# **LITERATURE REVIEW**

# **ON**

# **TOOL-KIT FOR CYBER SECURITY**

# **LITERATURE TITLE: -** TOOL-KIT FOR CYBER SECURITY

# **TEAM NAME: -** DEVIL\_DEVELOPERS.

# **GROUP MEMBERS:-**

1. **Abhishek Kishor Gandre (Leader)**
2. **Aakansha Arvind Ajmire**
3. **Gauri Ram Vyawahare**
4. **Shritej Narendra Nimbhorkar**
5. **Shyam Sanjay Sagane**
6. **Smit Kishor Vidhate**

# **GUIDE: - Prof. Nachiket Rathod**

**LITERATURE REVIEW:-**

Picture an employee at her computer, working with data. In the background, a hacker secretly accesses her company’s confidential files. He steals sensitive information and sells it to criminals, who then hold the company ransom for a profit.

It sounds like something out of a movie, but unfortunately, it’s a common occurrence in today’s online landscape. This is why Cyber Security has become such a vital part of any business strategy—and Cyber Security specialists are in demand now more than ever.

**Proposed Work and Objectives:-**

In New Digital World and Daily life the rate of cyber-crime increases very rapidly in day by day. We need to required audit or analysis our network, network-devices like routers, hub, switches, servers and others. Also we need to analysis system software and application software as well as hardware.

In Linux Operating System cyber security application was preinstall and in command line interface (cmd) and when we run this application we need to type command on terminal it’s get lot of time to run particular application. And if any condition command syntax or spelling will incorrect it’s give an error .but we are want one clicked on application and it can run application and it gives function and feature like it without getting error. As well as it tool kit gives lots of help to ctf players for solving hackathon task in at one toolkit.

**Analysis of Problem:-**

In computers security capture the Flag (CTF), "flags" are secrets hidden in purposefully-vulnerable programs or websites. Competitors steal flags either from other competitors (attack/defense-style CTFs) or from the organizers (jeopardy-style challenges. Several variations exist, including hiding flags in hardware devices.

Security CTFs are usually designed to serve as an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world. Classic activities include reverse-engineering, packet sniffing, protocols analysis, system administration, programming, cryptanalysis, and writing exploit, among others. In an attack/defense style competition, each team is given a machine (or a small network) to defend—typically on an isolated competition network. Teams are scored on both their success in defending their assigned machine(s) and on their success in attacking the other team's machines. A variation from classic flag-stealing is to "plant" own flags on opponent's machines.

In Our New Digital world “Hackathon” was organized by many Organization. During the hackathon solving CTF players having trouble (activities include reverse-engineering, packet sniffing, protocols analysis, system administration, programming, cryptanalysis, and writing exploit) when if command syntax will wrong, when website searching for task perform that time website particular url cannot remember or name of website by ctf player, others troubles.