Gabriele **Proietti Mattia**

Advanced Operating Systems and Virtualization

[Lab 10] Rootkit Analysis

Department of Computer, Control and Management Engineering "A. Ruberti", Sapienza University of Rome

gpm.name · proiettimattia@diag.uniroma1.it

A.Y. 2020/2021 · v1

Introduction

Examples are from the folders

https://github.com/gabrielepmattia/aosv-code-examples/tree/main/12-rootkit

Introduction

Rootkits

The term root-kit derives from the first UNIX malwares that allowed to grant root access. However, nowadays especially under Microsoft Windows, the term rootkits has taken on a more narrow definition. Rootkits in Windows refers to programs that use **system hooking** or modification to hide files, processes, registry keys, and other objects in order to hide programs and behaviors. In particular, Windows rootkits do not necessarily include any functionality to gain administrative privileges. In fact, many Windows rootkits require administrative privileges to even function.

As a consequence for "launching" a rootkit you need a privilege escalation, that is the purpose of another set of malwares.

A Rootkit Analysis

DIAG

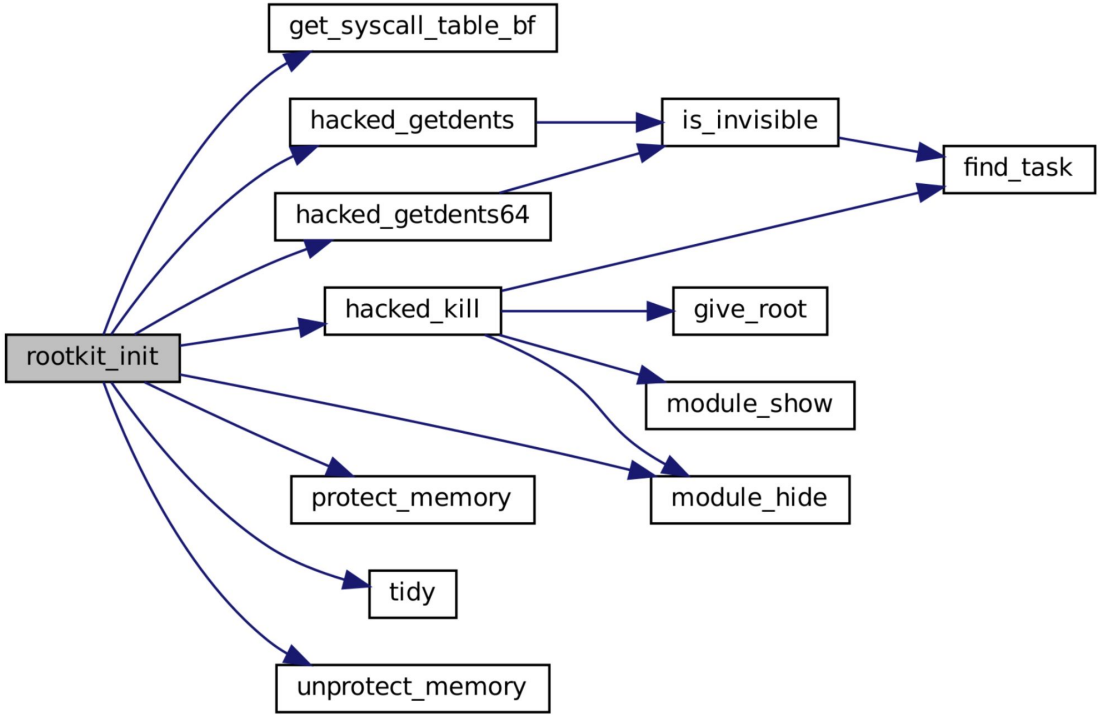
Capabilities

This rootkit has been written by Victor N. Ramos Mello in 2014. It offers the following capabilities:

- when loaded, the module starts invisible;
- hide/unhide any process by sending a signal 31;
- sending a signal 63(to any pid) makes the module become (in)visible;
- sending a signal 64(to any pid) makes the given user become root;
- files or directories starting with the `MAGIC_PREFIX` become invisible;

We obviously mount manually the rootkit so we assume that a privilege escalation has been already done and the attacker managed to mount the module.

module_init()


get_syscall_table_bf
hacked_getdents
is_invisible
find_task
hacked_getdents64
hacked_kill
give_root
rootkit_init
module_show
protect_memory
module_hide
tidy
unprotect_memory

Advanced Operating Systems and Virtualization

[Lab 10] Rootkit Analysis

LECTURER

Gabriele **Proietti Mattia**

gpm.name · proiettimattia@diag.uniroma1.it

DIAG