Name:GANESH

Reg No:145CS21702

Date:28-2-2023

Task:1

1. **<u>Dos attack using nmap:</u>**

Nmap is a network exploration and security auditing tool that can be used to scan networks and hosts for various purposes,including potential DOS attacks.

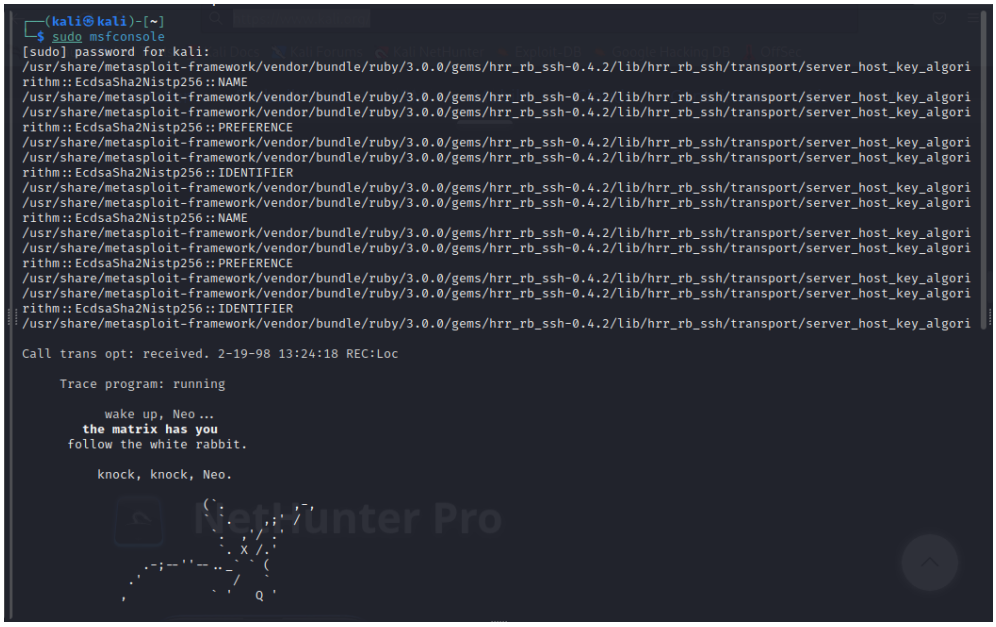
command:

$ msfconsole

Use auxiliary/dos/tcp/synflood

Set RHOSTS mitkundapura.com

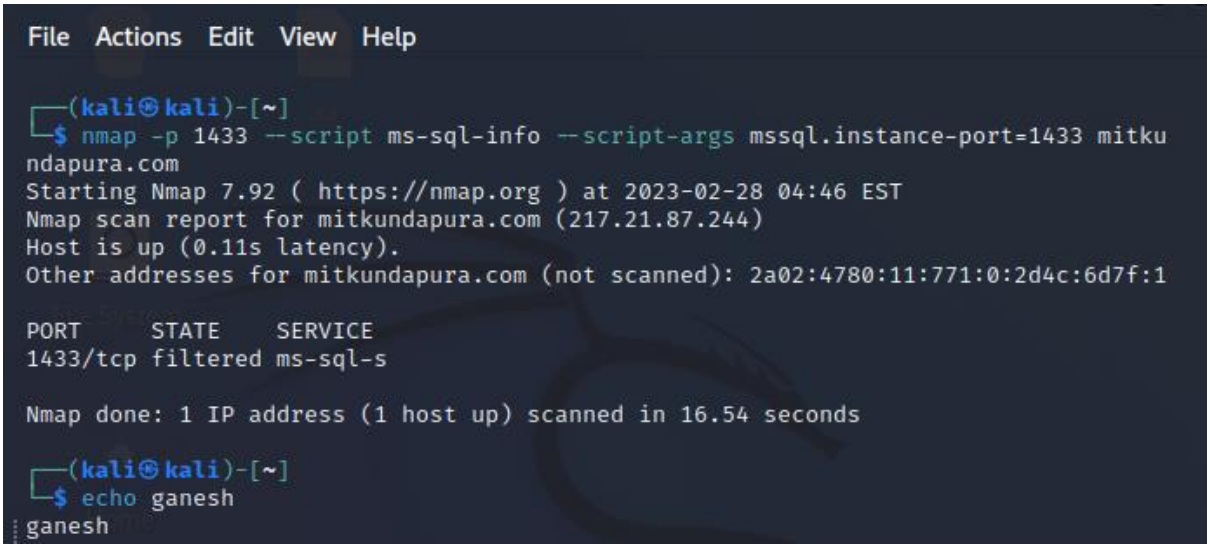
Run



2. **Sql empty password enumeration scanning using nmap:**

Nmap is one of the most popular tools used for the enumeration os a targeted host .nmap can use scans that provides the 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

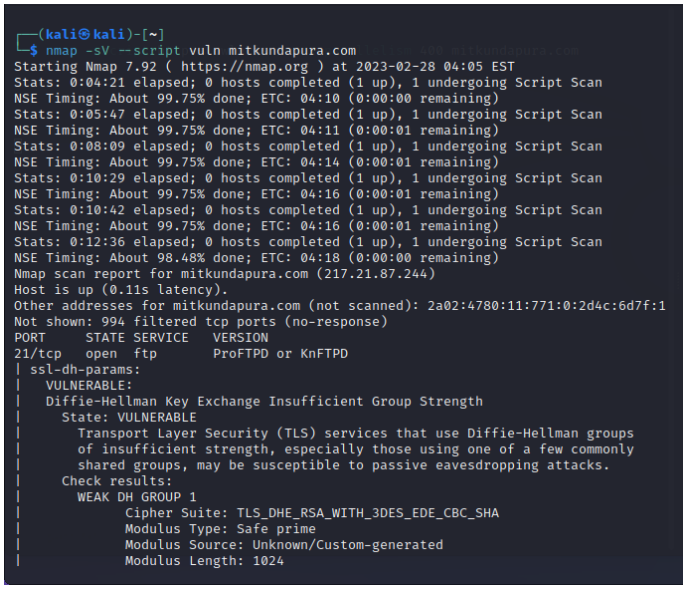


3. Vulnerability scan using nmap:

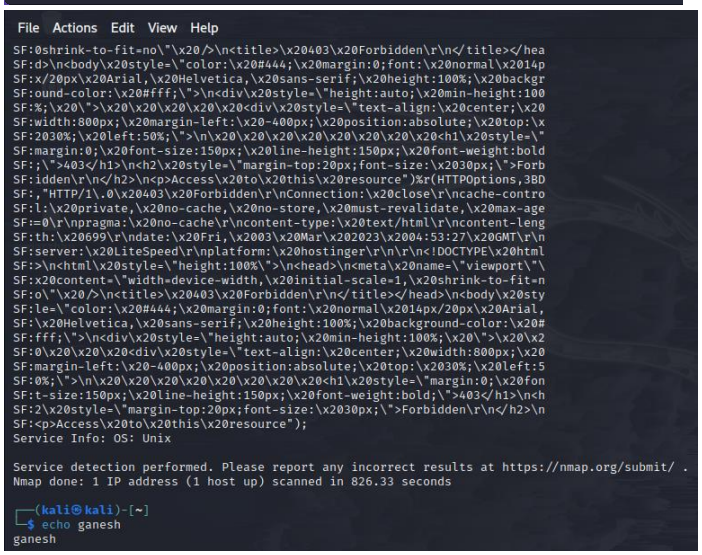
Vulnerability scanning using nmap is a process of identifying potential security issues in a system or network by running a set of scripts that are designed to detect common vulnerabilities in network services.

Command:

$ nmap -sV --script vuln mitkundapura.com



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-28 04:05 EST
Stats: 0:04:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:10 (0:00:00 remaining)
Stats: 0:05:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:11 (0:00:01 remaining)
Stats: 0:08:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:14 (0:00:01 remaining)
Stats: 0:10:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:16 (0:00:01 remaining)
Stats: 0:10:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 04:16 (0:00:01 remaining)
Stats: 0:12:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.48% done; ETC: 04:18 (0:00:00 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.11s 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
| 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_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
```



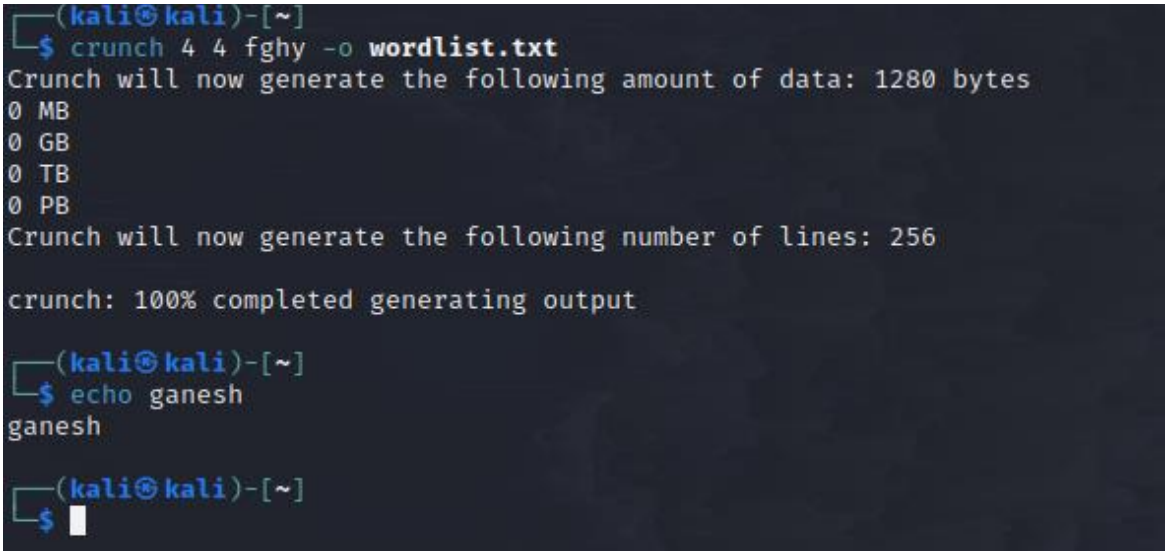
```
File  Actions  Edit  View  Help
SF:0shrink-to-fit=no\"\x20/>\n<title>\x20403\x20Forbidden\r\n</title></hea
SF:d>\n<body\x20style=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014p
SF:x/20px\x20Arial,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20backgr
SF:ound-color:\x20#fff;\">\n<div\x20style=\"height:auto;\x20min-height:100
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\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:\x20Fri,\x2003\x20Mar\x202023\x2004:53:27\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\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 826.33 seconds

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

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

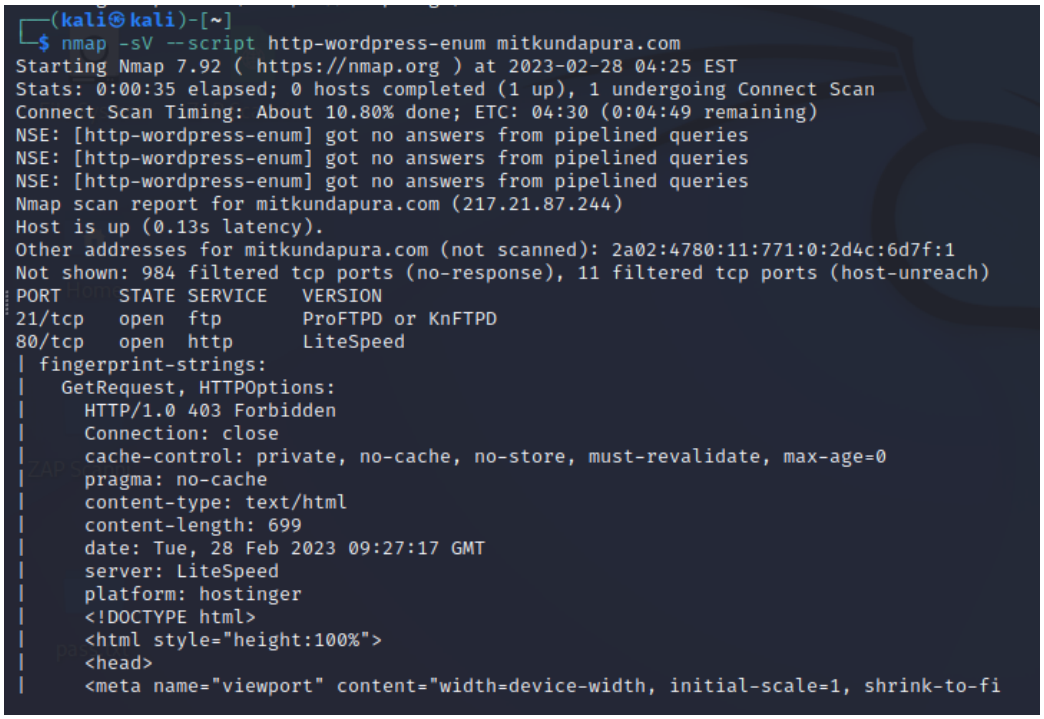


5. Wordpress scan using nmap:

The process of using the network exploration and security auditing tool nmap to identify WordPress installations on a target system and gather information about the WordPress site, plugins, and themes that are being used.

Command:

$nmap -sV --script http-wordpress-enum mitkundapura.com



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

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. The copied website can be browsed offline using any web browser.

Command for copying website:

$httrack mitkundapura.com