FOSS CLUB – EVALUATION ASSIGNMENT:

```
File Actions Edit View Help
  —(karan⊛ vbox)-[~]
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 0×20<link>
        inet6 fd00::5041:8833:5083:49a0 prefixlen 64 scopeid 0×0<global>
        inet6 fd00::a00:27ff:fe89:8814 prefixlen 64 scopeid 0x0<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 0×10<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
  –(karan❸ vbox)-[~]
___s 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
— 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

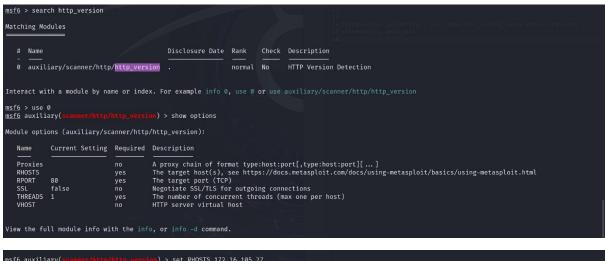
```
File Actions Edit View Help
64 bytes from 172.16.105.27: icmp_seq=6 ttl=255 time=4.60 ms
64 bytes from 172.16.105.27: icmp_seq=7 ttl=255 time=4.76 ms
64 bytes from 172.16.105.27: icmp_seq=8 ttl=255 time=4.21 ms
  – 172.16.105.27 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7033ms
rtt min/avg/max/mdev = 2.175/4.590/7.200/1.277 ms
  —(karan⊛ vbox)-[~]
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)
         STATE SERVICE
PORT
21/tcp
         open ftp
22/tcp
         open ssh
         open telnet
23/tcp
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

```
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
NOT SHOWN: 97/ TILLERED
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
                                         vsftpd 2.3.4
                                        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
                                        Linux telnetd
25/tcp
            open smtp
                                        Postfix smtpd
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
                                        ISC BIND 9.4.2
                                      netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp open
445/tcp open
512/tcp open exec
513/tcp open login?
                                        netkit-rsh rexecd
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath gimiregist.
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
                                        GNU Classpath grmiregistry
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)
5900/tcp open vnc
6000/tcp open X11
                                         (access denied)
6667/tcp open irc
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
8009/tcp open ajp13
8180/tcp open http
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

nmap -A -- used for OS scanning



```
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

```
| Path |
```

```
msf6 auxiliary(:conner/http/http.version) > searchsploit apache 2.2.8 |grep php

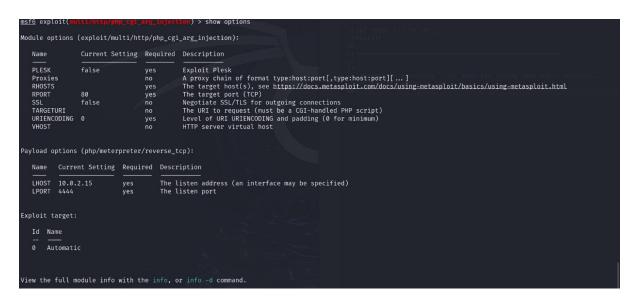
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c |
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py |
msf6 auxiliary(:conner/http/thtp.version) > grep cgi search php 5.4.2 |
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 | excellent Yes | PHP CGI Argument Injection |
msf6 auxiliary(:conner/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



show options – displays list of configuration for the selected exploits