Task Report 1

28/02/2023

Name: Darshan Achar
Register No. : 145cs20004

GOVERNMENT POLYTECHNIC UDUPI

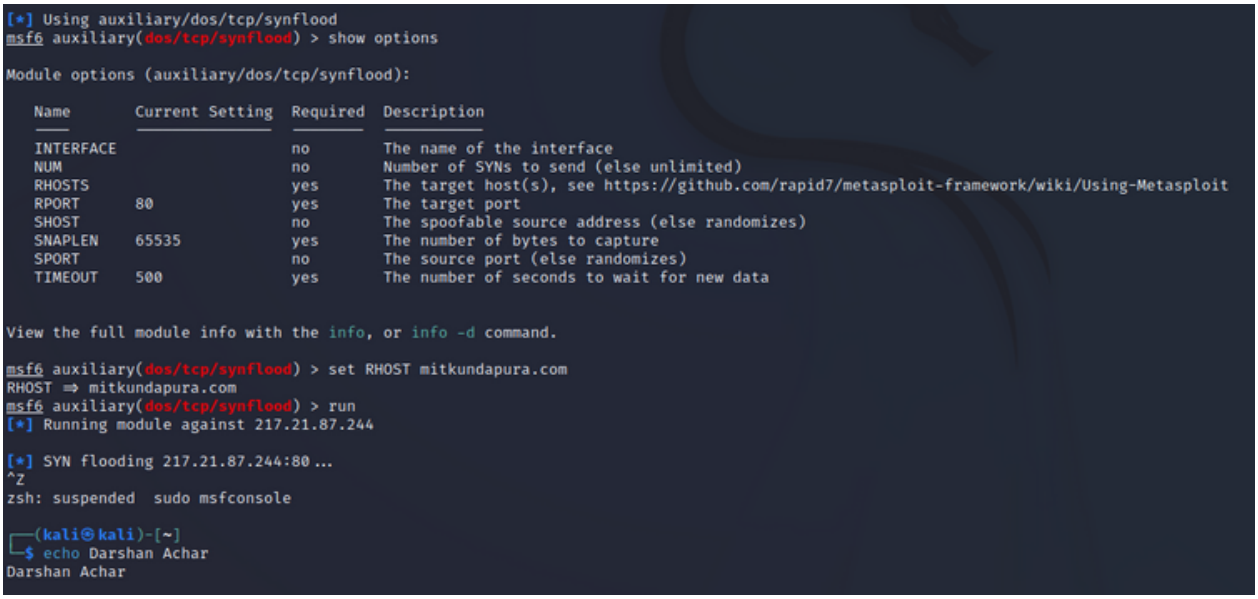
1.DoS attack using Nmap

A denial-of-service attack is a type of cyber-attack in which the perpetrator attempts to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to a network. The Nmap Scripting Engine (NSE) contains a plethora of scripts that can be used to launch DoS attacks.

Command (steps-by-steps):

1. msfconsole
2. use auxiliary /dos/tcp/synflood
3. show options
4. set RHOST <target>
5. run

Output:



2.SQL empty password enumeration scanning using Nmap.

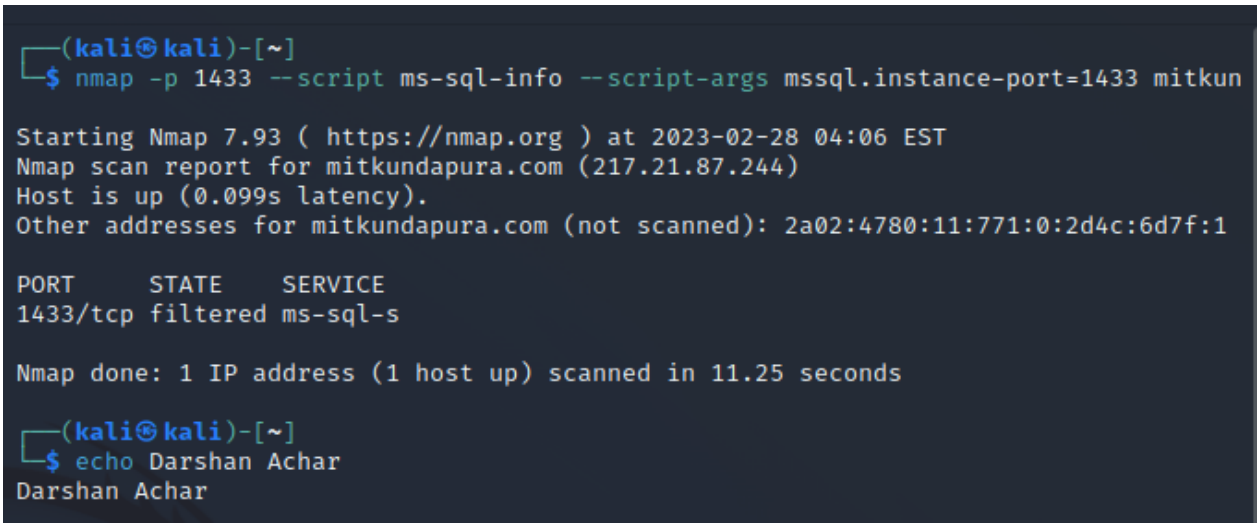
The ms-sql-empty-password.nse script tries to login to Microsoft SQL Servers with an empty password for the sysadmin (sa) account.

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.

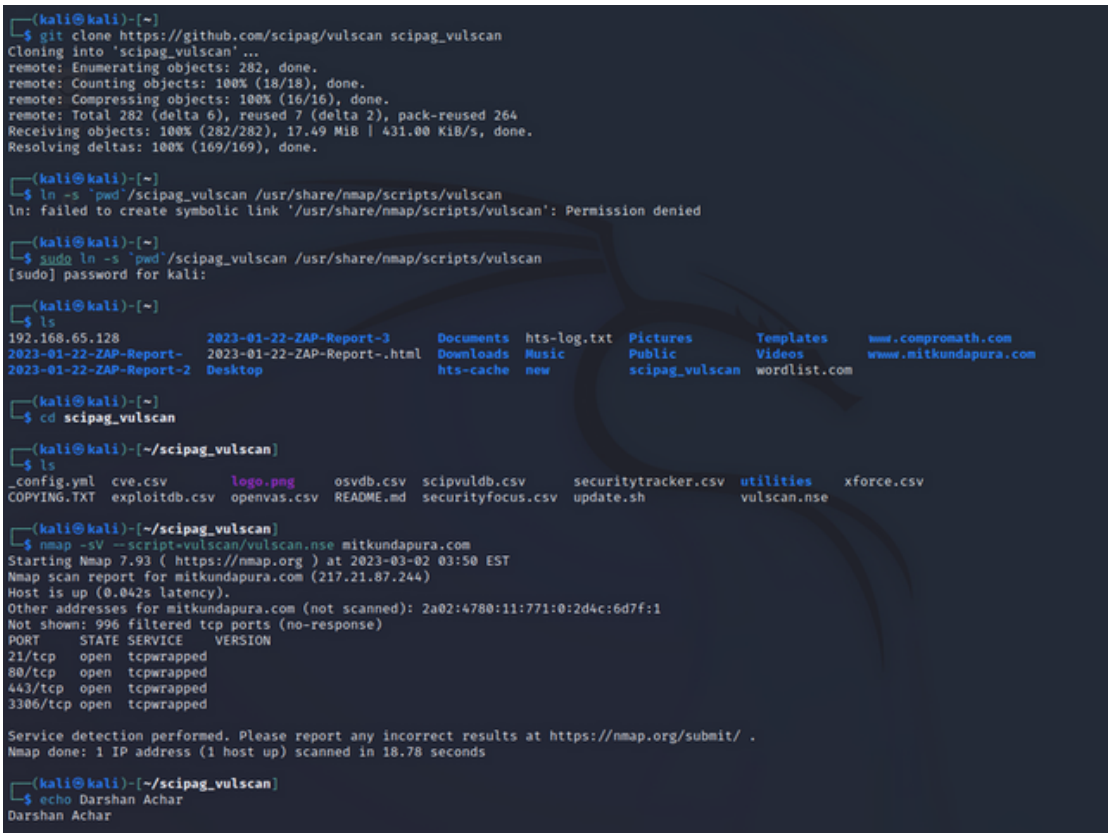
Nmap, or network mapper, is a toolkit for network functionality and penetration testing, which includes port scanning and vulnerability detection.

Nmap scripting engine (NSE) Script is one of Nmap's most popular and powerful features. Penetration testers and hackers use these Nmap vulnerability scan scripts to examine commonly known vulnerabilities.

The Common Vulnerabilities and Exposures (CVE) database contains publicly disclosed data security flaws. It is a reference model for detecting vulnerabilities and threats to information system security.

Command: nmap -sV --script=vulscan/vulscan.nse <target>

Output:

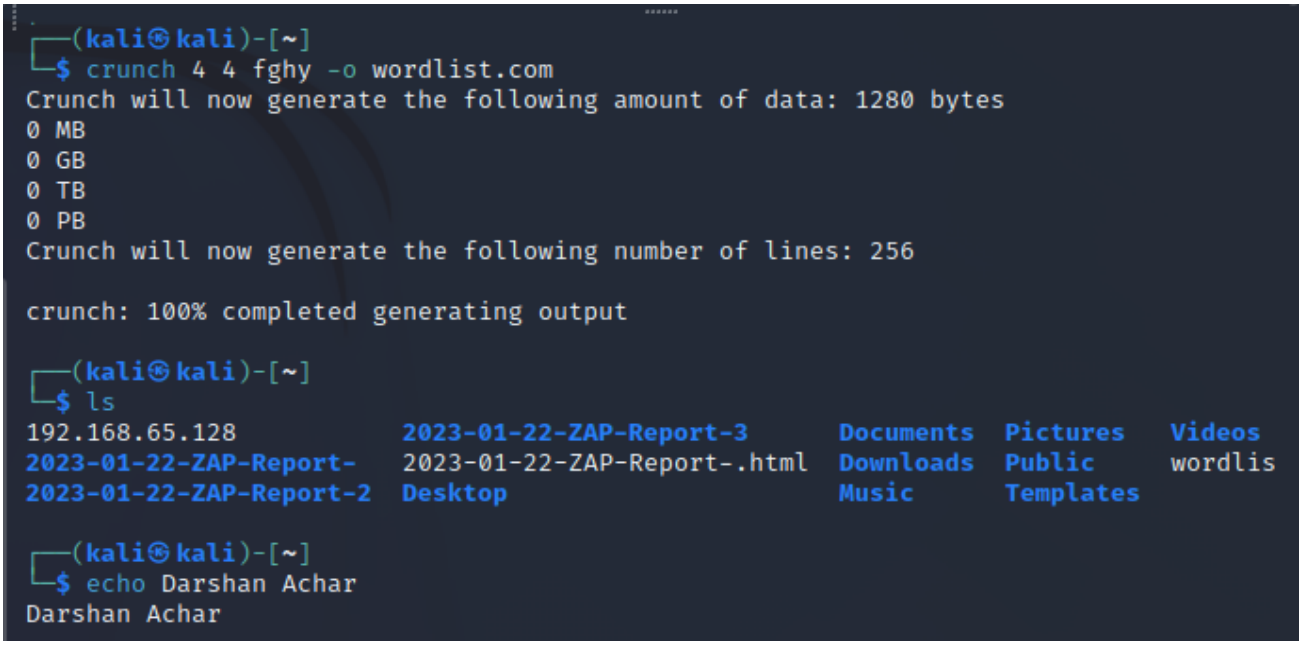


4.Create a password list using character "fghy". The password should be minimum and maximum length of 4 letters using tool Hydra.

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 wordlist.com

Output:



5.WordPress scan using Nmap.

WordPress is a free and open-source content management system written in HTML and paired with a MySQL or MariaDB database that supports HTTPS. A plugin architecture and a template system, referred to as "Themes" within WordPress, are among the features.

Command:

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

Output:

```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-wordpress-enum --script-args type="themes" mitkundapura.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:40 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.51s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 933 filtered tcp ports (no-response), 60 filtered tcp ports (host-unreac
PORT     STATE  SERVICE
20/tcp   closed ftp-data
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 220.50 seconds

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

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

HTTrack enables users to download websites from the Internet to their local computer. By default, HTTrack arranges the downloaded site based on the relative link structure of the original site. By opening a page of the downloaded (or "mirrored") website in a browser, you can browse it.

Command: httrack <target>

we can also use their Official software.
Output (software):