**Network**

**Security**

**Class 9**

**Lab 27**

|  |
| --- |
| Lab Objectives:  * Introduction to Ethical Hacking |

## Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. In this course, we will take you through the various concepts of Ethical Hacking and explain how you can use them in a real-time environment for your Network Security.



## 

## Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

## *Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call****Ethical Hacking****.*



## A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

# Types of Hacking

## We can divided hacking into different categories, based on what is being hacked. Here is a set of examples −

## IMG_256Website Hacking − Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

## Network Hacking − Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.



## IMG_256Email Hacking − It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

## Ethical Hacking − Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

## IMG_256Password Hacking − This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

## Computer Hacking − This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.



# Advantages of Hacking

## Hacking is quite useful in the following scenarios −

## To recover lost information, especially in case you lost your password.

## To perform penetration testing to strengthen computer and network security.

## To put adequate preventative measures in place to prevent security breaches.

## To have a computer system that prevents malicious hackers from gaining access.

# Disadvantages of Hacking

## Hacking is quite dangerous if it is done with harmful intent. It can cause −

## Massive security breach.

## Unauthorized system access on private information.

## Privacy violation.

## Hampering system operation.

## Denial of service attacks.

## Malicious attack on the system.

# Purpose of Hacking

## There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people involve in hacking activities −

## Just for fun

## Show-off

## Steal important information

## Damaging the system

## Hampering privacy

## Money extortion

## System security testing

## To break policy compliance

# Some Popular Tools for Ethical Hacking

## NMAP

## Metasploit

## Burp Suit

## Angry IP Scanner

## Cain & Abel

## Ettercap

## EtherPeek

## SuperScan

## QualysGuard

## WebInspect

## LC4

## LANguard Network Security Scanner

## Network Stumbler

## ToneLoc

## We will jump into details about these tools and ethical hacking methodologies from next class so that you can able to secure your network.