CS2017 Assignment Brief

Contents

Introduction

Welcome to the first CS2107 Assignment. In this assignment, you will be exploring how to examine Packet Capture (PCAP) files using a network protocol analyser, Wireshark.

This assignment takes the form of an information security Capture-The-Flag (CTF) style competition. In a CTF, participants solve problems involving security weaknesses to bypass defences to obtain a sensitive piece of information called the 'flag'. In this assignment, we will be exploring different common pitfalls in web applications.

Instructions

Grading Scheme and Due Date

This is an individual assignment. You are allowed to post questions on the IVLE forum but please ensure that the questions do not ask for the solution. Additionally, please do not post the answers to the challenges. When answering questions, please exercise some restraint.

This assignment is worth 12 out of 60 points allocated to all three assignments and about 5% of the grade for the entire module. The assignment consists of 9 challenges:

1. Installing Wireshark and Examining a PCAP (1 point)
2. Searching for the Flag Within a PCAP (1 point)
3. Filtering the Packet Capture by Protocol (1 point)
4. Filtering the Packet Capture by IP Address (1 point)
5. Observing TCP Streams (1 point)
6. Generating Statistics (1 point)
7. Finding Telnet Login Password (2 points)
8. Finding Web Form Login Password (2 points)
9. Extracting Files from PCAP (2 points)

The assignment is due 2 March 2018, 2359HRS.

General rules and Guidelines

1. Do not attack any infrastructure not explicitly authorised in this document.
2. Work individually. Discussion on the forum is allowed but please refrain from posting solutions.
3. The skills taught in this assignment are not to be used on any system you do not own or have express permission to test. This is a criminal offence under the Singapore Computer Misuse and Cybersecurity Act.
4. Ask the TAs for assistance only after you have exhausted every other avenue of self-help.

5. Every challenge will contain a flag and will provide the accepted flag format. Please ensure your submissions meet the flag format stated exactly. This means include the flag{} portion if the flag format asks for it.
6. Complete all the challenges before attempting the quiz to submit your flags on IVLE. Be very careful please, only one attempt will be allowed. It is recommended that you note down all your flags in a separate document.
7. The challenges are tested from the NUS WiFi within the School of Computing and NUS. Connectivity cannot be guaranteed anywhere else outside of NUS.

One of the most important skills in the information security field is the skill of seeking an answer independently. In each challenge, there may be hints hidden within the challenge and some may be necessary to complete them. It is expected that the participant be able to utilise resources discovered through Google or any other search engine to achieve the tasks.

While the challenges might not be covered in class, the topics in the assignment are very applicable to security problems in real life. In the long run, the practical skills gained would benefit participants immensely.

Creating a Linux Virtual Machine with Wireshark

1. Install Virtualbox (https://www.virtualbox.org/wiki/Downloads)

2. Create an Ubuntu Virtual Machine (https://www.ubuntu.com/download/desktop)

3. Run sudo apt-get install wireshark in the terminal

4. Move the entire assignment package onto the virtual machine using shared folders

Contact

Please direct any inquiries about the assignment to shirong@u.nus.edu

Acknowledgements

This assignment is a collective work of present and past teaching assistants, including Kion Shi Rong (AY 17/18), Nikolas Tay(AY 16/17), Jeremy Heng(AY 16/17)

PCAP Analysis

PCAP Analysis Packet captures are very commonly analysed in real security work to detect breaches as well as determine the chain-of-events after a breach has occurred. These captures contain a record of the network traffic. In this section, you will learn how to use Wireshark to analyse these packet capture files to extract information.

1. Installing Wireshark and Examining a PCAP

Flag Format: domain name in lowercase (e.g. google.com)

File: intro.pcapng

To complete this task, please install Wireshark on your Ubuntu virtual machine. This can be done by doing sudo apt-get install wireshark in the terminal.

After you have done this, please open the intro.pcapng file in Wireshark and provide the domain name queried for over DNS in the packet capture as the flag.

2. Searching for the Flag Within a PCAP

Flag Format: cs2107{<32 lowercase hexadecimal characters>}

File: haystack.pcapng

Use the packet search functionality to search for the string ‘cs2107{’ in the packet bytes. The search bar may be brought up through the ‘edit’ submenu or by using the shortcut CTRL-F. Please take extra care to set the parameters of the search properly so that a result may be found.

3. Filtering the Packet Capture by Protocol

Flag Format: flag{<32 lowercase hexadecimal characters>}

File: protocols.pcapng

While examining a realistic packet dump, it is not unusual to encounter more than one protocol, It is important to know how to drill down to specific protocols contained in the dump that you might want to inspect. In this task, please find the flag in ‘HTTP’ traffic. Please note that there are multiple false flags with the same flag format to prevent simple searching so please be careful.

4. Filtering the Packet Capture by IP Address

Flag Format: flag{<32 lowercase hexadecimal characters>}

File: ipfind.pcapng
Often, you would also wish to filter the packet dump by specific IP addresses once you have identified possible interesting targets. To complete this task, please look for the flag found in the packets involving the IP address 162.213.39.42.

5. Observing TCP Streams

Flag Format: flag{<32 lowercase hexadecimal characters>}

File: tcpstream.pcapng

In the tasks so far, we have been inspecting single packets for their contents. However, most communication over TCP involve streams that span across multiple packets. Thus, it is important to be able to observe the contents of the stream as a whole.

Hint: Follow TCP Stream option when right clicking on a packet may help.

6. Generating Statistics

Flag Format: integer

File: statistics.pcapng

In this task, you are required to find the number of ICMP packets contained in the packet dump. There are multiple statistics generators to choose from in the menu. Explore these options to achieve the objective.

Hint: Try Protocol Hierarchy.

7. Finding Telnet Login Password

Flag Format: cs2107{<32 lowercase hexadecimal characters>}

File: telnet.pcapng

Often, administrators would access a server from a remote location. SSH is recommend as it provides encryption. In this task, you are given a packet capture of remote access to a server. You are required to find the password that was used in the telnet login session.

8. Finding Web Form Login Password

Flag Format: cs2107{<32 lowercase hexadecimal characters>}

File: weblogin.pcapng

In this task, you are given a packet capture of a user web browsing activity. A login form was submitted over unencrypted http. You are required to find the password that was used in a login page.

9. Extracting Files from PCAP

Flag Format: cs2107{<32 lowercase hexadecimal characters>}

File: image.pcapng

In this task, you are given a packet capture of user web browsing activity. You are required to get the flag which is an image file.