|  |  |
| --- | --- |
| Course | Operating System Security |
| Assignment | Bonus Assignment |
| Student ID | 100899259 |
| Student Name | Maisha Khatoon |

# Hacker Defender

## What is the purpose of a rootkit?

A rootkit's function is to manage a hacked framework while evading detection by security software and framework directors.

Rootkits are typically used by attackers to carry out vengeful actions including stealing sensitive data, remotely managing the system, or launching other attacks from the compromised system. Assailants can employ rootkits to maintain control over a hacked system for longer periods of time because they can hide their presence and activity from security software.

## A general description of Hacker Defender

Hacker Defender is a well-known and highly sophisticated rootkit that is capable of hiding its existence on a compromised system while enabling attackers to manipulate the system and steal sensitive data from a distance.

## How does it work?

Hacker Defender is frequently distributed through a variety of techniques, such as exploiting programming flaws, implementing social design principles, or using a deception software. The rootkit can carry out a variety of malicious tasks after being installed, including keyboard recording, network traffic interruption, and remote order execution, among others.

## What does it affect?

The functioning framework, bit, device drivers, and other fundamental framework records are just a few of the many components of the framework that Hacker Defender affects. Additionally, it can disable security software, inject malicious code into legitimate cycles, and change system settings without the client's knowledge.

## What are the consequences of being infected by it?

The effects of being infected by Hacker Defender can be severe, ranging from information theft and unauthorized access to system resources to complete system split-up and the installation of other malware. The more damage Hacker Defender can do, the longer it will go unnoticed.

## How is this rootkit identified & removed?

Since Hacker Defender is designed to evade detection by antivirus software and other security measures, it can be difficult to distinguish it from other malware and to remove it. However, the rootkit can be identified and removed using specific rootkit scanners and manual examination of the framework's documents and cycles.

## How can a system be hardened against this type of rootkit?

To prevent a system from becoming infected by Hacker Defender, it is essential to implement strong security measures, such as keeping up with the newest developments, using reputable antivirus software, and avoiding shady downloads or communications. Additionally, employing interruption discovery and avoidance frameworks can assist in identifying and obstructing unwelcome activity and traffic on the company. Checking system logs frequently and maintaining strong points for defence can also help prevent malware like Hacker Defender and other types from becoming established in a system.