ASK.ME

# ASK MiM Extraction System

Anant Kaul

Shreyansh Anchlia

Kishor Sarswat

([ask.me.mitm@gmail.com](mailto:ask.me.mitm@gmail.com))

# **BACKGROUND**

A man-in-the-middle attack is a type of cyber-attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM. There are various types of man-in-the-middle attacks as follows:

* Rogue Access Point
* ARP Spoofing
* mDNS Spoofing
* DNS Spoofing

So, our tool aims to protect our users from such types of attacks, which can be very harmful for any type of organisation/ company or a simple user as well (personal information is the main concern).

# **AGENDA**

The main aim for a secured environment is just a simple trick which can be performed using a windows command prompt. But the speciality of our tool is to give the users an environment that runs at the background (ghost mode) without any interrupt unless there is a serious trouble, which can in turn harm your system as well as your organisation/ company or any sort of personal information like login credentials, card details and many more.

# **DOCUMENTAION**

This works on the principle that when a MiM attack is initiated with you, the ‘Default Gateway’ of the machine changes. of detection