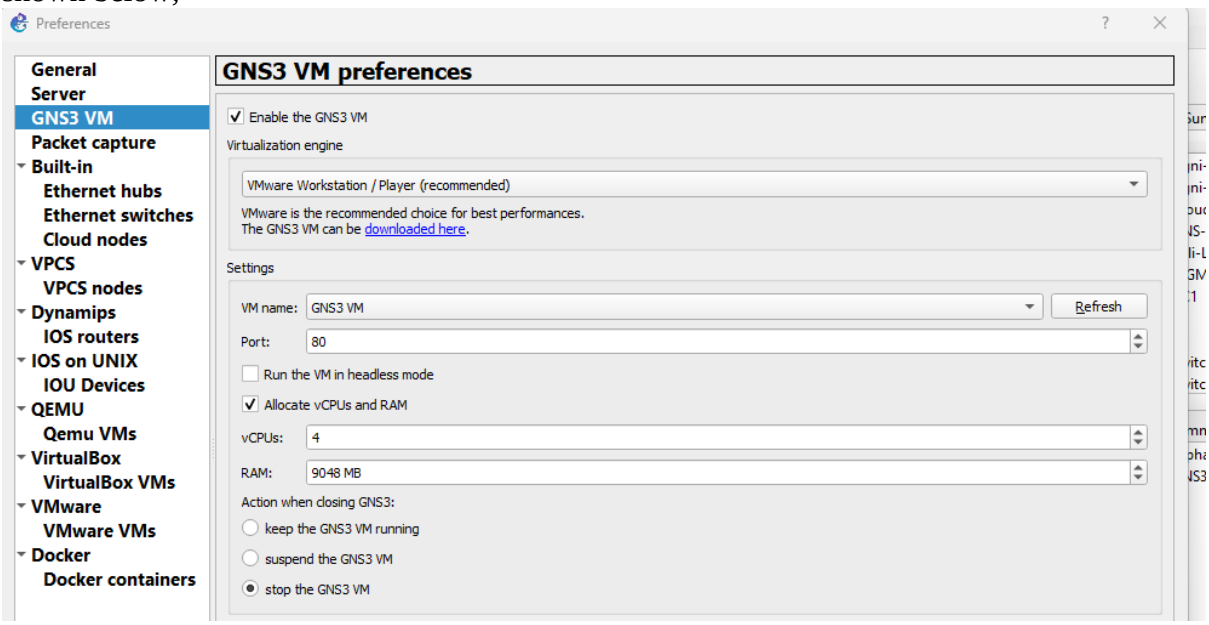


**Figure 2: GNS3 VM Lab Setup**

# 7 Startup all the nodes

After integrating the GNS3 enviornment the node will be automatically connected and the status summary is shown at the bottom right corner of the screen.

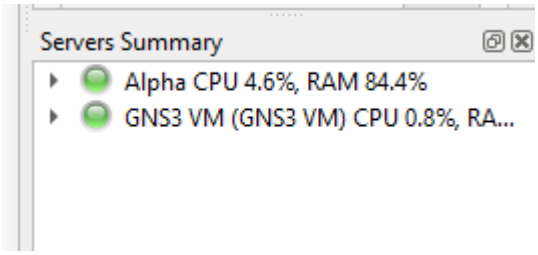


**Figure 3: Node Summary**

# 8 Docker Container

Docker images can be pulled by mentioning the name of the docker images in GNS3 by going to the preference of docker and creating a new docker container.

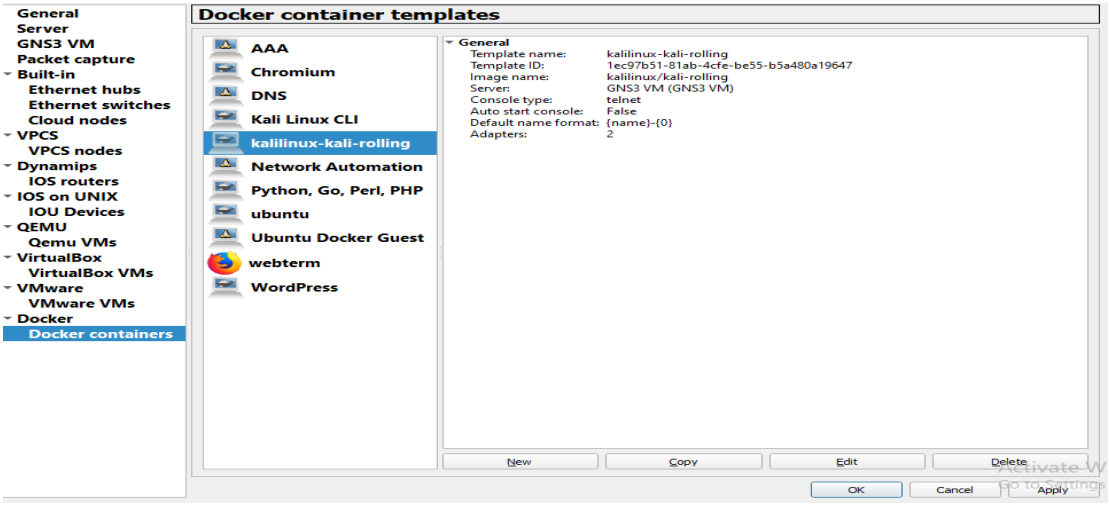


**Figure 4: Docker**

You can select existing images or give the link for the new mages, here we have used ubuntu as an existing image and pulled turnkeylinux/worpress:latest image which was a DNS server.

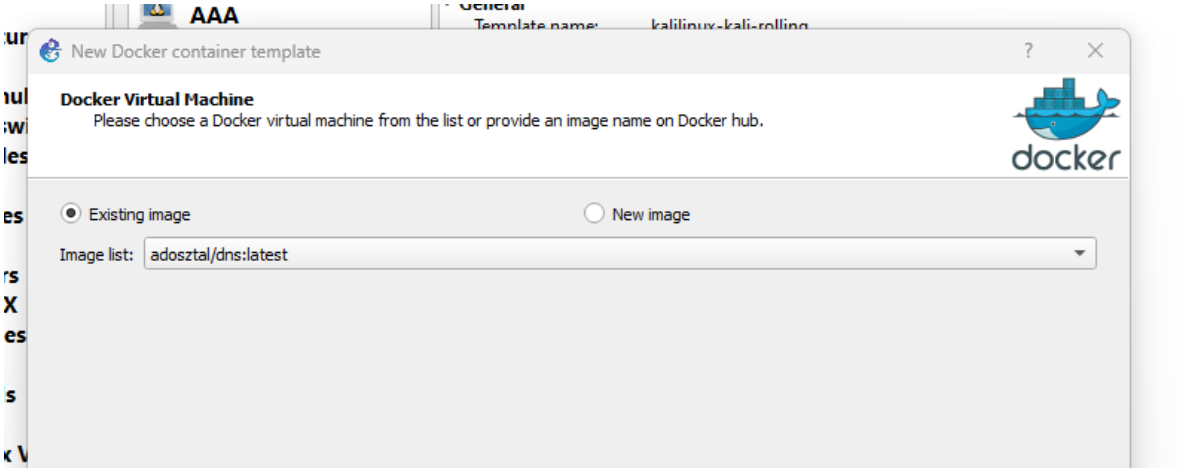


**Figure 5: Installing Docker Images**

# 9 GoldenEye Python Script

Goldeneye python script can be downloaded[10] using the git command executing it in linux, downloading the file and executing it to generate and attack sequence. Create a folder in kali linux in the name of goldeneye and execute git clone https://github.com/jseidl/GoldenEye.git url[11] on the termial to download the script file in that directory.

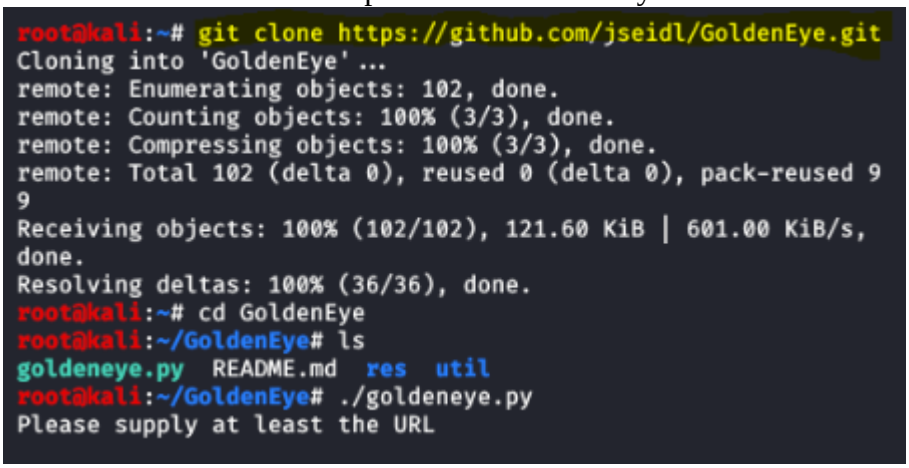


**Figure 6: Downloading GoldenEye Script**

# 10 References


D. T. Vojnak, B. S. (2019). Performance Comparison of the type-2 hypervisor VirtualBox and VMWare Workstation. *2019 27th Telecommunications Forum (TELFOR),*, (pp. 1-4). Belgrade, Serbia.

Sararwat, Y. (2022, 12 29). *Enhancing the security of a network fabric using firewalls and load balancer.* Retrieved 07 08, 2023, from https://norma.ncirl.ie: https://norma.ncirl.ie/6053/

Stoitsov, G., & Shotlekov, I. (2016). Sample network topologies for educational purposes implemented with GNS3. *MATTER: International Journal of Science and Technology, 04*(07), 106-115.


[10] https://www.geeksforgeeks.org/goldeneye-ddos-tool-in-kali-linux/

[11] https://github.com/jseidl/GoldenEye