

Name: Sushma

Reg.No:145cs20020

Date:28-2-2023

### Task:1

#### 1. Dos attack using nmap:

The nmap scripting engine has numerous scripts that can be used to perform dos attack. This specific recipe will demonstrate how to locate dos scripts, identify the usage of the script.

command:

```
$ nmap --script http-slowloris --max-parallelism 400 mitkundapura.com
```

```
(kali@kali)-[~/mitkundapura.com]
$ nmap --script http-slowloris --max-parallelism 400 mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:40 EST
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.55% done; ETC: 04:40 (0:00:19 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.60% done; ETC: 04:40 (0:00:26 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.05% done; ETC: 04:40 (0:00:31 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.10% done; ETC: 04:40 (0:00:31 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.20% done; ETC: 04:40 (0:00:31 remaining)
Stats: 0:32:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.98% done; ETC: 05:12 (0:00:00 remaining)

(kali@kali)-[~/mitkundapura.com]
$ echo sushma
sushma
```

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

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

```
(kali㉿kali)-[~]
$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 03:55 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.039s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1

PORT      STATE      SERVICE
1433/tcp  filtered  ms-sql-s

Nmap done: 1 IP address (1 host up) scanned in 16.86 seconds

(kali㉿kali)-[~]
$ echo sushma
sushma
```

### 3.Vulnerability scan using nmap:

One of the most well known vulnerability scanner is nmap\_vuln. The nmap script engine searches HTTP responses to identify CPE's for the script.

Command:

\$ nmap -sV --script vuln mitkundapura.com

```
(kali㉿kali)-[~/mitkundapura.com]
$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:27 EST
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 60.00% done; ETC: 04:29 (0:00:09 remaining)
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.27% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.88% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.04% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.19% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.19% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.49% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.65% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.80% done; ETC: 04:29 (0:00:00 remaining)
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.80% done; ETC: 04:29 (0:00:00 remaining)
```

```
SF:margin:0;\x20font-size:150px;\x20line-height:150px;\x20font-weight:bold
SF:;\x20>403</h1>\n<h2\x20style=\x20"margin-top:20px;font-size:\x2030px;\x20">Forb
SF:idden\r\n</h2>\n<p>Access\x20to\x20this\x20resource")%r(HTTPOptions,3BD
SF:,"HTTP/1.\x200\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:\x20Thu,\x2002\x20Mar\x202023\x2004:03:52\x20GMT\r\n
SF:server:\x20LiteSpeed\r\nPlatform:\x20hostinger\r\n\r\n<!DOCTYPE\x20html
SF:>\n<html\x20style=\x20"height:100%">\n<head>\n<meta\x20name=\x20"viewport"\x
SF:x20content=\x20"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=\x20"color:\x20#444;\x20margin:0;font:\x20normal\x2014px/20px\x20Arial,
SF:\x20Helvetica,\x20sans-serif;\x20height:100%; \x20background-color:\x20#
SF:fff;">\n<div\x20style=\x20"height:auto;\x20min-height:100%;\x20">\x20\x2
SF:0\x20\x20\x20<div\x20style=\x20"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\x20\x20\x20\x20\x20\x20\x20
SF:t-size:150px;\x20line-height:150px;\x20font-weight:bold;">403</h1>\n<h
SF:2\x20style=\x20"margin-top:20px;font-size:\x2030px;\x20">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 1100.58 seconds
```

```
(kali㉿kali)-[~/mitkundapura.com]
$ echo sushma
sushma
```

#### 4. Create a password list using characters "fghy" the password should be minimum and maximum length 4 letters using tool crunch

Crunch is a security tool that can be used for legitimate security testing and auditing purposes, and its usage should comply with ethical and legal guidelines. It is not ethical to use to perform any malicious activity.

Command:

```
$crunch 4 4 fghy -o pass.txt
```

```
(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o pass.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
ffff
ffffg
ffffh
ffffy
ffgff
ffggg
ffggh
ffgy
ffhf
ffhg

(kali㉿kali)-[~/mitkundapura.com]
└─$ echo sushma
sushma
```

#### 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 -sV --script http-wordpress-enum mitkundapura.com
```

```
(kali㉿kali)-[~]
└─$ nmap -sV --script http-wordpress-enum mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-28 04:25 EST
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 10.80% done; ETC: 04:30 (0:04:49 remaining)
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.13s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 984 filtered tcp ports (no-response), 11 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD or KnFTPD
80/tcp    open  http     LiteSpeed

| fingerprint-strings:
|_  GetRequest, HTTPOptions:
|_  HTTP/1.0 403 Forbidden
|_  Connection: close
|_  cache-control: private, no-cache, no-store, must-revalidate, max-age=0
|_  pragma: no-cache
|_  content-type: text/html
|_  content-length: 699
|_  date: Tue, 28 Feb 2023 09:27:17 GMT
|_  server: LiteSpeed
|_  platform: hostinger
|_  <!DOCTYPE html>
|_  <html style="height:100%">
|_  <head>
|_  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fi

(kali㉿kali)-[~/mitkundapura.com]
└─$ echo sushma
sushma
```



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

HTTrack is a free and open source website copying tool that allows you to download an entire website to your local computer for offline browsing.

Command for copying website:

```
$httrack mitkundapura.com
```

```
(kali@kali)-[~]
$ httrack mitkundapura.com
There is an index.html and a hts-cache folder in the directory
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok

Press <Y><Enter> to confirm, <N><Enter> to abort
y
Mirror launched on Thu, 02 Mar 2023 04:23:41 by HTTrack Website Copier/3.49-4+libh
tsjava.so.2 [XR&CO'2014]
mirroring mitkundapura.com with the wizard help..
Done.mitkundapura.com/ (0 bytes) - -4
Thanks for using HTTrack!

(kali@kali)-[~]
$ ls
2022-12-06-ZAP-Report-      fade.gif      mitkundapura.com  Videos
2022-12-06-ZAP-Report-.html HEY.txt      Music             virus.exe
backblue.gif              hts-cache    Pictures          wordlist.com
Desktop                   hts-log.txt  Public           wordlist.txt
Documents                 hts-nohup.out shreyas.exe
Downloads                 index.html   Templates

(kali@kali)-[~]
$ cd mitkundapura.com

(kali@kali)-[~/mitkundapura.com]
$ ls
index.html
```

```
(kali@kali)-[~/mitkundapura.com]
$ cat index.html
<HTML>
<!-- Created by HTTrack Website Copier/3.49-4 [XR&CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR&CO'2014], T
hu, 02 Mar 2023 09:19:16 GMT -->
<HEAD>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8"><META HTTP-EQUIV
="Refresh" CONTENT="0; URL=index.html"><TITLE>Page has moved</TITLE>
</HEAD>
<BODY>
<A HREF="index.html"><h3>Click here ... </h3></A>
</BODY>
<!-- Created by HTTrack Website Copier/3.49-4 [XR&CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR&CO'2014], T
hu, 02 Mar 2023 09:19:16 GMT -->
</HTML>

(kali@kali)-[~/mitkundapura.com]
$ echo sushma
sushma
```