Name:Nikhita

Reg.No:145cs20009

Date:28-02-2023

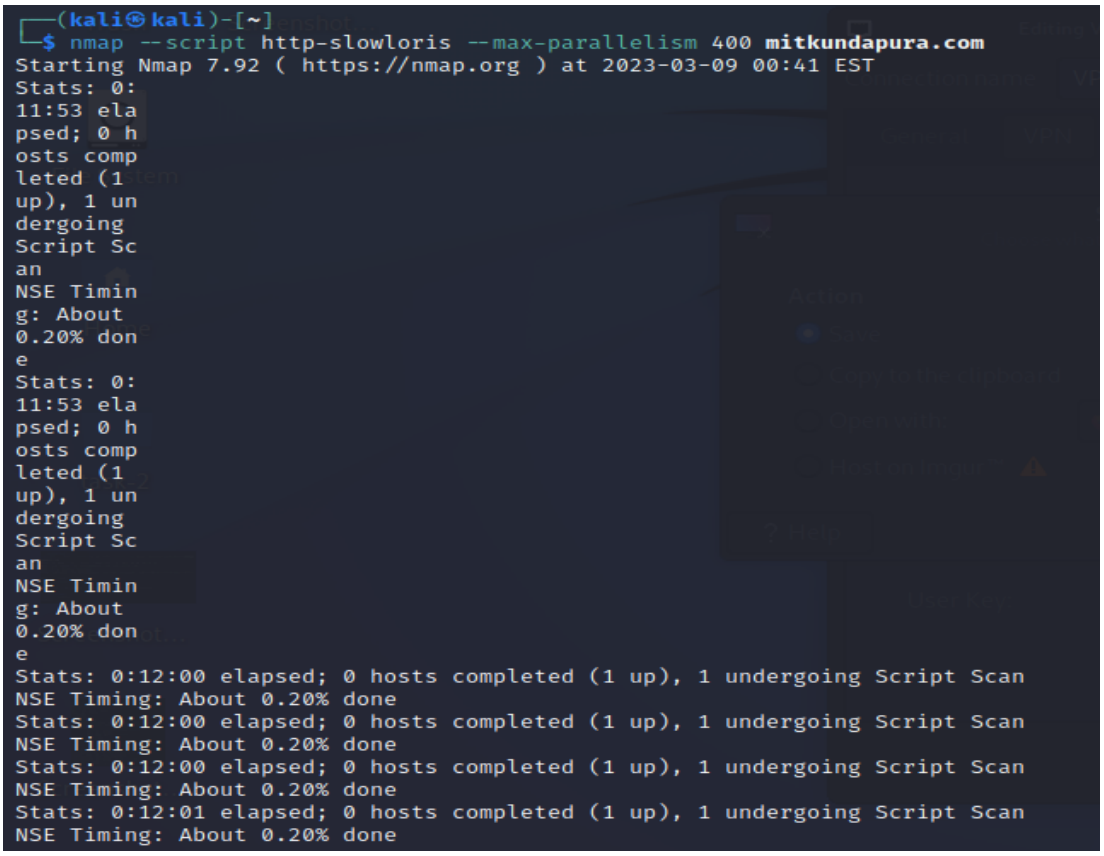
Task:1

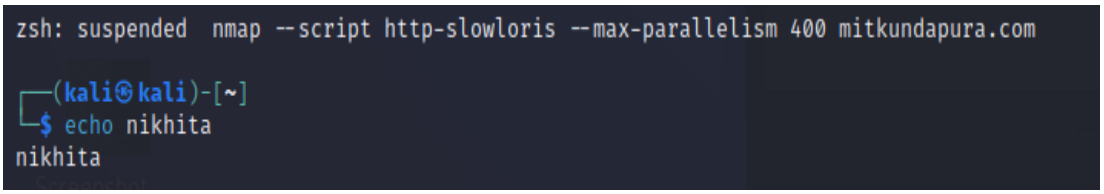
1. **Dos attack using nmap:**

   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:

   $nmap --script http-slowloris --max-parallelism 400 mitkundapura.com





2. **<u>Sql empty password enumeration scanning using nmap:</u>**

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 mitkun
dapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-09 00:45 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 17.01 seconds

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

3. **<u>Vulnerability scan using nmap:</u>**

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 2023-03-09 00:56 EST
Stats: 0:04:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 01:00 (0:00:00 remaining)
Stats: 0:04:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 01:00 (0:00:00 remaining)
Stats: 0:06:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
```

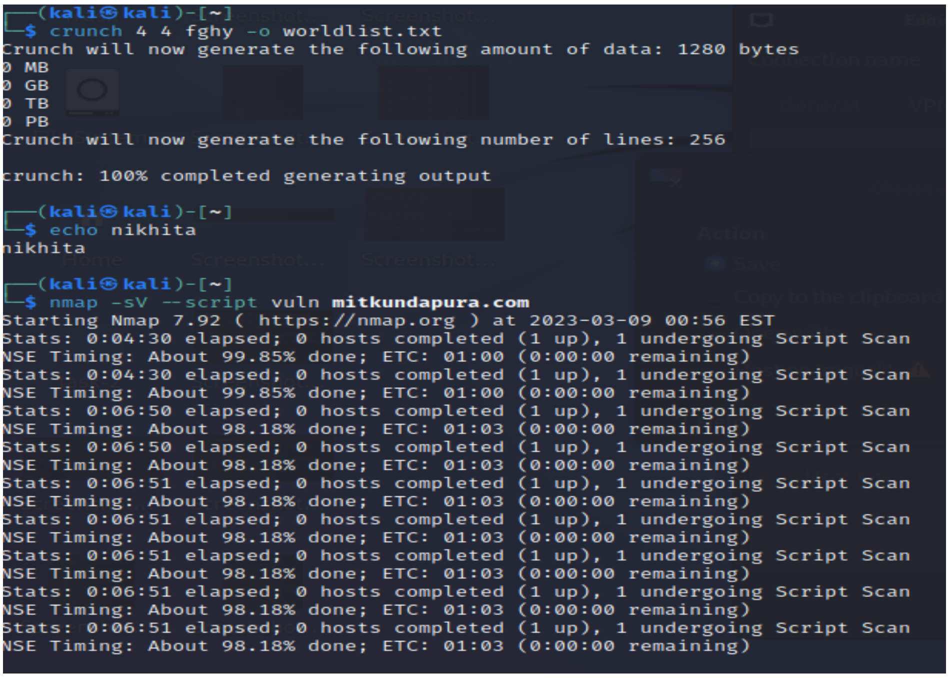
```
SF:,"HTTP/1\.0\x20403\x20Forbidden\r\nConnection:\x20close\r\ncache-contro
SF:l:\x20private,\x20no-cache,\x20no-store,\x20must-revalidate,\x20max-age
SF:=0\r\npragma:\x20no-cache\r\ncontent-type:\x20text/html\r\ncontent-leng
SF:th:\x20699\r\ndate:\x20Thu,\x2009\x20Mar\x202023\x2005:57:44\x20GMT\r\n
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 414.79 seconds

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

4. **Create a password list using charecters “fghy” the password should be minimum and maximum length 4 letters using tool hydra**

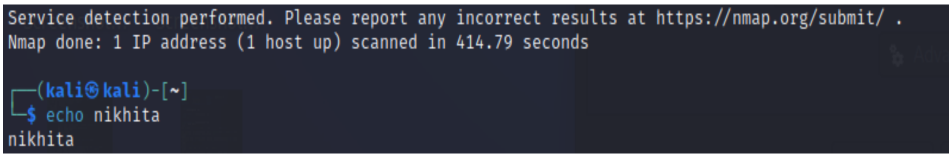
Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists. The wordlists are created through combination and permutation of a set of characters. You can determine the amount of characters and list size.

Command:

$crunch 4 4 fghy –o pass.txt



```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o worldlist.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 nikhita
nikhita

┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-09 00:56 EST
Stats: 0:04:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 01:00 (0:00:00 remaining)
Stats: 0:04:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 01:00 (0:00:00 remaining)
Stats: 0:06:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.18% done; ETC: 01:03 (0:00:00 remaining)
```



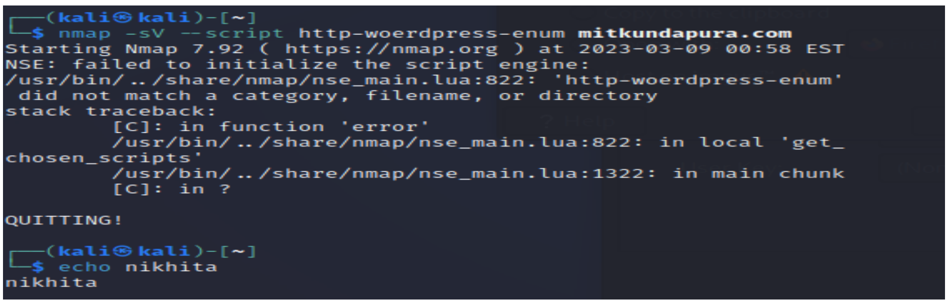
```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 414.79 seconds

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

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-woerdpress-enum mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-09 00:58 EST
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:822: 'http-woerdpress-enum'
 did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:822: in local 'get_
chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1322: in main chunk
        [C]: in ?

QUITTING!

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

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