A reversed approach to security - Hidden living (pratical session)

Alexandre Dulaunoy

29th January 2005

Contents

1	Introduction to Forensic Analysis	1
	1.1 Golden rules	2
	1.2 Source of information	2
2	Gathering	2
	2.1 Before events	2
	2.2 After events	3
3	Analyzing	3
4	A hidden life	3
	4.1 Rootkits	3

"When a thing is funny, search it carefully for a hidden truth." George Bernard Shaw

1 Introduction to Forensic Analysis

Forensic Computing is the way to reconstruct the past events from a computing device. Various actions are required in order to make efficient analysis like gathering data/information, analyzing the information. The actions done must provide data/information free (as much as possible) of distortion. On a computer, it's very easy to hide, mangle, change, update information in a "non-visible" way and great care must be taken to provide as much as possible the "reality" from the past. (check part II of the DESS curses)

The term "Forensic Analysis" often refers to the application of science in a law case. In Forensic Computing, it will be the application of science practices for reconstructing the past events from a computing device with or without a legal process.

Forensic analysis is often used to analyze a computer system after being compromised by an attacker but can be also used for various other purposes (reverse engineering, debugging, audit after a specific events on the system, monitoring...).

1.1 Golden rules

- Think twice before acting. Every action on a computer system can have an impact on the data (e.g. The access-time in various file system). On every action, there are implications.
- Don't work on original data. Don't work on original data. Don't work on original data.
- Don't trust anything on the system.
- Be imaginative. There is more than one way to analyze the collected information and "evidence". Attackers are also very imaginative and smart. The quality of data analyzing depends of your imagination...

These golden rules are applicable for the people doing the forensic analysis but we suppose that the attackers are following the same golden rules on the compromised system.

1.2 Source of information

Everything related to the data generated/handled by the computing device.

2 Gathering

The quality of the forensic analysis will depend of the quality of the data on the system. Quality is a difficult factor to meter for data or information on a system. For example, data must be in a good shape to make a complete analysis or should contain as much information as possible (e.g. think about complete IP frame including payload and not only headers).

2.1 Before events

It's often to difficult to have a very complete infrastructure in production environment regarding data capture. Except for the case of the Honeynets (cf. part1), the data capture is often limited to the classical audit and logging systems of the different systems. Logging before events is often small or incomplete. (think about the administrators not using hash fingerprint/checksums of binaries before going live...)

2.2 After events

Time is your enemy. You have to carefully analyze data by their orders of volatility. On a information system, the order is depending of the lifetime information in the different storage mechanisms. Attackers are often using techniques using lifetime and state of storage.

3 Analyzing

Practical and imaginative classes on the pcap capture given.

4 A hidden life

In the early eighties, attackers were compromising systems (mainly UNIX operating systems) without taking a lot of measures for being hidden. In that case, system administrators were able to use common UNIX system command to monitor activities on their systems. But knowledge of attacker were growing and starting to create tools to take over root or limit his ability to monitor the system. One of the first example is in a article from Phrack issue 25 (1989) : "HIDING OUT UNDER UNIX". The example was a simple C program to erase wtmp entries for the 'who' type programs. This was very basic but now methods have evolved to provide more complete solution to attacker to hide them self, their activities or limit their evidences.

4.1 Rootkits

Rootkits are kind of Trojan Horses including various kind of programs to change the behavior (without too much visibility) of the operating system to hide activities from the attackers. Rootkits can be very complex and using various approach to hide their self but also can provide back doors, dedicated services to the attacker and his friends.