Laboration in Network Security (Natsak09/DD2495)

Intrusion analysis

By: Pehr Söderman. Assistent: Erik Gustafsson ergu@kth.se

Introduction

The goal of this task is to give you a chance to familiarize yourself with some of the tools used for analysis of a network intrusion and let you explore what a typical intrusion looks like in a relatively safe manner.

Warning

The material in this lab is live. While the packet logs are safe to open in wireshark they contain malicious code which can (and will) infect a computer if extracted and executed. You might have to disable antivirus protection to be able to work with the material on a windows computer. We do not take responsibility if you decide to execute any code or commands you find in the logs.

Material supplied

Log 1: A packet log from the first day of the intrusion
(sha1: 92bf0a7958175a413f3f28a5b44eaa60722b43e3)
Log 2: A packet log from the third day of the intrusion
(sha1: 2a4f5a1cbeea215f2d9b3b6f70aaed914e4db18b)
These are two packet dumps from a real intrusion.

Recommended tools

These are some of the tools you can use to solve the problems. They are not strictly necessary, and you are free to use any other tool you find useful. Wireshark is strongly recommended as it will make the analysis much easier.

* Wireshark (Protocol analyzer)
* Tcpdump (Packet sniffer)
* P0f (passive OS fingerprinter)
* TCPFlow (TCP stream reassembler)
* Sha1 (Checksum tool)
* Strings (Basic unix tool)

- Snort (Intrusion Detection System)
-

Presentation of your results

You present your results in the form of a written article and turned in before 20/2/2009.

It is graded pass/fail. You are expected to give proper references, either to locations (packet numbers) in the supplied files, output from tools or to external sources for your answers. All

tools used should be listed in an appendix, along with a short description of your experience with the tool.
Any source of information is acceptable, as long as it is _referenced_ and evaluated (in case of internet sources that might be of dubious quality).
Using unreferenced sources will result in a failing grade.

Questions

The questions are not listed in order and are not necessarily easiest to solve in this order.

1: Create a detailed network map of all systems involved. Give relevant details on each system where available, such as OS, purpose and if you think it's controlled by the attacker.

2: Give as much relevant details as you can on the attack used to take over the server. Can you identify the specific service and vulnerability targeted? How?

3: Identify the tools the attacker downloaded. Which are these tools? What does each tool do?

4: Analyze and compare the protocol distribution Log 1 and Log 2. Which protocol stands out in Log 2? It's a protocol you would not expect in most networks today.

5: Why and for what does the attacker use this protocol?

6: Where are the attackers from? How did you reach this conclusion? How does this match with the IP addresses involved?

7: How much of the attack was automated? How do you come to this conclusion?

8: Give a detailed timeline of the attack, from start to finish.

9: What can you tell about the SSH session found in log 2?

10: What would you recommend doing with the server after your analysis?