**PROJECT OBJECTIVES**

The general objective of the study is to develop a Network Utility System that will cater the needs of the network administrator in network security.

Specifically the study aims:

1. To design and develop utility system with the following features:
2. ***Network Scanner*** compose of python scripts that was intended to scan the network to determine the details of each packets passing through the network.
3. ***Intrusion Detection System*** that detects the rules that was set to the network and the data allowed by the system’s firewall.
4. ***Network Mapper*** uses NMAP third party software to create a map of the network to scan active and inactive hosts, open and closed ports within a network.
5. ***Network-Attack Adviser*** helps the administrator to mitigate common network attack.
6. ***Logs Generator*** is the one responsible in collecting the scan results and saving it to a database.
7. To design and develop a utility system that will help network administrator in mitigating common network attacks
8. To design and develop a utility system that will generate a logs which will serve as a report for the network administrator while the system is running.

**ABSTRACT**

NetSec Manager: A Network Security Utility Software developed to support network administrators in scanning network for active ports, mapping the network to locate up and down host, detects the rules that was set to the network for managing network activities, generate logs results and advise common network attacks. **Network Scanner** helps administrator to scan active ports within the network, scan result will be saved in a database where the administrator can access and view the result via **Logs Generator.** Another feature of NetSec Manager is the **Network-Attack Adviser** which contains a list of common network attacks together with its countermeasure or mitigation. The fourth feature is the **Network Mapper** which to create a map of the network to scan up and down host, open and closed ports within a network. Lastly, it has **Intrusion Detection System** that can be used to detect the rules set within the network and the data allowed by the firewall. The proponents used Visual Basic to create the graphical user interface of the system because of its complexity and easy to use. It has also the capability of connecting process like Python programming language that the proponents use to create the process of each features. On the other hand, MySQL was considered to be the storage or database for result generator. Beneficiaries of the study will be the network and security administrator because the level of knowledge will fit the application. NetSec Manager was created to measure the data security in the network, robustness of the application, user-friendliness and timeliness of the application.

**BACKGROUND**

The world’s interconnection has become complex due to the improvements in technology and the Internet. With the advent in the development of these improvements, computer and network security has become a major concern. For instance, a certain person access a malicious site without knowing that there is an attacker behind that site that can destroy or retrieve important data in a computer or a server. Because of this occurrence, a lot of important transactions can be affected. Worst, most of these destructive programs have the capabilities of not being detected by an antivirus or an intrusion detection system. In addition, these strategies is not common to all people and several software can detect it. Every year, there are reports of security issues – not only in individual devices, but also through the network. Though there are different security and protection tools available online, still threats are becoming more sophisticated as time passes.

A number of tools are available online developed by the open source community – where most of these open-source programs are helpful in protecting the network itself, regardless of the number of clients connected to the network. With proper configuration and execution, these programs will be helpful for network administrators in managing the network.

Because of these observations, the need for a program that protect a system increase. The proponents planned creating a new type of system that will serve as a multi-tool for network administrators that will not only view and manage a network, but can also generate results and can detect rules that was set for the network.

**SYSTEM ANALYSIS**

Data loss, hacking and fraud are now encountered by IT people every day. Every hour, a new malware is created that can destroy or steal millions of data, this scenario can happen inside and outside of IT field. This problem has been occurring for the past years and increases the damage percentage every day. With this problem, the developers created a system which will help to lessen this problem by monitoring the network with a scanner that network administrators can use to locate the active ports, a system that can map the up and downs host and detect data allowed by the firewall. The system also aims to lessen the reports of malicious activities happening in a specific network where several people created tunnels and pathway from outside causing damages not only to data and department but also to one’s company name. The developers hope that after this system has been used and deploy into several system, it can prove that a small system can solve a huge crime within the cyber world.

**RECOMMENDATIONS**

The NetSec Manager was developed based on a theory that there exists a behavior in each and every network activity – either malicious or not. It has the capability to detect some of the malicious activities and the common attacks; scan packets passing through the network; map the network through the up and down hosts, and open and closed ports; and save logs to the database. The NetSec Manager used two third party applications, namely NMap and Snort, in order to produce more accurate results. The system was created using Python 2.7.11 and Visual Basic, and tested in Windows 8/8.1/10 operating systems. The logs were saved in MySQL database using XAMPP. Since this program focuses on network analysis, As per NetSec Manager operations, the possible beneficiaries of the system are the network and security administrator since the main features of this system is about scanning the network, generating scan results for monitoring, advising mitigation for common network attacks, intrusion detection system that will detect data allowed by the firewall and the event viewer which will display the processes in the terminal. Other beneficiaries may be the IT specialist who is also aware of this features.

**SYSTEM DIAGRAMS**

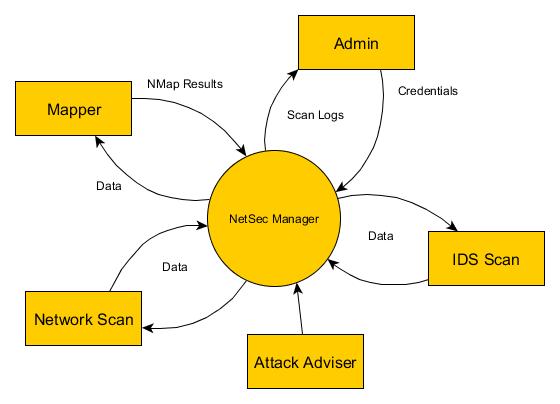
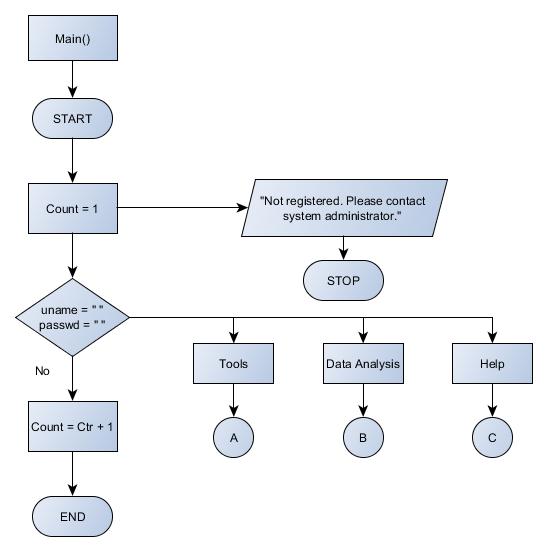


Figure 1: Conceptual Diagram

The Administrator will input his credentials (username and password) to operate the system. Once the system validated the credentials the administrator will be given four options: IDS scan, view the Attack Adviser, to scan the network, and Mapper to create a map of the network. If the administrator choose the IDS Scan, the snort will start scanning. If the administrator choose the Attack Adviser, it will display the attack adviser document. If the administrator choose to scan the network, NetSec Manager will start scanning the network while fetching the data, once the result is provided, the result will be saved to the database for documentation purposes. And if the administrator choose the Mapper, it will start mapping the IP Address.

Figure 2: Main Program of NetSec Manager

In figure 2. The main program of NetSec Manager is explained via program flowchart. Starting from the login menu, the administrator is given 3 times to enter his credentials. If the credentials is correct, NetSec Manager will redirect to the main menu consist of the 3 different modules: Tools, Data Analysis and Help. If the credentials did not match the credentials in the database, the system will prompt a display message regarding the error.

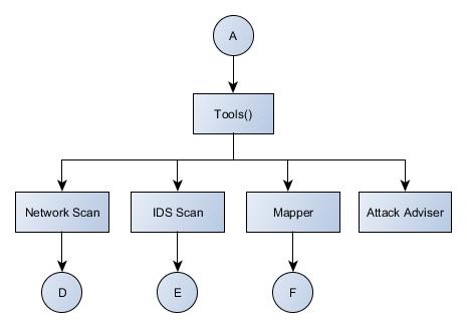


Figure 2.1: Tools module of the NetSec Manager

In figure 2.1, The Tool modules is expanded. Under the Tool module, the Network Scan, IDS Scan, Mapper and Attack Adviser module is located. This module is the one responsible in scanning the network, detecting the rules set in the network together with the data allowed by the firewall, the active and inactive host in the network, and the countermeasures for common network attacks. This modules is also connected to the system database for the generating of logs.

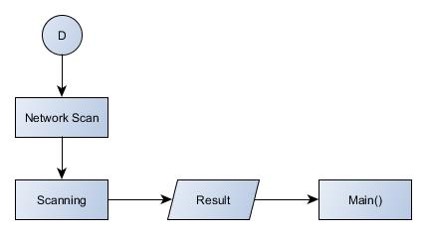


Figure 2.2: Network Scan module of the NetSec Manager

In figure 2.2, The Network Scan module is expanded. This module is the main feature of NetSec Manager. Once the scanning is initiated, the results of the scanning is automatically saved in the NetSec Manager database.

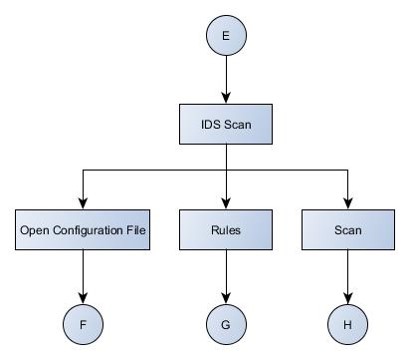


Figure 2.3: IDS Scan module of the NetSec Manager

In this figure, the IDS Scan module is expanded. IDS Scan module is composes of 3 sub modules, the Open Configuration File module, the IDS Rule module and the Start Scan module. The Open Configuration File display the Snort configuration file for minor settings regarding the program, IDS Rule display the different Snort rules where the administration can set his/her own rules for managing the network, lastly the Scan tab triggers the start of the network scan.

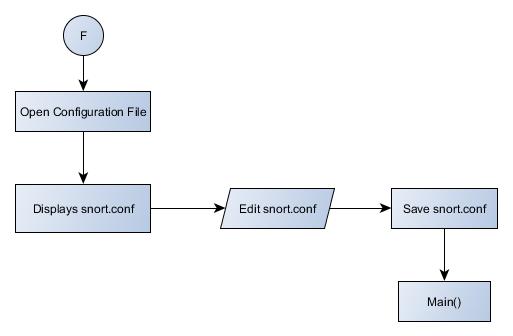


Figure 2.4: Open Configuration file module of the NetSec Manager

In this figure, the Open Configuration File module is expanded. In this module, the administrator can update or edit the IDS Configuration file to insert any changes he/she want to implement for the network.

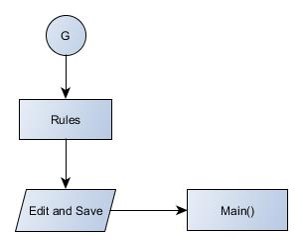


Figure 2.5: IDS Rules module of the NetSec Manager

In this figure, the list of Snort rules will be display. The administrator can view, edit and save the IDS rules that was set to be implemented in the network.

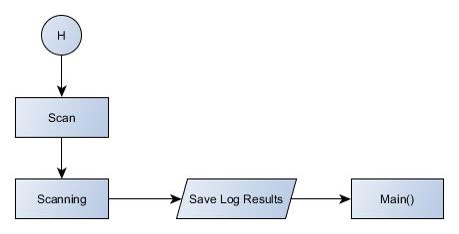


Figure 2.6: Scan Process module of the NetSec Manager

In this figure, the process of scanning the network is shown, once the administrator stops scanning the network, the results will be saved to the NetSec Manager database and the logs can be generated from the database for viewing purposes.

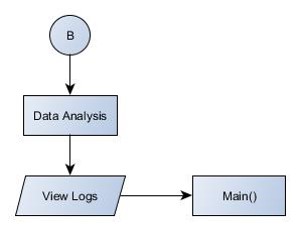


Figure 2.7: Data Analysis module of the NetSec Manager

This figure shows the expanded Data Analysis module. Under this module, the View Logs is located. View logs module contains the saved scan results fetched from the database.

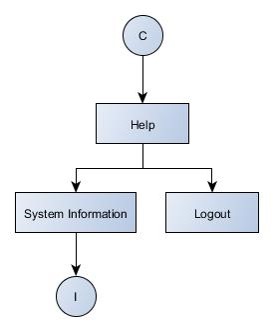


Figure 2.8 Help module of the NetSec Manager

In this figures, the Help module is expanded. The Help Module is composes of System Information which contains system requirements and the project developer profiles and the logout module.

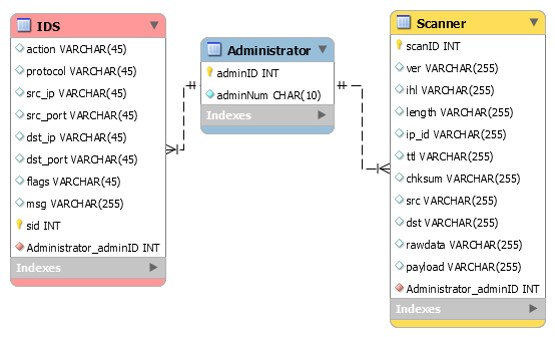


Figure 3: Entity-Relationship Diagram

NetSec Manager will use MySQL database system to generate results from Network Scan. NetSec Manager Entity Relationship Diagram composes of two tables: Administrator table that is connected to the Scanner table. Under the Administrator Table is the following attributes: Administrator ID, Administrator Number which will serve as the administrators credential in using the system. On the other hand, Scanner table contains Scan ID, IP Version, Internet Header Length, IP ID, Packet Time to Leave, Packet Checksum, Packet Source, Packet Destination, Packet Raw data, and Packet Payload and the foreign key of Administrator ID which will be gathered from the process happened in the terminal while the administrator is away.

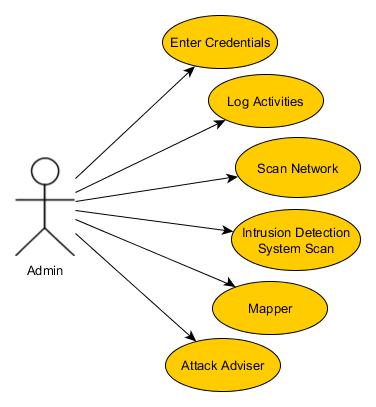


Figure 4: Unified Modeling Language

Unified Modeling Language helps the users how to visualize the design of a system. In this figure, the proponents shows the relationship of the administrator to the NetSec Manager features. The Administrator is the actor while the features is the use case. NetSec can be visualize with this UML since our system focuses on the use of the network and security administrator.

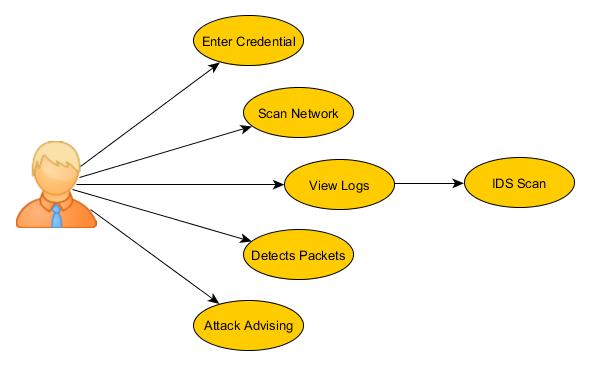


Figure 5: Use Case Diagram

The figure shows the use case diagram of NetSec. This shows the capability of the administrator in using the system. Once the network administrator has entered his/her credentials, through NetSec, he/she has the capability to sniff the network, view logs from the IDS scan, detects packets behavior through the IDS, and view attack advising.

**PROJECT MODULE SCREENSHOTS**

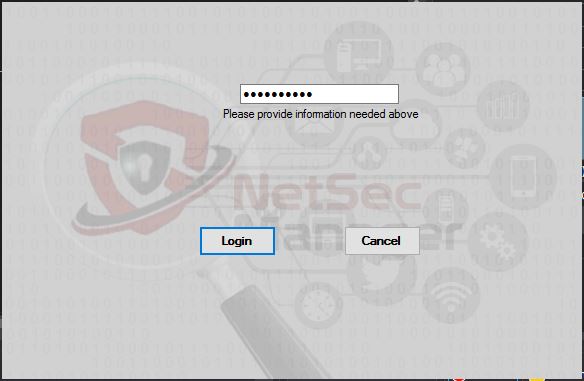


Figure 6: Screen Layout for Login Interface

This is the login screen layout of the NetSec Manager. In the input box, the network administrator will have to enter the given authentication key to be able to log-in and use the system. The administrator will be given two options, The Log-in and Cancel Button. Clicking the log-in button will give the network administrator access to the whole feature of the system. And clicking on cancel button will terminate the log-in screen.

****

Figure 6.1: Screen Layout for Main Menu

After the administrator has enter his credentials and authenticated in the database, the main menu screen layout will appear. On the upper left part is the 3 main modules of the system. Under the tools module are Network Scanner, IDS Scan, Mapper and Attack Adviser which consist of different process. In the data analysis module, the network administrator can be able to view the logs captured under the Network Scanner module. And under the Help module, the network administrator can either view the System Information and the log-out button of the system.

Figure 6.2: Screen Layout for Network Scanner



After the network administrator clicked on the Sniffer shown above, the scanning of network begins. The process can only be stop manually by the admin. While scanning, the process of scanning the network can be view as like the given figure above.

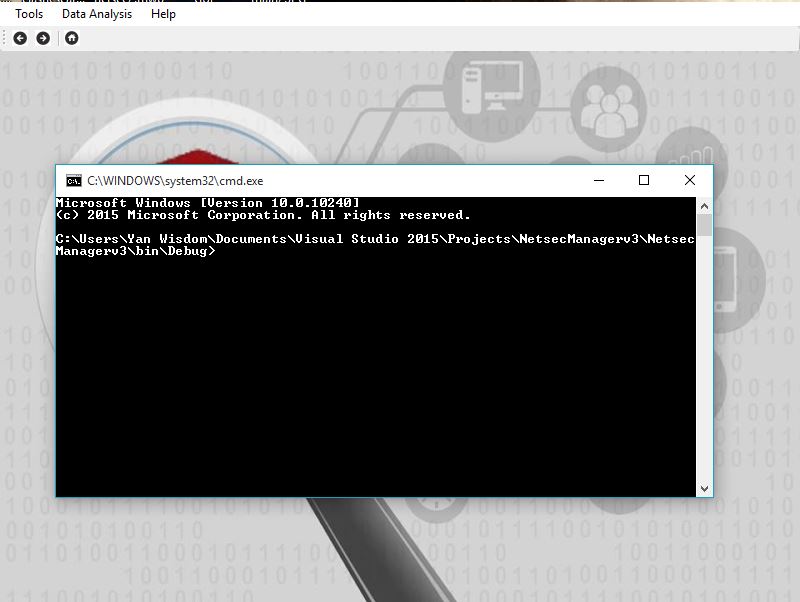
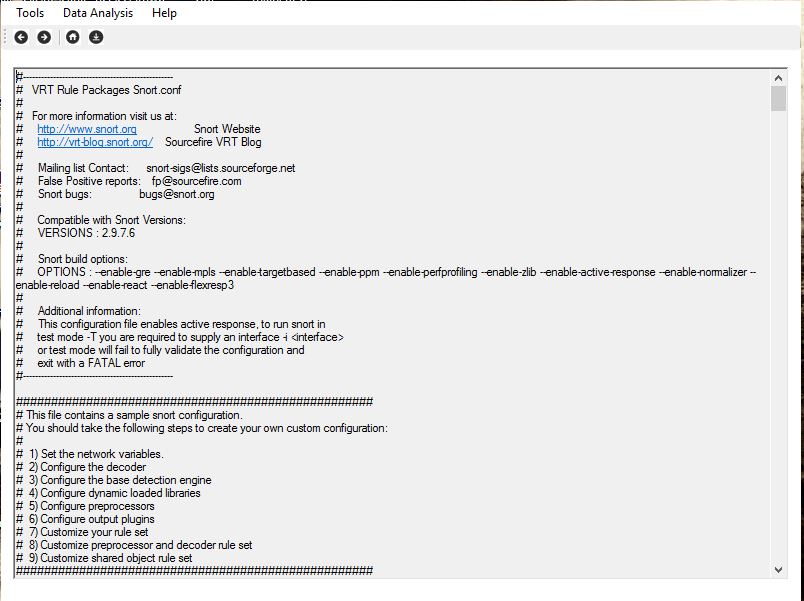


Figure 6.3: Screen Layout for IDS Scan

After clicking on Start Scan inside the IDS Scan, the command line screen will pop out and automatically starts scanning. The process of scanning the network can be view as like the given figure above.

Figure 6.4: Screen Layout for Open Configuration File

Clicking on the Open Configuration File opens the IDS configuration file in a text editor, where the network administrator will be able to set the rules he or she wants to enable, the speed of the scan, and the behavior of the IDS itself – on how to run in the network.

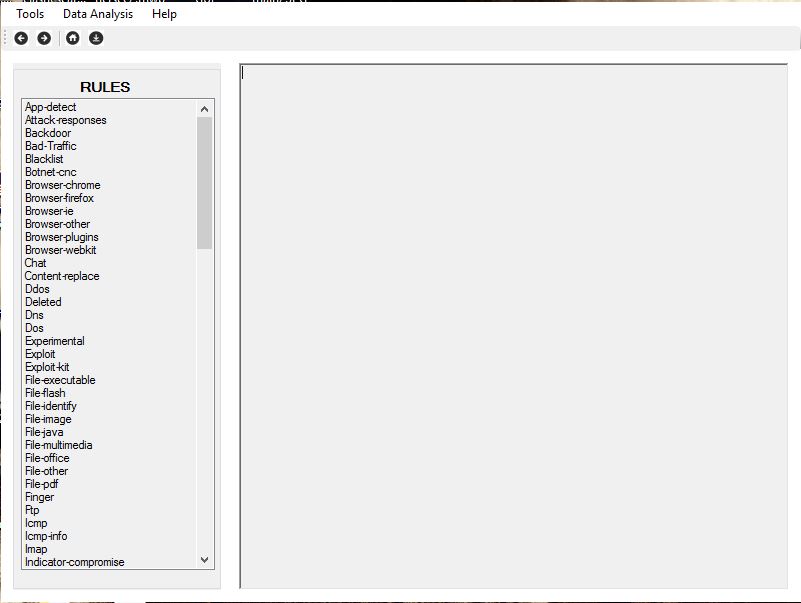


Figure 6.5: Screen Layout for Rules

When the administrator clicks the Rules module, it will automatically open the list of the Snort rule saved in the terminal. Then the administrator has the capability to view, edit and save the following rules.

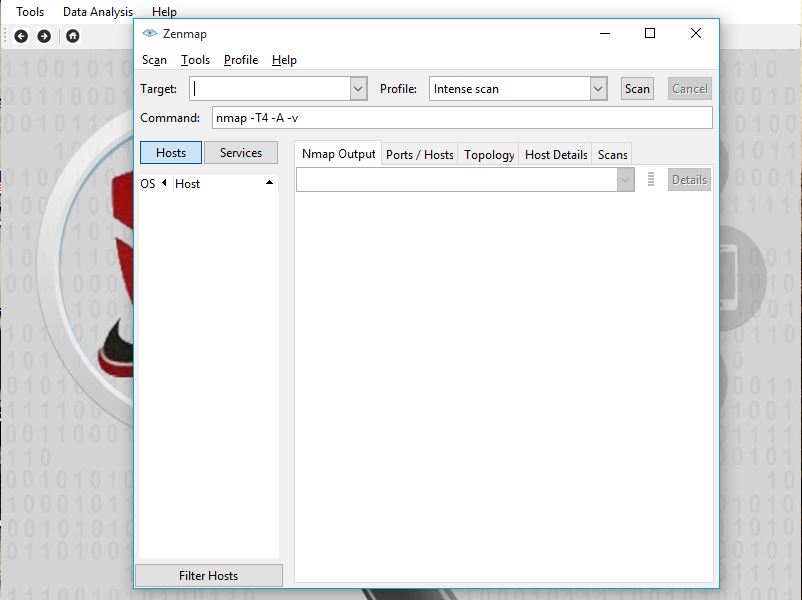
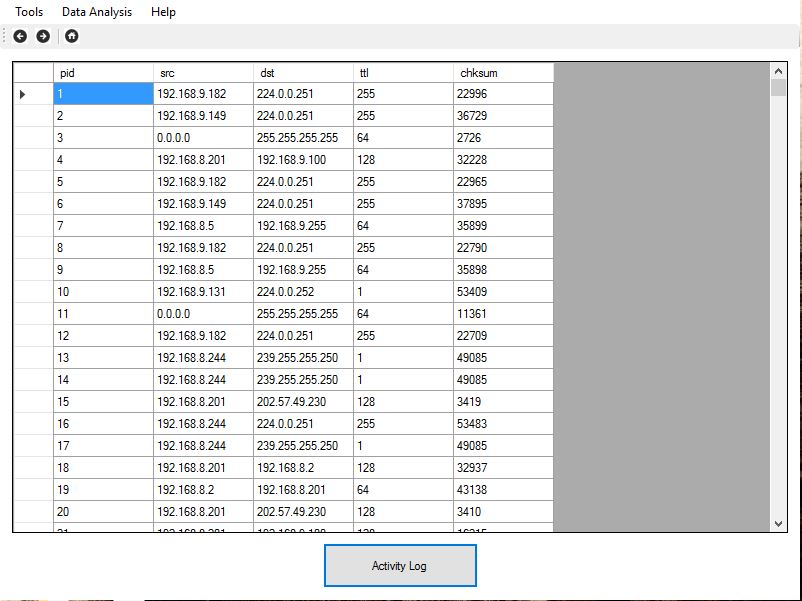
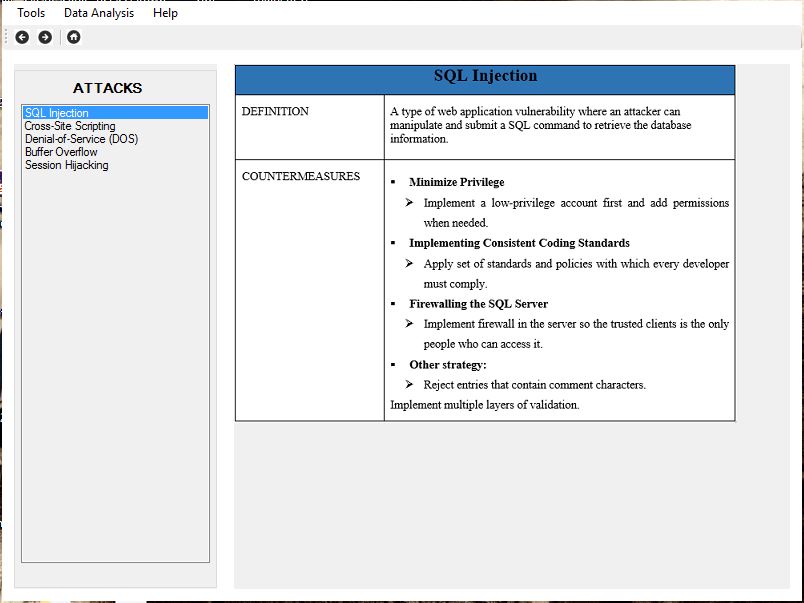


Figure 6.6: Screen Layout for Mapper

After clicking on Mapper under Tools Module, the Zenmap GUI Interface will pop out and ask the administrator what is the target IP Address and Scan Type. The process of networking mapping can be view as like the given figure above.

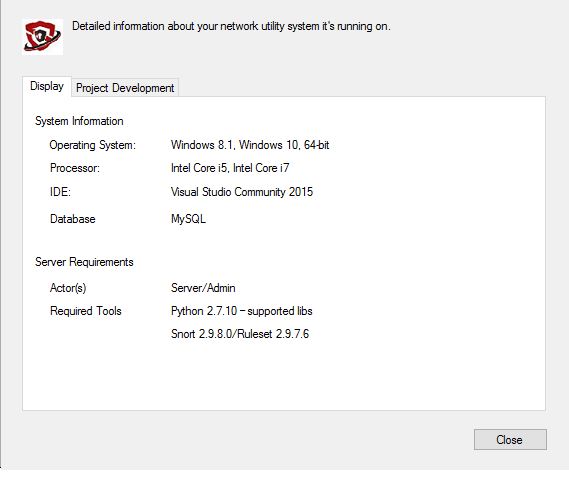
Figure 6.7: Screen Layout for Data Analysis

When the administrator clicks the Data Analysis button, data saved in the database will then be viewed in this interface. He or she will be able to view the logs generated during the network scan. Inside the generated data is the listed pid which is the generated Packet ID, While the src is the source ip and dst is the destination, Time to live (ttl) is for the packet to reach its destination, Lastly the chksum protects the header of IPv4 data packets against data corruption.

Figure 6.8: Screen Layout for Attack Adviser

The network administrator can seek help on how to mitigate common network attacks by clicking the Attack Adviser module. This contains the name of the attack, the definition, and the countermeasures in order to mitigate the said attack.

****Figure 6.9: Screen Layout for Help Module



When the administrator clicks the Help Module, two sub-menus will be displayed; System Information which contains a tab menu displaying the system and server requirements for the installation of the NetSec Manager. The other module is the logout button which will end the administrator’s session once clicked.

**SOURCE CODE LISTING**

1. **LOGIN MODULE**

//Form1 source code that is connected to mysql database.

Imports MySql.Data.MySqlClient

Public Class Form1

Dim conn As New MySqlConnection

Dim sql As MySqlCommand

Public Sub connect()

Dim dbname As String = "netsec2"

Dim server As String = "localhost"

Dim username As String = "root"

Dim password As String = ""

If Not conn Is Nothing Then conn.Close()

conn.ConnectionString = String.Format("server={0}; user id={1}; password={2}; database={3}; pooling=False", server, username, password, dbname)

Dim dbreader As MySqlDataReader

Try

conn.Open()

Dim Query As String

Query = "select \* from admin where AdminNum ='" & TextBox1.Text & "' "

sql = New MySqlCommand(Query, conn)

dbreader = sql.ExecuteReader

Dim count As Integer

count = 0

While dbreader.Read

count = count + 1

End While

If count = 1 Then

Form2.Show()

Me.Hide()

Else

MsgBox("Not registered. Please contact system administrator.")

End If

conn.Close()

Catch ex As MySqlException

MsgBox(ex.Message)

End Try

End Sub

Private Sub Button1\_Click(sender As Object, e As EventArgs) Handles Button1.Click

connect()

End Sub

Private Sub Button2\_Click(sender As Object, e As EventArgs) Handles Button2.Click

Me.Close()

End Sub

Private Sub Label2\_Click(sender As Object, e As EventArgs) Handles Label2.Click

End Sub

End Class

1. **MAIN MENU MODULE**

//Form2 source code that shows the main menu.

Public Class Form2

Private Sub DataAnalysisToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles DataAnalysisToolStripMenuItem.Click

Form3.Show()

Me.Close()

End Sub

Private Sub AttackAdviserToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles AttackAdviserToolStripMenuItem.Click

Form4.Show()

Me.Close()

End Sub

Private Sub RulesToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles RulesToolStripMenuItem.Click

Form5.Show()

Me.Close()

End Sub

Private Sub SystemInformationToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SystemInformationToolStripMenuItem.Click

Form6.Show()

End Sub

Private Sub OpenConfigurationFileToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles OpenConfigurationFileToolStripMenuItem.Click

Form7.Show()

Me.Close()

End Sub

Private Sub NmapCheatSheetToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapCheatSheetToolStripMenuItem.Click

Form8.Show()

Me.Close()

End Sub

Private Sub LogOutToolStripMenuitem\_Click(sender As Object, e As EventArgs) Handles LogOutToolStripMenuItem.Click

MsgBox("Thank you for using NetSec Manager", MsgBoxStyle.Information, "NetSec Manager: Log Out")

Form1.Show()

Me.Close()

End Sub

Private Sub NmapToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\nmap.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub StartScanToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles StartScanToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\cmd.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub SnifferToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SnifferToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\sniff\dist\scan.exe")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub Form2\_Load(sender As Object, e As EventArgs) Handles MyBase.Load

End Sub

End Class

1. **DATA ANALYSIS MODULE**

//Form3 source code shows the data analysis.

Imports MySql.Data.MySqlClient

Public Class Form3

Dim conn As MySqlConnection

Dim myCommand As New MySqlCommand

Dim myAdapter As New MySqlDataAdapter

Dim myData As New DataTable

Dim SQL As String

Private Sub HomeButton\_Click(sender As Object, e As EventArgs) Handles HomeButton.Click

Form2.Show()

Me.Close()

End Sub

Private Sub AttackAdviserToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles AttackAdviserToolStripMenuItem.Click

Form4.Show()

Me.Close()

End Sub

Private Sub RulesToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles RulesToolStripMenuItem.Click

Form5.Show()

Me.Close()

End Sub

Private Sub SystemInformationToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SystemInformationToolStripMenuItem.Click

Form6.Show()

End Sub

Private Sub OpenConfigurationFileToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles OpenConfigurationFileToolStripMenuItem.Click

Form7.Show()

Me.Close()

End Sub

Private Sub NmapCheatSheetToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapCheatSheetToolStripMenuItem.Click

Form8.Show()

Me.Close()

End Sub

Private Sub LogOutToolStripMenuitem\_Click(sender As Object, e As EventArgs) Handles LogOutToolStripMenuItem.Click

MsgBox("Thank you for using NetSec Manager", MsgBoxStyle.Information, "NetSec Manager: Log Out")

Form1.Show()

Me.Close()

End Sub

Private Sub NmapToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\nmap.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub StartScanToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles StartScanToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\cmd.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub SnifferToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SnifferToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\sniff\dist\scan.exe")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub DataGridView1\_CellContentClick(sender As Object, e As DataGridViewCellEventArgs) Handles DataGridView1.CellContentClick

End Sub

Private Sub Button1\_Click(sender As Object, e As EventArgs)

End Sub

Private Sub Button2\_Click(sender As Object, e As EventArgs)

End Sub

Private Sub Button1\_Click\_1(sender As Object, e As EventArgs) Handles Button1.Click

conn = New MySqlConnection()

SQL = "SELECT pid, src, dst, ttl, chksum FROM sniff"

'Connection String

conn.ConnectionString = "server=localhost;" \_

& "user id=root;" \_

& "password=;" \_

& "database=netsec"

Try

conn.Open()

myCommand.Connection = conn

myCommand.CommandText = SQL

myAdapter.SelectCommand = myCommand

myAdapter.Fill(myData)

DataGridView1.DataSource = myData

Catch ex As MySqlException

MessageBox.Show("Cannot connect to db" & ex.Message)

Finally

conn.Close()

conn.Dispose()

End Try

End Sub

End Class

1. **ATTACK ADVISER MODULE**

//Form4 source code shows the attack adviser.

Public Class Form4

Private Sub HomeButton\_Click(sender As Object, e As EventArgs) Handles HomeButton.Click

Form2.Show()

Me.Close()

End Sub

Private Sub DataAnalysisToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles DataAnalysisToolStripMenuItem.Click

Form3.Show()

Me.Close()

End Sub

Private Sub RulesToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles RulesToolStripMenuItem.Click

Form5.Show()

Me.Close()

End Sub

Private Sub SystemInformationToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SystemInformationToolStripMenuItem.Click

Form6.Show()

End Sub

Private Sub ListBox1\_SelectedIndexChanged(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles ListBox1.SelectedIndexChanged

Select Case ListBox1.SelectedIndex

Case 0

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Attacks (printscreen)\SQL Injection.PNG")

Case 1

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Attacks (printscreen)\Cross-Site Scripting.PNG")

Case 2

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Attacks (printscreen)\Denial-of-Service.PNG")

Case 3

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Attacks (printscreen)\Buffer overflow.PNG")

Case 4

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Attacks (printscreen)\Session hijacking.PNG")

End Select

End Sub

Private Sub OpenConfigurationFileToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles OpenConfigurationFileToolStripMenuItem.Click

Form7.Show()

Me.Close()

End Sub

Private Sub NmapCheatSheetToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapCheatSheetToolStripMenuItem.Click

Form8.Show()

Me.Close()

End Sub

Private Sub LogOutToolStripMenuitem\_Click(sender As Object, e As EventArgs) Handles LogOutToolStripMenuItem.Click

MsgBox("Thank you for using NetSec Manager", MsgBoxStyle.Information, "NetSec Manager: Log Out")

Form1.Show()

Me.Close()

End Sub

Private Sub NmapToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\nmap.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub StartScanToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles StartScanToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\cmd.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub SnifferToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SnifferToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\sniff\dist\scan.exe")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub PictureBox1\_Click(sender As Object, e As EventArgs) Handles PictureBox1.Click

PictureBox1.SizeMode = PictureBoxSizeMode.StretchImage

End Sub

End Class

1. **RULES MODULE**

//Form5 source code shows the rules –snor.conf.

Public Class Form5

Private Sub HomeButton\_Click(sender As Object, e As EventArgs) Handles HomeButton.Click

Form2.Show()

Me.Close()

End Sub

Private Sub DataAnalysisToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles DataAnalysisToolStripMenuItem.Click

Form3.Show()

Me.Close()

End Sub

Private Sub AttackAdviserToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles AttackAdviserToolStripMenuItem.Click

Form4.Show()

Me.Close()

End Sub

Private Sub SystemInformationToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SystemInformationToolStripMenuItem.Click

Form6.Show()

End Sub

Private Sub ListBox1\_SelectedIndexChanged(sender As Object, e As EventArgs) Handles ListBox1.SelectedIndexChanged

Select Case ListBox1.SelectedIndex

Case 0

RichTextBox1.LoadFile("C:\Snort\rules\app-detect.rules", RichTextBoxStreamType.PlainText)

Case 1

RichTextBox1.LoadFile("C:\Snort\rules\attack-responses.rules", RichTextBoxStreamType.PlainText)

Case 2

RichTextBox1.LoadFile("C:\Snort\rules\backdoor.rules", RichTextBoxStreamType.PlainText)

Case 3

RichTextBox1.LoadFile("C:\Snort\rules\bad-traffic.rules", RichTextBoxStreamType.PlainText)

Case 4

RichTextBox1.LoadFile("C:\Snort\rules\blacklist.rules", RichTextBoxStreamType.PlainText)

Case 5

RichTextBox1.LoadFile("C:\Snort\rules\botnet-cnc.rules", RichTextBoxStreamType.PlainText)

Case 6

RichTextBox1.LoadFile("C:\Snort\rules\browser-chrome.rules", RichTextBoxStreamType.PlainText)

Case 7

RichTextBox1.LoadFile("C:\Snort\rules\browser-firefox.rules", RichTextBoxStreamType.PlainText)

Case 8

RichTextBox1.LoadFile("C:\Snort\rules\browser-ie.rules", RichTextBoxStreamType.PlainText)

Case 9

RichTextBox1.LoadFile("C:\Snort\rules\browser-other.rules", RichTextBoxStreamType.PlainText)

Case 10

RichTextBox1.LoadFile("C:\Snort\rules\browser-plugins.rules", RichTextBoxStreamType.PlainText)

Case 11

RichTextBox1.LoadFile("C:\Snort\rules\browser-webkit.rules", RichTextBoxStreamType.PlainText)

Case 12

RichTextBox1.LoadFile("C:\Snort\rules\chat.rules", RichTextBoxStreamType.PlainText)

Case 13

RichTextBox1.LoadFile("C:\Snort\rules\content-replace.rules", RichTextBoxStreamType.PlainText)

Case 14

RichTextBox1.LoadFile("C:\Snort\rules\ddos.rules", RichTextBoxStreamType.PlainText)

Case 15

RichTextBox1.LoadFile("C:\Snort\rules\deleted.rules", RichTextBoxStreamType.PlainText)

Case 16

RichTextBox1.LoadFile("C:\Snort\rules\dns.rules", RichTextBoxStreamType.PlainText)

Case 17

RichTextBox1.LoadFile("C:\Snort\rules\dos.rules", RichTextBoxStreamType.PlainText)

Case 18

RichTextBox1.LoadFile("C:\Snort\rules\experimental.rules", RichTextBoxStreamType.PlainText)

Case 19

RichTextBox1.LoadFile("C:\Snort\rules\exploit.rules", RichTextBoxStreamType.PlainText)

Case 20

RichTextBox1.LoadFile("C:\Snort\rules\exploit-kit.rules", RichTextBoxStreamType.PlainText)

Case 21

RichTextBox1.LoadFile("C:\Snort\rules\file-executable.rules", RichTextBoxStreamType.PlainText)

Case 22

RichTextBox1.LoadFile("C:\Snort\rules\file-flash.rules", RichTextBoxStreamType.PlainText)

Case 23

RichTextBox1.LoadFile("C:\Snort\rules\file-identify.rules", RichTextBoxStreamType.PlainText)

Case 24

RichTextBox1.LoadFile("C:\Snort\rules\file-image.rules", RichTextBoxStreamType.PlainText)

Case 25

RichTextBox1.LoadFile("C:\Snort\rules\file-java.rules", RichTextBoxStreamType.PlainText)

Case 26

RichTextBox1.LoadFile("C:\Snort\rules\file-multimedia.rules", RichTextBoxStreamType.PlainText)

Case 27

RichTextBox1.LoadFile("C:\Snort\rules\file-office.rules", RichTextBoxStreamType.PlainText)

Case 28

RichTextBox1.LoadFile("C:\Snort\rules\file-other.rules", RichTextBoxStreamType.PlainText)

Case 29

RichTextBox1.LoadFile("C:\Snort\rules\file-pdf.rules", RichTextBoxStreamType.PlainText)

Case 30

RichTextBox1.LoadFile("C:\Snort\rules\finger.rules", RichTextBoxStreamType.PlainText)

Case 31

RichTextBox1.LoadFile("C:\Snort\rules\fpt.rules", RichTextBoxStreamType.PlainText)

Case 32

RichTextBox1.LoadFile("C:\Snort\rules\icmp.rules", RichTextBoxStreamType.PlainText)

Case 33

RichTextBox1.LoadFile("C:\Snort\rules\icmp-info.rules", RichTextBoxStreamType.PlainText)

Case 34

RichTextBox1.LoadFile("C:\Snort\rules\imap.rules", RichTextBoxStreamType.PlainText)

Case 35

RichTextBox1.LoadFile("C:\Snort\rules\indicator-compromise.rules", RichTextBoxStreamType.PlainText)

Case 36

RichTextBox1.LoadFile("C:\Snort\rules\indicator-obfuscation.rules", RichTextBoxStreamType.PlainText)

Case 37

RichTextBox1.LoadFile("C:\Snort\rules\indicator-scan.rules", RichTextBoxStreamType.PlainText)

Case 38

RichTextBox1.LoadFile("C:\Snort\rules\indicator-shellcode.rules", RichTextBoxStreamType.PlainText)

Case 39

RichTextBox1.LoadFile("C:\Snort\rules\info.rules", RichTextBoxStreamType.PlainText)

Case 40

RichTextBox1.LoadFile("C:\Snort\rules\local.rules", RichTextBoxStreamType.PlainText)

Case 41

RichTextBox1.LoadFile("C:\Snort\rules\malware-backdoor.rules", RichTextBoxStreamType.PlainText)

Case 42

RichTextBox1.LoadFile("C:\Snort\rules\malware-cnc.rules", RichTextBoxStreamType.PlainText)

Case 43

RichTextBox1.LoadFile("C:\Snort\rules\malware-other.rules", RichTextBoxStreamType.PlainText)

Case 44

RichTextBox1.LoadFile("C:\Snort\rules\malware-tools.rules", RichTextBoxStreamType.PlainText)

Case 45

RichTextBox1.LoadFile("C:\Snort\rules\misc.rules", RichTextBoxStreamType.PlainText)

Case 46

RichTextBox1.LoadFile("C:\Snort\rules\multimedia.rules", RichTextBoxStreamType.PlainText)

Case 47

RichTextBox1.LoadFile("C:\Snort\rules\mysql.rules", RichTextBoxStreamType.PlainText)

Case 48

RichTextBox1.LoadFile("C:\Snort\rules\netbios.rules", RichTextBoxStreamType.PlainText)

Case 49

RichTextBox1.LoadFile("C:\Snort\rules\nntp.rules", RichTextBoxStreamType.PlainText)

Case 50

RichTextBox1.LoadFile("C:\Snort\rules\oracle.rules", RichTextBoxStreamType.PlainText)

Case 51

RichTextBox1.LoadFile("C:\Snort\rules\os-linux.rules", RichTextBoxStreamType.PlainText)

Case 52

RichTextBox1.LoadFile("C:\Snort\rules\os-mobile.rules", RichTextBoxStreamType.PlainText)

Case 53

RichTextBox1.LoadFile("C:\Snort\rules\os-other.rules", RichTextBoxStreamType.PlainText)

Case 54

RichTextBox1.LoadFile("C:\Snort\rules\os-solaris.rules", RichTextBoxStreamType.PlainText)

Case 55

RichTextBox1.LoadFile("C:\Snort\rules\os-windows.rules", RichTextBoxStreamType.PlainText)

Case 56

RichTextBox1.LoadFile("C:\Snort\rules\other-ids.rules", RichTextBoxStreamType.PlainText)

Case 57

RichTextBox1.LoadFile("C:\Snort\rules\p2p.rules", RichTextBoxStreamType.PlainText)

Case 58

RichTextBox1.LoadFile("C:\Snort\rules\phishing-spam.rules", RichTextBoxStreamType.PlainText)

Case 59

RichTextBox1.LoadFile("C:\Snort\rules\policy.rules", RichTextBoxStreamType.PlainText)

Case 60

RichTextBox1.LoadFile("C:\Snort\rules\policy-multimedia.rules", RichTextBoxStreamType.PlainText)

Case 61

RichTextBox1.LoadFile("C:\Snort\rules\policy-other.rules", RichTextBoxStreamType.PlainText)

Case 62

RichTextBox1.LoadFile("C:\Snort\rules\policy-social.rules", RichTextBoxStreamType.PlainText)

Case 63

RichTextBox1.LoadFile("C:\Snort\rules\policy-spam.rules", RichTextBoxStreamType.PlainText)

Case 64

RichTextBox1.LoadFile("C:\Snort\rules\pop2.rules", RichTextBoxStreamType.PlainText)

Case 65

RichTextBox1.LoadFile("C:\Snort\rules\pop3.rules", RichTextBoxStreamType.PlainText)

Case 66

RichTextBox1.LoadFile("C:\Snort\rules\protocol-dns.rules", RichTextBoxStreamType.PlainText)

Case 67

RichTextBox1.LoadFile("C:\Snort\rules\protocol-finger.rules", RichTextBoxStreamType.PlainText)

Case 68

RichTextBox1.LoadFile("C:\Snort\rules\protocol-ftp.rules", RichTextBoxStreamType.PlainText)

Case 69

RichTextBox1.LoadFile("C:\Snort\rules\protocol-icmp.rules", RichTextBoxStreamType.PlainText)

Case 70

RichTextBox1.LoadFile("C:\Snort\rules\protocol-imap.rules", RichTextBoxStreamType.PlainText)

Case 71

RichTextBox1.LoadFile("C:\Snort\rules\protocol-nntp.rules", RichTextBoxStreamType.PlainText)

Case 72

RichTextBox1.LoadFile("C:\Snort\rules\protocol-other.rules", RichTextBoxStreamType.PlainText)

Case 73

RichTextBox1.LoadFile("C:\Snort\rules\protocol-pop.rules", RichTextBoxStreamType.PlainText)

Case 74

RichTextBox1.LoadFile("C:\Snort\rules\protocol-rpc.rules", RichTextBoxStreamType.PlainText)

Case 75

RichTextBox1.LoadFile("C:\Snort\rules\protocol-scada.rules", RichTextBoxStreamType.PlainText)

Case 76

RichTextBox1.LoadFile("C:\Snort\rules\protocol-services.rules", RichTextBoxStreamType.PlainText)

Case 77

RichTextBox1.LoadFile("C:\Snort\rules\protocol-snmp.rules", RichTextBoxStreamType.PlainText)

Case 78

RichTextBox1.LoadFile("C:\Snort\rules\protocol-telnet.rules", RichTextBoxStreamType.PlainText)

Case 79

RichTextBox1.LoadFile("C:\Snort\rules\protocol-tftp.rules", RichTextBoxStreamType.PlainText)

Case 80

RichTextBox1.LoadFile("C:\Snort\rules\protocol-voip.rules", RichTextBoxStreamType.PlainText)

Case 81

RichTextBox1.LoadFile("C:\Snort\rules\pua-adware.rules", RichTextBoxStreamType.PlainText)

Case 82

RichTextBox1.LoadFile("C:\Snort\rules\pua-other.rules", RichTextBoxStreamType.PlainText)

Case 83

RichTextBox1.LoadFile("C:\Snort\rules\pua-p2p.rules", RichTextBoxStreamType.PlainText)

Case 84

RichTextBox1.LoadFile("C:\Snort\rules\pua-toolbars.rules", RichTextBoxStreamType.PlainText)

Case 85

RichTextBox1.LoadFile("C:\Snort\rules\rpc.rules", RichTextBoxStreamType.PlainText)

Case 86

RichTextBox1.LoadFile("C:\Snort\rules\rservices.rules", RichTextBoxStreamType.PlainText)

Case 87

RichTextBox1.LoadFile("C:\Snort\rules\scada.rules", RichTextBoxStreamType.PlainText)

Case 88

RichTextBox1.LoadFile("C:\Snort\rules\scan.rules", RichTextBoxStreamType.PlainText)

Case 89

RichTextBox1.LoadFile("C:\Snort\rules\server-apache.rules", RichTextBoxStreamType.PlainText)

Case 90

RichTextBox1.LoadFile("C:\Snort\rules\server-iis.rules", RichTextBoxStreamType.PlainText)

Case 91

RichTextBox1.LoadFile("C:\Snort\rules\server-mail.rules", RichTextBoxStreamType.PlainText)

Case 92

RichTextBox1.LoadFile("C:\Snort\rules\server-mssql.rules", RichTextBoxStreamType.PlainText)

Case 93

RichTextBox1.LoadFile("C:\Snort\rules\server-mysql.rules", RichTextBoxStreamType.PlainText)

Case 94

RichTextBox1.LoadFile("C:\Snort\rules\server-oracle.rules", RichTextBoxStreamType.PlainText)

Case 95

RichTextBox1.LoadFile("C:\Snort\rules\server-other.rules", RichTextBoxStreamType.PlainText)

Case 96

RichTextBox1.LoadFile("C:\Snort\rules\server-samba.rules", RichTextBoxStreamType.PlainText)

Case 97

RichTextBox1.LoadFile("C:\Snort\rules\server-webapp.rules", RichTextBoxStreamType.PlainText)

Case 98

RichTextBox1.LoadFile("C:\Snort\rules\shellcode.rules", RichTextBoxStreamType.PlainText)

Case 99

RichTextBox1.LoadFile("C:\Snort\rules\smtp.rules", RichTextBoxStreamType.PlainText)

Case 100

RichTextBox1.LoadFile("C:\Snort\rules\snmp.rules", RichTextBoxStreamType.PlainText)

Case 101

RichTextBox1.LoadFile("C:\Snort\rules\specific-threats.rules", RichTextBoxStreamType.PlainText)

Case 102

RichTextBox1.LoadFile("C:\Snort\rules\spyware-put.rules", RichTextBoxStreamType.PlainText)

Case 103

RichTextBox1.LoadFile("C:\Snort\rules\sql.rules", RichTextBoxStreamType.PlainText)

Case 104

RichTextBox1.LoadFile("C:\Snort\rules\telnet.rules", RichTextBoxStreamType.PlainText)

Case 105

RichTextBox1.LoadFile("C:\Snort\rules\tftp.rules", RichTextBoxStreamType.PlainText)

Case 106

RichTextBox1.LoadFile("C:\Snort\rules\virus.rules", RichTextBoxStreamType.PlainText)

Case 107

RichTextBox1.LoadFile("C:\Snort\rules\voip.rules", RichTextBoxStreamType.PlainText)

Case 108

RichTextBox1.LoadFile("C:\Snort\rules\web-activex.rules", RichTextBoxStreamType.PlainText)

Case 109

RichTextBox1.LoadFile("C:\Snort\rules\web-attacks.rules", RichTextBoxStreamType.PlainText)

Case 110

RichTextBox1.LoadFile("C:\Snort\rules\web-cgi.rules", RichTextBoxStreamType.PlainText)

Case 111

RichTextBox1.LoadFile("C:\Snort\rules\web-client.rules", RichTextBoxStreamType.PlainText)

Case 112

RichTextBox1.LoadFile("C:\Snort\rules\web-coldfusion.rules", RichTextBoxStreamType.PlainText)

Case 113

RichTextBox1.LoadFile("C:\Snort\rules\web-frontpage.rules", RichTextBoxStreamType.PlainText)

Case 114

RichTextBox1.LoadFile("C:\Snort\rules\web-iis.rules", RichTextBoxStreamType.PlainText)

Case 115

RichTextBox1.LoadFile("C:\Snort\rules\web-misc.rules", RichTextBoxStreamType.PlainText)

Case 116

RichTextBox1.LoadFile("C:\Snort\rules\web-php.rules", RichTextBoxStreamType.PlainText)

Case 117

RichTextBox1.LoadFile("C:\Snort\rules\x11.rules", RichTextBoxStreamType.PlainText)

End Select

End Sub

Private Sub SaveButton\_Click(sender As Object, e As EventArgs) Handles SaveButton.Click

Select Case ListBox1.SelectedIndex

Case 0

RichTextBox1.SaveFile("C:\Snort\rules\app-detect.rules", RichTextBoxStreamType.PlainText)

Case 1

RichTextBox1.SaveFile("C:\Snort\rules\attack-responses.rules", RichTextBoxStreamType.PlainText)

Case 2

RichTextBox1.SaveFile("C:\Snort\rules\backdoor.rules", RichTextBoxStreamType.PlainText)

Case 3

RichTextBox1.SaveFile("C:\Snort\rules\bad-traffic.rules", RichTextBoxStreamType.PlainText)

Case 4

RichTextBox1.SaveFile("C:\Snort\rules\blacklist.rules", RichTextBoxStreamType.PlainText)

Case 5

RichTextBox1.SaveFile("C:\Snort\rules\botnet-cnc.rules", RichTextBoxStreamType.PlainText)

Case 6

RichTextBox1.SaveFile("C:\Snort\rules\browser-chrome.rules", RichTextBoxStreamType.PlainText)

Case 7

RichTextBox1.SaveFile("C:\Snort\rules\browser-firefox.rules", RichTextBoxStreamType.PlainText)

Case 8

RichTextBox1.SaveFile("C:\Snort\rules\browser-ie.rules", RichTextBoxStreamType.PlainText)

Case 9

RichTextBox1.SaveFile("C:\Snort\rules\browser-other.rules", RichTextBoxStreamType.PlainText)

Case 10

RichTextBox1.SaveFile("C:\Snort\rules\browser-plugins.rules", RichTextBoxStreamType.PlainText)

Case 11

RichTextBox1.SaveFile("C:\Snort\rules\browser-webkit.rules", RichTextBoxStreamType.PlainText)

Case 12

RichTextBox1.SaveFile("C:\Snort\rules\chat.rules", RichTextBoxStreamType.PlainText)

Case 13

RichTextBox1.SaveFile("C:\Snort\rules\content-replace.rules", RichTextBoxStreamType.PlainText)

Case 14

RichTextBox1.SaveFile("C:\Snort\rules\ddos.rules", RichTextBoxStreamType.PlainText)

Case 15

RichTextBox1.SaveFile("C:\Snort\rules\deleted.rules", RichTextBoxStreamType.PlainText)

Case 16

RichTextBox1.SaveFile("C:\Snort\rules\dns.rules", RichTextBoxStreamType.PlainText)

Case 17

RichTextBox1.SaveFile("C:\Snort\rules\dos.rules", RichTextBoxStreamType.PlainText)

Case 18

RichTextBox1.SaveFile("C:\Snort\rules\experimental.rules", RichTextBoxStreamType.PlainText)

Case 19

RichTextBox1.SaveFile("C:\Snort\rules\exploit.rules", RichTextBoxStreamType.PlainText)

Case 20

RichTextBox1.SaveFile("C:\Snort\rules\exploit-kit.rules", RichTextBoxStreamType.PlainText)

Case 21

RichTextBox1.SaveFile("C:\Snort\rules\file-executable.rules", RichTextBoxStreamType.PlainText)

Case 22

RichTextBox1.SaveFile("C:\Snort\rules\file-flash.rules", RichTextBoxStreamType.PlainText)

Case 23

RichTextBox1.SaveFile("C:\Snort\rules\file-identify.rules", RichTextBoxStreamType.PlainText)

Case 24

RichTextBox1.SaveFile("C:\Snort\rules\file-image.rules", RichTextBoxStreamType.PlainText)

Case 25

RichTextBox1.SaveFile("C:\Snort\rules\file-java.rules", RichTextBoxStreamType.PlainText)

Case 26

RichTextBox1.SaveFile("C:\Snort\rules\file-multimedia.rules", RichTextBoxStreamType.PlainText)

Case 27

RichTextBox1.SaveFile("C:\Snort\rules\file-office.rules", RichTextBoxStreamType.PlainText)

Case 28

RichTextBox1.SaveFile("C:\Snort\rules\file-other.rules", RichTextBoxStreamType.PlainText)

Case 29

RichTextBox1.SaveFile("C:\Snort\rules\file-pdf.rules", RichTextBoxStreamType.PlainText)

Case 30

RichTextBox1.SaveFile("C:\Snort\rules\finger.rules", RichTextBoxStreamType.PlainText)

Case 31

RichTextBox1.SaveFile("C:\Snort\rules\fpt.rules", RichTextBoxStreamType.PlainText)

Case 32

RichTextBox1.SaveFile("C:\Snort\rules\icmp.rules", RichTextBoxStreamType.PlainText)

Case 33

RichTextBox1.SaveFile("C:\Snort\rules\icmp-info.rules", RichTextBoxStreamType.PlainText)

Case 34

RichTextBox1.SaveFile("C:\Snort\rules\imap.rules", RichTextBoxStreamType.PlainText)

Case 35

RichTextBox1.SaveFile("C:\Snort\rules\indicator-compromise.rules", RichTextBoxStreamType.PlainText)

Case 36

RichTextBox1.SaveFile("C:\Snort\rules\indicator-obfuscation.rules", RichTextBoxStreamType.PlainText)

Case 37

RichTextBox1.SaveFile("C:\Snort\rules\indicator-scan.rules", RichTextBoxStreamType.PlainText)

Case 38

RichTextBox1.SaveFile("C:\Snort\rules\indicator-shellcode.rules", RichTextBoxStreamType.PlainText)

Case 39

RichTextBox1.SaveFile("C:\Snort\rules\info.rules", RichTextBoxStreamType.PlainText)

Case 40

RichTextBox1.SaveFile("C:\Snort\rules\local.rules", RichTextBoxStreamType.PlainText)

Case 41

RichTextBox1.SaveFile("C:\Snort\rules\malware-backdoor.rules", RichTextBoxStreamType.PlainText)

Case 42

RichTextBox1.SaveFile("C:\Snort\rules\malware-cnc.rules", RichTextBoxStreamType.PlainText)

Case 43

RichTextBox1.SaveFile("C:\Snort\rules\malware-other.rules", RichTextBoxStreamType.PlainText)

Case 44

RichTextBox1.SaveFile("C:\Snort\rules\malware-tools.rules", RichTextBoxStreamType.PlainText)

Case 45

RichTextBox1.SaveFile("C:\Snort\rules\misc.rules", RichTextBoxStreamType.PlainText)

Case 46

RichTextBox1.SaveFile("C:\Snort\rules\multimedia.rules", RichTextBoxStreamType.PlainText)

Case 47

RichTextBox1.SaveFile("C:\Snort\rules\mysql.rules", RichTextBoxStreamType.PlainText)

Case 48

RichTextBox1.SaveFile("C:\Snort\rules\netbios.rules", RichTextBoxStreamType.PlainText)

Case 49

RichTextBox1.SaveFile("C:\Snort\rules\nntp.rules", RichTextBoxStreamType.PlainText)

Case 50

RichTextBox1.SaveFile("C:\Snort\rules\oracle.rules", RichTextBoxStreamType.PlainText)

Case 51

RichTextBox1.SaveFile("C:\Snort\rules\os-linux.rules", RichTextBoxStreamType.PlainText)

Case 52

RichTextBox1.SaveFile("C:\Snort\rules\os-mobile.rules", RichTextBoxStreamType.PlainText)

Case 53

RichTextBox1.SaveFile("C:\Snort\rules\os-other.rules", RichTextBoxStreamType.PlainText)

Case 54

RichTextBox1.SaveFile("C:\Snort\rules\os-solaris.rules", RichTextBoxStreamType.PlainText)

Case 55

RichTextBox1.SaveFile("C:\Snort\rules\os-windows.rules", RichTextBoxStreamType.PlainText)

Case 56

RichTextBox1.SaveFile("C:\Snort\rules\other-ids.rules", RichTextBoxStreamType.PlainText)

Case 57

RichTextBox1.SaveFile("C:\Snort\rules\p2p.rules", RichTextBoxStreamType.PlainText)

Case 58

RichTextBox1.SaveFile("C:\Snort\rules\phishing-spam.rules", RichTextBoxStreamType.PlainText)

Case 59

RichTextBox1.SaveFile("C:\Snort\rules\policy.rules", RichTextBoxStreamType.PlainText)

Case 60

RichTextBox1.SaveFile("C:\Snort\rules\policy-multimedia.rules", RichTextBoxStreamType.PlainText)

Case 61

RichTextBox1.SaveFile("C:\Snort\rules\policy-other.rules", RichTextBoxStreamType.PlainText)

Case 62

RichTextBox1.SaveFile("C:\Snort\rules\policy-social.rules", RichTextBoxStreamType.PlainText)

Case 63

RichTextBox1.SaveFile("C:\Snort\rules\policy-spam.rules", RichTextBoxStreamType.PlainText)

Case 64

RichTextBox1.SaveFile("C:\Snort\rules\pop2.rules", RichTextBoxStreamType.PlainText)

Case 65

RichTextBox1.SaveFile("C:\Snort\rules\pop3.rules", RichTextBoxStreamType.PlainText)

Case 66

RichTextBox1.SaveFile("C:\Snort\rules\protocol-dns.rules", RichTextBoxStreamType.PlainText)

Case 67

RichTextBox1.SaveFile("C:\Snort\rules\protocol-finger.rules", RichTextBoxStreamType.PlainText)

Case 68

RichTextBox1.SaveFile("C:\Snort\rules\protocol-ftp.rules", RichTextBoxStreamType.PlainText)

Case 69

RichTextBox1.SaveFile("C:\Snort\rules\protocol-icmp.rules", RichTextBoxStreamType.PlainText)

Case 70

RichTextBox1.SaveFile("C:\Snort\rules\protocol-imap.rules", RichTextBoxStreamType.PlainText)

Case 71

RichTextBox1.SaveFile("C:\Snort\rules\protocol-nntp.rules", RichTextBoxStreamType.PlainText)

Case 72

RichTextBox1.SaveFile("C:\Snort\rules\protocol-other.rules", RichTextBoxStreamType.PlainText)

Case 73

RichTextBox1.SaveFile("C:\Snort\rules\protocol-pop.rules", RichTextBoxStreamType.PlainText)

Case 74

RichTextBox1.SaveFile("C:\Snort\rules\protocol-rpc.rules", RichTextBoxStreamType.PlainText)

Case 75

RichTextBox1.SaveFile("C:\Snort\rules\protocol-scada.rules", RichTextBoxStreamType.PlainText)

Case 76

RichTextBox1.SaveFile("C:\Snort\rules\protocol-services.rules", RichTextBoxStreamType.PlainText)

Case 77

RichTextBox1.SaveFile("C:\Snort\rules\protocol-snmp.rules", RichTextBoxStreamType.PlainText)

Case 78

RichTextBox1.SaveFile("C:\Snort\rules\protocol-telnet.rules", RichTextBoxStreamType.PlainText)

Case 79

RichTextBox1.SaveFile("C:\Snort\rules\protocol-tftp.rules", RichTextBoxStreamType.PlainText)

Case 80

RichTextBox1.SaveFile("C:\Snort\rules\protocol-voip.rules", RichTextBoxStreamType.PlainText)

Case 81

RichTextBox1.SaveFile("C:\Snort\rules\pua-adware.rules", RichTextBoxStreamType.PlainText)

Case 82

RichTextBox1.SaveFile("C:\Snort\rules\pua-other.rules", RichTextBoxStreamType.PlainText)

Case 83

RichTextBox1.SaveFile("C:\Snort\rules\pua-p2p.rules", RichTextBoxStreamType.PlainText)

Case 84

RichTextBox1.SaveFile("C:\Snort\rules\pua-toolbars.rules", RichTextBoxStreamType.PlainText)

Case 85

RichTextBox1.SaveFile("C:\Snort\rules\rpc.rules", RichTextBoxStreamType.PlainText)

Case 86

RichTextBox1.SaveFile("C:\Snort\rules\rservices.rules", RichTextBoxStreamType.PlainText)

Case 87

RichTextBox1.SaveFile("C:\Snort\rules\scada.rules", RichTextBoxStreamType.PlainText)

Case 88

RichTextBox1.SaveFile("C:\Snort\rules\scan.rules", RichTextBoxStreamType.PlainText)

Case 89

RichTextBox1.SaveFile("C:\Snort\rules\server-apache.rules", RichTextBoxStreamType.PlainText)

Case 90

RichTextBox1.SaveFile("C:\Snort\rules\server-iis.rules", RichTextBoxStreamType.PlainText)

Case 91

RichTextBox1.SaveFile("C:\Snort\rules\server-mail.rules", RichTextBoxStreamType.PlainText)

Case 92

RichTextBox1.SaveFile("C:\Snort\rules\server-mssql.rules", RichTextBoxStreamType.PlainText)

Case 93

RichTextBox1.SaveFile("C:\Snort\rules\server-mysql.rules", RichTextBoxStreamType.PlainText)

Case 94

RichTextBox1.SaveFile("C:\Snort\rules\server-oracle.rules", RichTextBoxStreamType.PlainText)

Case 95

RichTextBox1.SaveFile("C:\Snort\rules\server-other.rules", RichTextBoxStreamType.PlainText)

Case 96

RichTextBox1.SaveFile("C:\Snort\rules\server-samba.rules", RichTextBoxStreamType.PlainText)

Case 97

RichTextBox1.SaveFile("C:\Snort\rules\server-webapp.rules", RichTextBoxStreamType.PlainText)

Case 98

RichTextBox1.SaveFile("C:\Snort\rules\shellcode.rules", RichTextBoxStreamType.PlainText)

Case 99

RichTextBox1.SaveFile("C:\Snort\rules\smtp.rules", RichTextBoxStreamType.PlainText)

Case 100

RichTextBox1.SaveFile("C:\Snort\rules\snmp.rules", RichTextBoxStreamType.PlainText)

Case 101

RichTextBox1.SaveFile("C:\Snort\rules\specific-threats.rules", RichTextBoxStreamType.PlainText)

Case 102

RichTextBox1.SaveFile("C:\Snort\rules\spyware-put.rules", RichTextBoxStreamType.PlainText)

Case 103

RichTextBox1.SaveFile("C:\Snort\rules\sql.rules", RichTextBoxStreamType.PlainText)

Case 104

RichTextBox1.SaveFile("C:\Snort\rules\telnet.rules", RichTextBoxStreamType.PlainText)

Case 105

RichTextBox1.SaveFile("C:\Snort\rules\tftp.rules", RichTextBoxStreamType.PlainText)

Case 106

RichTextBox1.SaveFile("C:\Snort\rules\virus.rules", RichTextBoxStreamType.PlainText)

Case 107

RichTextBox1.SaveFile("C:\Snort\rules\voip.rules", RichTextBoxStreamType.PlainText)

Case 108

RichTextBox1.SaveFile("C:\Snort\rules\web-activex.rules", RichTextBoxStreamType.PlainText)

Case 109

RichTextBox1.SaveFile("C:\Snort\rules\web-attacks.rules", RichTextBoxStreamType.PlainText)

Case 110

RichTextBox1.SaveFile("C:\Snort\rules\web-cgi.rules", RichTextBoxStreamType.PlainText)

Case 111

RichTextBox1.SaveFile("C:\Snort\rules\web-client.rules", RichTextBoxStreamType.PlainText)

Case 112

RichTextBox1.SaveFile("C:\Snort\rules\web-coldfusion.rules", RichTextBoxStreamType.PlainText)

Case 113

RichTextBox1.SaveFile("C:\Snort\rules\web-frontpage.rules", RichTextBoxStreamType.PlainText)

Case 114

RichTextBox1.SaveFile("C:\Snort\rules\web-iis.rules", RichTextBoxStreamType.PlainText)

Case 115

RichTextBox1.SaveFile("C:\Snort\rules\web-misc.rules", RichTextBoxStreamType.PlainText)

Case 116

RichTextBox1.SaveFile("C:\Snort\rules\web-php.rules", RichTextBoxStreamType.PlainText)

Case 117

RichTextBox1.SaveFile("C:\Snort\rules\x11.rules", RichTextBoxStreamType.PlainText)

End Select

End Sub

Private Sub OpenConfigurationFileToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles OpenConfigurationFileToolStripMenuItem.Click

Form7.Show()

Me.Close()

End Sub

Private Sub NmapCheatSheetToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapCheatSheetToolStripMenuItem.Click

Form8.Show()

Me.Close()

End Sub

Private Sub LogOutToolStripMenuitem\_Click(sender As Object, e As EventArgs) Handles LogOutToolStripMenuItem.Click

MsgBox("Thank you for using NetSec Manager", MsgBoxStyle.Information, "NetSec Manager: Log Out")

Form1.Show()

Me.Close()

End Sub

Private Sub NmapToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\nmap.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub StartScanToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles StartScanToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\cmd.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub SnifferToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SnifferToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\sniff\dist\scan.exe")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

End Class

1. **SYSTEM INFORMATION MODULE**

//Form6 source code that shows the system and server requirements.

Public Class Form6

Private Sub PictureBox1\_Click(sender As Object, e As EventArgs) Handles PictureBox1.Click

End Sub

Private Sub TabPage1\_Click(sender As Object, e As EventArgs) Handles TabPage1.Click

End Sub

Private Sub TabPage2\_Click(sender As Object, e As EventArgs) Handles TabPage2.Click

End Sub

Private Sub Label1\_Click(sender As Object, e As EventArgs) Handles Label1.Click

End Sub

Private Sub Label2\_Click(sender As Object, e As EventArgs) Handles Label2.Click

End Sub

Private Sub Label3\_Click(sender As Object, e As EventArgs) Handles Label3.Click

End Sub

Private Sub Label4\_Click(sender As Object, e As EventArgs) Handles Label4.Click

End Sub

Private Sub Label5\_Click(sender As Object, e As EventArgs) Handles Label5.Click

End Sub

Private Sub Label6\_Click(sender As Object, e As EventArgs) Handles Label6.Click

End Sub

Private Sub Label7\_Click(sender As Object, e As EventArgs) Handles Label7.Click

End Sub

Private Sub Label8\_Click(sender As Object, e As EventArgs) Handles Label8.Click

End Sub

Private Sub Label9\_Click(sender As Object, e As EventArgs)

End Sub

Private Sub Label10\_Click(sender As Object, e As EventArgs)

End Sub

Private Sub Label11\_Click(sender As Object, e As EventArgs) Handles Label11.Click

End Sub

Private Sub Label12\_Click(sender As Object, e As EventArgs) Handles Label12.Click

End Sub

Private Sub Label13\_Click(sender As Object, e As EventArgs) Handles Label13.Click

End Sub

Private Sub Label14\_Click(sender As Object, e As EventArgs) Handles Label14.Click

End Sub

Private Sub Label15\_Click(sender As Object, e As EventArgs) Handles Label15.Click

End Sub

Private Sub Label16\_Click(sender As Object, e As EventArgs) Handles Label16.Click

End Sub

Private Sub Label17\_Click(sender As Object, e As EventArgs) Handles Label17.Click

End Sub

Private Sub Label18\_Click(sender As Object, e As EventArgs) Handles Label18.Click

End Sub

Private Sub Label19\_Click(sender As Object, e As EventArgs) Handles Label19.Click

End Sub

Private Sub Label20\_Click(sender As Object, e As EventArgs) Handles Label20.Click

End Sub

Private Sub Label21\_Click(sender As Object, e As EventArgs) Handles Label21.Click

End Sub

Private Sub Label22\_Click(sender As Object, e As EventArgs) Handles Label22.Click

End Sub

Private Sub Label23\_Click(sender As Object, e As EventArgs) Handles Label23.Click

End Sub

Private Sub Label24\_Click(sender As Object, e As EventArgs) Handles Label24.Click

End Sub

Private Sub Label26\_Click(sender As Object, e As EventArgs) Handles Label26.Click

End Sub

Private Sub Label27\_Click(sender As Object, e As EventArgs) Handles Label27.Click

End Sub

Private Sub Label28\_Click(sender As Object, e As EventArgs) Handles Label28.Click

End Sub

Private Sub Label29\_Click(sender As Object, e As EventArgs) Handles Label29.Click

End Sub

Private Sub Button1\_Click(sender As Object, e As EventArgs) Handles Button1.Click

Me.Close()

End Sub

End Class

1. **OPEN CONFIGURATION FILE MODULE**

//Form7 source code that shows open configuration file from snort.conf.

Public Class Form7

Private Sub HomeButton\_Click(sender As Object, e As EventArgs) Handles HomeButton.Click

Form2.Show()

Me.Close()

End Sub

Private Sub DataAnalysisToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles DataAnalysisToolStripMenuItem.Click

Form3.Show()

Me.Close()

End Sub

Private Sub AttackAdviserToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles AttackAdviserToolStripMenuItem.Click

Form4.Show()

Me.Close()

End Sub

Private Sub RulesToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles RulesToolStripMenuItem.Click

Form5.Show()

Me.Close()

End Sub

Private Sub SystemInformationToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SystemInformationToolStripMenuItem.Click

Form6.Show()

End Sub

Private Sub NmapCheatSheetToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapCheatSheetToolStripMenuItem.Click

Form8.Show()

Me.Close()

End Sub

Private Sub LogOutToolStripMenuitem\_Click(sender As Object, e As EventArgs) Handles LogOutToolStripMenuItem.Click

MsgBox("Thank you for using NetSec Manager", MsgBoxStyle.Information, "NetSec Manager: Log Out")

Form1.Show()

Me.Close()

End Sub

Private Sub RichTextBox1\_Click(sender As Object, e As EventArgs) Handles RichTextBox1.Click

RichTextBox1.LoadFile("C:\Snort\etc\snort.conf", RichTextBoxStreamType.PlainText)

End Sub

Private Sub SaveButton\_Click(sender As Object, e As EventArgs) Handles SaveButton.Click

RichTextBox1.SaveFile("C:\Snort\etc\snort.conf", RichTextBoxStreamType.PlainText)

End Sub

Private Sub NmapToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\nmap.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub StartScanToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles StartScanToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\cmd.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub SnifferToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SnifferToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\sniff\dist\scan.exe")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

End Class

1. **CHEAT SHEET MODULE**

//Form8 source code that shows cheat sheet document.

Public Class Form8

Private Sub HomeButton\_Click(sender As Object, e As EventArgs) Handles HomeButton.Click

Form2.Show()

Me.Close()

End Sub

Private Sub DataAnalysisToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles DataAnalysisToolStripMenuItem.Click

Form3.Show()

Me.Close()

End Sub

Private Sub AttackAdviserToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles AttackAdviserToolStripMenuItem.Click

Form4.Show()

Me.Close()

End Sub

Private Sub RulesToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles RulesToolStripMenuItem.Click

Form5.Show()

Me.Close()

End Sub

Private Sub SystemInformationToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SystemInformationToolStripMenuItem.Click

Form6.Show()

End Sub

Private Sub OpenConfigurationFileToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles OpenConfigurationFileToolStripMenuItem.Click

Form7.Show()

Me.Close()

End Sub

Private Sub LogOutToolStripMenuitem\_Click(sender As Object, e As EventArgs) Handles LogOutToolStripMenuItem.Click

MsgBox("Thank you for using NetSec Manager", MsgBoxStyle.Information, "NetSec Manager: Log Out")

Form1.Show()

Me.Close()

End Sub

Private Sub ListBox1\_SelectedIndexChanged(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles ListBox1.SelectedIndexChanged

Select Case ListBox1.SelectedIndex

Case 0

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Nmap Cheat Sheet.PNG")

Case 1

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Aggregate Time Options.PNG")

Case 2

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Base Syntax.PNG")

Case 3

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Fine-Grained Timing Options.PNG")

Case 4

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Misc Options.PNG")

Case 5

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Notable Scripts.PNG")

Case 6

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Output Formats.PNG")

Case 7

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Probing Options.PNG")

Case 8

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Scan Types.PNG")

Case 9

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Script Categories.PNG")

Case 10

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Scripting Engine.PNG")

Case 11

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Target Ports.PNG")

Case 12

PictureBox1.Image = Image.FromFile("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Images\Nmap Cheat Sheet\Target Specification.PNG")

End Select

End Sub

Private Sub NmapToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles NmapToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\nmap.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub StartScanToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles StartScanToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\cmd.bat")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub SnifferToolStripMenuItem\_Click(sender As Object, e As EventArgs) Handles SnifferToolStripMenuItem.Click

Dim config As New ProcessStartInfo("C:\Users\Yan Wisdom\Documents\Visual Studio 2015\Projects\NetsecManagerv3\NetsecManagerv3\Processes\scan.exe")

config.RedirectStandardError = True

config.RedirectStandardOutput = True

config.CreateNoWindow = False

config.WindowStyle = ProcessWindowStyle.Hidden

config.UseShellExecute = False

Dim process As Process = Process.Start(config)

End Sub

Private Sub PictureBox1\_Click(sender As Object, e As EventArgs) Handles PictureBox1.Click

PictureBox1.SizeMode = PictureBoxSizeMode.StretchImage

End Sub

End Class

1. **PROCESS MODULE (SCRIPTS)**

//**cmd.bat**

@echo off

start cmd.exe "C:\Windows\System32"

//**nmap.bat**

**@echo off**

start zenmap.exe "C:\Program Files (x86)\Nmap\zenmap.exe"

exit

//**rules.bat**

@echo off

start C:\Snort\rules

//**snortconf.bat**

@echo off

start notepad++ "C:\Snort\etc\snort.conf"

exit

//**wireshark.bat**

@echo off

start wireshark.exe

exit

//**ipWhois.py**

"""

IP Who.is modified code.

12.18.15 - (c) amabinal

"""

#imports

import cgitb

from ipwhois import IPWhois

from pprint import pprint

import socket

# import optparse

cgitb.enable()

# main logic: Search for IP (view details)

ipadd = input('Please enter the IP address: (enclosed with single quotes)')

who = socket.inet\_aton(ipadd)#IPWhois(ipadd)

# text to IP conversions

ipconv = socket.inet\_ntoa(who)

#who.is logic

obj = IPWhois(ipconv)

ipresult = obj.lookup\_rdap(depth=1)

pprint(ipresult)

# switches

"""def Main():

parser = optparse.OptionParser('usage %prog '+'-i <IP address>')

parser.add\_option('-i', dest='ipadd', type='string', help='Specify IP address')

(options) = parser.parse\_args()

if (options.ipadd == None):

print parser.usage

exit(0)

else:

ipout = str(options.ipadd)

for ipadd in ipout:

ipWho(ipadd)

# main logic: View my IP

# main logic: Search for IP (with proxy)

# main logic: quit Modified IP Whois

if \_\_name\_\_ == '\_\_main\_\_':

Main()

"""

//**scan.py**

#Nmap Port Scanner

import optparse

import nmap

def nmapScan(tgtHost, tgtPort):

nScan = nmap.PortScanner()

nScan.scan(tgtHost, tgtPort)

state = nScan[tgtHost]['tcp'][int(tgtPort)]['state']

print " [\*] " + tgtHost + " tcp/" +tgtPort + " " + state

def Main():

parser = optparse.OptionParser('usage %prog '+'-H <target host> -p <target port>')

parser.add\_option('-H', dest='tgtHost', type='string', help='specify target host')

parser.add\_option('-p', dest='tgtPort', type='string', help='specify target port[s] seperated by comma')

(options, args) = parser.parse\_args()

if (options.tgtHost == None) | (options.tgtPort == None):

print parser.usage

exit(0)

else:

tgtHosts = str(options.tgtHost).split(',')

tgtPorts = str(options.tgtPort).split(',')

for tgtHost in tgtHosts:

for tgtPort in tgtPorts:

nmapScan(tgtHost, tgtPort)

if \_\_name\_\_ == '\_\_main\_\_':

Main()

**DEFINITION OF TERMS**

**CONCEPTUAL DIAGRAMS** Displays the interaction between the system and the users/entities; shows the movement of data within the system to and/or from the entities.

**DENIAL-OF-SERVICE (DOS)** An attempt to make a machine or network resource unavailable to its intended users.

**DNSPYTHON** A DNS toolkit for Python. It supports almost all record types.

**Intrusion Detection System** Known as intrusion detection system, IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

**IPV4 ADDRESS** Known as the Internet Protocol version 4, it is a unique identifier to assigned to a network device, either automatically or set by the user.

**MAC ADDRESS.** Known as media access control address, MAC address is a unique identifier assigned to network interfaces for communications in the physical network segment.

**MYSQL CONNECTOR PYTHON** A standardized database driver for Python platforms and development.

**NETADDR** A Python library for representing and manipulating network addresses.

**NETIFACES** Provides a way for Python programmers to get access to a list of the network interfaces on the local machine, and to obtain the addresses of those network interfaces.

**PORT** Virtual data connection between computer programs possibly through a computer network.

**PYTHON** A general-purpose, object-oriented interpreted language used for countless standalone projects or scripting applications.

**SNORT.** An open-source and lightweight network intrusion detection system for UNIX derivatives and Windows

**SQL INJECTION.** A code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.

**TCP/IP** Internet protocols, namely, TCP (Transmission Internet Protocol), the first networking protocols defined in the Internet protocol suite.

**VISUAL BASIC** A programming environment from Microsoft in which a programmer uses a graphical user interface (GUI).

**XAMMP** A free open source cross-platform web server solution stack package.

**BIBLIOGRAPHY**

https://www.python.org/

https://nmap.org/

https://www.snort.org/

stackoverflow.com/

https://pypi.python.org/