Lab 2a: Invoking Snort

Details

Aim: To provide a foundation in invoking and controlling Snort

Activities

1. If Visual Studio is installed on your machine, download the following solution [1]:

http://www.dcs.napier.ac.uk/~bill/SnortCaller.zip

An outline of the code is:

```
public void runShort(string arguments)
{
  processCaller = new ProcessCaller(this);
  processCaller.FileName = @"c:\snort\bin\snort.exe";
  processCaller.Arguments = arguments;
  processCaller.StdErrReceived += new DataReceivedHandler(writeStreamInfo);
  processCaller.StdOutReceived += new DataReceivedHandler(writeStreamInfo);
  processCaller.Completed += new EventHandler(processCompletedOrCanceled);
  processCaller.Cancelled += new EventHandler(processCompletedOrCanceled);

  this.richTextBox1.Text = "Started function.  Please stand by.."
                + Environment.NewLine;

  processCaller.Start();
}
private void btnInterface_Click(object sender, System.E
{

    this.runShort("-W");
}
```

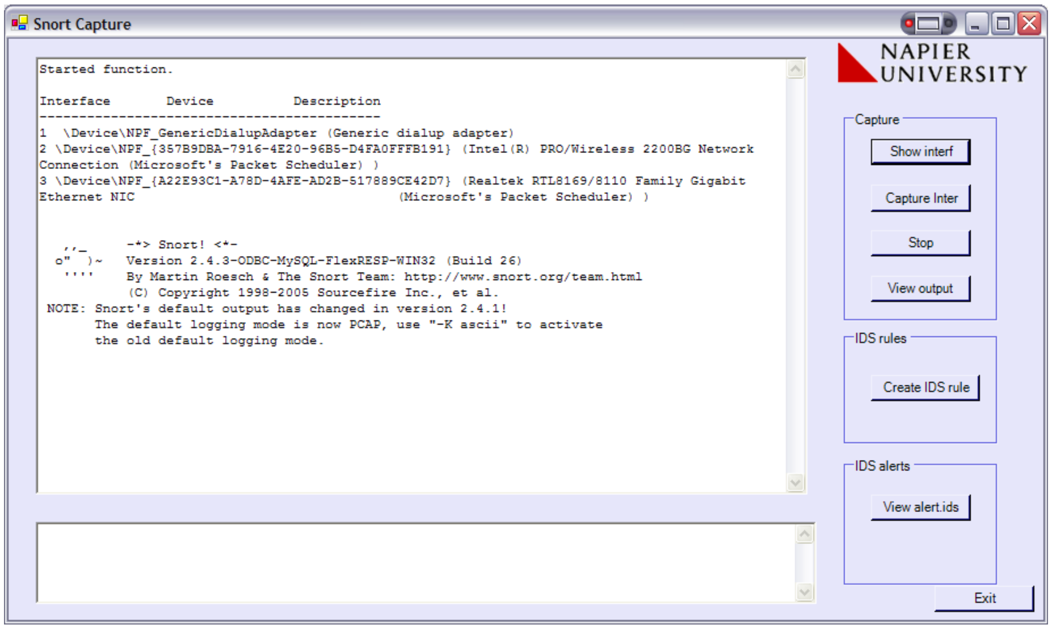
This defines the Snort arguments that are used to run the program.

2. In the Project listing, **double click** on the SnortCaller.cs file, then **double click** on the **Show interf** button, and add the following highlighted code:

```
private void btnInterface_Click(object sender, System.EventArgs e)
{
   this.runShort("-W");
}
```

3. Run the program, and show that the output is similar to the output in Figure 1:

What is/are your interface(s)?



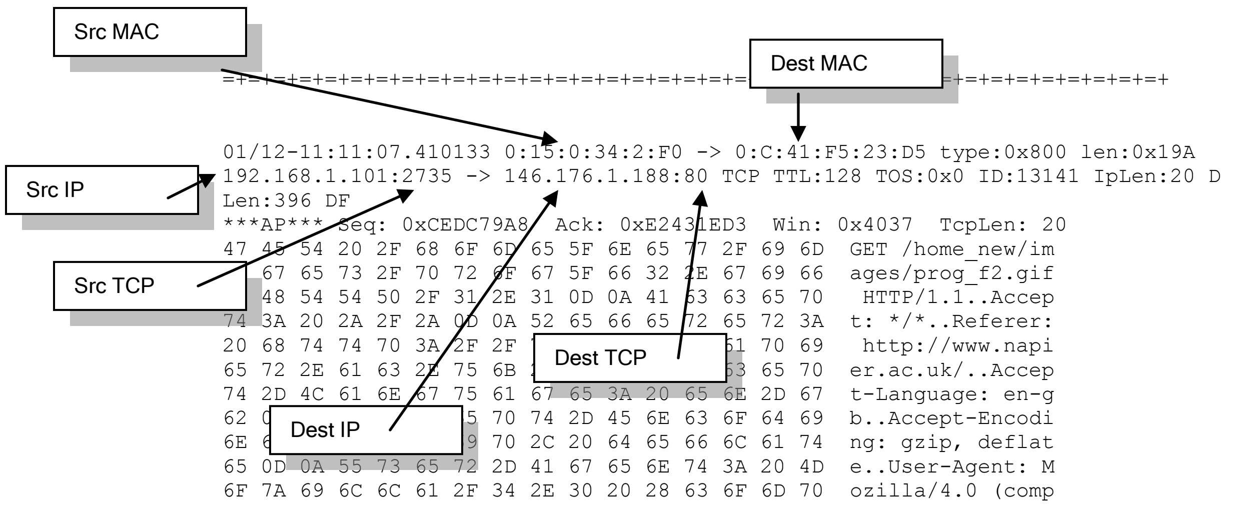
```
Started function.

Interface       Device          Description
-------------------------------------------
1  \Device\NPF_GenericDialupAdapter (Generic dialup adapter)
2 \Device\NPF_{357B9DBA-7916-4E20-96B5-D4FA0FFFB191} (Intel(R) PRO/Wireless 2200BG Network
Connection (Microsoft's Packet Scheduler) )
3 \Device\NPF_{A22E93C1-A78D-4AFE-AD2B-517889CE42D7} (Realtek RTL8169/8110 Family Gigabit
Ethernet NIC                                         (Microsoft's Packet Scheduler) )


   ,,_      -*> Snort! <*-
  o"  )~    Version 2.4.3-ODBC-MySQL-FlexRESP-WIN32 (Build 26)
   ''''     By Martin Roesch & The Snort Team: http://www.snort.org/team.html
            (C) Copyright 1998-2005 Sourcefire Inc., et al.
 NOTE: Snort's default output has changed in version 2.4.1!
       The default logging mode is now PCAP, use "-K ascii" to activate
       the old default logging mode.
```

Figure 1:

4. **Double click** on the **Capture Inter** button, and add the following highlighted code. Replace the c:\\bill with c:\\yourMatricNo, and replace the value after the –i option with the interface number. This should log to the folder defined.

```
private void btnStart_Click(object sender, System.EventArgs e)
{
  if (!Directory.Exists("c:\\bill")) Directory.CreateDirectory("c:\\bill");
  this.runShort("-dev -i 1 -p -l c:\\bill -K ascii");
}
```

5. Run the program and get Snort to capture the packets, and then stop it with the **Stop** button (Figure 2). Generate some Web traffic, and view the output, and verify that it is capturing data packets, such as:



```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=[illegible]=+=+=+=+=+=+=+=+=+

01/12-11:11:07.410133 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x19A
192.168.1.101:2735 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:13141 IpLen:20 D
Len:396 DF
***AP*** Seq: 0xCEDC79A8  Ack: 0xE2431ED3  Win: 0x4037  TcpLen: 20
47 45 54 20 2F 68 6F 6D 65 5F 6E 65 77 2F 69 6D  GET /home_new/im
[illegible] 67 65 73 2F 70 72 6F 67 5F 66 32 2E 67 69 66  ages/prog_f2.gif
[illegible] 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70   HTTP/1.1..Accep
74 3A 20 2A 2F 2A 0D 0A 52 65 66 65 72 65 72 3A  t: */*..Referer:
20 68 74 74 70 3A 2F 2F [illegible] 61 70 69   http://www.napi
65 72 2E 61 63 2E 75 6B [illegible] 63 65 70  er.ac.uk/..Accep
74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 67  t-Language: en-g
62 0[illegible]5 70 74 2D 45 6E 63 6F 64 69  b..Accept-Encodi
6E 6[illegible]9 70 2C 20 64 65 66 6C 61 74  ng: gzip, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D  e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70  ozilla/4.0 (comp
```

6. Select one of the TCP data packets, and determine the following:

The source IP address:

The source TCP port:

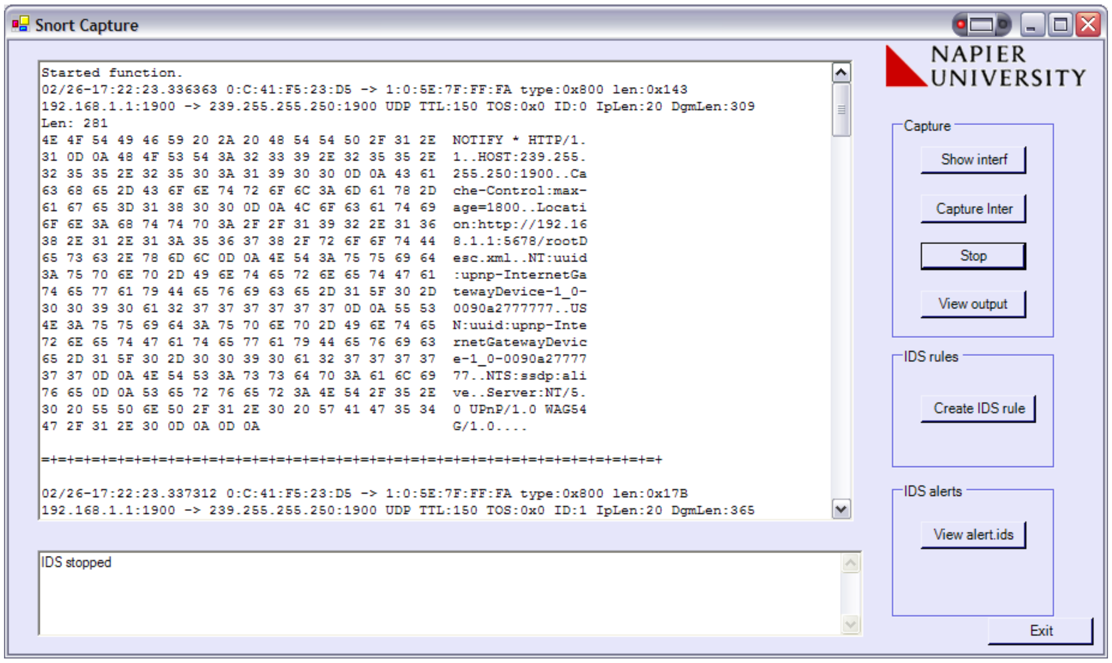
The destination IP address:

The destination TCP port:

The source MAC address:

The destination MAC address:

The TCP flags:



```
Started function.
02/26-17:22:23.336363 0:C:41:F5:23:D5 -> 1:0:5E:7F:FF:FA type:0x800 len:0x143
192.168.1.1:1900 -> 239.255.255.250:1900 UDP TTL:150 TOS:0x0 ID:0 IpLen:20 DgmLen:309
Len: 281
4E 4F 54 49 46 59 20 2A 20 48 54 54 50 2F 31 2E  NOTIFY * HTTP/1.
31 0D 0A 48 4F 53 54 3A 32 33 39 2E 32 35 35 2E  1..HOST:239.255.
32 35 35 2E 32 35 30 3A 31 39 30 30 0D 0A 43 61  255.250:1900..Ca
63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 6D 61 78 2D  che-Control:max-
61 67 65 3D 31 38 30 30 0D 0A 4C 6F 63 61 74 69  age=1800..Locati
6F 6E 3A 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36  on:http://192.16
38 2E 31 2E 31 3A 35 36 37 38 2F 72 6F 6F 74 44  8.1.1:5678/rootD
65 73 63 2E 78 6D 6C 0D 0A 4E 54 3A 75 75 69 64  esc.xml..NT:uuid
3A 75 70 6E 70 2D 49 6E 74 65 72 6E 65 74 47 61  :upnp-InternetGa
74 65 77 61 79 44 65 76 69 63 65 2D 31 5F 30 2D  tewayDevice-1_0-
30 30 39 30 61 32 37 37 37 37 37 37 0D 0A 55 53  0090a2777777..US
4E 3A 75 75 69 64 3A 75 70 6E 70 2D 49 6E 74 65  N:uuid:upnp-Inte
72 6E 65 74 47 61 74 65 77 61 79 44 65 76 69 63  rnetGatewayDevic
65 2D 31 5F 30 2D 30 30 39 30 61 32 37 37 37 37  e-1_0-0090a27777
37 37 0D 0A 4E 54 53 3A 73 73 64 70 3A 61 6C 69  77..NTS:ssdp:ali
76 65 0D 0A 53 65 72 76 65 72 3A 4E 54 2F 35 2E  ve..Server:NT/5.
30 20 55 50 6E 50 2F 31 2E 30 20 57 41 47 35 34  0 UPnP/1.0 WAG54
47 2F 31 2E 30 0D 0A 0D 0A                       G/1.0....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/26-17:22:23.337312 0:C:41:F5:23:D5 -> 1:0:5E:7F:FF:FA type:0x800 len:0x17B
192.168.1.1:1900 -> 239.255.255.250:1900 UDP TTL:150 TOS:0x0 ID:1 IpLen:20 DgmLen:365
```

```
IDS stopped
```

Figure 2:

7. **Double click** on the **View Output** button, and add the following highlighted code. Replace the c:\\bill with c:\\yourMatricNo.

```
private void btnView_Click(object sender, System.EventArgs e)
```

```
{
   openFileDialog1.InitialDirectory="c:\\bill";
   openFileDialog1.ShowDialog();
   Process.Start("wordpad.exe", openFileDialog1.FileName);
}
```

8. Run the program, and select the **View Output** button, and verify that you get the output seen in Figure 3, and open one of the IDS files in the subfolders, and verify the output, as shown in Figure 4.

What are the contents of the folder:

Go into one of the folders and view the contents of the IDS file. What does it contain:

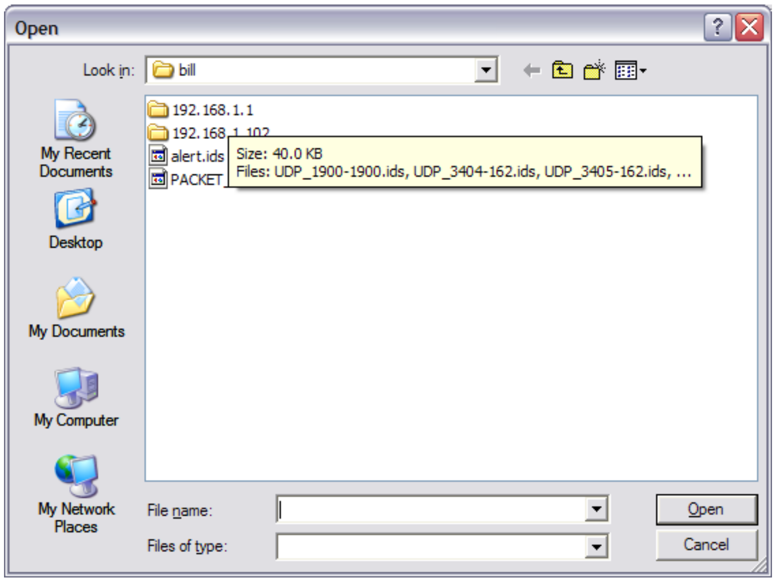
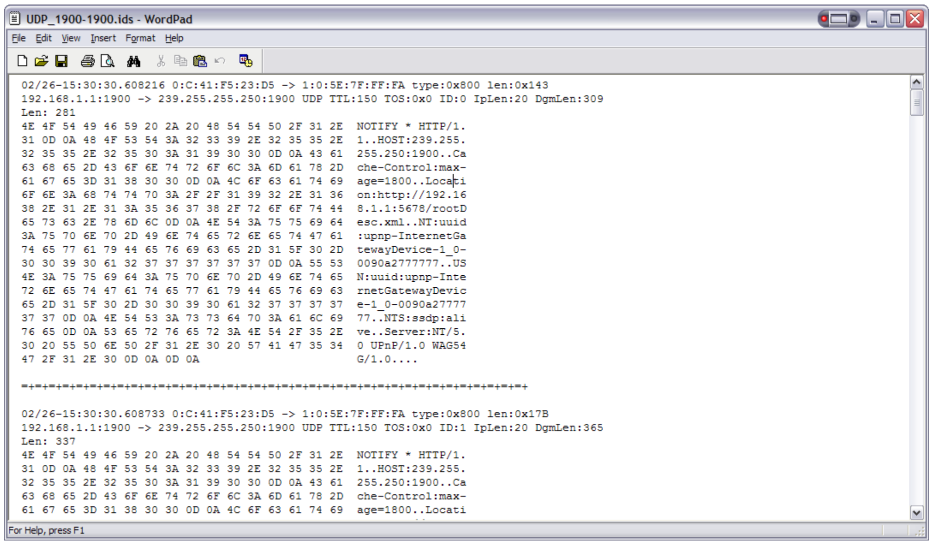


Figure 3:


UDP_1900-1900.ids - WordPad
File Edit View Insert Format Help
For Help, press F1

```
02/26-15:30:30.608216 0:C:41:F5:23:D5 -> 1:0:5E:7F:FF:FA type:0x800 len:0x143
192.168.1.1:1900 -> 239.255.255.250:1900 UDP TTL:150 TOS:0x0 ID:0 IpLen:20 DgmLen:309
Len: 281
4E 4F 54 49 46 59 20 2A 20 48 54 54 50 2F 31 2E  NOTIFY * HTTP/1.
31 0D 0A 48 4F 53 54 3A 32 33 39 2E 32 35 35 2E  1..HOST:239.255.
32 35 35 2E 32 35 30 3A 31 39 30 30 0D 0A 43 61  255.250:1900..Ca
63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 6D 61 78 2D  che-Control:max-
61 67 65 3D 31 38 30 30 0D 0A 4C 6F 63 61 74 69  age=1800..Locati
6F 6E 3A 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36  on:http://192.16
38 2E 31 2E 31 3A 35 36 37 38 2F 72 6F 6F 74 44  8.1.1:5678/rootD
65 73 63 2E 78 6D 6C 0D 0A 4E 54 3A 75 75 69 64  esc.xml..NT:uuid
3A 75 70 6E 70 2D 49 6E 74 65 72 6E 65 74 47 61  :upnp-InternetGa
74 65 77 61 79 44 65 76 69 63 65 2D 31 5F 30 2D  tewayDevice-1_0-
30 30 39 30 61 32 37 37 37 37 37 37 0D 0A 55 53  0090a2777777..US
4E 3A 75 75 69 64 3A 75 70 6E 70 2D 49 6E 74 65  N:uuid:upnp-Inte
72 6E 65 74 47 61 74 65 77 61 79 44 65 76 69 63  rnetGatewayDevic
65 2D 31 5F 30 2D 30 30 39 30 61 32 37 37 37 37  e-1_0-0090a27777
37 37 0D 0A 4E 54 53 3A 73 73 64 70 3A 61 6C 69  77..NTS:ssdp:ali
76 65 0D 0A 53 65 72 76 65 72 3A 4E 54 2F 35 2E  ve..Server:NT/5.
30 20 55 50 6E 50 2F 31 2E 30 20 57 41 47 35 34  0 UPnP/1.0 WAG54
47 2F 31 2E 30 0D 0A 0D 0A                       G/1.0....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/26-15:30:30.608733 0:C:41:F5:23:D5 -> 1:0:5E:7F:FF:FA type:0x800 len:0x17B
192.168.1.1:1900 -> 239.255.255.250:1900 UDP TTL:150 TOS:0x0 ID:1 IpLen:20 DgmLen:365
Len: 337
4E 4F 54 49 46 59 20 2A 20 48 54 54 50 2F 31 2E  NOTIFY * HTTP/1.
31 0D 0A 48 4F 53 54 3A 32 33 39 2E 32 35 35 2E  1..HOST:239.255.
32 35 35 2E 32 35 30 3A 31 39 30 30 0D 0A 43 61  255.250:1900..Ca
63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 6D 61 78 2D  che-Control:max-
61 67 65 3D 31 38 30 30 0D 0A 4C 6F 63 61 74 69  age=1800..Locati
```

Figure 4:

9. **Double click** on the **Create IDS rule** button, and add the following code:

```
private void btnIDSRule_Click(object sender, System.EventArgs e)
{
   string rule;

rule = "alert tcp any any -> any 80 (content:\"napier\"; msg:\"Napier detected\";)";
   StreamWriter SW;
   SW=File.CreateText("c:\\snort\\bin\\napier.txt");
   SW.WriteLine(rule);
   SW.Close();
   statusIDS.Text+="IDS updated... please restart Snort";
}
```

which writes a Snort rule to the napier.txt file.

10. **Double click** on the **View alert.ids** button, and add the following code (remember to replace the c:\\bill with c:\\yourMatricNo):

```
private void btnViewAlert_Click(object sender, System.EventArgs e)
{
  if (File.Exists("c:\\bill\\alert.ids"))
  {
        Process.Start("wordpad.exe", "c:\\bill\\alert.ids");
  }
  else statusIDS.Text+="File does not exist...";
}
```

also update the line:

```
this.runShort("-dev -i 1 -p -l c:\\bill -K ascii");
```

with (to allow Snort to read-in the newly created rules file):

```
this.runShort("-dev -i 1 -p -l c:\\bill -K ascii –c c:\\snort\\bin\\napier.txt");
```

11. Run the program, and capture some Web traffic with the name **napier** in it. Then **Stop** the capture, and select the **View alert.ids** button (Figure 5).

What are the contents of the alert.ids file:

Did it detect "napier":

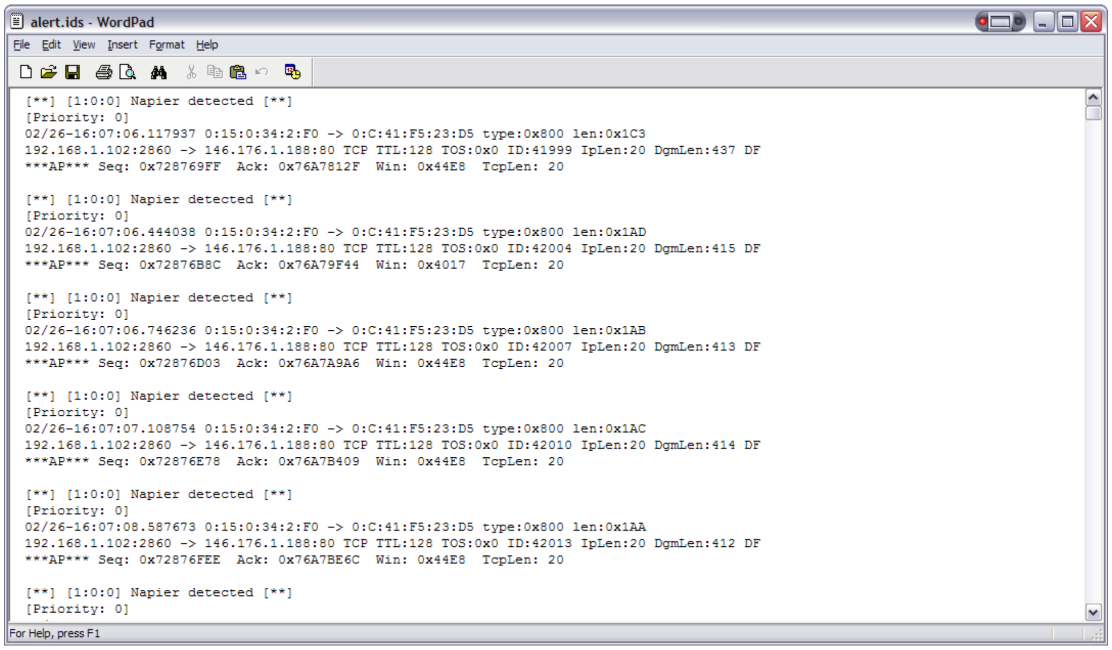
12. Next download the client and server programs from:

http://www.dcs.napier.ac.uk/~bill/dotNetClientServer.zip

13. In groups of two, one person should run the server on their computer, and the other person runs the client, and connects to the server on port **1001**. Make sure that you can chat, before going onto the next part of the tutorial (Figure 6).

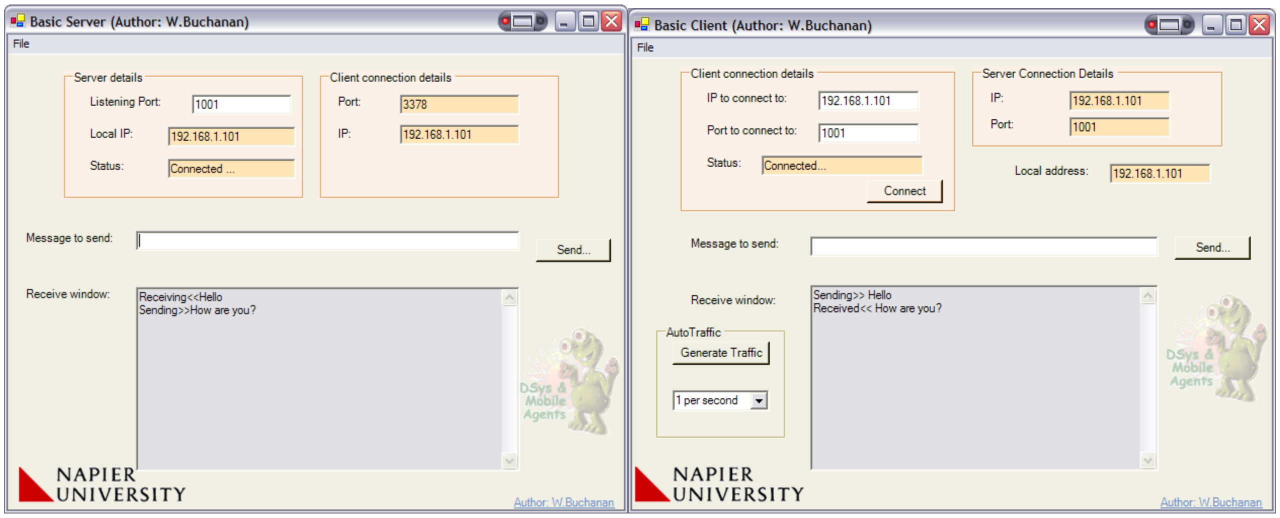
14. Write a Snort rule which detects the word "napier" in the communications between the client and server.

What is the Snort rule for this:



```
[**] [1:0:0] Napier detected [**]
[Priority: 0]
02/26-16:07:06.117937 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x1C3
192.168.1.102:2860 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:41999 IpLen:20 DgmLen:437 DF
***AP*** Seq: 0x728769FF  Ack: 0x76A7812F  Win: 0x44E8  TcpLen: 20

[**] [1:0:0] Napier detected [**]
[Priority: 0]
02/26-16:07:06.444038 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x1AD
192.168.1.102:2860 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:42004 IpLen:20 DgmLen:415 DF
***AP*** Seq: 0x72876B8C  Ack: 0x76A79F44  Win: 0x4017  TcpLen: 20

[**] [1:0:0] Napier detected [**]
[Priority: 0]
02/26-16:07:06.746236 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x1AB
192.168.1.102:2860 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:42007 IpLen:20 DgmLen:413 DF
***AP*** Seq: 0x72876D03  Ack: 0x76A7A9A6  Win: 0x44E8  TcpLen: 20

[**] [1:0:0] Napier detected [**]
[Priority: 0]
02/26-16:07:07.108754 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x1AC
192.168.1.102:2860 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:42010 IpLen:20 DgmLen:414 DF
***AP*** Seq: 0x72876E78  Ack: 0x76A7B409  Win: 0x44E8  TcpLen: 20

[**] [1:0:0] Napier detected [**]
[Priority: 0]
02/26-16:07:08.587673 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x1AA
192.168.1.102:2860 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:42013 IpLen:20 DgmLen:412 DF
***AP*** Seq: 0x72876FEE  Ack: 0x76A7BE6C  Win: 0x44E8  TcpLen: 20

[**] [1:0:0] Napier detected [**]
[Priority: 0]
```

Figure 5:



Server details
Listening Port: 1001
Local IP: 192.168.1.101
Status: Connected ...

Client connection details
Port: 3378
IP: 192.168.1.101

Message to send:

Receive window:
Receiving<<Hello
Sending>>How are you?

Client connection details
IP to connect to: 192.168.1.101
Port to connect to: 1001
Status: Connected...

Server Connection Details
IP: 192.168.1.101
Port: 1001

Local address: 192.168.1.101

Message to send:

Receive window:
Sending>> Hello
Received<< How are you?

1 per second

Figure 6:

Note: If you want the complete solution at any time, use:

http://www.dcs.napier.ac.uk/~bill/SnortCallerComplete.zip

[1] Code is based on http://www.codeproject.com/csharp/LaunchProcess.asp.

Lab 2b: IDS 2 (Snort)

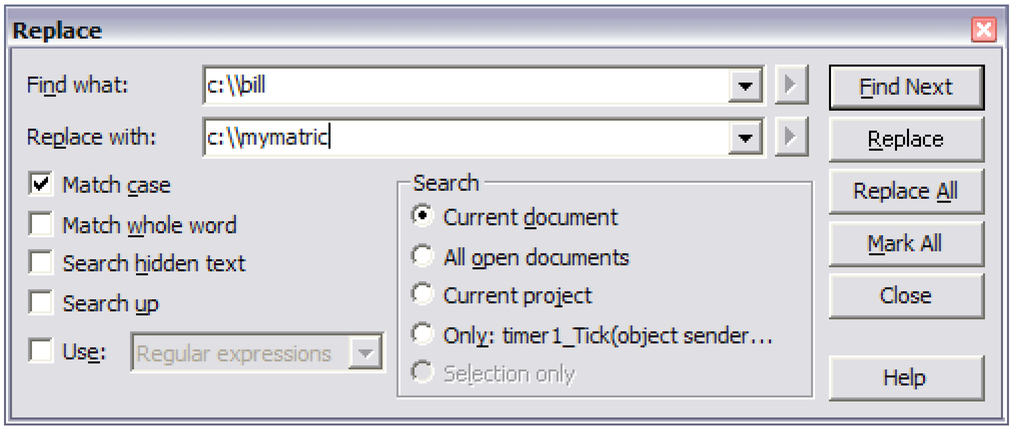
Details

Aim: To use Snort to detect attacks

Note: To enhance the development, you can use the following program:

http://www.dcs.napier.ac.uk/~bill/SnortAnalyser.zip

Before you start... double click on the form, and reveal the code. Now select **Edit**, then **Find and Replace**, and then **Replace**. After this, change all the occurrences of c:\\bill to c:\\mymatric (where *mymatric* is your matriculation number), such as:



Find what: c:\\bill

Replace with: c:\\mymatric

[✓] Match case

[ ] Match whole word

[ ] Search hidden text

[ ] Search up

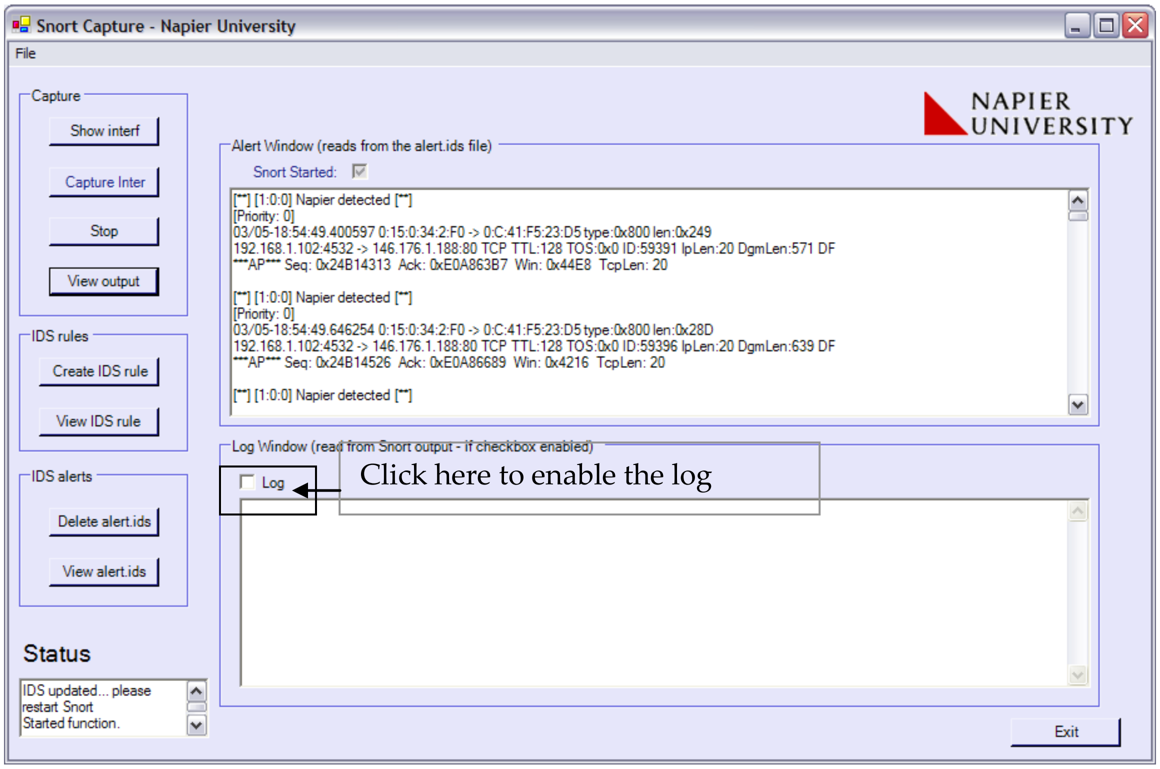
[ ] Use: Regular expressions

Search: [● Current document] ○ All open documents ○ Current project ○ Only: timer1_Tick(object sender… ○ Selection only

To update the rules, **double click** on the **Create IDS rule** button, and add the necessary rules. For example to add two rules:

```
   string rule1,rule2;

rule1 = "alert tcp any any -> any 80 (content:\"napier\"; msg:\"Napier detected\";)";
rule2 = "alert tcp any any -> any 80 (content:\"fred\"; msg:\"Napier detected\";)";

   StreamWriter SW;
   SW=File.CreateText("c:\\snort\\bin\\napier.txt");
   SW.WriteLine(rule1);
   SW.WriteLine(rule2);
   SW.Close();
```

Run the program, and verify that it detects the presence of the word "Napier" in the outgoing network traffic, such as:



```
[**] [1:0:0] Napier detected [**]
[Priority: 0]
03/05-18:54:49.400597 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x249
192.168.1.102:4532 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:59391 IpLen:20 DgmLen:571 DF
***AP*** Seq: 0x24B14313  Ack: 0xE0A863B7  Win: 0x44E8  TcpLen: 20

[**] [1:0:0] Napier detected [**]
[Priority: 0]
03/05-18:54:49.646254 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x28D
192.168.1.102:4532 -> 146.176.1.188:80 TCP TTL:128 TOS:0x0 ID:59396 IpLen:20 DgmLen:639 DF
***AP*** Seq: 0x24B14526  Ack: 0xE0A86689  Win: 0x4216  TcpLen: 20

[**] [1:0:0] Napier detected [**]
```

```
IDS updated... please
restart Snort
Started function.
```

Activities

1. Write rules which will detect the word **Intel** in the payload, so that the alerts are:

A. Intel found on outgoing WWW traffic (port 80). Change it so that it detects Intel either in upper or lower case.

B. Intel found on incoming WWW traffic (port 80).

Verify your rules by running tests.

What are the rules:

2. Write a rule which detects the following:

A. An incoming Web page with the words “John” and “Napier”.

What is the rule:

Show that it works with the site: http://www.johnnapier.com/
and not with: http://www.napier.ac.uk

3. Run the program, and click on the **Log** checkbox, and start Snort (with **Capture Inter**). Run Snort, and ping one or more hosts. From the Log window, scroll until you find your ping activity. From this locate the ARP and ping activity (see Appendix A for an example of the packets):

What information does the sending ARP and also the receiving ARP packet have:

What are the contents of the ping packet:

4. Run the program, and click on the **Log** checkbox, and start Snort (with **Capture Inter**). Run Snort, and access the main Web site of the University of Edinburgh (www.ed.ac.uk). From the Log window, scroll until you find your DNS activity (see Appendix A for an example of the packets):

What information does the sending DNS and also the receiving DNS packet have:

Which TCP port does the DNS server use:

From the contents of the DNS return, and using nslookup on www.ed.ac.uk, is it possible to determent the IP address that is returned from the DNS server (see Appendix A)? Yes/No

5. A typical signature of a network attack is a port scan, where an intruder scans the open ports on a host. Using Netstat, determine your connected ports, and using netstat –a, determine the all your listening port.

Some of the connected ports:
Some of the listening ports:

6. A factor in security is to determine the TCP ports which are listening on hosts, as these can be one way that an intruder can gain access to a host. Also it is possible to detect an intruder if they are scanning a network. Thus, download the NMAP portscanner. Note: **DO NOT PORT SCAN ANY OTHER MACHINE THAN YOUR NEIGHBOURS COMPUTER**. An example is at:

http://download.insecure.org/nmap/dist/nmap-3.95-win32.zip

A sample run is:

```
> nmap 192.168.1.1
Starting Nmap 3.95 ( http://www.insecure.org/nmap ) at 2006-01-12 13:26 GMT Standard Time
Interesting ports on 192.168.1.1:
(The 1668 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 00:0C:41:F5:23:D5 (The Linksys Group)
Nmap finished: 1 IP address (1 host up) scanned in 2.969 seconds
```

For your host, and using NMAP, complete the following:

Which ports are open:

Using the command netstat –a verify that these ports are open:

7. Download the client and server program, and run the server on one machine and set its listening port to 1001. Rerun the port scanner from your neighbour's machine.

↳http://www.dcs.napier.ac.uk/~bill/dotNetClientServer.zip

Does the port scanner detect the new server port: Yes/No

8. Next with the server listing on port 1001. Now write a Snort rule which detects the incoming SYN flag for a connection from a client to the server.

What is the Snort rule:

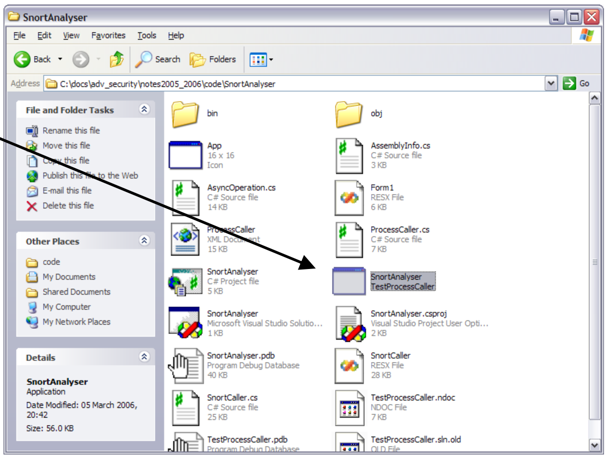
9. Write a rule for Snort which allows a port scan to be detected, and verify that it works:

Snort rule:

Did it detect the port scan: Yes/no

Note

If you ever want to run the program as a stand-alone file, you will find the EXE in the solution folder, such as:


SnortAnalyser
File Edit View Favorites Tools Help
Back Search Folders
Address C:\docs\adv_security\notes2005_2006\code\SnortAnalyser
Go
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
code
My Documents
Shared Documents
My Computer
My Network Places
Details
SnortAnalyser
Application
Date Modified: 05 March 2006, 20:42
Size: 56.0 KB
bin
obj
App 16 x 16 Icon
AssemblyInfo.cs C# Source file 3 KB
AsyncOperation.cs C# Source file 14 KB
Form1 RESX File 6 KB
ProcessCaller XML Document 15 KB
ProcessCaller.cs C# Source file 7 KB
SnortAnalyser C# Project file 5 KB
SnortAnalyser TestProcessCaller
SnortAnalyser Microsoft Visual Studio Solutio... 1 KB
SnortAnalyser.csproj Visual Studio Project User Opti... 2 KB
SnortAnalyser.pdb Program Debug Database 40 KB
SnortCaller RESX File 28 KB
SnortCaller.cs C# Source file 25 KB
TestProcessCaller.ndoc NDOC File 7 KB
TestProcessCaller.pdb Program Debug Database
TestProcessCaller.sln.old OLD File

Appendix

ARP. An ARP packet has the format:

```
03/05-19:59:56.376568 ARP who-has 192.168.1.101 tell 192.168.1.102

03/05-19:59:56.378315 ARP reply 192.168.1.101 (0:C:41:38:9B:A4) is-at
0:60:B3:9F:CA:E1
```

Ping (echo). A ping packet has the following format:

```
03/05-19:59:56.378331 0:15:0:34:2:F0 -> 0:60:B3:9F:CA:E1 type:0x800 len:0x4A
192.168.1.102 -> 192.168.1.101 ICMP TTL:128 TOS:0x0 ID:2861 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:4096  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
```

Ping (echo-reply). A ping packet has the following format:

```
03/05-19:59:56.379672 0:C:41:38:9B:A4 -> 0:15:0:34:2:F0 type:0x800 len:0x4A
192.168.1.101 -> 192.168.1.102 ICMP TTL:128 TOS:0x0 ID:21803 IpLen:20 DgmLen:60
Type:0  Code:0  ID:512  Seq:4096  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
```

ping payload

DNS (request). A DNS request packet has the following format:

```
03/05-20:21:33.008948 0:15:0:34:2:F0 -> 0:C:41:F5:23:D5 type:0x800 len:0x48
192.168.1.102:1082 -> 195.92.195.94:53 UDP TTL:128 TOS:0x0 ID:3318 IpLen:20
DgmLen:58
Len: 30
80 07 01 00 00 01 00 00 00 00 00 00 03 77 77 77  ............www
02 68 77 02 61 63 02 75 6B 00 00 01 00 01        .hw.ac.uk.....
```

DNS Server port

DNS (reply). A DNS rely packet has the following format:

```
03/05-20:21:33.037234 0:C:41:F5:23:D5 -> 0:15:0:34:2:F0 type:0x800 len:0xF6
195.92.195.94:53 -> 192.168.1.102:1082 UDP TTL:62 TOS:0x0 ID:0 IpLen:20
DgmLen:232 DF
Len: 204
80 07 81 80 00 01 00 01 00 04 00 04 03 77 77 77  ............www
02 68 77 02 61 63 02 75 6B 00 00 01 00 01 C0 0C  .hw.ac.uk.......
00 01 00 01 00 00 B4 36 00 04 89 C3 96 32 C0 10  .......6.....2..
00 02 00 01 00 00 B4 36 00 0C 03 6E 73 32 02 6A  .......6...ns2.j
61 03 6E 65 74 00 C0 10 00 02 00 01 00 00 B4 36  a.net..........6
00 0A 07 6E 65 6D 65 73 69 73 C0 10 C0 10 00 02  ...nemesis......
00 01 00 00 B4 36 00 0C 09 6E 61 6D 65 73 65 72  .....6...nameser
76 65 C0 10 C0 10 00 02 00 01 00 00 B4 36 00 0C  ve...........6..
09 6E 65 74 73 65 72 76 65 31 C0 10 C0 3A 00 01  .netserve1...:..
00 01 00 00 D3 24 00 04 C1 3F 69 11 C0 52 00 01  .....$...?i..R..
00 01 00 00 B4 36 00 04 89 C3 97 6E C0 68 00 01  .....6.....n.h..
00 01 00 01 16 D9 00 04 89 C3 97 69 C0 80 00 01  ...........i....
00 01 00 00 B4 36 00 04 89 C3 96 3D              .....6.....=
```