# **CTF Topic: PDF Analysis With PDF**



# **1. Introduction**



Malware developers apply various methods to hide their malware and make it undetected by the defensive measure in place of the victim system. These techniques are ever changing and change frequently with the time given for them to evolve. Here we have listed some of the common measures malware developers apply to hide their malware from the defensive measures in place of the victims system.

**Fileless Malware**

Usually, malwares use command line tools such as power shell to execute payload and generate a connection with the malware developer, Malwares reside in memory and don’t need any installation into the hard disk for them to execute a payload

**Rootkits**

Rootkits are another form of malware which is produced to gain unauthorized root access / administrative level access to a victim's system while concealing their presence, they modify the operating system at a basic level and intercept the system messages to hide their presence.

**Changing Code**

Malware authors change their code (not the code logic itself) to hide it , this can trick malware analyzing software’s, common methods for changing code can involve encryption and continuously changing the malwares code to evade analyzing software’s which use signature based analyzing algorithms.

**Impersonating as a valid file**

Malwares often conceal themselves by changing their appearance to that of a legitimate system file for eg: a malware’s name might be svchosst.exe whereas there is a system file with the name svchost.exe.

# **Let's Begin The Challenge**

# **Question**

**Flag 1 :** Which is a system file svchosst.exe or svchost.exe

**Answer :** svchost.exe

**Flag 2 :** Which command line tool do malwares use to execute their payload

**Answer :** powershell

**Flag 3 :** Which level of access do rootkits try to get

**Answer :** administrative