**G. H. RAISONI COLLEGE OF ENGG., NAGPUR**

**(An Autonomous Institute)**

**Department of Computer Science & Engg.**



**Date: 23-09-2021**

**Practical Subject: DCN Pr A2**

**Session: 2021-22**

**Student Details:**

| **Roll Number** | 01 |
| --- | --- |
| **Name** | Anand Suralkar |
| **Semester** | 9th |
| **Section** | A |
| **Batch** | CSE |

**Practical Details: Practical Number-8;**

| Practical Aim | To capture local network traffic and analyze different protocols using  Wireshark Network protocol analyzer |
| --- | --- |
| Theory & Syntax | Theory: Packet Analysis  Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorising packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.  Packet Capture (Packet Sniffing)  A packet sniffer is an application which can capture and analyse network traffic which is passing through a system’s Network Interface Card (NIC). The sniffer sets the card to promiscuous mode which means all traffic is read, whether it is addressed to that machine or not. The figure below shows an attacker sniffing packets from the network, and the Wireshark packet sniffer/analyser (formerly known as ethereal).  Capture and Analyse Traffic using Wireshark.  In this exercise, the fundamentals of the Wireshark Packet Sniffer and Protocol Analyser tool will be introduced. Then Wireshark will be used to perform basic protocol analysis on TCP/IP network traffic.    The Wireshark User Guide can be found at:  <http://www.wireshark.org/docs/wsug_html_chunked/>  (Optional) Download and install Wireshark on your PC.  Wireshark is a network packet sniffer (and protocol analyzer) that runs on many platforms, including Windows XP and Vista. If Wireshark is not currently available on your PC, you can download theLatest Windows Version from [[here] Wireshark 1.2.6 Windown Installer.](http://media-2.cacetech.com/wireshark/win32/wireshark-win32-1.2.6.exe)  Other Versions of Wireshark from <http://www.wireshark.org/download.html>. The current version ofWireshark, at time of writing, is version 1.2.6. The initial Wireshark installation screen is shown below  Click the **I Agree** button to the License agreement, then select options (or accept defaults) clicking the **Next** button on each screen when prompted.  **Note:** On the **Install WinPcap?** window, select the install WinPcap options and select **Start WinPcap service** option, if you want to have other users besides those with administrative privileges to runWireshark.  **Capture Traffic using Wireshark**    ***Select a Network Interface to Capture Packets through.***  Start the Wireshark application. When Wireshark is first run, a default, or blank window is shown.  To list the available network interfaces, select the **Capture->Interfaces** menu option.    Wireshark should display a popup window such as the one shown in [Figure 2.](#kix.svs8cfu4askg) To capture network traffic click the **Start** button for the network interface you want to capture traffic on. Windows can have a long list of virtual interfaces, before the Ethernet Network Interface Card (NIC).  Generate some network traffic with a Web Browser, such as Internet Explorer or Chrome. Your Wireshark window should show the packets, and now look something like.    To stop the capture, select the **Capture->Stop** menu option, Ctrl+E, or the Stop toolbar button. What you have created is a Packet Capture or **‘*pcap’***, which you can now view and analyse using the Wireshark interface, or save to disk to analyse later.  The capture is split into 3 parts:   1. **Packet List Panel –** this is a list of packets in the current capture. It colours the packets based onthe protocol type. When a packet is selected, the details are shown in the two panels below. 2. **Packet Details Panel –** this shows the details of the selected packet. It shows the differentprotocols making up the layers of data for this packet. Layers include Frame, Ethernet, IP, TCP/UDP/ICMP, and application protocols such as HTTP. 3. **Packet Bytes Panel –** shows the packet bytes in Hex and ASCII encodings.   To select more detailed options when starting a capture, select the **Capture->Options** menu option, or **Ctrl+K**, or the Capture Options button on the toolbar (the wrench). This should show a window such as shown below    **Wireshark Capture Options**  Some of the more interesting options are:   * ***Capture Options > Interface* -**Again the important thing is to select the correct NetworkInterface to capture traffic through. * ***Capture Options > Capture File* –**useful to save a file of the packet capture in real time, in caseof a system crash. * ***Display Options > Update list of packets in real time* –**A display option, which should bechecked if you want to view the capture as it happens (typically switched off to capture straight to a file, for later analysis). * ***Name Resolution > MAC name resolution –*** resolves the first 3 bytes of the MAC Address, theOrganisation Unique Identifier (OUI), which represents the Manufacturer of the Card. * ***Name Resolution > Network name resolution –*** does a DNS lookup for the IP Addressescaptured, to display the network name. Set to off by default, so covert scans do not generate this DNS traffic, and tip off who’s packets you are sniffing.   Make sure the **MAC name resolution** is selected. Start the capture, and generate some Web traffic again, then stop the capture. |
| Program |  |
| Output |  |
| Conclusion | Thus, we have install, configure and analyze local network traffic and analyze different protocols using Wireshark Network protocol analyzer. |