Name:SUDEEP

Date:28-2-2023

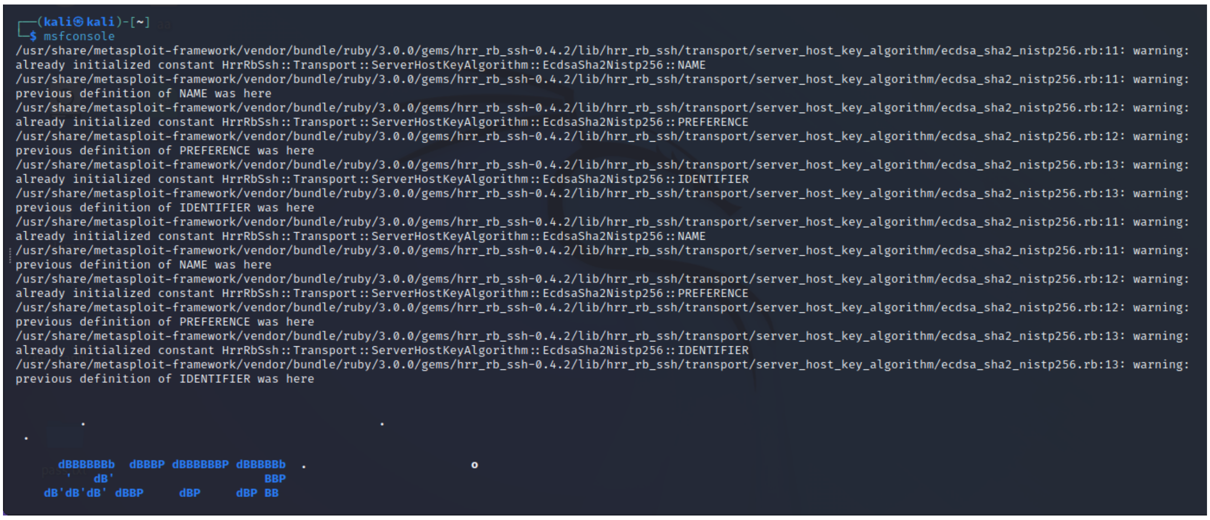
Task:1

1. **<u>Dos attack using nmap:</u>**

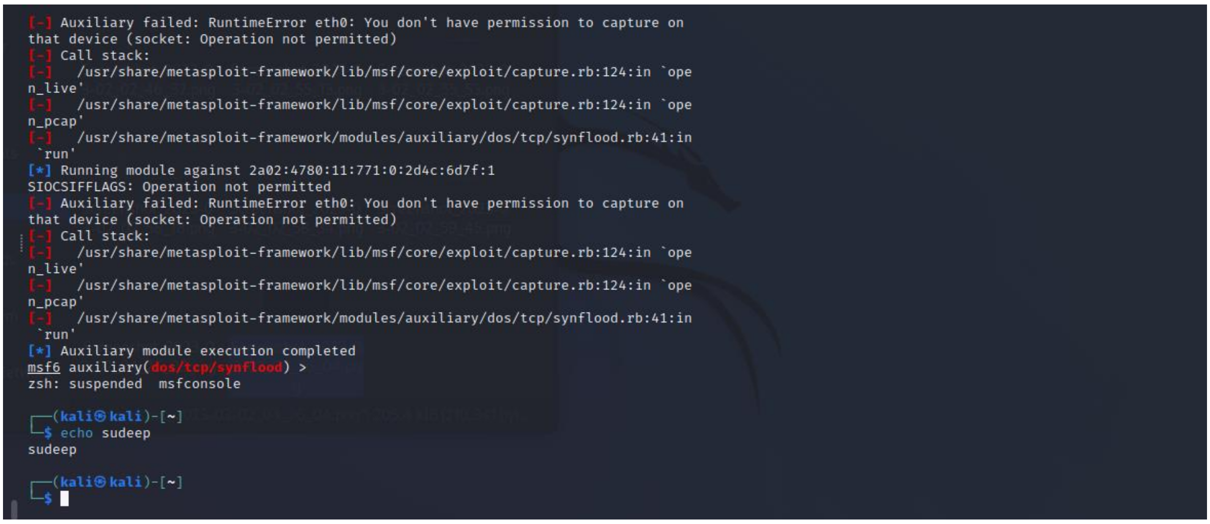
   The nmap scripting engine has numerous scripts that can be used to perform dos attack.This specific recipe will demonstrate how to locate dos scripts,identity the usage of the script.

   command:

   $ msfconsole
   Use auxiliary/dos/tcp/synflood
   Set RHOSTS mitkundapura.com
   Run



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning:
already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning:
previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning:
already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning:
previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning:
already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning:
previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning:
already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning:
previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning:
already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning:
previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning:
already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning:
previous definition of IDENTIFIER was here


         .                                         .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
```



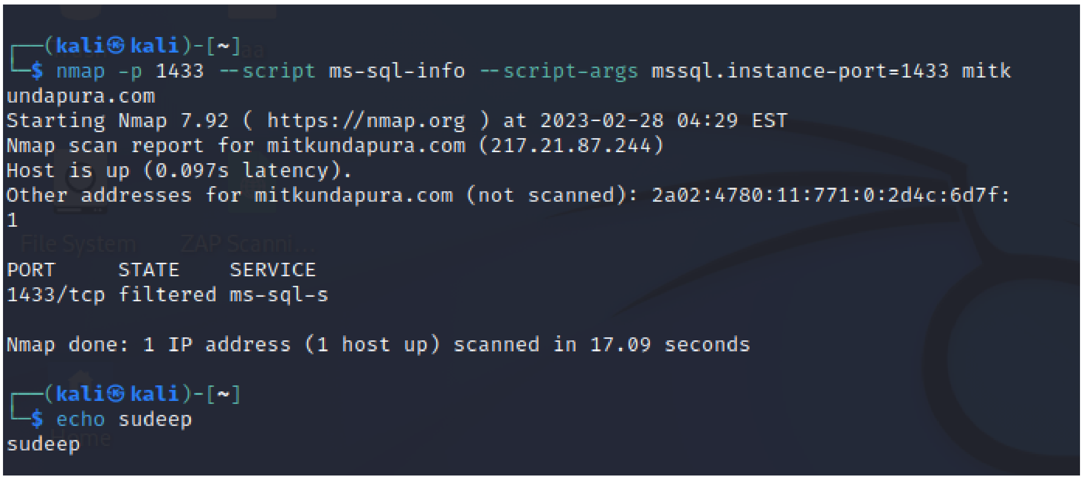
```
[-] Auxiliary failed: RuntimeError eth0: You don't have permission to capture on
that device (socket: Operation not permitted)
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `ope
n_live'
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `ope
n_pcap'
[-]   /usr/share/metasploit-framework/modules/auxiliary/dos/tcp/synflood.rb:41:in
 `run'
[*] Running module against 2a02:4780:11:771:0:2d4c:6d7f:1
SIOCSIFFLAGS: Operation not permitted
[-] Auxiliary failed: RuntimeError eth0: You don't have permission to capture on
that device (socket: Operation not permitted)
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `ope
n_live'
[-]   /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `ope
n_pcap'
[-]   /usr/share/metasploit-framework/modules/auxiliary/dos/tcp/synflood.rb:41:in
 `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >
zsh: suspended  msfconsole

┌──(kali㉿kali)-[~]
└─$ echo sudeep
sudeep

┌──(kali㉿kali)-[~]
└─$ 
```

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



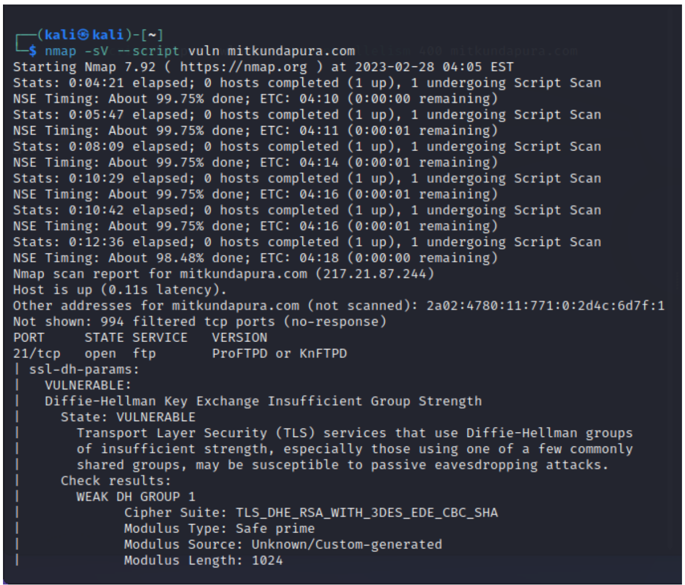
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitk
undapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-28 04:29 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.097s latency).
Other addresses for mitkundapura.com (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 17.09 seconds

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

3. Vulnerability scan using nmap:

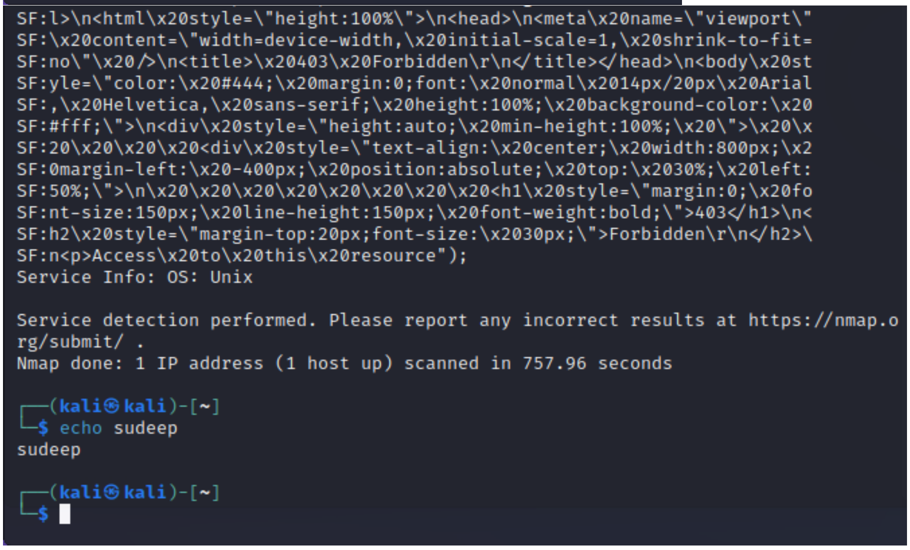
One of the most well known vulnerability scanner is nmap_vulner.The nmap script engine searches HTTP responses to identity CPE’s for the script.

Command:

$ nmap -sV --script vuln mitkundapura.com



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-28 04:05 EST
Stats: 0:04:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:10 (0:00:00 remaining)
Stats: 0:05:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:11 (0:00:01 remaining)
Stats: 0:08:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:14 (0:00:01 remaining)
Stats: 0:10:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:16 (0:00:01 remaining)
Stats: 0:10:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:16 (0:00:01 remaining)
Stats: 0:12:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.48% done; ETC: 04:18 (0:00:00 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.11s 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   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_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
```



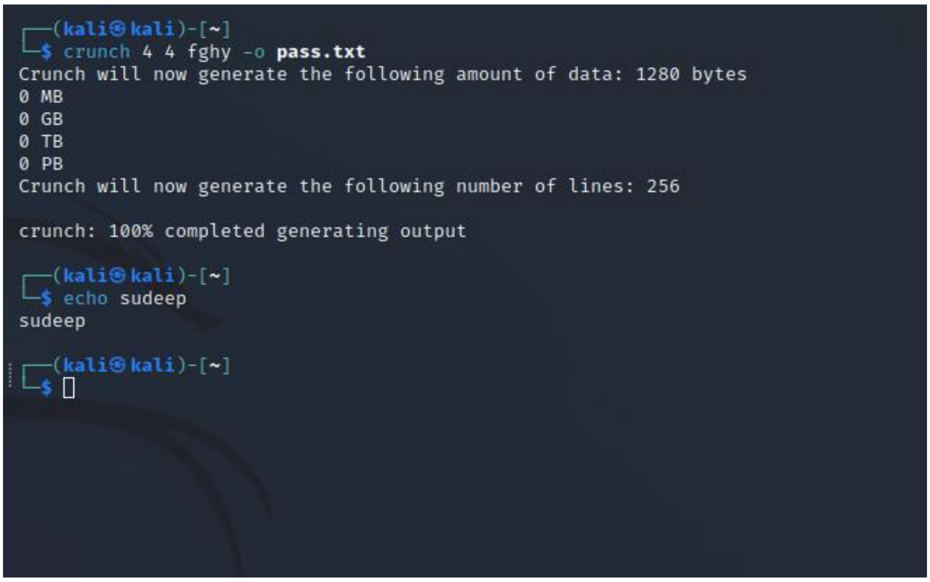
```
SF:l>\n<html\x20style=\"height:100%\">\n<head>\n<meta\x20name=\"viewport\"
SF:\x20content=\"width=device-width,\x20initial-scale=1,\x20shrink-to-fit=
SF:no\"\x20/>\n<title>\x20403\x20Forbidden\r\n</title></head>\n<body\x20st
SF:yle=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014px/20px\x20Arial
SF:,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20background-color:\x20
SF:#fff;\">\n<div\x20style=\"height:auto;\x20min-height:100%;\x20\">\x20\x
SF:20\x20\x20\x20<div\x20style=\"text-align:\x20center;\x20width:800px;\x2
SF:0margin-left:\x20-400px;\x20position:absolute;\x20top:\x2030%;\x20left:
SF:50%;\">\n\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20style=\"margin:0;\x20fo
SF:nt-size:150px;\x20line-height:150px;\x20font-weight:bold;\">403</h1>\n<
SF:h2\x20style=\"margin-top:20px;font-size:\x2030px;\">Forbidden\r\n</h2>\
SF:n<p>Access\x20to\x20this\x20resource");
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 757.96 seconds

┌──(kali㉿kali)-[~]
└─$ echo sudeep
sudeep

┌──(kali㉿kali)-[~]
└─$ █
```

4. **<u>Create a password list using charecters “fghy” the password should be minimum and maximum length 4 letters using tool crunch</u>**

Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists. The wordlists are created through combination and permutation of a set of characters. You can determine the amount of characters and list size.

Command:

$crunch 4 4 fghy –o pass.txt



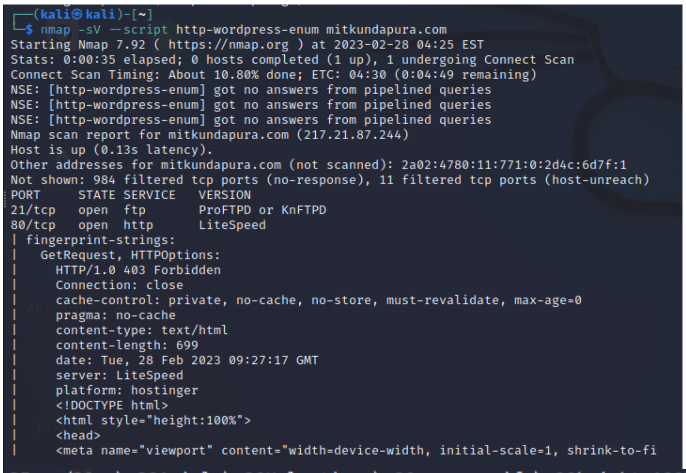
```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o pass.txt
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ echo sudeep
sudeep

┌──(kali㉿kali)-[~]
└─$ ▯
```

5. **Wordpress scan using nmap:**

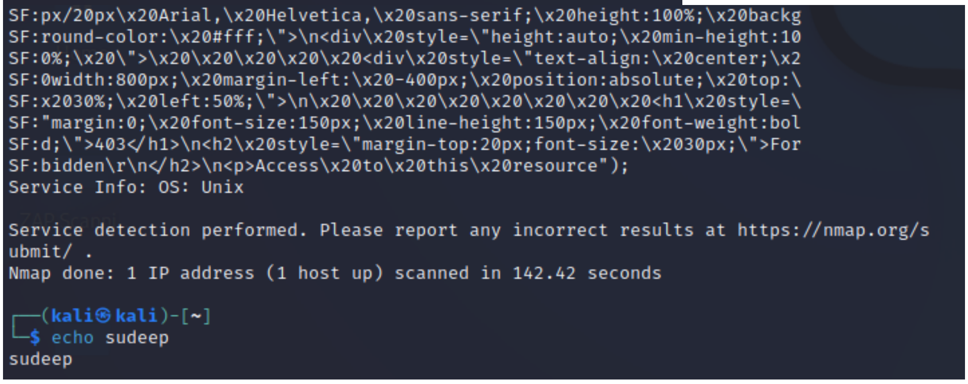
Word press as a publishing platform,security testing is the important part of ensuring the installation is secure.Nmap has a couple of NSE scripts specifically for the testing of wordpress installations.

Command:

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



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script http-wordpress-enum mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-28 04:25 EST
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 10.80% done; ETC: 04:30 (0:04:49 remaining)
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 (0.13s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 984 filtered tcp ports (no-response), 11 filtered tcp ports (host-unreach)
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp       ProFTPD or KnFTPD
80/tcp   open  http      LiteSpeed
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Connection: close
|     cache-control: private, no-cache, no-store, must-revalidate, max-age=0
|     pragma: no-cache
|     content-type: text/html
|     content-length: 699
|     date: Tue, 28 Feb 2023 09:27:17 GMT
|     server: LiteSpeed
|     platform: hostinger
|     <!DOCTYPE html>
|     <html style="height:100%">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fi
```



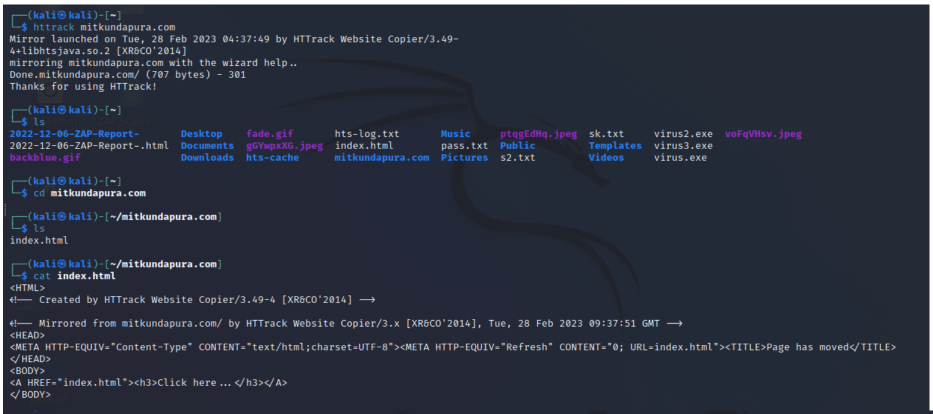
```
SF:px/20px\x20Arial,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20backg
SF:round-color:\x20#fff;\">\n<div\x20style=\"height:auto;\x20min-height:10
SF:0%;\x20\">\x20\x20\x20\x20\x20<div\x20style=\"text-align:\x20center;\x2
SF:0width:800px;\x20margin-left:\x20-400px;\x20position:absolute;\x20top:\
SF:x2030%;\x20left:50%;\">\n\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20style=\
SF:"margin:0;\x20font-size:150px;\x20line-height:150px;\x20font-weight:bol
SF:d;\">403</h1>\n<h2\x20style=\"margin-top:20px;font-size:\x2030px;\">For
SF:bidden\r\n</h2>\n<p>Access\x20to\x20this\x20resource");
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.42 seconds

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

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

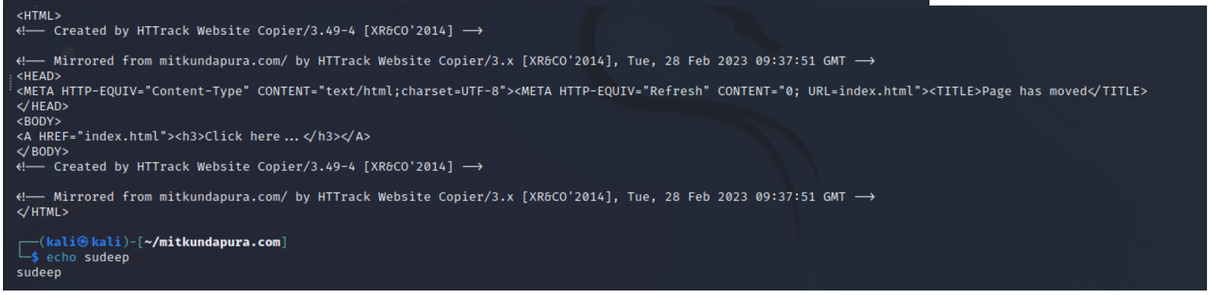
HTTrack is a free and open source website copying tool that allows you to download an entire website to your local computer for offline browsing.

Command for copying website:

$httrack mitkundapura.com



```
┌──(kali㉿kali)-[~]
└─$ httrack mitkundapura.com
Mirror launched on Tue, 28 Feb 2023 04:37:49 by HTTrack Website Copier/3.49-
4+libhtsjava.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
2022-12-06-ZAP-Report-       Desktop    fade.gif       hts-log.txt       Music      ptqgEdHq.jpeg  sk.txt     virus2.exe  voFqVHsv.jpeg
2022-12-06-ZAP-Report-.html  Documents  gGYwpxXG.jpeg  index.html        pass.txt   Public         Templates  virus3.exe
backblue.gif                 Downloads  hts-cache      mitkundapura.com  Pictures   s2.txt         Videos     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], Tue, 28 Feb 2023 09:37:51 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>
```



```
<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], Tue, 28 Feb 2023 09:37:51 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], Tue, 28 Feb 2023 09:37:51 GMT -->
</HTML>

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