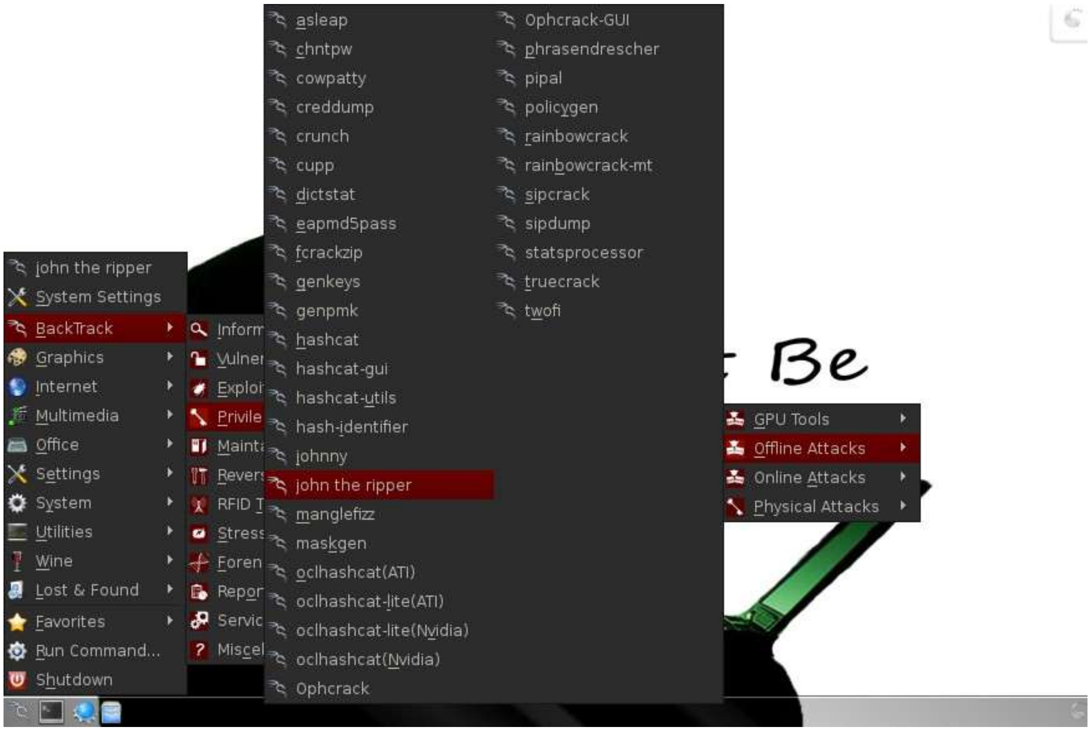
Practical – 8

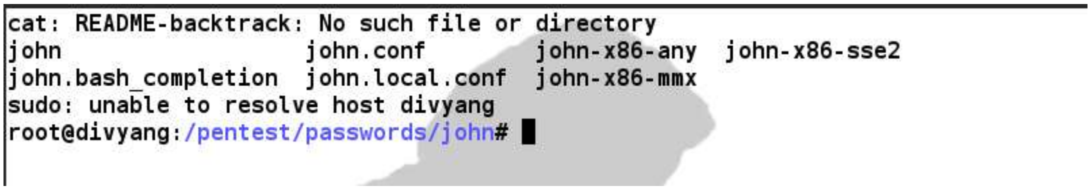
Aim: Perform brute force attack using John the RIPPER

- **What is John the Ripper.?**
  - "John the RIPPER" is a very useful and fast password cracking program. It is the favourite among hackers for cracking .htpasswd (DES) encrypted passwords and now can handle other encryptions such as LM and MD5. This is a very useful tool to have and is completely free too. This practical shows that how to install and run it in standard mode.
  - This has become the most popular password testing and also breaking applications since it brings together several password crackers in one bundle, auto detects password hash types, and also provides a easy to customize cracker. It may be work towards numerous encrypted password types such as many crypt password hash types most often available on various Unix types.

- **Start John the ripper in Backtrack.**
  - Now that we have a couple of regular users in our system with simple passwords, we now need to open John the Ripper. John the Ripper is a simple, but powerful password cracker without a GUI
  - We can access it from BackTrack by going to the BackTrack button on the bottom left, then Backtrack, Privilege Escalation, Password Attacks, Offline Attacks, and finally select John the Ripper from the multiple password cracking tools available.



  - If we selected the correct menu item, it will open a terminal that looks like this.

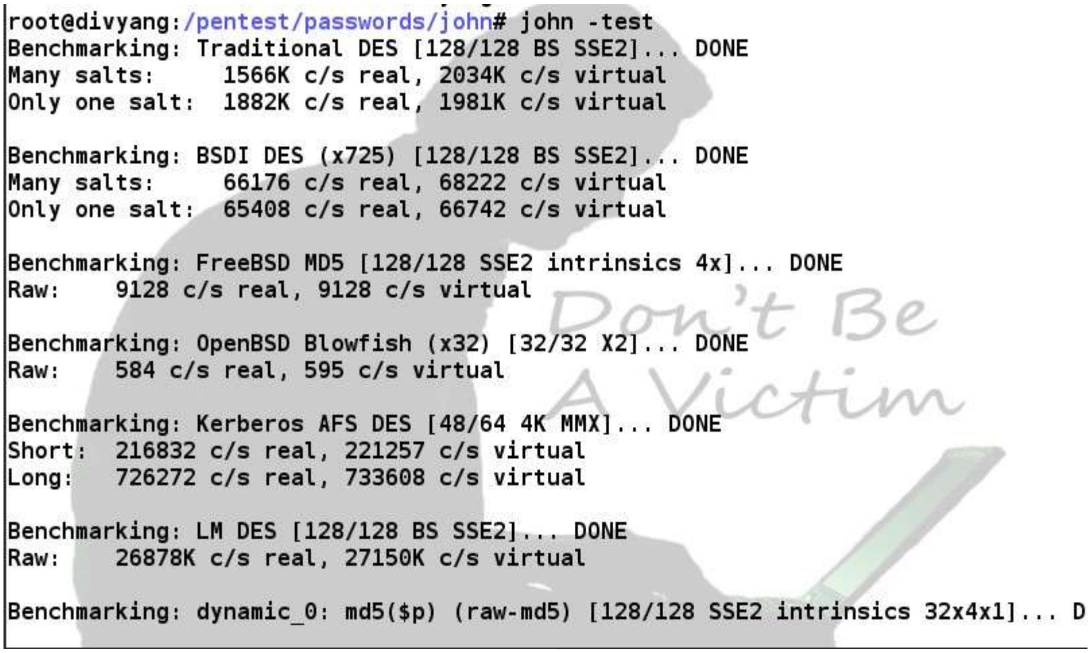


```
cat: README-backtrack: No such file or directory
john                  john.conf         john-x86-any  john-x86-sse2
john.bash_completion  john.local.conf   john-x86-mmx
sudo: unable to resolve host divyang
root@divyang:/pentest/passwords/john# █
```

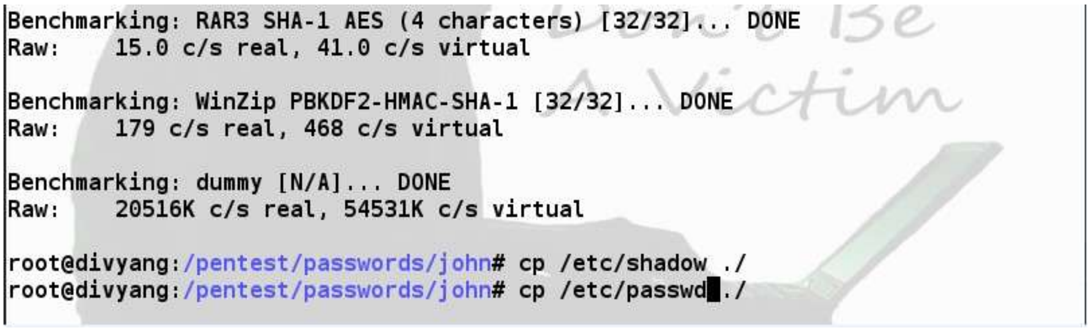
- **Test John the Ripper.**
  command: john -test
  - This command will send John the Ripper through a variety of benchmark tests to estimate how long it will take to break the passwords on your system. Your terminal will look something like this.
  - Now that John has estimated how long each of the encryption schemes will take to crack, let's put him to work on cracking our passwords.

- **Copy the Password Files to Our Current Directory.**
  - Linux stores its passwords in /etc/shadow, so what we want to do is copy this file to our current directory along with the /etc/passwd file, then "unshadow" them and store them in file we'll call passwords. So, let's type both:

    cp /etc/shadow ./ cp
    /etc/passwd ./



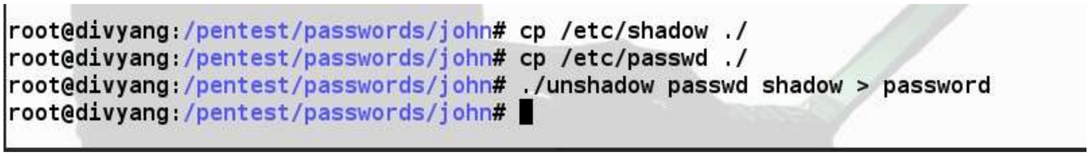
```
root@divyang:/pentest/passwords/john# john -test
Benchmarking: Traditional DES [128/128 BS SSE2]... DONE
Many salts:     1566K c/s real, 2034K c/s virtual
Only one salt:  1882K c/s real, 1981K c/s virtual

Benchmarking: BSDI DES (x725) [128/128 BS SSE2]... DONE
Many salts:     66176 c/s real, 68222 c/s virtual
Only one salt:  65408 c/s real, 66742 c/s virtual

Benchmarking: FreeBSD MD5 [128/128 SSE2 intrinsics 4x]... DONE
Raw:    9128 c/s real, 9128 c/s virtual

Benchmarking: OpenBSD Blowfish (x32) [32/32 X2]... DONE
Raw:    584 c/s real, 595 c/s virtual

Benchmarking: Kerberos AFS DES [48/64 4K MMX]... DONE
Short:  216832 c/s real, 221257 c/s virtual
Long:   726272 c/s real, 733608 c/s virtual

Benchmarking: LM DES [128/128 BS SSE2]... DONE
Raw:    26878K c/s real, 27150K c/s virtual

Benchmarking: dynamic_0: md5($p) (raw-md5) [128/128 SSE2 intrinsics 32x4x1]... D
```



```
Benchmarking: RAR3 SHA-1 AES (4 characters) [32/32]... DONE
Raw:    15.0 c/s real, 41.0 c/s virtual

Benchmarking: WinZip PBKDF2-HMAC-SHA-1 [32/32]... DONE
Raw:    179 c/s real, 468 c/s virtual

Benchmarking: dummy [N/A]... DONE
Raw:    20516K c/s real, 54531K c/s virtual

root@divyang:/pentest/passwords/john# cp /etc/shadow ./
root@divyang:/pentest/passwords/john# cp /etc/passwd█./
```

- **Unshadow**
  - Next we need to combine the information in the /etc/shadow and the /etc/passwd files, so that John can do forward work on files.

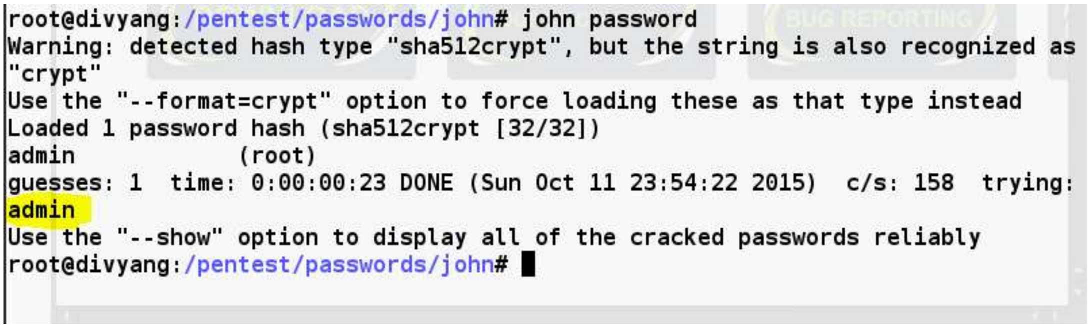
    ./unshadow passwd shadow > passwords



```
root@divyang:/pentest/passwords/john# cp /etc/shadow ./
root@divyang:/pentest/passwords/john# cp /etc/passwd ./
root@divyang:/pentest/passwords/john# ./unshadow passwd shadow > password
root@divyang:/pentest/passwords/john# █
```

- **Crack**
  - Now that we have unshadowed the critical files, we can simply let John run on our password file.

    type: **john passwords**



```
root@divyang:/pentest/passwords/john# john password
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [32/32])
admin            (root)
guesses: 1  time: 0:00:00:23 DONE (Sun Oct 11 23:54:22 2015)  c/s: 158  trying:
admin
Use the "--show" option to display all of the cracked passwords reliably
root@divyang:/pentest/passwords/john# █
```

  - John the Ripper will proceed to attempt to crack your passwords. As you can see, it cracked the password of system highlighted above more complex passwords will take significantly more time, but all we need is just one user with a simple password and we have access to the account in.