Ensuring Telnet Login Security by Ethical Hacking using Wireshark and Promisc Detect

Shilpa Rayanagoudar[1] , Priya Hampannavar[2] , Dr. Rajashekarappa[3]
[1,2]M. Tech in Information Technology, Dept. of ISE, SDM College of Engineering and Technology,(Affiliated to VTU, Belagavi), Dharwad, Karnataka,India
[3]Dept. of ISE, SDM College of Engineering and Technology,(Affiliated to VTU,Belagavi), Dharwad, Karnataka, India

ABSTRACT
Telnet is a protocol that facilitates user to connect to remote computers over a TCP/IP network. The Telnet program runs on client's computer and connects client's computer to a server on the network. A valid Username and Password enables client to login and start a telnet session. The login mechanism is believed to provide the required security by maintaining confidentiality of the login data. However, this approach still exhibits vulnerabilities. This paper demonstrates ethically hacking telnet to obtain login details of user using the Wireshark tool. Potential threats that are likely occur on a computer or network are identified through Ethical Hacking. Thus, helping to secure the system from potential attacks by tools like Promiscdetect, sniffdet, etc which checks if any network adapter(s) is running in promiscuous mode.

Keywords
Telnet , Wireshark , Ethical hacking, Promiscdetect

1. INTRODUCTION
Telnet provides client with a virtual terminal connection that facilitates bidirectional interactive text-oriented communication over the network and makes communication possible between the client(host) and the server(remote destination). A host can connect to the telnet server using the telnet client software installed on their system over a TCP/IP network[1]. Once the process of connection establishment is over , your client acts as virtual terminal and helps communicate with the remote host. In order to establish connection user needs to login to the host system which requires the client to already have an account in that system. This process of login requires username and password to be entered by the client to connect to the remote host. This paper further explains the methodology of ethically hacking the system to obtain thus entered username and password during login by the client using the Wireshark tool. In order to identify potential threats on a computer or network we define the terms ethical hacker or ethical hacking that are opted by individual or company respectively. An ethical hacker searches for any weak points through bypassing system security and helps identify vulnerabilities that could be exploited by malicious hackers [4]. In order to avoid any potential attacks the organizations then use this information to improve the system security. Wireshark is an excellent tool that helps to demonstrate ethical hacking in form of retrieving username and password from the logged in telnet session by the user [3].Promiscdetect is a command line utility which indicates whether any sniffing activity is carried out in the machine or system by analyzing if any network adapter(s) is running in promiscuous mode.

2. LITERATURE SURVEY

SL. No	Paper Title	Journal	Year of Publication	Description
1	"TELNET: the mother of all (application) protocols"	"IEEE Internet Computing , Volume: 2, Issue: 3, "	1998	Understanding telnet for reemote login and working of telnet application protocol in real time communication between two endpoints.
2	"Analysis and Application of Wireshark in TCP/IP Protocol Teaching"	"IEEE International Conference on E-Health Networking, Digital Ecosystems and Technologies"	2010	Understanding the use of Wireshark in TCP/IP Protocol Analysis and inspacting TCP/IP packets to resolve network traffic.
3	"TCP and UDP Packets Analysis Using Wireshark "	"International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7"	2015	Deep Analysis of TCP and UDP Packets to troubleshoot network traffic problems.

4	"Ethical Hacking: A Technique To Enhance Information Security"	"International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 2, Issue 12"	2013	Understanding the concept of Ethical Hacking for its use in security purposes.
5	"Ethical Hacking: A Security Technique "	"International Journal of Advanced Research in Computer Science and Software Engineering 5(4), April-2015, pp. 325-329 (IJARCSSE) ."	2015	Understanding the mechanism of Ethical Hacking and exploring intrusion detection measures to safegaurd the system.

Table 1 : Analysis of related work

3. METHODOLOGY

Data Flow Diagram (DFD)

Data flow diagram is a graphical representation of system's data (i.e. information) flow which helps developers to visualize different processes involved in software system easily. DFD uses top-down approach to design the system. Developers use data flow diagrams in both design and analysis phase of the SDLC (software development life cycle).

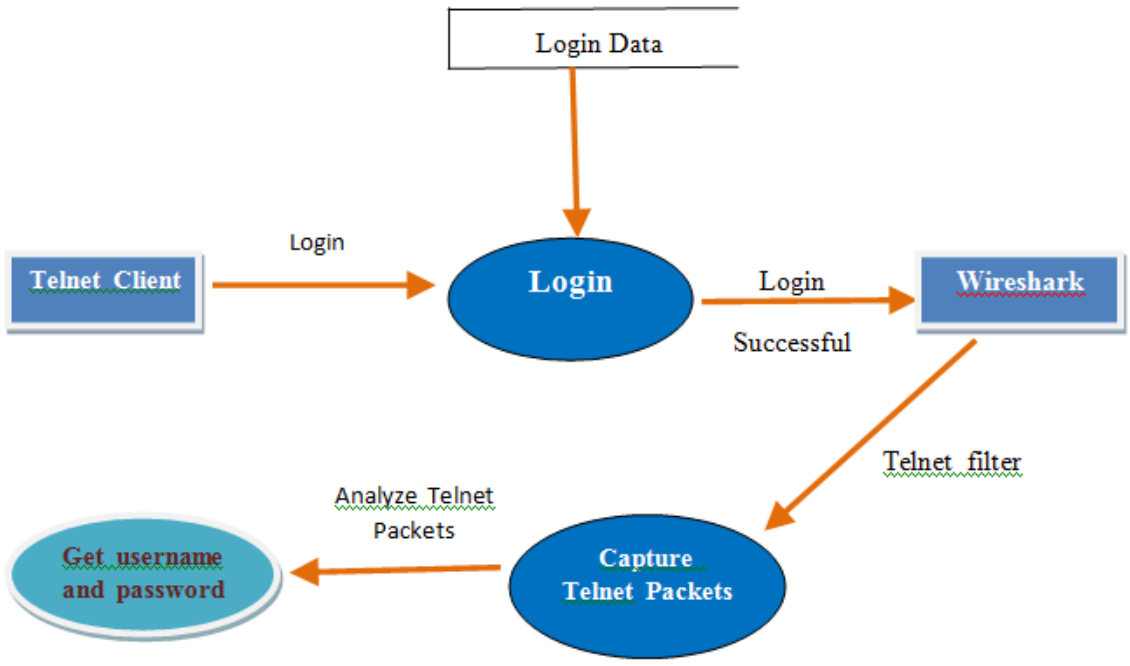

Figure 1 : Data flow diagram for hacking telnet using wireshark ethically

The above figure shows context Data Flow Diagram for ethically hacking telnet using wireshark. It contains a process that represents business activity or function where system data is transformed and manipulated to perform specific operation. It also contains entity that represents person or computer system communicating with the system to send or receive data. The connectors between process and the entities represent data exchange.

In this figure, Telnet client and wireshark are the external entities who will interact with the software system. Based on the diagram , Telnet client logins to the system . After successful login, wireshark captures telnet packets . Then user analyzes individual packet to get username and password.

4. IMPLEMENTATION

Wireshark is a tool used to analyze packets and protocols in a real time communication [2] . It is also known as Ethereal. It captures packets and displays them in human readable format . The tool includes special features like filters, colour coding and more which help to inspect every single

packet and helps to get knowledge about network

traffic in depth. It also assists in resolving troubleshoot networking problems.

To practically work on wireshark , the system should have some basic requirements mentioned below :

Hardware specifications

OS Name: Microsoft Windows 7 Ultimate

System Type : X64-based PC

Processor: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3300 Mhz, 2 Core(s)

RAM : 4.00 GB

Software Specification

Operating system : Windows 07

Tools : Wireshark 2.2.4

Command Line Interpreter (CLI) : Telnet

Capturing and analyzing packets in wireshark

Step 1: Wireshark can be downloaded from it's official website https://www.wireshark.org for Windows or MAC OS X. For operating systems like LINUX or UNIX , wireshark can be found in it's package repositories . After complete downloading of wireshark tool , we should install it on our machine and launch the application. There is a interface list to choose the interface to start capturing packages on the interface.

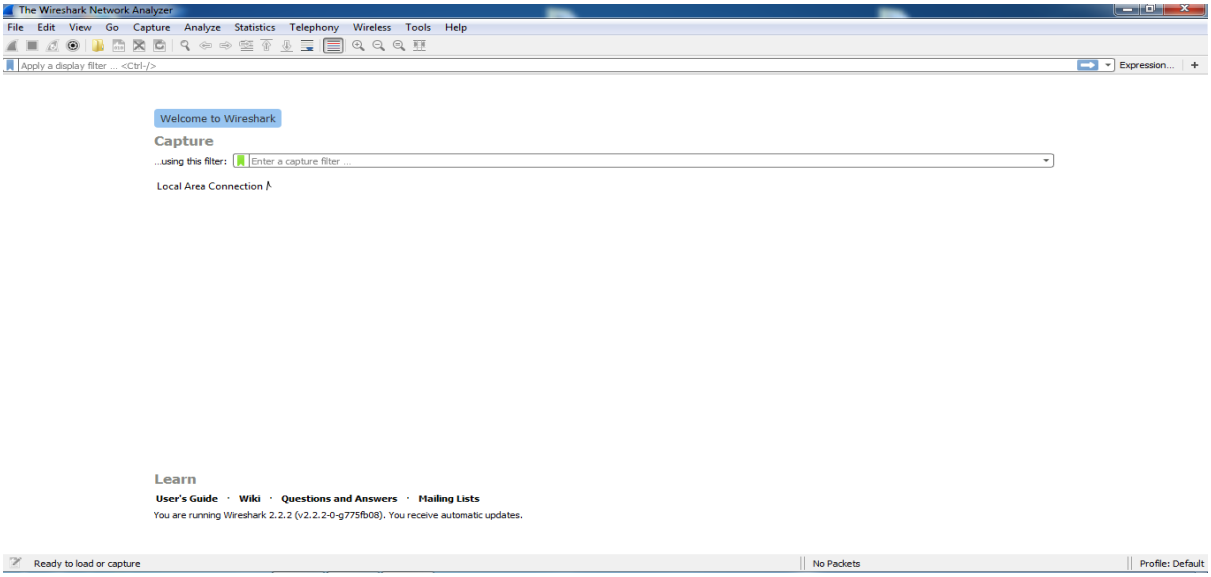

Figure 2 : Wireshark interface

Step 2 : When we want to inspect something specific , then apply filter by typing it into filter box present at the top of the window and click on Apply button. For example if we want to see only telnet packets ,then type "telnet" in filter box.

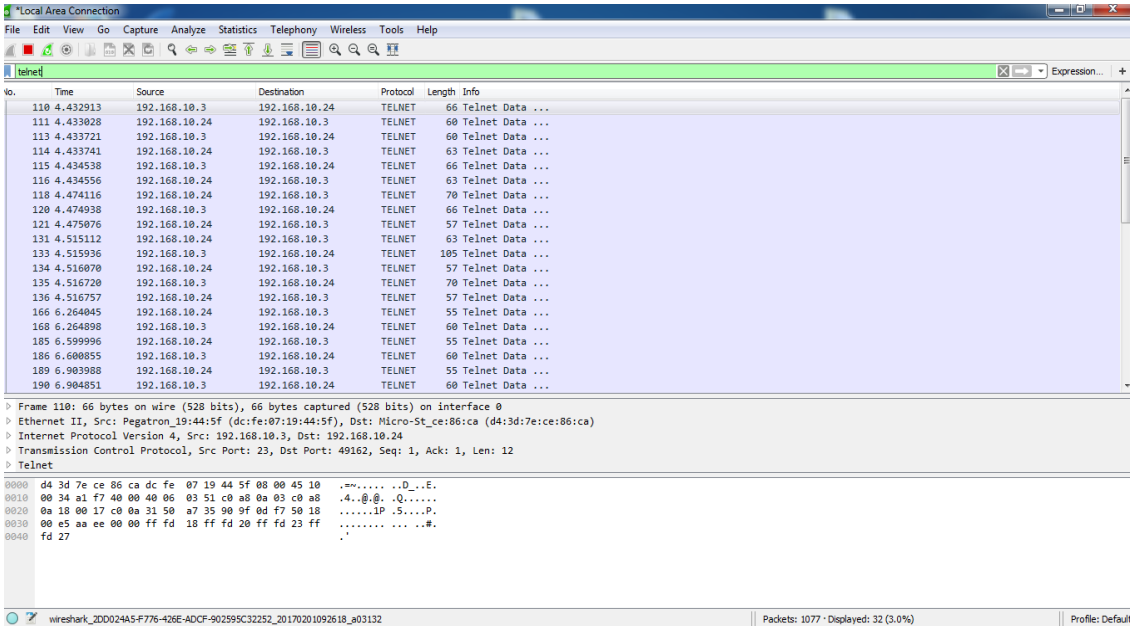

Figure 3 : Wireshark window for displaying packets

Step 3 : Open the telnet client in interactive mode from command prompt. Login to the telnet using proper credentials.

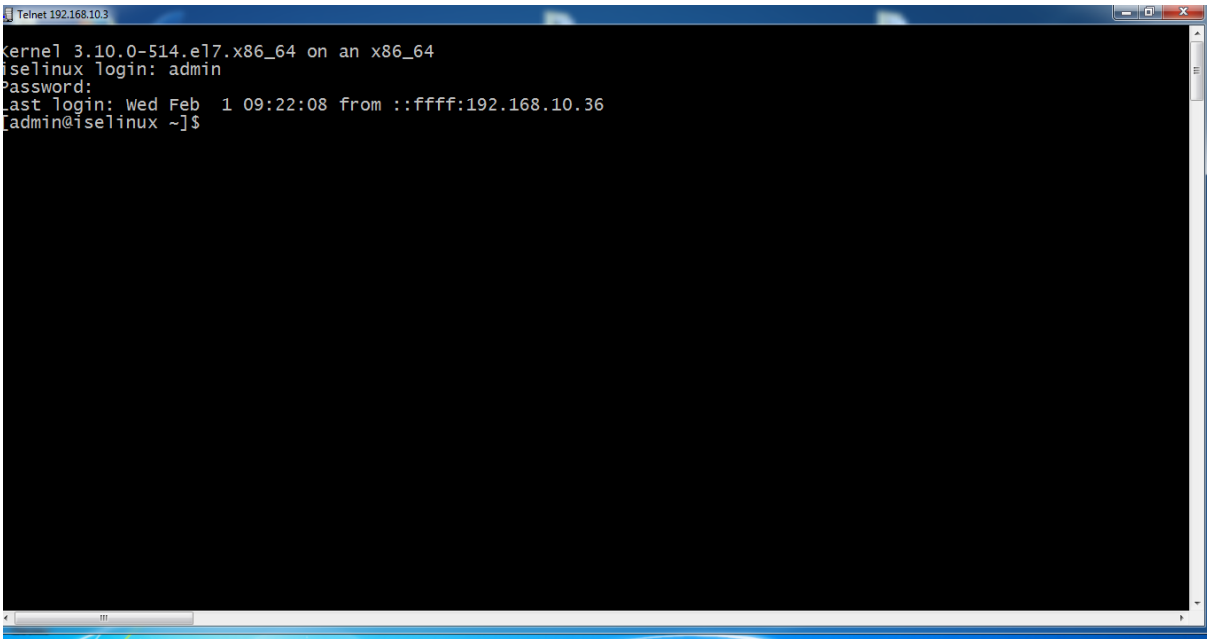

Figure 4 : Telent client login

Step 4 : Now open wireshark and type telnet in the filter box. As soon as we type telnet, only telnet packets get captured in the interface. Click on each packet on the interface and see the username and password character by character at the bottom of the wi

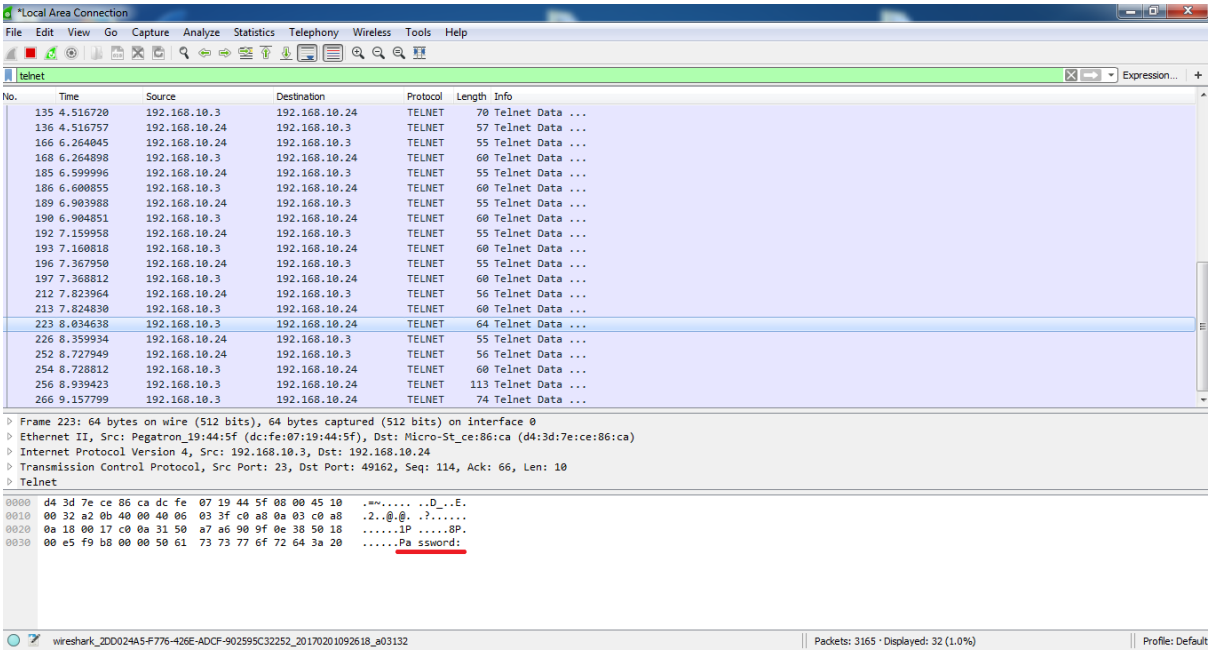

Figure 5 : Inspecting telnet packets to get username and password of telnet client

Detection Of Telnet Sniffing In Wireshark By Promisc detect

As we have installed wireshark for windows system,the sniffing tool should also support on the windows system.Promiscdetect is a sniffing tool for windows based system. For linux based systems, Sniffdet can be used as the sniffing tool.

Step 1: Download and install Promiscdetect.exe on the windows machine.

Step 2: Once the telnet login session has begun and the wireshark starts capturing telnet packets,open the command prompt(cmd) and run the command Promiscdetect.exe.

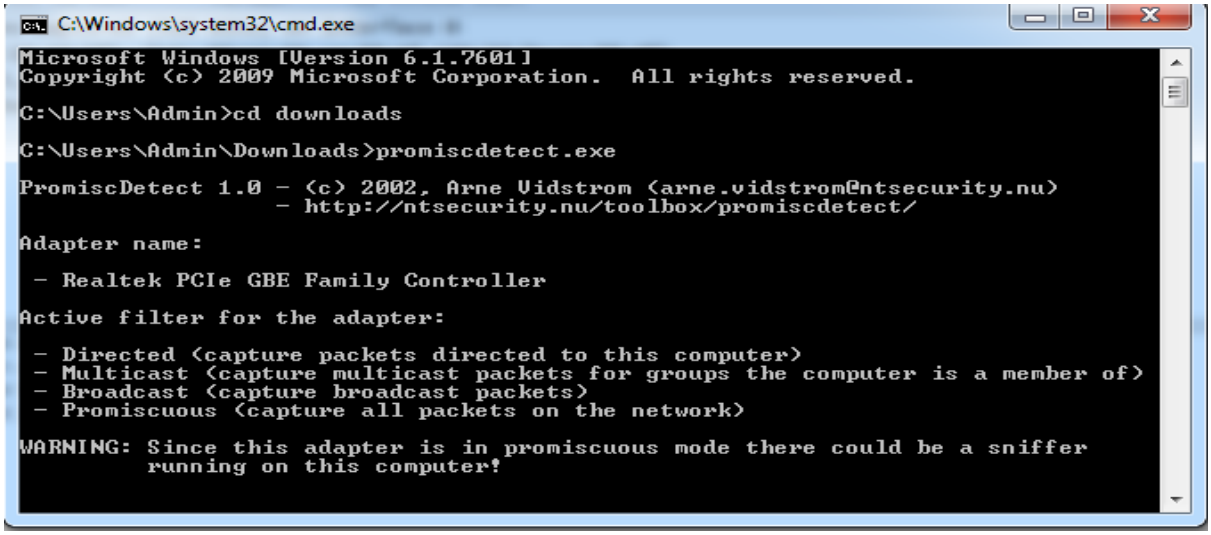

Figure 6 : Detecting sniffing activity

5. UNIT TESTING

Unit testing is a testing technique in which smallest part of the system or application like interfaces, functions , classes are tested individually for proper working of the system . Below are the test cases written for ethically hacking telnet using wireshark:

Table 2 : Unit test cases for complete working of the system

SL. No	Test Case	Input Data	Expected output	Actual output	Remarks
1.	Test if Wireshark is capturing TCP/IP Packets	TCP/IP filter	We should see Wireshark capturing TCP/IP packets	Captured TCP/IP packets	Test successful
2.	Test if user is able to login telnet client successfully	Correct username and password	User must successfully login to telnet client	Telnet login successful	Test successful
3.	Test if Wireshark is capturing Telnet Packets	Telnet filter	We should see Wireshark capturing telnet packets after client login.	Captured telnet packets	Test successful
4.	Test to inspect if captured telnet packets contain username and password of user	Captured telnet packets	We should see username and password in each packet character by character	Each packet containing information regarding telnet username and password	Test successful

6. FUTURE SCOPE

In the proposed implementation, wireshark and Promiscdetect tools are used to sniff telnet password and detect sniffing attack respectively on a single machine. In future , wireshark can be used to access username and password on a server connected to multiple telnet clients. It can also be used to resolve any troubleshoot networking issues related to packets in a real time communication. Proper methadologies should be designed to protect telnet data safe and confidential like determining whether unauthorized person is running wireshark on the network connected with multiple devices using network- or host-based utilities such as Sniffdet for UNIX based system , PromisDetect for windows based system.

7. CONCLUSION

Wireshark is a powerful tool which can be used in TCP/IP protocol teaching. It can be used to learn practical knowledge of network traffic analysis. Many IT industries use wireshark for network troubleshooting and protection of packets during communication between two endpoints.On the other side of

advantages , wireshark is used to capture telnet packets which can sniff username and password of the client working on the telnet by analyzing individual packet. So it's important to have a clear knowledge of wireshark and promiscdetect tools with proper usages in practical scenarios.

8. REFERENCES

[1] R.Khare and Irvine , "TELNET: the mother of all (application) protocols" , IEEE Internet Computing , Volume: 2, Issue: 3, Jun 1998 .

[2] Shaoqiang Wang, DongSheng Xu and ShiLiang Yan, " Analysis and Application of Wireshark in TCP/IP Protocol Teaching", IEEE International Conference on E- Health Networking, Digital Ecosystems and Technologies 2010.

[3] Mahesh Kumar and Rakhi Yadav, "TCP and UDP Packets Analysis Using Wireshark", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015.

[4] Sonal Beniwal and Sneha , " Ethical Hacking: A Security Technique", International Journal of Advanced Research in Computer Science and Software Engineering 5(4), April- 2015, pp. 325-329 (IJARCSSE) .

[5] Gurpreet K. Juneja , "Ethical Hacking: A Technique To Enhance Information Security", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 2, Issue 12, December 2013

[6] Using Wireshark, Web:http://www.howtogeek.com/104278/how-to-use-wireshark- to-capture-filter-and-inspect-packets/

[7] Mike Chapple, Wireshark tutorial: How to sniff network traffic, Web: http://searchsecurity.techtarget.com/tip/Wireshark-tutorial-How-to-sniff-network- traffic

[8] Wireshark Site, Web: https://www.wireshark.org/

[9] Behrouz A Forouzan, "Data Communication and Networking", cGraw-Hill, 4th Edition.