

HYDRA TOOL

Usually used to do brute force attack

Hydra -L <file path> -p <file path> target(protocol):"Ip Address".

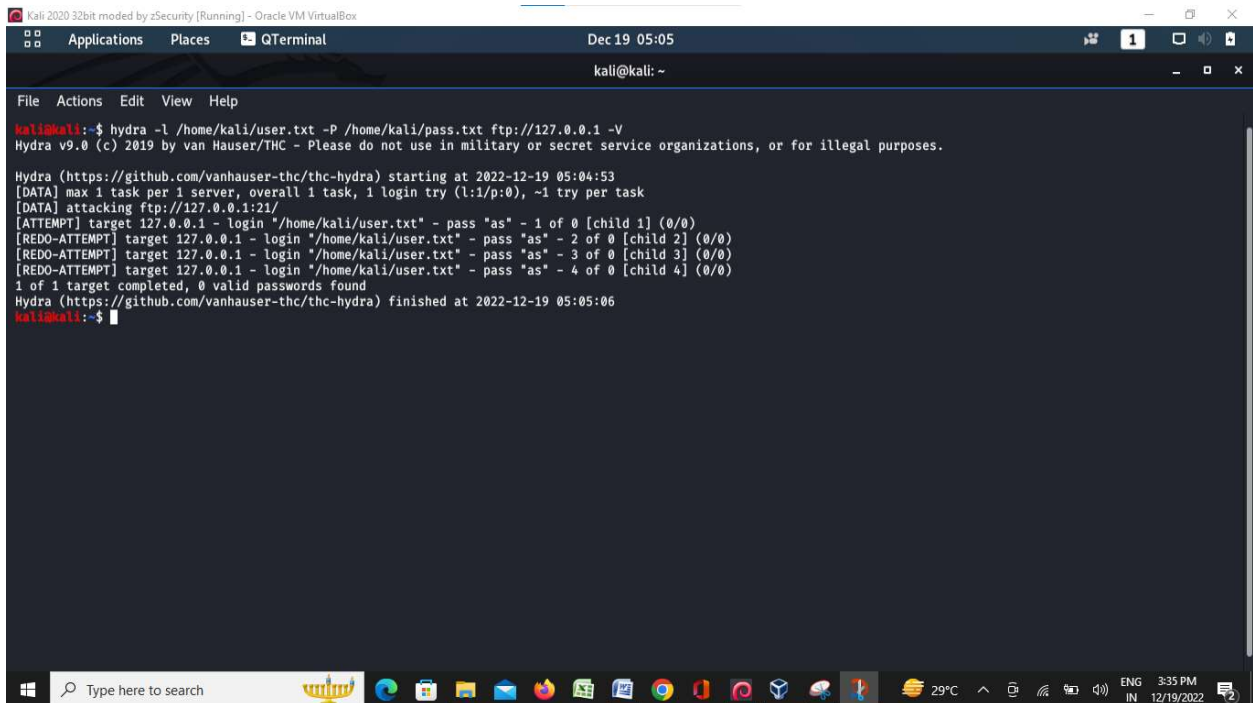
L is user name

P password

Then use hydra -L /home/kali/user.txt -P /home/kali/pass.txt <telnet://10.0.1.15>

Then u able to see the password successfully

Then we have done the brute force attack



```
kali 2020 32bit modded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 19 05:05
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ hydra -l /home/kali/user.txt -P /home/kali/pass.txt ftp://127.0.0.1 -V
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-19 05:04:53
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:p:0), ~1 try per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "/home/kali/user.txt" - pass "as" - 1 of 0 [child 1] (0/0)
[REDO-ATTEMPT] target 127.0.0.1 - login "/home/kali/user.txt" - pass "as" - 2 of 0 [child 2] (0/0)
[REDO-ATTEMPT] target 127.0.0.1 - login "/home/kali/user.txt" - pass "as" - 3 of 0 [child 3] (0/0)
[REDO-ATTEMPT] target 127.0.0.1 - login "/home/kali/user.txt" - pass "as" - 4 of 0 [child 4] (0/0)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-19 05:05:06
kali@kali:~$
```

C

AUXILLARY SCANNER

```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe27:298c  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:27:29:8c  txqueuelen 1000  (Ethernet)
    RX packets 21291  bytes 17396721 (16.5 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 12772  bytes 2432300 (2.3 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 72904  bytes 11334526 (10.8 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 72904  bytes 11334526 (10.8 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

kali@kali:~$
```

First using the ifconfig to know know the host ip address .

Then using auxillary scanner to scan the whole process of scanning

Use auxillary/scanner/ssh

Auxillary/scanner/ssh_login

Auxillary/scanner/ssh_login show options

Show options is displayed

Which shows the various file system

Then know about the USERNAME_FILE user.txt

PASS_FILE pass.txt

And again show options which is included among it

```
Kali 2020 32bit modded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 18 02:57
kali@kali: ~

File Actions Edit View Help

+ -- metasploit v5.0.76-dev
+ -- 1971 exploits - 1088 auxiliary - 339 post
+ -- 558 payloads - 45 encoders - 10 nops
+ -- 7 evasion

msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS false          no        Try blank passwords for all users
BRUTEFORCE_SPEED 5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false          no        Try each user/password couple stored in the current database
DB_ALL_PASS     false          no        Add all passwords in the current database to the list
DB_ALL_USERS    false          no        Add all users in the current database to the list
PASSWORD        no             no        A specific password to authenticate with
PASS_FILE       no             no        File containing passwords, one per line
RHOSTS          no             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT           22             yes       The target port
STOP_ON_SUCCESS false          yes       Stop guessing when a credential works for a host
THREADS         1              yes       The number of concurrent threads (max one per host)
USERNAME        no             no        A specific username to authenticate as
USERPASS_FILE   no             no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false          no        Try the username as the password for all users
USER_FILE       no             no        File containing usernames, one per line
VERBOSE         false          yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) > set USER_FILE user.txt
USER_FILE => user.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE pass.txt
PASS_FILE => pass.txt
msf5 auxiliary(scanner/ssh/ssh_login) > show options
```

Once show options is displayed: _>make sure that you type the rhost of the particular host

```
Kali 2020 32bit modded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 18 02:59
kali@kali: ~

File Actions Edit View Help

msf5 auxiliary(scanner/ssh/ssh_login) > set USER_FILE user.txt
USER_FILE => user.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE pass.txt
PASS_FILE => pass.txt
msf5 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS false          no        Try blank passwords for all users
BRUTEFORCE_SPEED 5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false          no        Try each user/password couple stored in the current database
DB_ALL_PASS     false          no        Add all passwords in the current database to the list
DB_ALL_USERS    false          no        Add all users in the current database to the list
PASSWORD        no             no        A specific password to authenticate with
PASS_FILE       pass.txt        no        File containing passwords, one per line
RHOSTS          no             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT           22             yes       The target port
STOP_ON_SUCCESS false          yes       Stop guessing when a credential works for a host
THREADS         1              yes       The number of concurrent threads (max one per host)
USERNAME        no             no        A specific username to authenticate as
USERPASS_FILE   no             no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false          no        Try the username as the password for all users
USER_FILE       user.txt        no        File containing usernames, one per line
VERBOSE         false          yes       Whether to print output for all attempts

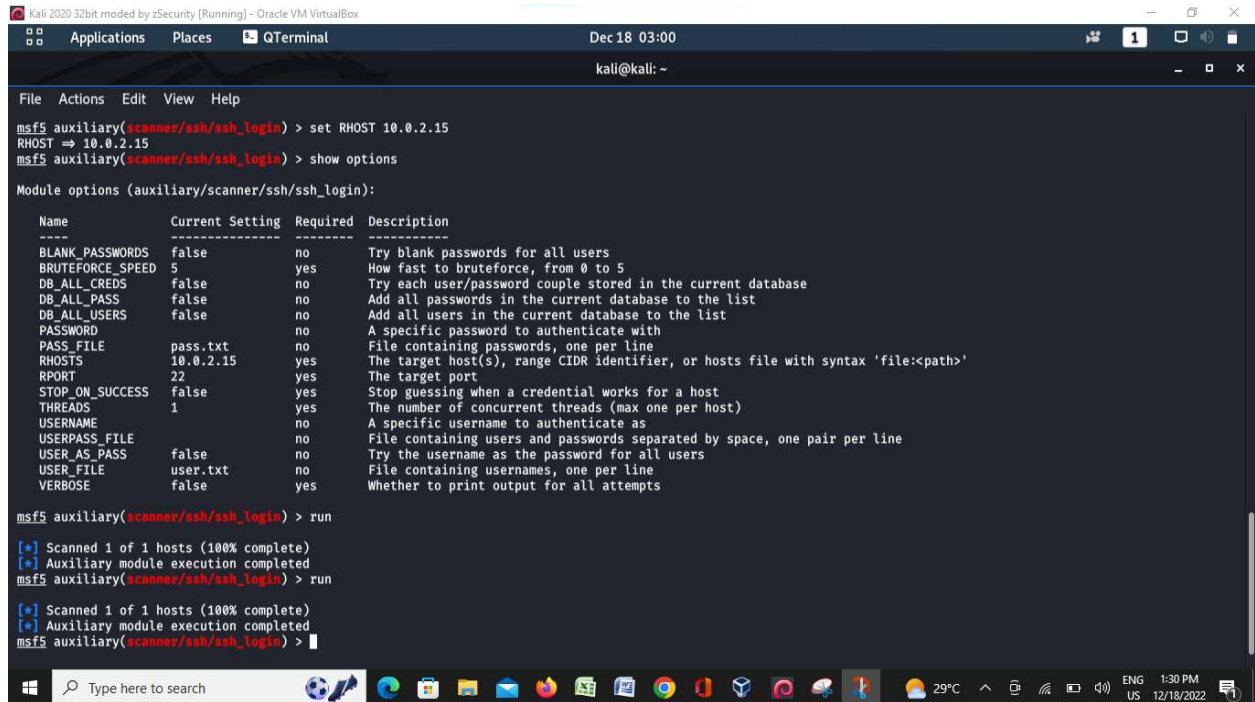
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOST 10.0.2.15
RHOST => 10.0.2.15
msf5 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
```

As my ip address is set s 10.0.2.15

Among then as=gain show options to enable the particular auxillary is done accordingly

Then after sometime evaluate this through the following process



```
Kali 2020 32bit modded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 18 03:00
kali@kali: ~
File Actions Edit View Help
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOST 10.0.2.15
RHOST => 10.0.2.15
msf5 auxiliary(scanner/ssh/ssh_login) > show options
Module options (auxiliary/scanner/ssh/ssh_login):
-----
Name           Current Setting  Required  Description
-----
BLANK_PASSWORDS false           no        Try blank passwords for all users
BRUTEFORCE_SPEED 5                yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
DB_ALL_PASS      false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
PASSWORD         pass.txt         no        A specific password to authenticate with
PASS_FILE        10.0.2.15       yes       File containing passwords, one per line
RHOSTS           22              yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT            22              yes       The target port
STOP_ON_SUCCESS  false           yes       Stop guessing when a credential works for a host
THREADS          1               yes       The number of concurrent threads (max one per host)
USERNAME         user.txt         no        A specific username to authenticate as
USERPASS_FILE    user.txt         no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false           no        Try the username as the password for all users
USER_FILE        user.txt         no        File containing usernames, one per line
VERBOSE          false           yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

Thus after completing this one we have enabled us the run that's the final part

It shows auxillary is finally executed

And completed

Result: HENCE AUXILLARY SCANNER IS COMPLETED.

AUTOMATED SCRIPTS

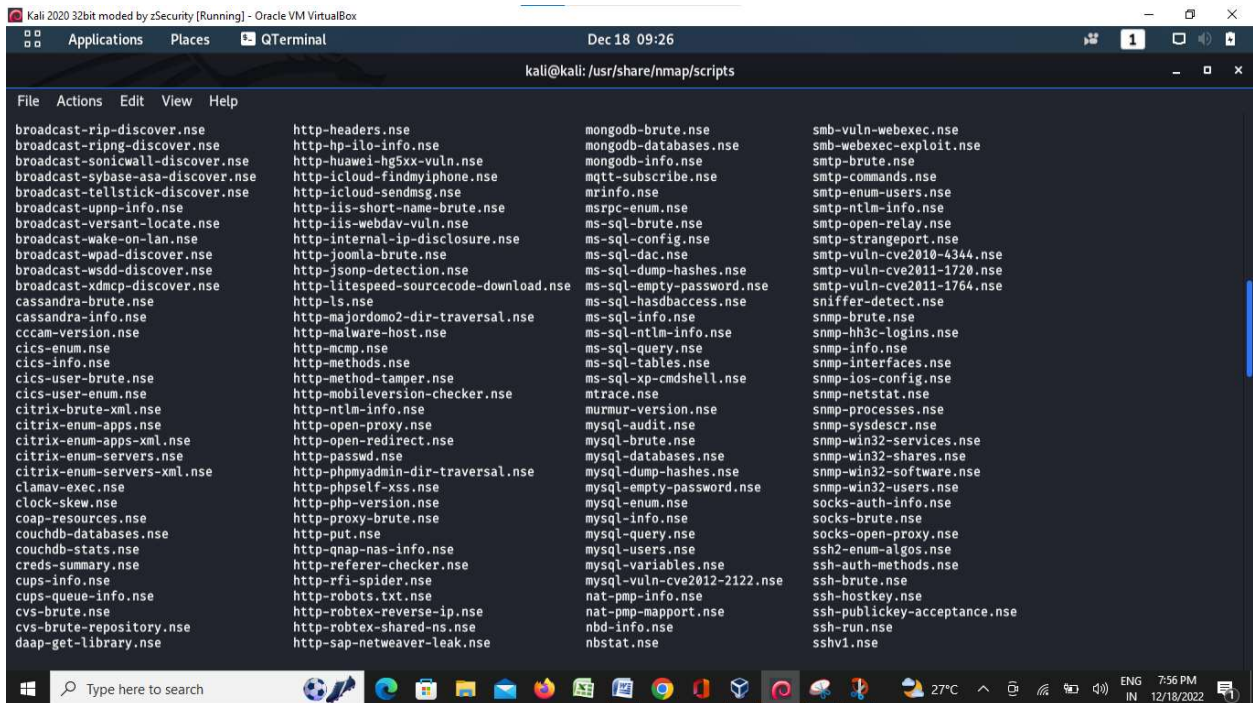
First of all type the scripts as follows

```
cd /usr/share/nmap/scripts
```

```
cd /usr/share/nmap/scripts ls
```

you will be able to see a list of all the scripts as below

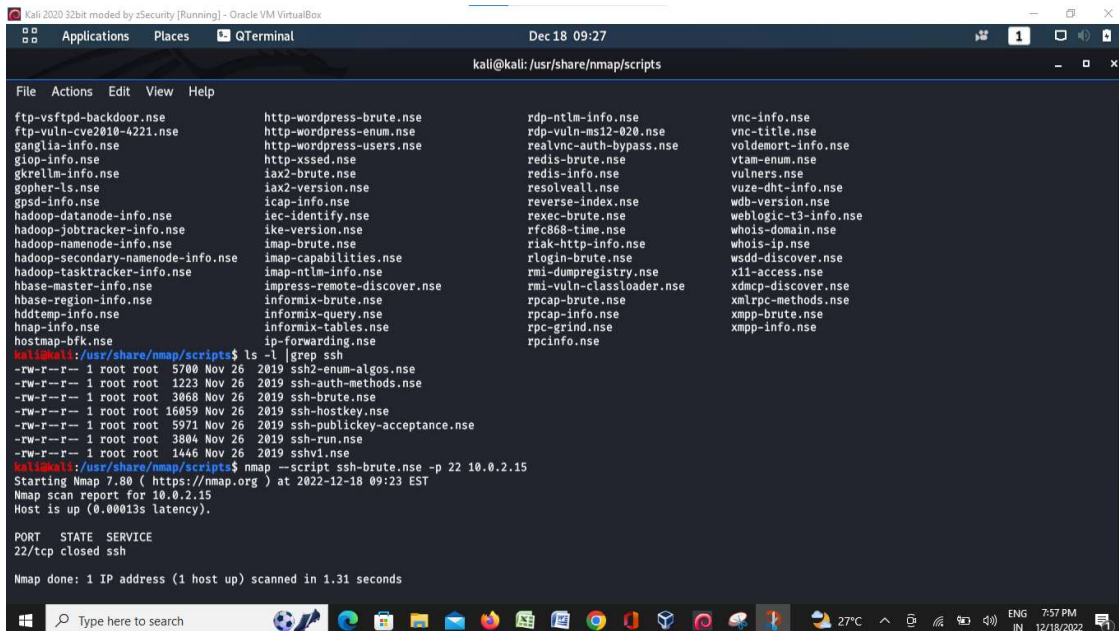
```
Kali 2020 32bit modded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 18 09:26
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
kali@kali:~$ cd /usr/share/nmap/scripts
kali@kali:~$ cd /usr/share/nmap/scripts$ ls
acarsd-info.nse          hostmap-crtsh.nse      ip-geolocation-geoplugin.nse  rsa-vuln-roca.nse
address-info.nse        hostmap-robtex.nse    ip-geolocation-ipinfodb.nse  rsync-brute.nse
afp-brute.nse           http-adobe-coldfusion-apsa1301.nse  ip-geolocation-map-bing.nse  rsync-list-modules.nse
afp-ls.nse              http-affiliate-id.nse  ip-geolocation-map-google.nse  rtsp-methods.nse
afp-path-vuln.nse       http-apache-negotiation.nse  ip-geolocation-map-kml.nse  rtsp-url-brute.nse
afp-serverinfo.nse      http-apache-server-status.nse  ip-geolocation-maxmind.nse  rusers.nse
afp-showmount.nse       http-aspnet-debug.nse    ip-https-discover.nse       s7-info.nse
afp-auth.nse            http-auth-finder.nse     ipidseq.nse                 samba-vuln-cve-2012-1182.nse
afp-brute.nse           http-auth.nse           ipmi-brute.nse              script.db
afp-headers.nse         http-avaya-lpoffice-users.nse  ipmi-cipher-zero.nse       servicetags.nse
afp-methods.nse         http-awstatstotals-exec.nse  ipmi-version.nse           shodan-api.nse
afp-request.nse         http-axis2-dir-traversal.nse  ipv6-multicast-mld-list.nse  sip-brute.nse
allseeingeye-info.nse   http-backup-finder.nse     ipv6-node-info.nse         sip-call-spoof.nse
amqp-info.nse           http-barracuda-dir-traversal.nse  ipv6-ra-flood.nse         sip-enum-users.nse
asn-query.nse           http-bigip-cookie.nse      irc-botnet-channels.nse     sip-methods.nse
auth-owners.nse        http-brute.nse           irc-brute.nse              skypev2-version.nse
auth-spoof.nse         http-cakephp-version.nse    irc-info.nse               smb2-capabilities.nse
backorifice-brute.nse   http-chrono.nse          irc-sasl-brute.nse          smb2-security-mode.nse
backorifice-info.nse   http-cisco-anyconnect.nse  irc-unrealircd-backdoor.nse  smb2-time.nse
bacnet-info.nse        http-coldfusion-subzero.nse  iscsi-brute.nse            smb2-vuln-uptime.nse
banner.nse             http-comments-displayer.nse  iscsi-info.nse             smb-brute.nse
bitcoin-getaddr.nse     http-config-backup.nse     isns-info.nse              smb-double-pulsar-backdoor.nse
bitcoin-info.nse       http-cookie-flags.nse      jdwp-exec.nse              smb-enum-domains.nse
bitcoinrpc-info.nse    http-cors.nse             jdwp-info.nse              smb-enum-groups.nse
bittorrent-discovery.nse  http-cross-domain-policy.nse  jdwp-inject.nse            smb-enum-processes.nse
bjnp-discover.nse      http-csrf.nse             jdwp-version.nse           smb-enum-services.nse
broadcast-ataoe-discover.nse  http-date.nse             knx-gateway-discover.nse    smb-enum-sessions.nse
broadcast-avahi-dos.nse  http-default-accounts.nse  knx-gateway-info.nse       smb-enum-shares.nse
broadcast-bjnp-discover.nse  http-devframework.nse    krb5-enum-users.nse        smb-enum-users.nse
broadcast-db2-discover.nse  http-dlink-backdoor.nse    ldap-brute.nse             smb-flood.nse
broadcast-dhcp6-discover.nse  http-dombased-xss.nse    ldap-novell-getpass.nse    smb-ls.nse
broadcast-dhcp-discover.nse  http-domino-enum-passwords.nse  ldap-rootse.nse           smb-mbenum.nse
```

After that in order to filter the command ou will be able to identify the ssh alone through `ls -l |grep ssh`

Then you will be able to a list of ssh scripts among them then you need to sort them out through the following as `nmap --script ssh-brute.nse -p 10.0.2.15`

Then you will be able to identify the ssh ports and thehosts that we are able to find among them .



```
Kali 2020 32bit moded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 18 09:27
kali@kali: /usr/share/nmap/scripts

File Actions Edit View Help

hadoop-namenode-info.nse      imap-brute.nse                riak-http-info.nse           whois-ip.nse
hadoop-secondary-namenode-info.nse  imap-capabilities.nse        rlogin-brute.nse            wsdd-discover.nse
hadoop-tasktracker-info.nse    imap-ntlm-info.nse           rmi-dumpregistry.nse        x11-access.nse
hbase-master-info.nse         impress-remote-discover.nse   rmi-vuln-classloader.nse    xdmcp-discover.nse
hbase-region-info.nse         informix-brute.nse            rpcap-brute.nse              xmlrpc-methods.nse
hddtemp-info.nse              informix-query.nse            rpcap-info.nse               xmpp-brute.nse
hnmap-info.nse                 informix-tables.nse           rpc-grind.nse                xmpp-info.nse
hostmap-bfk.nse                ip-forwarding.nse            rpcinfo.nse

kali@kali: /usr/share/nmap/scripts$ ls -l |grep ssh
-rw-r--r-- 1 root root 5700 Nov 26 2019 ssh2-enum-algos.nse
-rw-r--r-- 1 root root 1223 Nov 26 2019 ssh-auth-methods.nse
-rw-r--r-- 1 root root 3068 Nov 26 2019 ssh-brute.nse
-rw-r--r-- 1 root root 16059 Nov 26 2019 ssh-hostkey.nse
-rw-r--r-- 1 root root 5971 Nov 26 2019 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root 3804 Nov 26 2019 ssh-run.nse
-rw-r--r-- 1 root root 1446 Nov 26 2019 sshv1.nse
kali@kali: /usr/share/nmap/scripts$ nmap --script ssh-brute.nse -p 22 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-18 09:23 EST
Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
kali@kali: /usr/share/nmap/scripts$ nmap --script ssh-brute.nse -P 22 10.0.2.15
Warning: You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-18 09:24 EST
Nmap scan report for 10.0.2.15
Host is up (0.00025s latency).
All 1000 scanned ports on 10.0.2.15 are closed

Nmap done: 2 IP addresses (1 host up) scanned in 1.37 seconds
kali@kali: /usr/share/nmap/scripts$
```

Hence the ports are visible among them to enable them to know about the 2 ip address s 1 hostsetup among them.

Result: AUTOMATED SCRIPTS HAS BEEN IMPLEMENTED.

John the ripper

Following is a command to get the john

John <options> <file name>

Hence save the hash file you need to crack in hash.txt

Then use cd Desktop

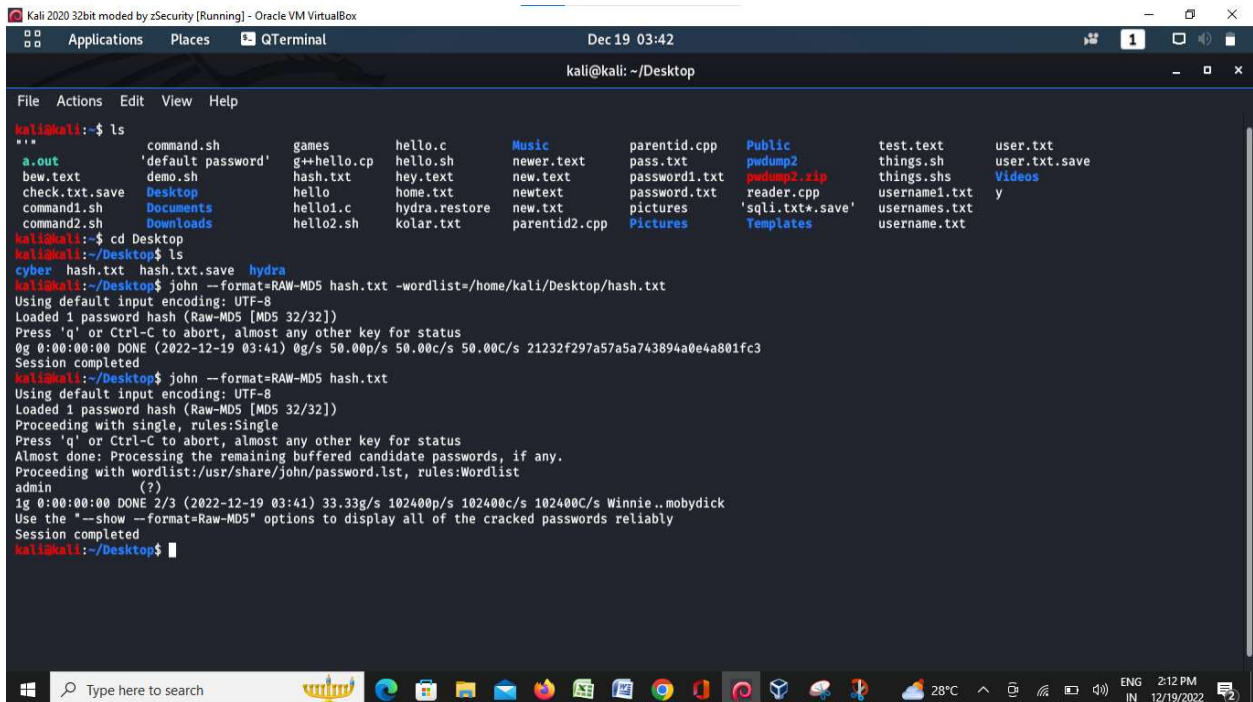
Then again use john hash.txt

If it cannot open due to ASCII value to find crack through the password as

John -format=RAW-MD5 hash.txt -wordlist=Home/kali/Desktop/hash.txt

Then finally you able to crack the hash file and the wordlist of the file

Hence the password encrypted could be cracked easily



```
Kali 2020 32bit modded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 19 03:42
kali@kali: ~/Desktop

File Actions Edit View Help

kali@kali:~$ ls
...
a.out      'default password'  games      hello.c      Music      parentid.cpp  Public      test.text  user.txt
bew.text   demo.sh             g++hello.cp hello.sh     newer.text pass.txt      pwdump2     things.sh  user.txt.save
check.txt.save Desktop            hash.txt   hey.text    new.text   password1.txt pxdump2.rip things.shs  Videos
command1.sh Documents         hello      home.txt   newtext    password.txt  reader.cpp  username1.txt  usernames.txt
command2.sh Downloads        hello1.c   hydra.restore new.txt    pictures      'sqli.txt*.save'  usernames.txt  username.txt
command2.sh

kali@kali:~$ cd Desktop
kali@kali:~/Desktop$ ls
cyber hash.txt hash.txt.save hydra
kali@kali:~/Desktop$ john --format=RAW-MD5 hash.txt -wordlist=/home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2022-12-19 03:41) 0g/s 50.00p/s 50.00c/s 21232f297a57a5a743894a0e4a801fc3
Session completed
kali@kali:~/Desktop$ john --format=RAW-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 32/32])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
admin
(?)
1g 0:00:00:00 DONE 2/3 (2022-12-19 03:41) 33.33g/s 102400p/s 102400c/s 102400C/s Winnie..mobydick
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
kali@kali:~/Desktop$
```

RESULT: Hence this could be cracked easily through john ripper.

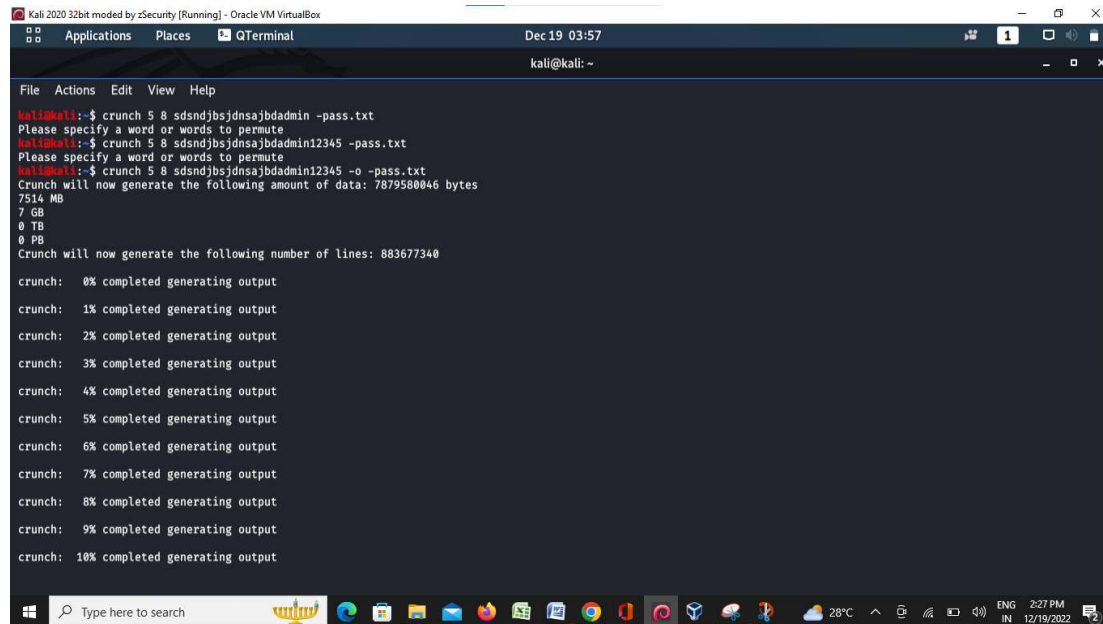
CRUNCH

USE crunch tool the now about the pass as the length and the min and max as the string of characters

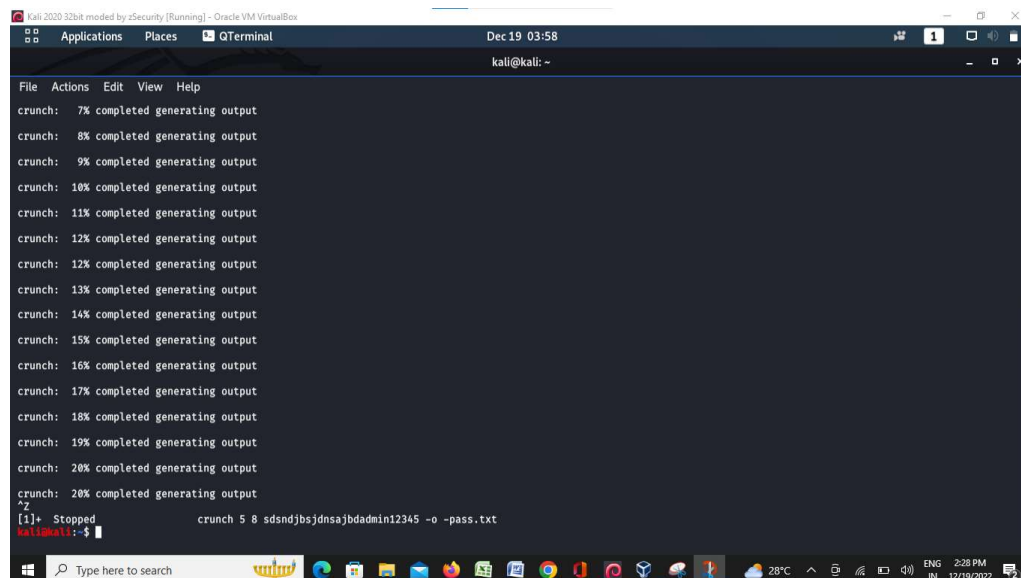
Among them as crunch 5 8 axdsdsdsd admin -o pass.txt

It takes about 7514Mb and 883677340 lines to crack

Thus it takes a large ram to complete the task and could be a time as enlth to crack thus is displayed among them.



```
Kali 2020 32bit moded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 19 03:57
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ crunch 5 8 sdsndjbsjdnsajbdadmin -pass.txt
Please specify a word or words to permute
kali@kali:~$ crunch 5 8 sdsndjbsjdnsajbdadmin12345 -pass.txt
Please specify a word or words to permute
kali@kali:~$ crunch 5 8 sdsndjbsjdnsajbdadmin12345 -o -pass.txt
Crunch will now generate the following amount of data: 7879580046 bytes
7514 MB
7 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 883677340
crunch: 0% completed generating output
crunch: 1% completed generating output
crunch: 2% completed generating output
crunch: 3% completed generating output
crunch: 4% completed generating output
crunch: 5% completed generating output
crunch: 6% completed generating output
crunch: 7% completed generating output
crunch: 8% completed generating output
crunch: 9% completed generating output
crunch: 10% completed generating output
```



```
Kali 2020 32bit moded by zSecurity [Running] - Oracle VM VirtualBox
Applications Places QTerminal Dec 19 03:58
kali@kali: ~
File Actions Edit View Help
crunch: 7% completed generating output
crunch: 8% completed generating output
crunch: 9% completed generating output
crunch: 10% completed generating output
crunch: 11% completed generating output
crunch: 12% completed generating output
crunch: 12% completed generating output
crunch: 13% completed generating output
crunch: 14% completed generating output
crunch: 15% completed generating output
crunch: 16% completed generating output
crunch: 17% completed generating output
crunch: 18% completed generating output
crunch: 19% completed generating output
crunch: 20% completed generating output
crunch: 20% completed generating output
^Z
[1]+ Stopped                  crunch 5 8 sdsndjbsjdnsajbdadmin12345 -o -pass.txt
kali@kali:~$
```

RESULT: Cracked the crunch tools using the crunch option of the length of file and file path.