Configuration Manual

MSc Research Project
MSc Cybersecurity

Salint George Mukalath
Student ID: 21136548

School of Computing
National College of Ireland

Supervisor: Mr Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Salint George Mukalath………………………………………………………………………

Student ID: ………21136548……………………………………………………………………………………..……

Programme: ………MSc Cybersecurity…………………………… **Year:** ……2022-23…..

Module: ………MSc Research Project…………….…………………………………………………….………

Lecturer: ………Mr Jawad Salahuddin…………………………………………………………….………

Submission Due Date: ………01 Feb 2023………..……………………………………………………………….………

Project Title: ………Novel Technique to Detect and Defend Address Resolution Protocol Poisoning

Word Count: ………1043……………………… **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: ……Salint George Mukalath……………………………………………………

Date: ……27 Jan 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

Salint George Mukalath
Student ID: 21136548

1 Introduction

The ARP spoofing defence technique consist of several software integrations. This configuration manual provides the detailed explanation of the system requirements, the tools' details, and the steps to implement the system. It explores the lab set up for enabling the actual experiment in a controlled environment.

2 System Requirements

2.1 Hardware Requirements

The recommended hardware requirements for the host machine are as follows.

- Processor: 11th Gen Intel(R) Core (TM) i7-1195G7 @ 2.90GHz 2.92 GHz
- RAM: 16 GB
- Storage: 500 GB SSD
- OS: Windows 11 Home 64bit
- Graphics: NVIDIA GeForce MX 450

2.2 Software Requirements

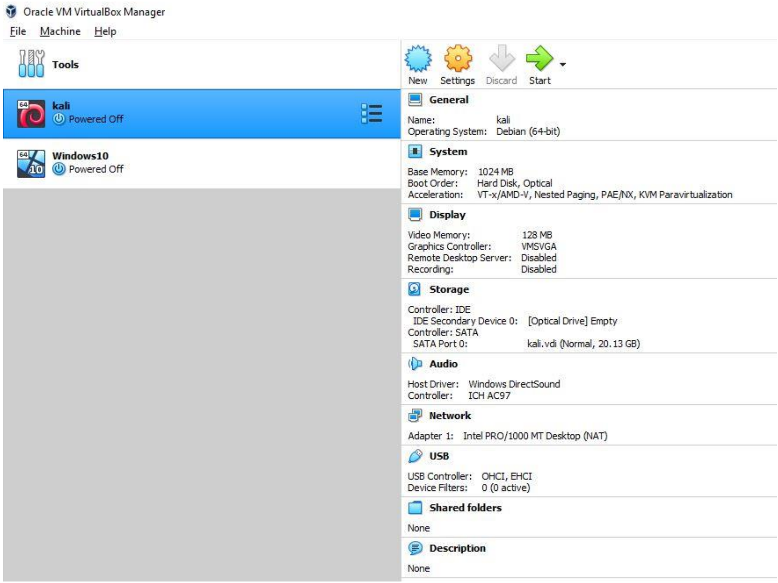
The below list of software use for the complete installation and implementation of the research experiment.

- Oracle VM Virtual box 6.1
- Kali Linux
- Windows 10
- Python 2.7.18
- Scapy
- Anaconda
- SHA 256 algorithm
- Npcap
- Sublime Text

3 Installation

3.1 Virtual box

Install Oracle VM virtual box 6.1 with Kali Linux and windows 10 as the machines integrated in it for the victim and attacker respectively.



kali
Powered Off

Windows10
Powered Off

General
Name: kali
Operating System: Debian (64-bit)

System
Base Memory: 1024 MB
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali.vdi (Normal, 20.13 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description
None

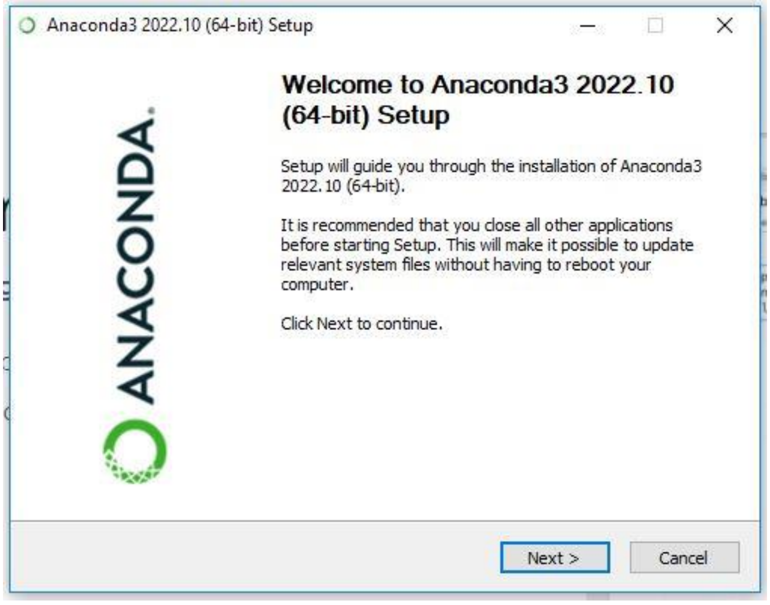
Figure 1: Virtual Machines

3.2 Kali Linux & Windows 10

In this research project the Debian base Kali Linux is being act as the defence machine since it is equipped with security tools such as scapy, nmap etc. Kali Linux is an open-source platform for the study and research in cybersecurity field. Windows 10 is one of the stable windows editions from Microsoft.

3.3 Anaconda Distribution

Install anaconda distribution which is the open-source python repository for the environment creation ("Anaconda | Anaconda Distribution," n.d.). This is required for our attacker machine (Windows 10) for the python environment creation.



Welcome to Anaconda3 2022.10 (64-bit) Setup

Setup will guide you through the installation of Anaconda3 2022.10 (64-bit).

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Figure 2: Anaconda 3 Installation

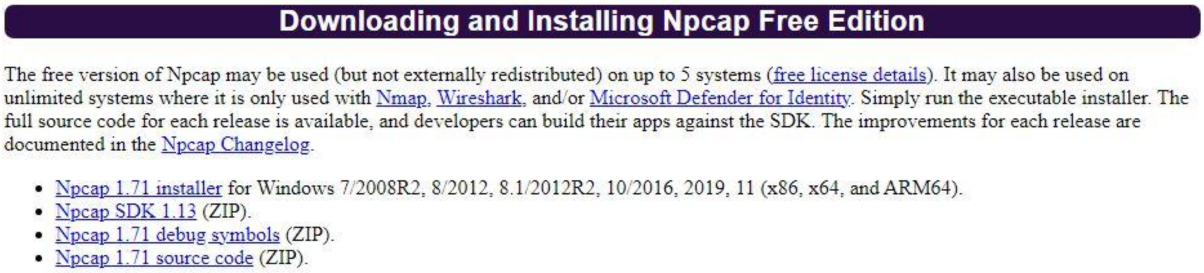
We created the environment named “network” in the anaconda repository. The commands are as follows,

conda create -n network python=2.7.18

3.4 Npcap 1.71

Npcap is the packet capturing tool for Windows machines which allows to capture raw network traffic including wireless, local host and VPN traffic, moreover it permits to send raw packets. This tool can be downloaded from the below link. Npcap has installed in Windows 10 attacker machine.

https://npcap.com



Downloading and Installing Npcap Free Edition

The free version of Npcap may be used (but not externally redistributed) on up to 5 systems (free license details). It may also be used on unlimited systems where it is only used with Nmap, Wireshark, and/or Microsoft Defender for Identity. Simply run the executable installer. The full source code for each release is available, and developers can build their apps against the SDK. The improvements for each release are documented in the Npcap Changelog.

- Npcap 1.71 installer for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019, 11 (x86, x64, and ARM64).
- Npcap SDK 1.13 (ZIP).
- Npcap 1.71 debug symbols (ZIP).
- Npcap 1.71 source code (ZIP).

Figure 3: Npcap editions

3.5 Python

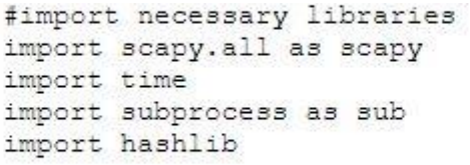
Python is considered as one of the popular and powerful programming language in the modern world. We use both python 2 and python 3 languages, as python 2 helps with inbuilt library features whereas Python 3 helps to enhance with latest features. We used python 2.7.18 in windows 10 for enabling the ARP attack mechanism. The python download link is as follows.
https://www.python.org/downloads/release/python-2718/

3.6 Scapy

Scapy is a powerful packet manipulation tool to enable the user with sniff and forge the network packets. It can easily do certain tasks such as traceroute, probing, network discovery. It can be easily do the arpspoof as well (“Introduction — Scapy 2.5.0 documentation,” n.d.). Scapy will be a default tool in most of the security systems such as Kali linux, hence in this project there is no separate installation in Kali Linux.

3.7 SHA 256 Algorithm

Secure Hash Algorithm 256 is a cryptographic algorithm which uses for data integrity verification. In python there is an inbuilt SHA 256 hash function which installed in the Kali machine.

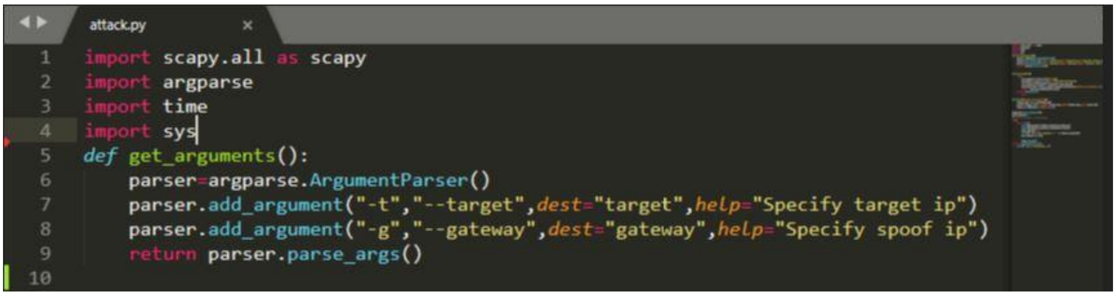


```
#import necessary libraries
import scapy.all as scapy
import time
import subprocess as sub
import hashlib
```

Figure 4: SHA library

3.8 Sublime Text

Sublime Text is one of the popular text editors for the python language. It has been installed in both Kali and Windows machines. It is lightweight fast and reliable editor for the application development(Schäferhoff, 2016) .



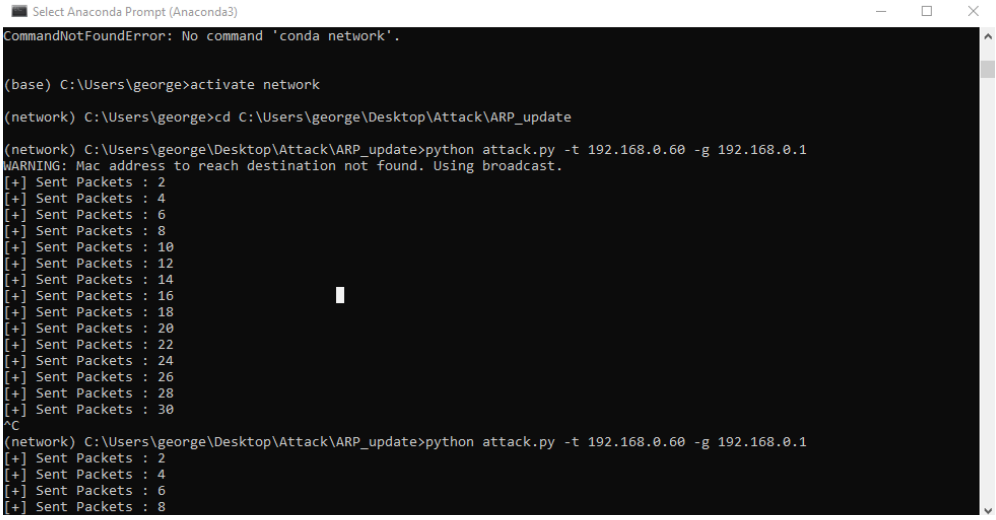
```
import scapy.all as scapy
import argparse
import time
import sys
def get_arguments():
    parser=argparse.ArgumentParser()
    parser.add_argument("-t","--target",dest="target",help="Specify target ip")
    parser.add_argument("-g","--gateway",dest="gateway",help="Specify spoof ip")
    return parser.parse_args()
```

Figure 5: Sublime Text

4 ARP Attack module

Since the attacking machine is Windows 10 the ARP spoofing attack is performing here. The command to execute this as follows,

Python attack.py -t <target IP> -g <gateway IP>



```
CommandNotFoundError: No command 'conda network'.


(base) C:\Users\george>activate network

(network) C:\Users\george>cd C:\Users\george\Desktop\Attack\ARP_update

(network) C:\Users\george\Desktop\Attack\ARP_update>python attack.py -t 192.168.0.60 -g 192.168.0.1
WARNING: Mac address to reach destination not found. Using broadcast.
[+] Sent Packets : 2
[+] Sent Packets : 4
[+] Sent Packets : 6
[+] Sent Packets : 8
[+] Sent Packets : 10
[+] Sent Packets : 12
[+] Sent Packets : 14
[+] Sent Packets : 16
[+] Sent Packets : 18
[+] Sent Packets : 20
[+] Sent Packets : 22
[+] Sent Packets : 24
[+] Sent Packets : 26
[+] Sent Packets : 28
[+] Sent Packets : 30
^C
(network) C:\Users\george\Desktop\Attack\ARP_update>python attack.py -t 192.168.0.60 -g 192.168.0.1
[+] Sent Packets : 2
[+] Sent Packets : 4
[+] Sent Packets : 6
[+] Sent Packets : 8
```

Figure 6: Code execution

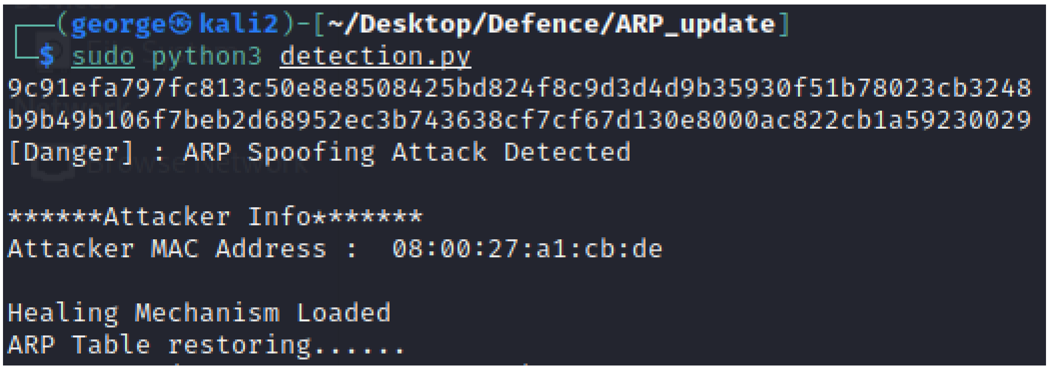
5 Defense Module

Kali machine is the victim machine hence the defence system is performing here. Here we are using certain system which consist of certain commands and program as follows.

5.1 Defense python code

Run the python program detection.py in this module for the arp spoof detection and healing process. Apply the below command in Kali command terminal.

sudo python3 detection.py

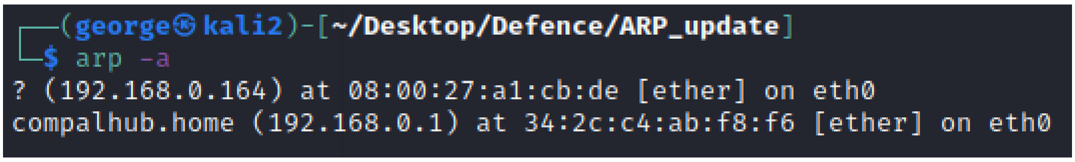


```
┌──(george㉿kali2)-[~/Desktop/Defence/ARP_update]
└─$ sudo python3 detection.py
9c91efa797fc813c50e8e8508425bd824f8c9d3d4d9b35930f51b78023cb3248
b9b49b106f7beb2d68952ec3b743638cf7cf67d130e8000ac822cb1a59230029
[Danger] : ARP Spoofing Attack Detected

******Attacker Info*******
Attacker MAC Address :  08:00:27:a1:cb:de

Healing Mechanism Loaded
ARP Table restoring......
```

Figure 7: Execution of detection module

5.2 List ARP table

The command arp -a is to view the address resolution protocol table which shows the immediate node's hardware address. Here it will be the address of gateway.



```
┌──(george㉿kali2)-[~/Desktop/Defence/ARP_update]
└─$ arp -a
? (192.168.0.164) at 08:00:27:a1:cb:de [ether] on eth0
compalhub.home (192.168.0.1) at 34:2c:c4:ab:f8:f6 [ether] on eth0
```

Figure 8: ARP table

References

Anaconda | Anaconda Distribution (no date) *Anaconda*. Available at: https://www.anaconda.com/products/distribution (Accessed: 14 December 2022).

Introduction — Scapy 2.5.0 documentation (no date). Available at: https://scapy.readthedocs.io/en/latest/introduction.html (Accessed: 14 December 2022).

Npcap: Windows Packet Capture Library & Driver (no date). Available at: https://npcap.com/ (Accessed: 14 December 2022).

Schäferhoff, N. (2016) *The Sublime Text Code Editor - An In-Depth Review*, *Elegant Themes Blog*. Available at: https://www.elegantthemes.com/blog/resources/the-sublime-text-code-editor-an-in-depth-review (Accessed: 14 December 2022).