Windows password cracking using PupyRat

Pratheesh K Francis, Reshma Sarah Rony, Sandra Sebastian

Amal Jyothi College Of Engineering, Kanjirappally, 2019

Abstract

Password cracking has become one of the popular means for breaking into ones privacy. To avoid this, various methods have been adapted to store passwords in such a way an intruder cannot find it easily. One such method is to keep the password hashed.

Hashing refers to the process of changing the source data into hashed codes. This is done using hashing algorithms. Hashed codes are irreversible but they can be cracked using certain tools by turning candidate passwords into hashes, and then checking them against the unknown password.

In this paper we focus on cracking windows passwords which are stored as hashed code in the system using the tools PupyRat and findmyhash. Solutions to evade these problems are also proposed in this paper. To obtain the windows password from a target we use PupyRat. It is a multi-function RAT (Remote Administration Tool) and exploitation tool mainly written in python which can exploit a targeted system and retrieve confidential data stored in the system.

1. Introduction

Backdoors are a type of malware used by both authorized and unauthorized users to access system data. They function by appending the payload with the actual transmitted data. This payload perform intended actions on the target once it is run in the target machine.

PupyRat is such a tool of Kali Linux that uses payload as a backdoor to gain access to the targeted system. On running the payload, the attacker gains access to the victim system and gets the stored credentials. The Windows password is stored in hashed form as the Security Accounts Manager (SAM) file which the attacker tries to reverse.

findmyhash is a python script which takes the target hash and checks different hash cracking websites for result.