Universität Zürich[UZH]

0690 - Communication Systems Lab Course

Exercise 5

1) Introduction
2) Tasks

October 18, 2022

Assistants: Christian Killer, Jan von der Assen, Dr. Alberto Huertas

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland

1 Introduction

In this lab, you will learn how to analyze the traffic log output of a honeypot and determine information about the attacks that occurred. The goal is to learn the behavior of attackers and also the countermeasures that should be taken to make your system safe.

2 Tasks

You are the system administrator, and you know that a machine from your network was compromised. The file `attack.log` contains logs recorded during the time of the attack. Download the file from the web page and use Wireshark to analyze it. Answer the following questions:

1. As a first step, try to get an overview of the network traffic in the log file, for which Wireshark will help you process the data with the *statistics* tab (`https://wiki.wireshark.org/Statistics`):
   (a) Which application-layer protocols were used over UPD?
   (b) Which application-layer protocols were used over TCP?
   (c) Which application-layer protocol had the highest number of packets?
   (d) Which two hosts exchanged the highest number of IPv4 packets?
   (e) Which host sent the highest number of IPv4 packets?
   (f) How many packets can be attributed to SSH traffic?
2. Now, try to investigate the actual packets and spend some time trying to find where the attacker exploits a vulnerability or misconfiguration. In which packet did the attacker succeed to exploit a vulnerability?

   Hints: The vulnerability/misconfiguration is part of the OWASP top ten security risks. The top-down view established in tasks 1a and 1b may guide you in your analysis.
3. Which kind of vulnerability does the attacker exploit?
4. What is the IP address of the attacker? How about the physical location (country of origin) of the IP address?
5. What is the IP address and location of the victim?
6. Aside from exploiting the vulnerability, which other activities are performed by the attacker?
7. Write down the time when the attacker opens a remote shell? How does he do it?

8. What is the IP address of the machine where the attacker stores the root kit?
9. Follow the TCP Stream where the rootkit is sent to the breached machine. What can you find out about it's content?
10. What would you recommend someone to protect his/her server from this type of attack?

Do not forget to send your configuration files and answers to vonderassen and killer@ifi.uzh.ch.