A Project: Stressful Password Sniffer

Surisack Phouapanya, psurisack (at) wustl.edu; **Marlon I. Calero,** marlon.i.calero (at) go.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract

Authentication is a key component of network security. If authentication credentials such as passwords are compromised, then it allows an attacker to masquerade as a legitimate user of the computing system. Often, this can give the attacker ultimate access to a system if the attacker can masquerade as an administrative user.

In this project, we demonstrate the ease at which passwords can be intercepted in a Man-in-the-Middle attack using our own software program. The reader will learn to be very careful with passwords used in Telnet, FTP, and HTTP, as often times, these passwords are sent bare-naked in the clear. Although HTTP passwords can be in cipher text form, it will be shown that such passwords can be cracked easily.

Keywords:

Password Authentication, Password Sniffer, Man in the Middle, Telnet, FTP, HTTP, MD5, WinPcap

Table of Contents

1. Introduction

The program is a network packet sniffer that sniffs out server IP addresses, usernames, and passwords. It is built in Windows 7 and the setup described in this manual is based around a Windows 7 machine but the ideas portrayed can be applied to other systems. The program currently only captures Telnet, FTP, and HTTP passwords. The program can capture clear text and it can also capture and decrypt md5 passwords in HTTP packets. The basic idea is to use the program to implement a Man-in-the-Middle attack. The Windows 7 PC is used to create a fake Wi-Fi hot spot that will act as bait for clients to use to connect to the internet. When clients connect and send out network packets, the program will collect the passwords real-time and print them out to screen. Any password cracking also happens in real time. Cracking is done by using the John the Ripper program. From the client point of view, he or she would not normally suspect a Man-in-the-Middle attack is occurring.

In this report, we will first describe the vulnerable protocols that are exploited, the WinPcap API used in the program, the setup of the project, and how to run the program. Then we will list limitations of the program, provide a summary, give the references, and list acronyms used throughout this report.

The program was created for academic purposes and is not to be used for real world exploitation.

2 Vulnerable Protocols

The program only captures three types of protocols. These protocols are similar to one another in that passwords are transmitted in the clear and these passwords are easy to recognize in the packet structure. The protocols that will be described in order are Telnet, FTP, and HTTP.

2.1 Telnet

Telnet rides on the TCP protocol and it itself is a protocol that allows for two-way interactive communication over the internet or a LAN. It is also one of the oldest internet standards [7]. Due to its age, it should come as no surprise that when the protocol was specified, network security was not a point of emphasis. One of the biggest vulnerability with the Telnet protocol is that it transmits the userâ€™s password in the clear. In fact, during user authentication, both the username and the user password are sent in the clear character by character.

2.2 Telnet Packet Analysis

Telnet packets can be differentiated from other types of packets because these packets have a destination address of 23. When the user is inputting his username or password, these Telnet packets have a very specific packet length. Specifically, the packet length in bytes is the summation of the lengths of the Ethernet header, the IP header, the TCP header, and a single Telnet byte. This last byte will be a character which is either a letter in the username or a letter in the password during user authentication.

2.3 FTP

Like Telnet, FTP is an older protocol that also that transmits usernames and passwords in the clear. It is a network protocol that is used to transfer files from one host to another using a client-server interface [8].

2.4 FTP Packet Analysis

FTP uses port 21 for communication. Like Telnet, FTP rides on TCP and in the packet, any byte of data following the TCP header is an FTP data byte. The attacker can sniff the usernames and passwords by looking for the key terms â€œUSERâ€ and â€œPASSâ€, respectively. The actual username or password will follow these key terms in the packet.

2.5 HTTP

HTTP is an application protocol operating in the client-server model and it acts as the backbone for the communication of data in the World Wide Web [9]. The user would enter his username and password in the web browser (the client) and then HTTP packets would be created and then sent to the web server for user authentication. In regular HTTP, these packets contain the username in the clear and the password is either also in the clear or in the form of a hash.

2.6 HTTP Packet Analysis

HTTP packets are sent to port 80 on the server. In the packet, like the previous two protocols, the HTTP data bytes start after the end of the TCP header bytes. When the user inputs his username and password, these two items will be send in a â€œPOSTâ€ HTTP packet. That is to say, the first bytes of the HTTP packet will literally contain the ASCII characters â€œPOSTâ€. The username and password can be obtained by searching for terms such as â€œuser=â€, â€œname=â€, â€œmd5password=â€, â€œpassâ€, or any other terms that can act as the key for a username or a password. The character â€œ&â€ or the end of the packet acts as the end of the username or password value. As previously mentioned, HTTP passwords can be in hash form and in this case, the hash can be stored and a password cracker such as John the Ripper can be used to crack the password.

3 WinPcapAPI

The WinPcap API is an invaluable tool for capturing any network packets that can be captured on a network interface. If the network interface is configured for promiscuous mode, the API will allow any host computer to capture packets that can come through the local network, even if those packets are not destined for the host computer. What follows are a list of important components of the API [1] :

pcap_findalldevs_ex

The host computer may have more than one network card. This command helps the program obtain a listing of all network interfaces that can be used for packet capture.

pcap_freealldevs

This frees the list of network interfaces. This function is invoked after a network interface is chosen for capture at which point the list is no longer is needed.

pcap_open

This function opens a single interface for packet capture and creates a handle to the interface. The handle can be

defined to operate in promiscuous mode by supplying the right function arguments.

pcap_compile

Each interface handle can be configured to filter for packets that contain specific protocols or parameters. This function is used to create the filter for the interface handle.

pcap_setfilter

After the filter is created, this function is called to set the filter on the interface handle.

pcap_loop

When packets are captured and filtered, the packets are sent to the callback function. The function here links the callback function to the interface handle. When the correct packet is received, the call back function is invoked and the packet is further processed inside the call back function.

4 Project Setup

The project setup requires a number of tools. A list of tools is the following: a network card that can create its own Wi-Fi hotspot, Visual Studio 2010 Ultimate (or similar), a computer running Windows 7 (or similar), a password cracker software like John the Ripper, the source code for the password sniffer program, and a client computer to act as the test user. The setup of some of these tools are described below.

4.1 Visual Studio 2010

The following instructions were inspired from the video found in [3].

- Download the main.c code from here:
- main.c
- http://students.cec.wustl.edu/~marlon.i.calero/Stressful_PW_Sniffer.html
- Download WinPcap packet capture library development pack from here:
- http://www.winpcap.org/devel.htm
- Unzip the file into the C drive.
- Open Visual Studio 2010 and create a new project as a Win32 Console Application with an empty project.
- Add main.c to the project.
- Right-click the project and select Properties.
- Under Configuration Properties -> C/C++ -> Additional Include Directories, add "C:\WpdPack\Include".
- Under Configuration Properties -> Linker -> Input -> Additional Dependencies, add "wpcap.lib" and "ws2_32.lib".
- Under Configuration Properties -> Linker -> General -> Additional Library Directories, add C:\WpdPack\Lib. Build the program.

4.2 John the Ripper Password Cracker

Further description of this program can be found in [6].

- Download the community enhanced version for Windows from here:
- http://www.openwall.com/john/
- Unzip the file and place it in "Visual Studio 2010\Projects\solution_name\project name".
- Rename the top directory to "john".
- With running the program, newly cracked username/passwords will be sent to screen.
- Previously cracked hashes will be in "Visual Studio 2010\Projects\solution_name\project name\john\run\john.pot"

4.3 Fake Wi-Fi hotspot

The following steps were taken from the video in [4]:

- Open the command prompt in Administrative Mode.
- Check if the Windows 7 machine has a network device that can create a Wi-Fi hotspot by inputting "netsh wlan show drivers". If output contains "Hosted network supported: Yes", then the machine is suitable for a Man-in-the-Middle attack.
- Create a connection by typing in the command "netsh wlan set hostednetwork mode=allow ssid= choose_name key=choose_8_character_key". In the previous command, change the ssid and key as appropriate.
- Start the hosted network: "netsh wlan start hostednetwork".
- Open "Open Network and Sharing Center". Notice that the hosted network has no internet access. To gain internet access, the hosted network will tap into the internet connection of the normal non-hosted connection.
- Select the normal non-hosted connection and then select Properties -> Sharing tab.
- Check the checkbox, "Allow other network users to connect through this computer's Internet connection". In the dropdown box, select the connection for the hosted network.

5 Running the Program

At startup, the program will list the network devices by number. Choose the number that corresponds to the hosted network that is to be connected to by the clients. The program will confirm the selection and will start polling for passwords. When a packet containing a user name and a password is captured, the program will display the type of protocol, the server IP address that the client is connecting to, the user's name, and the user's password. The program will do this for all packets until the program is closed. Telnet usernames and passwords are sent to screen letter by letter in real time. For the other protocols, the usernames and passwords are sent to screen after the user inputs the username or password and presses the (Enter) key. "X" out of the program to close it.

A screenshot of a running program is seen in Figure 1. The program first asks for the selection of a network interface and interface â€œ2â€ is chosen. The screenshot shows in order the capture of a Telnet session, an FTP session, an HTTP session with clear text password, and an HTTP session with the cracked MD5 password. As can be seen, the cracked password is â€œgodzillaâ€!

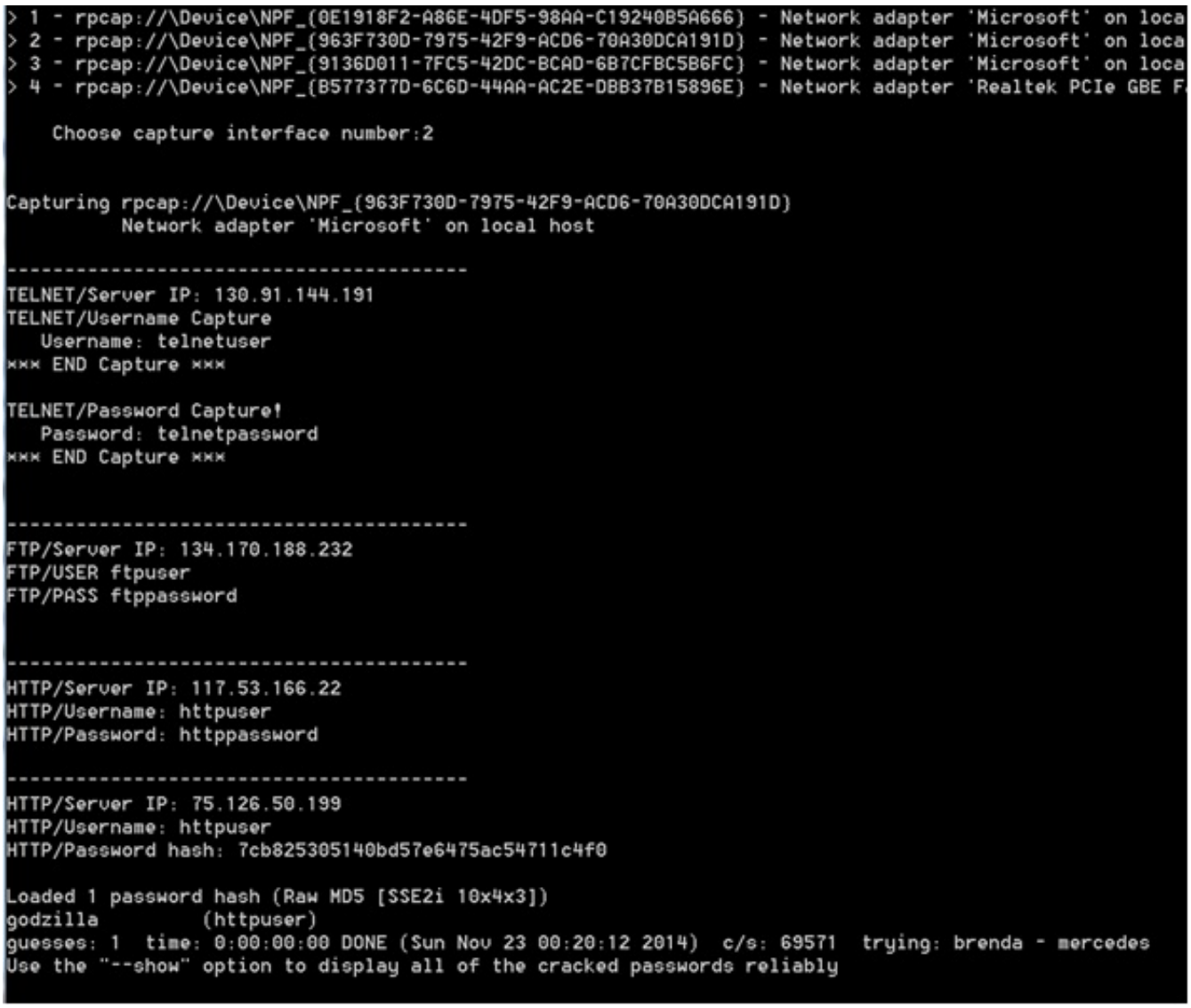

Figure 1

6 Program Limitations

The program behaves very much like a program in beta. The program has been tested with some sites and situations but not all sites and situations have not been tested for various reasons, including development time constraints. The program was tested using only a single client. Program behavior with multiple clients is unknown but the program should be able to service multiple clients.

For Telnet, it will output non-alphabetic characters, such as (back space), that are typed by the user. For HTTP, password cracking is limited to the abilities of the John the Ripper program. Wordlists can be added to this program to enhance md5 cracking. Password cracking is limited to just md5.

For program can be improved upon by testing it at different sites in the internet. Surely, some sites will cause the program to fail and analysis can be done to determine the cause of failure. One of the reasons why a failure can occur is because the search keys in the packets such as â€œpass=â€ or â€œUSERâ€ may be different at untested sites. The program can be made more robust by accounting for more search keys.

7 Summary

The password sniffer program offered an example of why protocols like Telnet, FTP, and HTTP have been improved upon or abandoned in some use cases. This is because it is much too easy for anyone to obtain the user authentication information using a password sniffer. The program also emphasizes the need to have multiple passwords for different accounts. This is because if a user were to use the same username and password for FTP and an online banking website, once the FTP credentials are uncovered, essentially the userâ€™s online bank login information are compromised as well. Then it is not difficult for an attacker to track the online activity of the user and determine the userâ€™s exact online banking website and use the compromised information to login to the userâ€™s online bank account. It was also shown that password cracking can be easily done for simple or common passwords. To make password cracking more difficult, passwords should be long and complex to deter at minimum a good dictionary attack.

8 References

[1] WinPcap, "The industry-standard windows packet capture library," http://www.winpcap.org/

[2] WinPcap, "WinPcap tutorial: a step by step guide to using WinPcap," http://www.winpcap.org/docs/docs_412/html/group__wpcap__tut.html

[3] Dan Lo, "How to: Program Development with Winpcap Using Microsoft VisualStudio," https://www.youtube.com/watch?v=QIZ9fmV5rMQ

[4] iTech, "How to turn your Windows 7/8 Laptop into a WiFi Hotspot 2014," https://www.youtube.com/watch?v=zFHIvCMTqbQ

[5] Martin Casado, "The Sniffer's Guide to Raw Traffic," http://yuba.stanford.edu/~casado/pcap/section1.html

[6] John the Ripper, "John the Ripper password cracker," http://www.openwall.com/john/

[7] Wikipedia, â€œTelnet,â€ http://en.wikipedia.org/wiki/Telnet

[8] Wikipedia, â€œFile Transfer Protocol,â€ http://en.wikipedia.org/wiki/File_Transfer_Protocol

[9] Wikipedia, â€œHypertext Transfer Protocol,â€ http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

9 Acronyms

API	Application Programming Interface
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
WinPCap	Windows Packet Capture API
MD5	Message Digest 5

Last Modified: December 1, 2014
This and other papers on current issues in network security are available online at
http://www.cse.wustl.edu/~jain/cse571-14/index.html
Back to Raj Jain's Home Page