**Network**

**Security**

**Class 9**

**Lab 30**

|  |
| --- |
| Lab Objectives:  * Operating System Finger Printing |

## The term OS fingerprinting in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer. This could be −

## Active Fingerprinting − Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS. In the following section, we have given an example to explain how you can use NMAP tool to detect the OS of a target domain.

## Passive Fingerprinting − Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host.

## We have the following four important elements that we will look at to determine the operating system −

## TTL − What the operating system sets the Time-To-Live on the outbound packet.

## Window Size − What the operating system sets the Window Size at.

## DF − Does the operating system set the Don't Fragment bit.

## TOS − Does the operating system set the Type of Service, and if so, at what.

## By analyzing these factors of a packet, you may be able to determine the remote operating system. This system is not 100% accurate, and works better for some operating systems than others.

# Basic Steps

## Before attacking a system, it is required that you know what operating system is hosting a website. Once a target OS is known, then it becomes easy to determine which vulnerabilities might be present to exploit the target system.

## Below is a simple nmap command which can be used to identify the operating system serving a website and all the opened ports associated with the domain name, i.e., the IP address.