**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. 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 checking 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.

## If you do not have nmap command installed on your Linux system, then you can install it using the following command −

$sudo apt install nmap

## 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. Suppose you want to check about daraz.

$sudo nmap -O -v www.daraz.com.bd

## Result is:

## You have seen that [www.daraz.com.bd](http://www.daraz.com.bd) is using Linux Operating System to host their website.

# Quick Fix

## You can hide your main system behind a secure proxy server or a VPN so that your complete identity is safe and ultimately your main system remains safe.

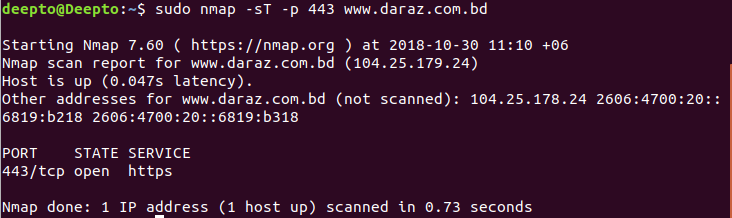
# Port Scanning

## We have just seen information given by nmap command. This command lists down all the open ports on a given server. See the previous result again. You can see this port report.

|  |  |  |
| --- | --- | --- |
| **PORT** | **STATE** | **SERVICE** |
| 22/tcp | open | ssh |
| 80/tcp | open | http |
| 443/tcp | open | https |
| 3306/tcp | open | mysql |

You can also check if a particular port is opened or not using the following command −I am checking 443 port

*sudo nmap -sT -p 443 www.daraz.com.bd*



## Once a hacker knows about open ports, then he can plan different attack techniques through the open ports.

# Quick Fix

## It is always recommended to check and close all the unwanted ports to safeguard the system from malicious attacks.

# DNS Enumeration

## Domain Name Server (DNS) is like a map or an address book. In fact, it is like a distributed database which is used to translate an IP address 192.111.1.120 to a name www.example.com and vice versa.



## DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. The idea is to gather as much interesting details as possible about your target before initiating an attack.

## You can use nslookup command available on Linux to get DNS and host-related information.

### The interactive mode

## The interactive mode is entered by typing the nslookup command without any arguments:

## [IMG_256](https://geek-university.com/wp-content/images/linux/nslookup_interactive_mode.jpg?x13092)

## To find the IP address of a host, simply type the hostname:

## [IMG_257](https://geek-university.com/wp-content/images/linux/nslookup_hostname.jpg?x13092)

## [IMG_258](https://geek-university.com/wp-content/images/linux/nslookup_ip_address.jpg?x13092)To perform a reverse DNS lookup, enter the IP address of a host:

## To display MX records (the mail servers responsible for accepting email messages on behalf of a recipient’s domain), set the DNS query type to MX:

## [IMG_259](https://geek-university.com/wp-content/images/linux/nslookup_mx.jpg?x13092)

## To display NS records, set the DNS query type to NS:

## [IMG_260](https://geek-university.com/wp-content/images/linux/nslookup_ns.jpg?x13092)

### The non-interactive mode

## The non-interactive mode is invoked by typing the nslookup command, followed by the name or the IP address of the host to be looked up.

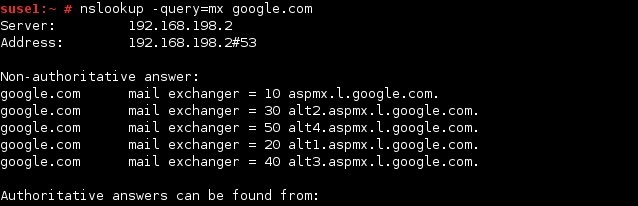
## For example, to display the IP address of a hostname, use the following command:

## [IMG_261](https://geek-university.com/wp-content/images/linux/nslookup_command_hostname.jpg?x13092)

## To do a reverse DNS lookup, use the following command:

## [IMG_262](https://geek-university.com/wp-content/images/linux/nslookup_command_reverse_dns_lookup.jpg?x13092)

## To display the MX records, use the -query=mx option:

[](https://geek-university.com/wp-content/images/linux/nslookup_command_mx.jpg?x13092)

## To display the NS records, use the -query=ns option:

## [IMG_264](https://geek-university.com/wp-content/images/linux/nslookup_command_ns.jpg?x13092)

## To display the SOA record (information about the domain), use the -query=soa option:

## [IMG_265](https://geek-university.com/wp-content/images/linux/nslookup_command_soa.jpg?x13092)

## [IMG_266](https://geek-university.com/wp-content/images/linux/nslookup_command_any.jpg?x13092)To display all the available DNS records, use the -query=any option:

# What we have learned today:

## OS detection using Nmap

## Port Scanning

## Name Server Information using NsLookup