Lab 10: TCP Forensics

Details

Aim: To provide a foundation in analysing TCP packets

Activities

1. .NET provides an excellent interface to capturing and reading back data packets. For this lab download the solution from:

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

It has a Windows interface, such as:

Figure 1: Inteface

2. For the **Open** button add the following code:

```
PcapDevice device=null;
Packet packet=null;

openFileDialog1.ShowDialog();

try
{
   device = SharpPcap.GetPcapOfflineDevice(openFileDialog1.FileName);
   device.PcapOpen();

}
catch (Exception e1)
{
   MessageBox.Show("Error: " + e1.Message);
```

```
      return;
   }

   while( (packet=device.PcapGetNextPacket()) != null )
   {
      if (packet is TCPPacket)
      {
         TCPPacket tcp = (TCPPacket)packet;
         string srcIp = tcp.SourceAddress;
         string dstIp = tcp.DestinationAddress;
         int srcPort = tcp.SourcePort;
         int dstPort = tcp.DestinationPort;

         DateTime time = packet.PcapHeader.Date;
         int len = packet.PcapHeader.PacketLength;

         this.lbOutput.Items.Add(showFlags(tcp)+" Time: " +time.Hour+":"
            + time.Minute+ ":"+time.Second+
            " IP Src: " + srcIp+ " TCP Src " + srcPort+
            " IP Dest: " + dstIp+ " TCP Dest " + dstPort);

         ASCIIEncoding utf = new System.Text.ASCIIEncoding();
         string s = utf.GetString(tcp.Data);

         this.lbOutput.Items.Add("  Content: " + s);

      }
   }
```

3. Now download the file:

http://www.dcs.napier.ac.uk/~bill/capture2.zip

Read the file in, and determine the start of each conversation with the server, and complete Table 1 (note that the first entry has already been added).

Note: Identify a connection with the SYN, SYN/ACK and ACK flag sequence.

What is the domain name of the remote server?

What is the application protocol used?

For the first connection what is the HTTP request send (note look for commands such as GET, Accept: and so on)?

For the first connection what is the format of the HTTP reply (note look for a request such as HTTP/1.1 200)?

Table 1:

Connection	Src IP	Src Port	Dst IP	Dst Port
1	*192.168.1.102*	*1386*	*66.102.9.147*	*80*
2				
3				
4				
5				
6				
7				
8				

4. Now download the file:

http://www.dcs.napier.ac.uk/~bill/capture2.zip

Read the file in, and determine the start of each conversation with the server, and complete Table 1 (note that the first entry has already been added).

Note: Identify a connection with the SYN, SYN/ACK and ACK flag sequence.

What is the domain name of the remote server?

What is the trace of the traffic to and from the client to the server:

Which TCP ports are used on the server:

Table 1:

Connection	Src IP	Src Port	Dst IP	Dst Port
1	*192.168.1.102*	*1433*	*198.175.98.64*	*21*
2				
3				
4				
5				
6				
7				
8				