CS 161
Computer Security

Dawn Song
Fall 2012

Lab 4
Network Security and Malware

Due Date: October 31, 2012 by 11:59pm

Introduction

In this lab, you will learn how to work with real network security related issues. You will primarily be using `wireshark` for examining packet traces. `Wireshark` is a free and open-source packet analyzer.

No collaboration beyond your lab partner is allowed! Maximum group size is 2. Solutions submitted after a deadline will not be graded.

Running `wireshark` to capture live traffic other than your own maybe unethical. This lab is not an invitation for you to start sniffing data on any networks other than with informed consent of all involved parties. If you are uncertain about where to draw the line, come talk to the course staff first.

Getting Started

We will be using Wireshark as the primary tool for packet inspection. You can either install `wireshark` on your local machine following the instructions in the `wireshark` manual (`http://www.wireshark.org/docs/wsug_html_chunked/`), or you can download a virtual machine from `http://www.eecs.berkeley.edu/~mor/cs161/lab4-vm.tar.gz` (Username: `ubuntu`, Password: `ubuntu`).

Once you have the `wireshark` setup, download the required files for this lab from `http://www.eecs.berkeley.edu/~mor/cs161/pcaps.tar.gz`.

Suggested reading: Wireshark user guide at `http://www.wireshark.org/docs/wsug_html_chunked/`

Problems

0. Learn how to use wireshark

This is to make sure that you get used to of using Wireshark. Open the file `q1.pcap` in Wireshark and try using the following filters:

1. `ip.addr==192.168.1.102`
2. `ip.src>=192.168.1.1 and ip.src<=192.168.255.255`
3. `ip.dst>=192.168.1.1 and ip.dst<=192.168.255.255`
4. `ip.addr>=192.168.1.1 and ip.addr<=192.168.255.255`
5. `tcp contains traffic`
6. `http.response.code=404`

Understand what do these filters do.

1. YouTube becomes NoTube

You got your first internship as network security manager at a high school, and, on the second day of your work, found that YouTube was unable to open and displayed page could not be loaded when people tried to access YouTube. Luckily, you had started monitoring the traffic since your first day work here. So your job became easy and simple–analyze the web traffic in q1.pcap trace to find out how the attacker disrupted your YouTube access.

1. Find out the type of attack being launched?
2. What were the victims' IP addresses?
3. How much downtime did this attack cause?

Hint: search for failed connections, there are 4 victims.

2. The mysterious wall post

After successfully solving the youtube problem, you were so excited to send a message to your best friend on facebook. But your message got also posted on your friends wall, which shows there was someone in school attacking the network. Fortunately, you could locate the computer the hacker used, and have collected the last days web traffic to analyze.

1. Examine the web traffic in q2.pcap to find evidence of the attack used for the wall post.
2. Find the secret wall post, the timestamp when it occurred and the cookie value (c_user) of the attacker.

Hints: Check POST requests, cookie values

3. Information theft from a web server

The principle called you about the leakage of some exams last night, but did not tell you which files on the server were exams for security concerns. However, you always monitor the server traffic, so you pull out the data collected last night to analyze.

1. Analyze the web accesses in the q3.pcap. Determine the type of attack used to access the file.
2. What was the file name? How do you know it was successfully accessed?

4. The leaked URL

The security issue had been a problem for a while. You had locked one suspicious user and collected his web traffic. He talked about it during an unencrypted Facebook chat with someone, but the URL itself was encrypted.

1. Analyze the chat traffic in the q4.pcap. Determine how by sniffing the session you could have extracted the URL.
2. What is the URL?

Submission

The submission instructions will be provided by Oct 25th.