

**Reverse Engineering Malware Assignment**

|  |  |
| --- | --- |
| Type | 32 bit Windows Executable |
| Filename |  |
| Md5hash |  |
| URL Download |  |

|  |
| --- |
| <student name> |
| <student id> |

|  |
| --- |
| <student name> |
| <student id> |

<DATE>

**Table of Contents**

# Lab Setup

<This section describes the lab setup which you will be using to analyse the malware>

## VMware Setup

<Describes the version of VMware, Host OS, Guest OS>

## Network Diagram

<Describes the virtual network setup of your VMs. You will need at least two VMs to analyse the malware>

## Network Configuration

<Describes the configuration of your server & victim in terms of routing, proxy used etc.>

# Passive Information Gathering (IDA Pro)



## Imported APIs

<describes important useful APIs that the malware imports>

### Windows API 1

<purpose>

<MSDN Reference>

### Windows API 1

<purpose>

<MSDN Reference>

### Windows API 1

<purpose>

<MSDN Reference>

Etc…

# Code Analysis (IDA Pro)



## Graph of Major Subroutines from Main Function

<Put in the graph of major subroutines calls from Main function>

## Description of Subroutines

### Subroutine 1

<purpose>

### Subroutine 2

<purpose>

### Subroutine 3

<purpose>

Etc..

# Patching (OllyDBG)



Patch the malicious code of existing malware.

# General Analysis

What type of malware is it?

What are the functionalities of the malware?

Were you able to interact with the malware? How?