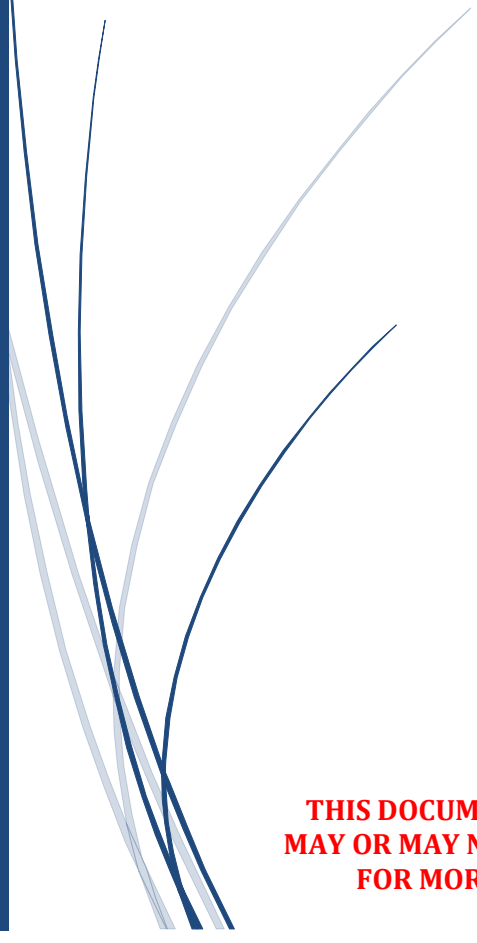
Chapter 4

Enumeration

Lab Manual



THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: NetBIOS Enumeration

In windows execute the following command.

nbtstat –A target IP

This command will display the connected devices NetBIOS names.

```
C:\Users\CSPL>nbtstat -A 192.168.0.139
Wireless Network Connection:
Node IpAddress: [192.168.0.109] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    2K3            <00>  UNIQUE      Registered
    VICTIM         <00>  GROUP       Registered
    VICTIM         <1C>  GROUP       Registered
    2K3            <20>  UNIQUE      Registered
    VICTIM         <1B>  UNIQUE      Registered
    VICTIM         <1E>  GROUP       Registered
    VICTIM         <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 00-0C-29-A8-A9-FA
```

The following command is used to display cached information of NETBIOS

nbtstat –c

```
C:\Users\CSPL>nbtstat -c
Wireless Network Connection:
Node IpAddress: [192.168.0.109] Scope Id: []

                NetBIOS Remote Cache Name Table

       Name             Type       Host Address    Life [sec]
    --------------------------------------------------------
    2K3            <20>  UNIQUE          192.168.0.139       550
```

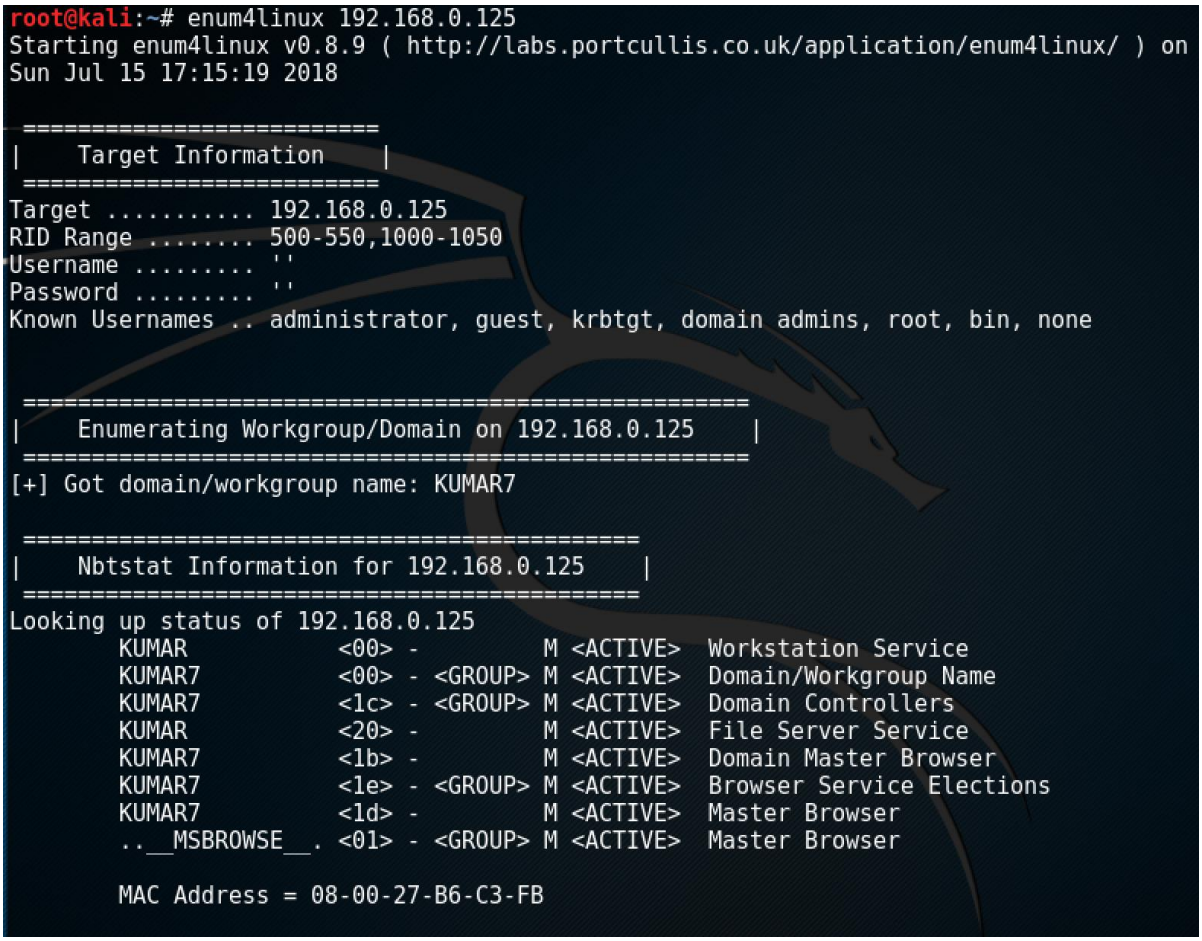
In Kali Linux open a terminal and execute the below command

nbtscan <network range>

```
root@kali:~# nbtscan 192.168.0.0/24
Doing NBT name scan for addresses from 192.168.0.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.0.0      Sendto failed: Permission denied
192.168.0.109    <unknown>        <server>  <unknown>        74:de:2b:90:31:d4
192.168.0.105    ROUTER-X         <server>  <unknown>        44:6d:57:29:cb:f2
192.168.0.106    DESKTOP-6E59HTK  <server>  <unknown>        84:ef:18:a4:7a:31
192.168.0.139    2K3              <server>  <unknown>        00:0c:29:a8:a9:fa
192.168.0.131    WIN-KKMVR607Q21  <server>  <unknown>        08:00:27:c9:0a:82
192.168.0.255    Sendto failed: Permission denied
```

Practical 2: Enumerating Linux operating system with enum4linux tool

Enum4linux is used to enumerate Linux machines. This tool works only in a LAN environment. It is used to extract a number of user accounts, user names, length of the password and last time when password changed. Let us consider Metasploitable OS (Linux) as a target and perform enumeration.



```
 ========================================
|    Session Check on 192.168.0.125    |
 ========================================
[+] Server 192.168.0.125 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 192.168.0.125    |
 ============================================
Domain Name: KUMAR7
Domain Sid: S-1-5-21-1928287797-289972450-5230789
[+] Host is part of a domain (not a workgroup)

 ======================================
|    OS information on 192.168.0.125    |
 ======================================
[+] Got OS info for 192.168.0.125 from smbclient: Domain=[KUMAR7] OS=[Windows Server
2003 R2 3790 Service Pack 2] Server=[Windows Server 2003 R2 5.2]
[+] Got OS info for 192.168.0.125 from srvinfo:
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ============================
|    Users on 192.168.0.125    |
 ============================
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED
```

This command is used to grab users list of targeted machine.

```
root@kali:~# enum4linux -U 192.168.1.107
```

```
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
enum4linux complete on Sat Jun  9 02:55:34 2018
```

We can use ***-S*** option to extract file sharing details from the target system

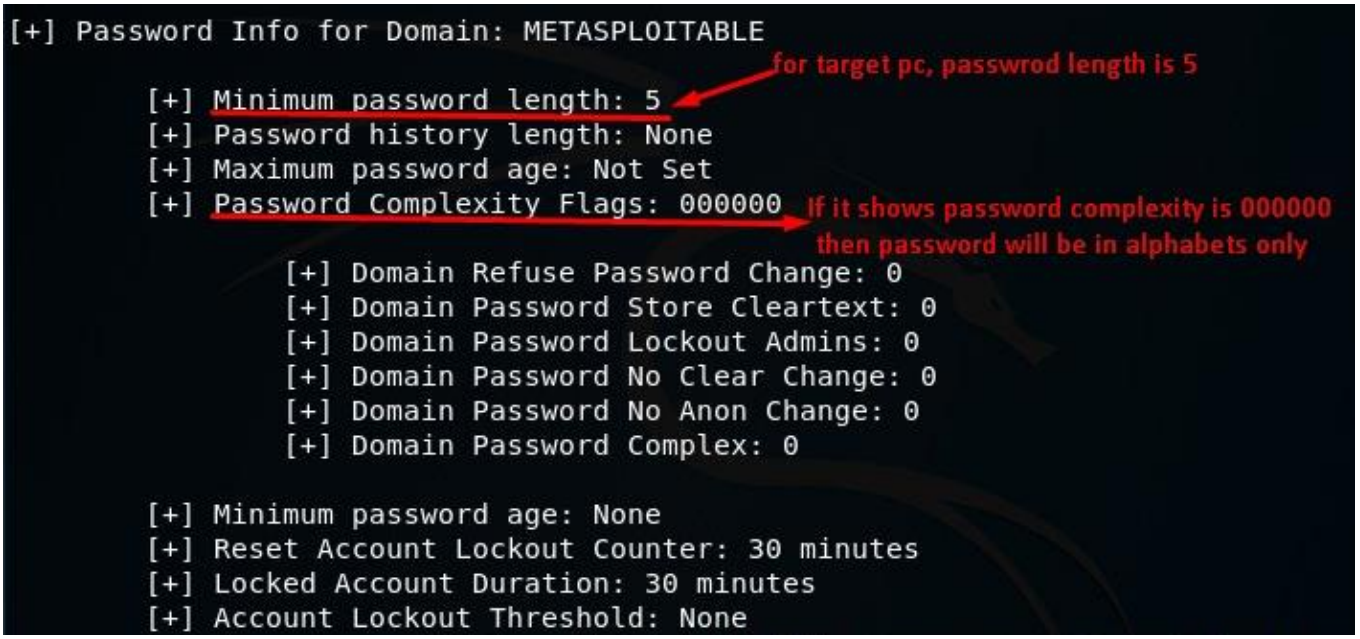
```
root@kali:~# enum4linux -S 192.168.1.107
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4li
nux/ ) on Sat Jun  9 03:02:19 2018

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.1.107
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, no
ne


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.1.107    |
 =====================================================
[+] Got domain/workgroup name: WORKGROUP

 ======================================
|    Session Check on 192.168.1.107    |
 ======================================
[+] Server 192.168.1.107 allows sessions using username '', password ''
```

```
 ========================================
|    Share Enumeration on 192.168.1.107    |
 ========================================
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            DESKTOP-H8OMKLU

[+] Attempting to map shares on 192.168.1.107
//192.168.1.107/print$  Mapping: DENIED, Listing: N/A
//192.168.1.107/tmp     Mapping: OK, Listing: OK
//192.168.1.107/opt     Mapping: DENIED, Listing: N/A
//192.168.1.107/IPC$    [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.1.107/ADMIN$  Mapping: DENIED, Listing: N/A
enum4linux complete on Sat Jun  9 03:02:20 2018
```

here, it identifies few shared files. but only one is vunerable through which we can able to access the shared files without authentication details.

-P option of enum4linux helps in identifying target system's password length(Password policy information).

```
root@kali:~# enum4linux -P 192.168.1.107
```


[+] Password Info for Domain: METASPLOITABLE
for target pc, passwrod length is 5
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
If it shows password complexity is 000000
then password will be in alphabets only
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None

Practical 3: Nmap enumeration commands

In the terminal, execute ***locate *.nse***
The above command lists nmap scripts that can be used to perform enumeration.

SMB enumeration with NMAP Script

```
root@kali:~# nmap -p445 192.168.0.132 --script=smb-enum-sessions.nse

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-05 15:10 IST
Nmap scan report for 192.168.0.132
Host is up (0.00020s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:82:FF:00 (Cadmus Computer Systems)

Host script results:
| smb-enum-sessions:
|   Users logged in
|_    KUMAR7\Administrator since <unknown>

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Shares Enumeration with NMAP Script

```
root@kali:~# nmap --script=smb-enum-shares.nse 192.168.0.132 -p445,139

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-05 15:07 IST
Nmap scan report for 192.168.0.132
Host is up (0.00028s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:82:FF:00 (Cadmus Computer Systems)

Host script results:
| smb-enum-shares:
|   ADMIN$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   C$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   IPC$
|     Anonymous access: READ <not a file share>
|     Current user ('guest') access: READ <not a file share>
|   NETLOGON
|     Anonymous access: <none>
|     Current user ('guest') access: READ
|   SYSVOL
|     Anonymous access: <none>
|     Current user ('guest') access: READ
|   Share
|     Anonymous access: <none>
|_    Current user ('guest') access: READ

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

OS Enumeration with NMAP Script

```
root@kali:~# nmap -p445 --script=/usr/share/nmap/scripts/smb-os-discove
ry.nse 192.168.0.141
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-09 08:25 EDT
Nmap scan report for 192.168.0.141
Host is up (0.0050s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: B4:B6:76:6B:B3:40 (Intel Corporate)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-06-09T08:25:01-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
root@kali:~#
```

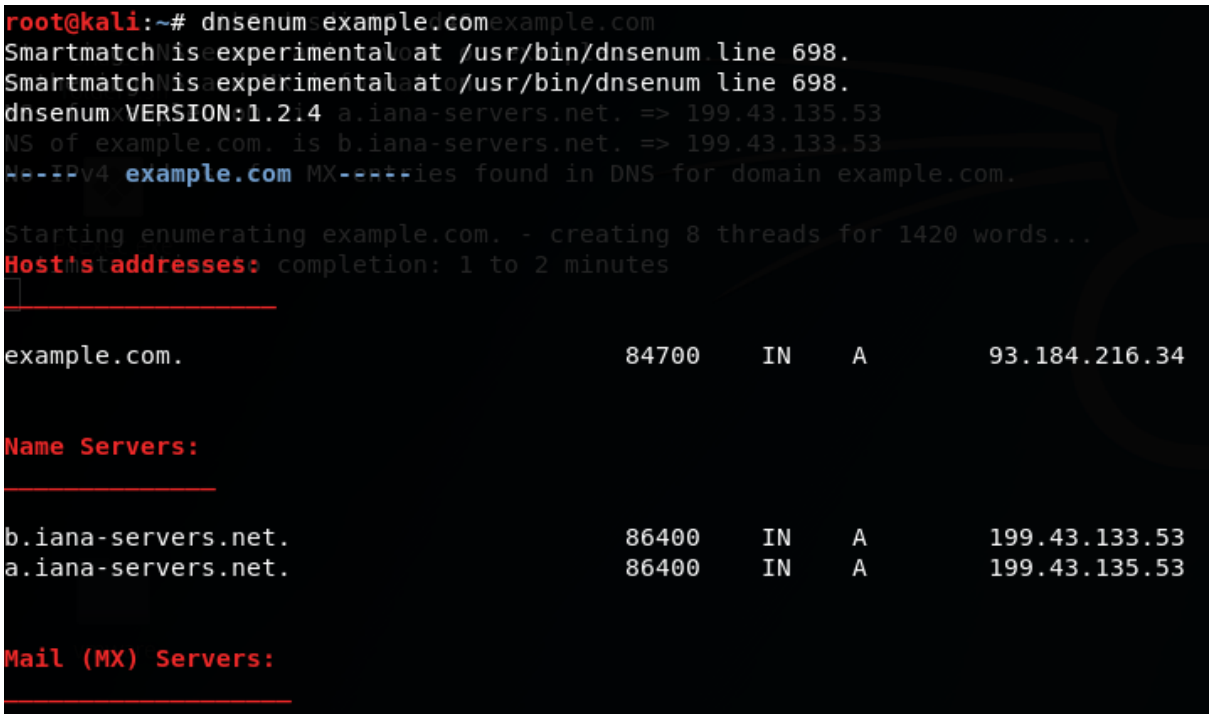
Enumerating Algorithms with NMAP script

```
root@kali:~# nmap --script=ssh2-enum-algos.nse 192.168.0.131 --open -p22

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-05 15:05 IST
Nmap scan report for 192.168.0.131
Host is up (0.00021s latency).
PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (7)
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (3)
|       ssh-rsa
|       ssh-dss
|       ecdsa-sha2-nistp256
|   encryption_algorithms: (13)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
|       arcfour128
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       aes192-cbc
|       aes256-cbc
|       arcfour
|       rijndael-cbc@lysator.liu.se
|   mac_algorithms: (11)
```

Practical 4: DNS Enumeration

Execute the following command to perform DNS enumeration on given domain.

dnsenum example.com



Practical 5: DNS Enumeration with dnsrecon

Execute the following command to extract VOIP server's information.

dnsrecon -t srv -d example.com

-t option specifies the type of attack, ***-d*** specifies the domain name and ***srv*** is used to identify services running on target DNS server and ***axfr*** can identify zone transfer details of a given domain.

```
root@kali:~# dnsrecon -t srv -d ufone.com
[*] Enumerating Common SRV Records against ufone.com
[*]      SRV _sipfederationtls._tcp.ufone.com access01.ufone.com 42.83.84.72
5061 10
[*]      SRV _sipfederationtls._tcp.ufone.com access01.ufone.com 42.83.84.73
5061 10
[*]      SRV _sip._tls.ufone.com access02.ufone.com 221.120.238.134 443 10
[*]      SRV _sip._tls.ufone.com access02.ufone.com 221.120.238.133 443 10
[*]      SRV _sip._tls.ufone.com access01.ufone.com 42.83.84.73 443 0
[*]      SRV _sip._tls.ufone.com access01.ufone.com 42.83.84.72 443 0
[+] 6 Records Found
```

```
root@kali:~# dnsrecon -t axfr -d ufone.com
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for ufone.com name servers
[*] Resolving SOA Record
[+]      SOA ns01.ufonegsm.net 202.125.152.252
[*] Resolving NS Records
[*] NS Servers found:
[*]     NS ns02.ufonegsm.net 202.125.152.195
[*]     NS ns03.ufonegsm.net 42.83.87.31
[*]     NS ns01.ufonegsm.net 202.125.152.252
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 202.125.152.195
[+] 202.125.152.195 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*]
[*] Trying NS server 202.125.152.252
[+] 202.125.152.252 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*]
[*] Trying NS server 42.83.87.31
[+] 42.83.87.31 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
root@kali:~#
```

Practical 6: DNS dictionary attack

atk6-dnsdict6 is used to extract sub-domains along with IP address details.

```
root@kali:~# atk6-dnsdict6 -d46 altoromutual.com
```

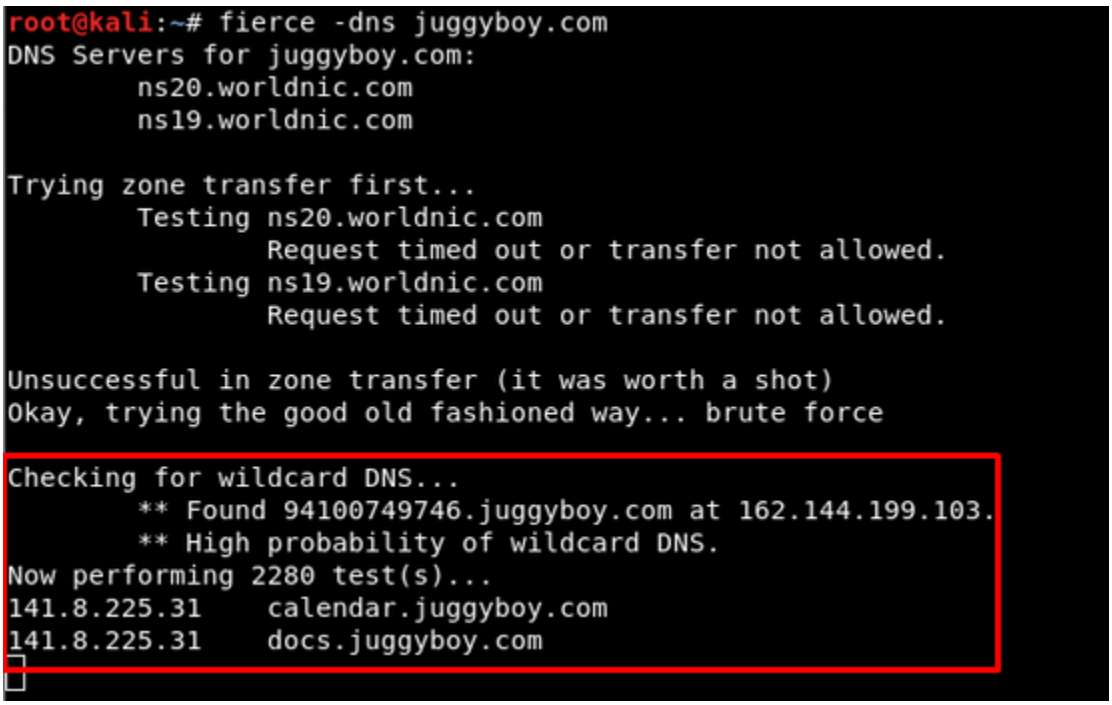
```
Starting DNS enumeration work on altoromutual.com. ...
Gathering NS and MX information...
NS of altoromutual.com. is ns1-206.akam.net. => 193.108.91.206
NS of altoromutual.com. is ns1-99.akam.net. => 193.108.91.99
Warning: no mail server (MX) information found

Starting enumerating altoromutual.com. - creating 8 threads for 1420 words...
Estimated time to completion: 1 to 2 minutes
dev.altoromutual.com. => 65.61.137.117
www.altoromutual.com. => 65.61.137.117

Found 2 domain names and 1 unique ipv4 address for altoromutual.com.
```

Practical 7: DNS enumeration with fierce

The fierce tool works as similar to the dnsdict6 tool and contains 2280 keywords to perform a brute-force attack on target and confirm sub-domains.

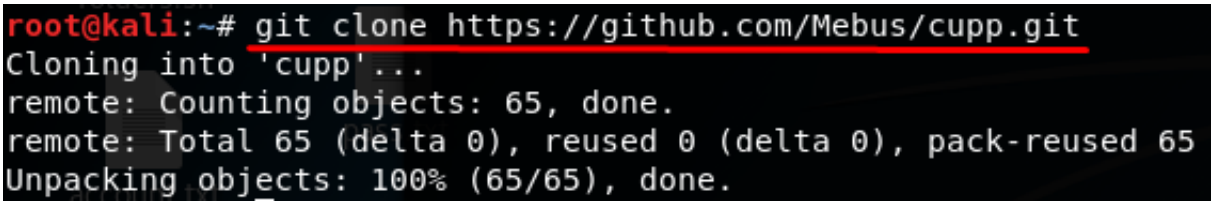
Execute the following command:

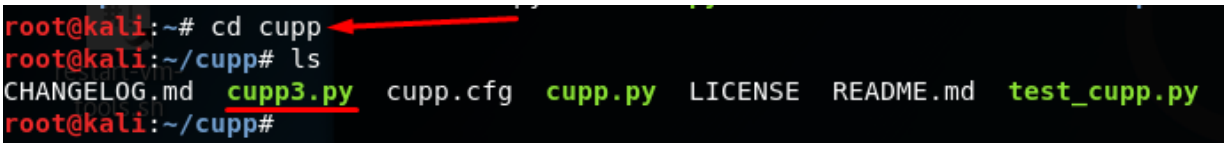
fierce -dns juggyboy.com



Practical 8: Creating wordlist using CUPP(Common User Password Profiler)

To install **cupp** on Kali Linux, execute the following command





The above ***cupp.py*** command with option ***-i*** starts an interactive session for creating a wordlist based on information provided.

```
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

First Name: Rahul
Surname: Sharma
Nickname: Share
Birthdate (DDMMYYYY): 01021990


Partner's name: Rohini
Partner's nickname: Tigress
Partner's birthdate (DDMMYYYY): 03041992


Child's name: Roman
Child's nickname: cisco
Child's birthdate (DDMMYYYY): 05062003

Pet's name:
```

```
Pet's name: Krypto
Company name: Stark Industries

Do you want to add some key words about the victim? Y/[N]: Y
Please enter the words, comma-separated. [i.e. hacker,juice,black], spaces will be removed: superman,batman,ironman,quicksilver
```

GIVE Y, So you can add keywords about the target Like below

```
Do you want to add some key words about the victim? Y/[N]: Y
Please enter the words, comma-separated. [i.e. hacker,juice,black], spaces will be removed: superman,batman,ironman,quicksilver
Do you want to add special characters at the end of words? Y/[N]: Y
Do you want to add some random numbers at the end of words? Y/[N]: Y
Leet mode? (i.e. leet = 1337) Y/[N]: Y
```

Give Y for them if you want to include them in your dictionary

```
[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to rahul.txt, counting 37474 words.
[+] Now load your pistolero with rahul.txt and shoot! Good luck!
```

After creating the wordlist, we can find the wordlist file in cupp directory

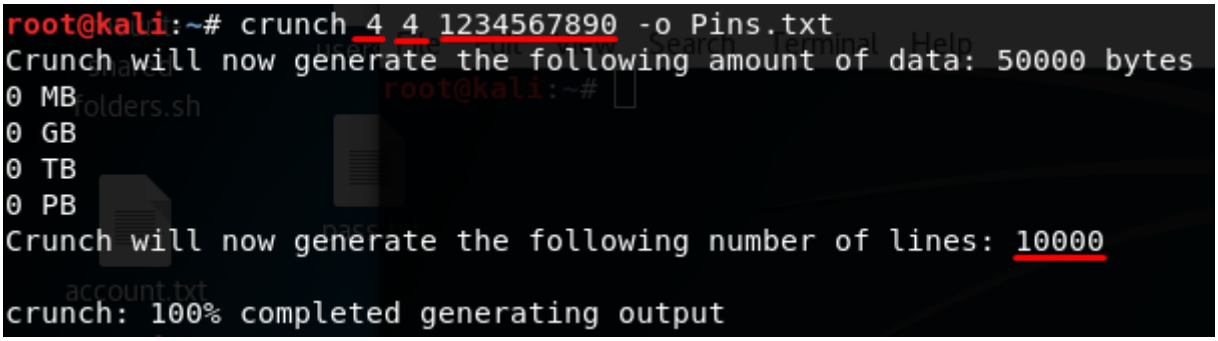
```
root@kali:~/cupp# ls
CHANGELOG.md  cupp3.py  cupp.cfg  cupp.py  LICENSE  rahul.txt  README.md  test_cupp.py
```

Practical 9: Creating wordlist using crunch

a crunch is a popular tool for creating a wordlist based on given words, letters, numbers and specials characters.

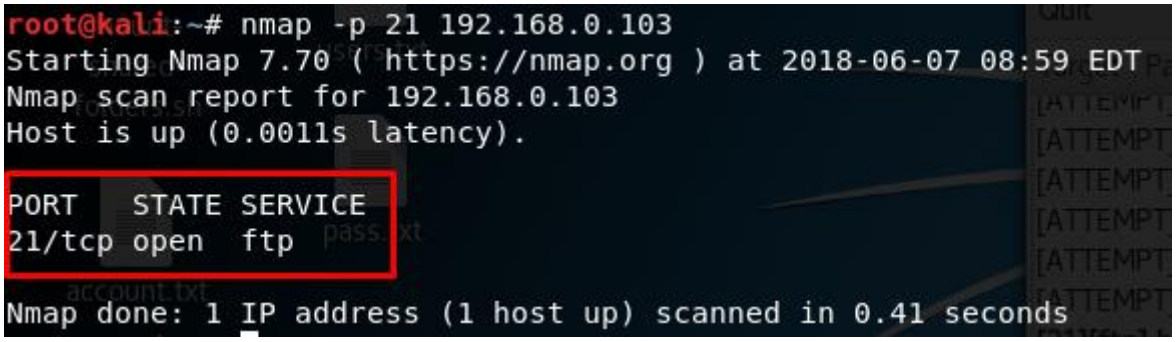
In the following command, first **4** represents the minimum length of the word and second **4** represents the maximum length of the word

Note: Make sure to verify the number of lines and file size before crunch starts creating a wordlist.



Practical 10: Cracking Login Credentials using Hydra tool

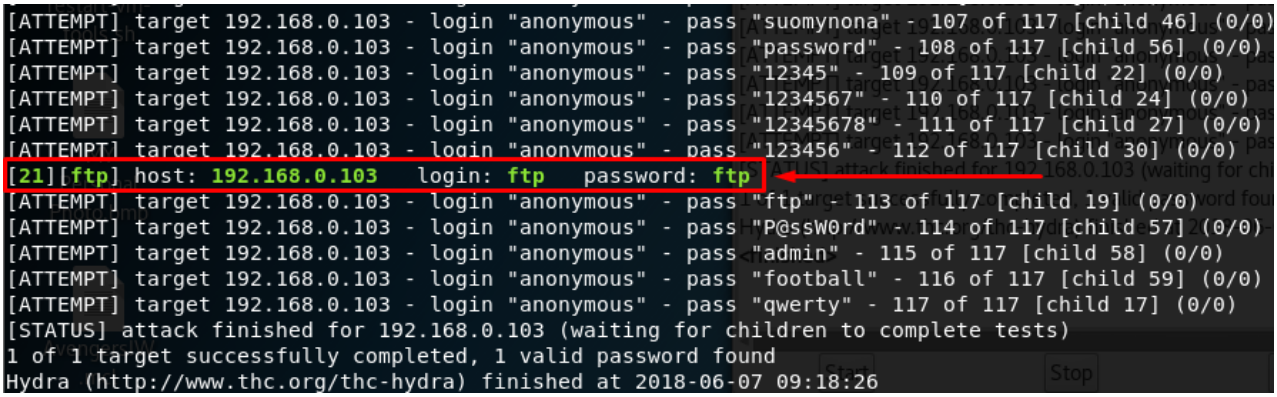
After performing port scanning using nmap, we have identified that the target is running ***ftp*** service.



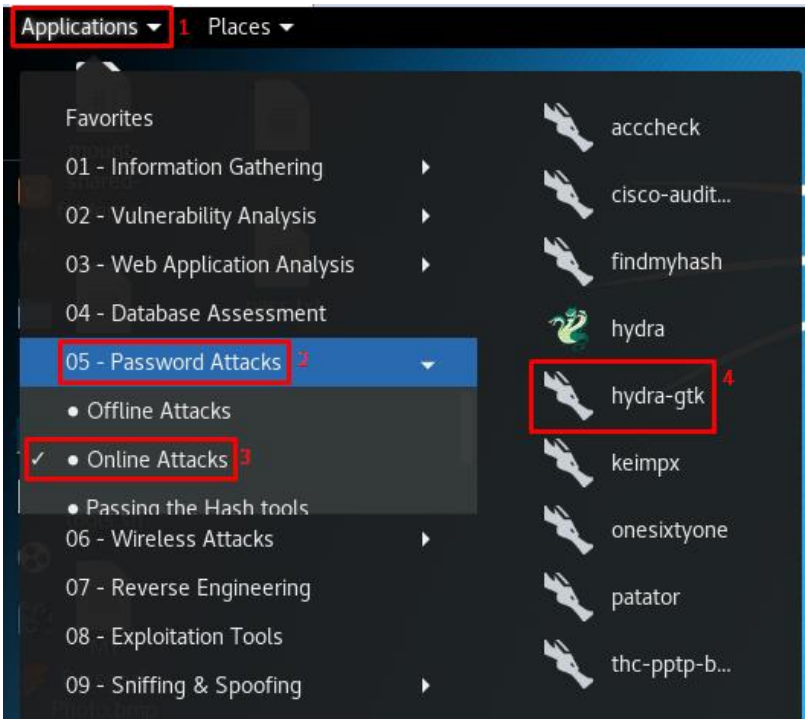
Execute the following command that starts hydra and performs a brute force attack using ***username*** and ***password*** files on the target.

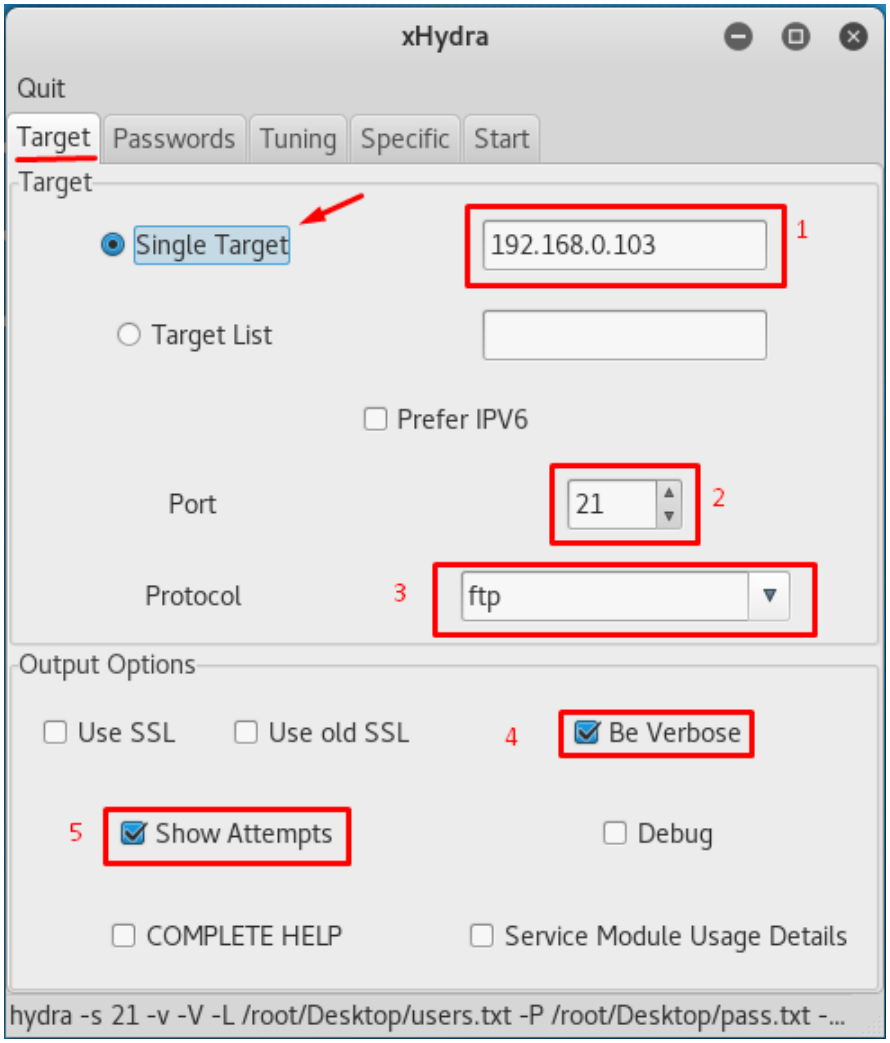
Hydra -s 21 -v -L /root/Desktop/users.txt -P /root/Desktop/pass.txt -t 60 192.168.0.103 ftp

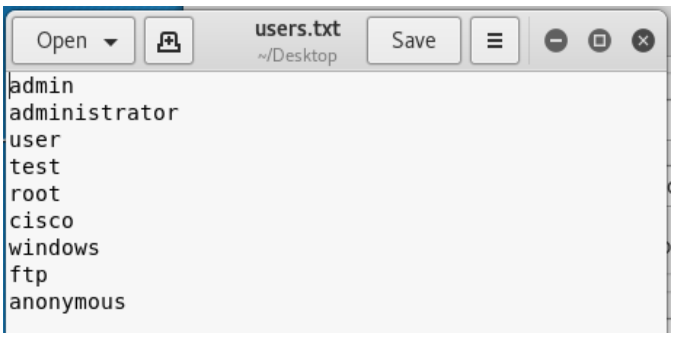
On a successful match of the login id and password for a particular service, it displays a confirmation message as shown below.

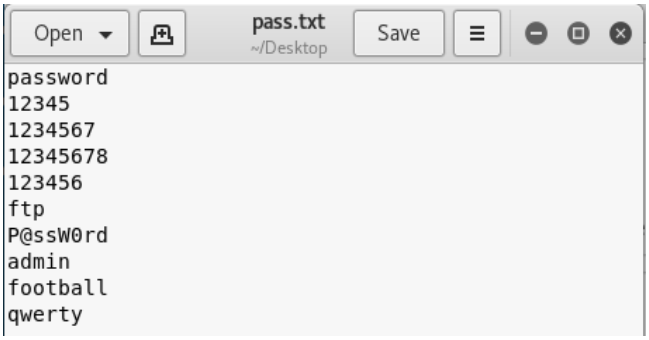


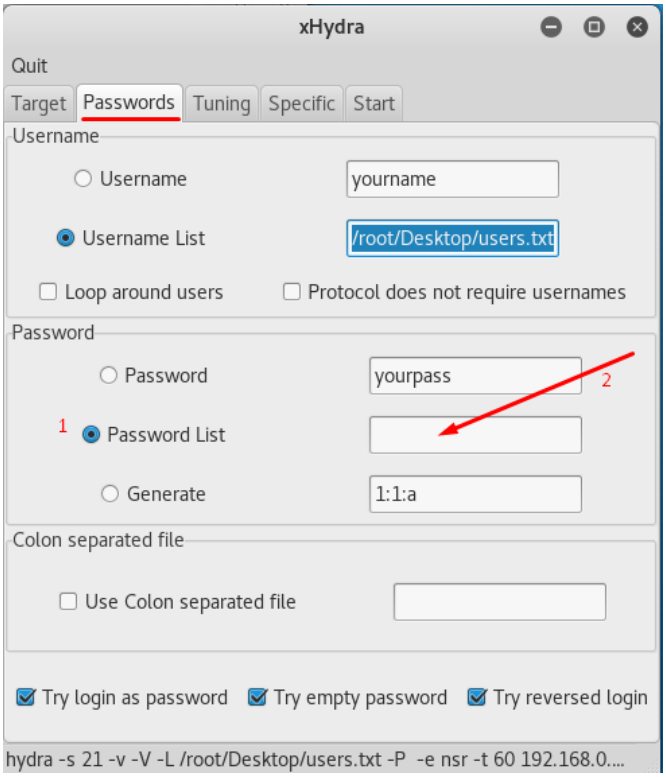
To run a graphical version of ***Hydra,*** follow the steps shown in below images

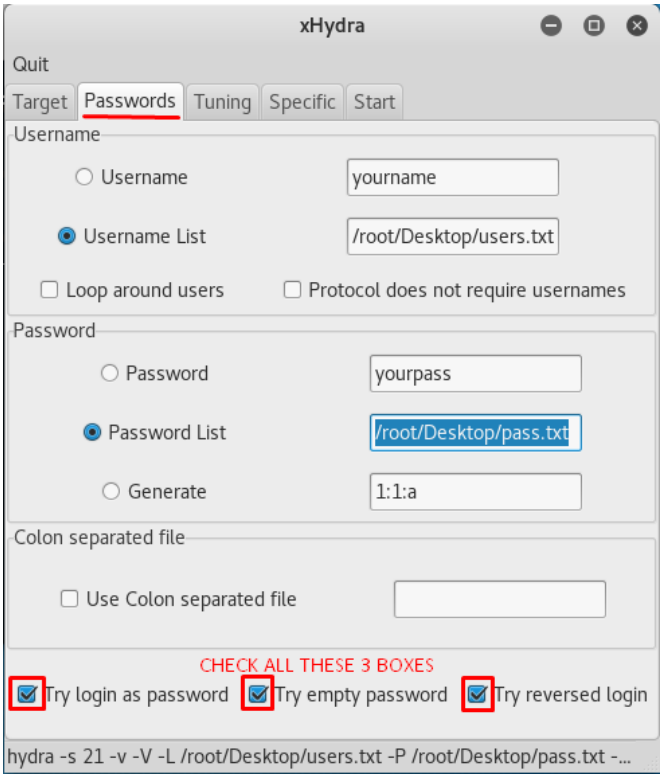


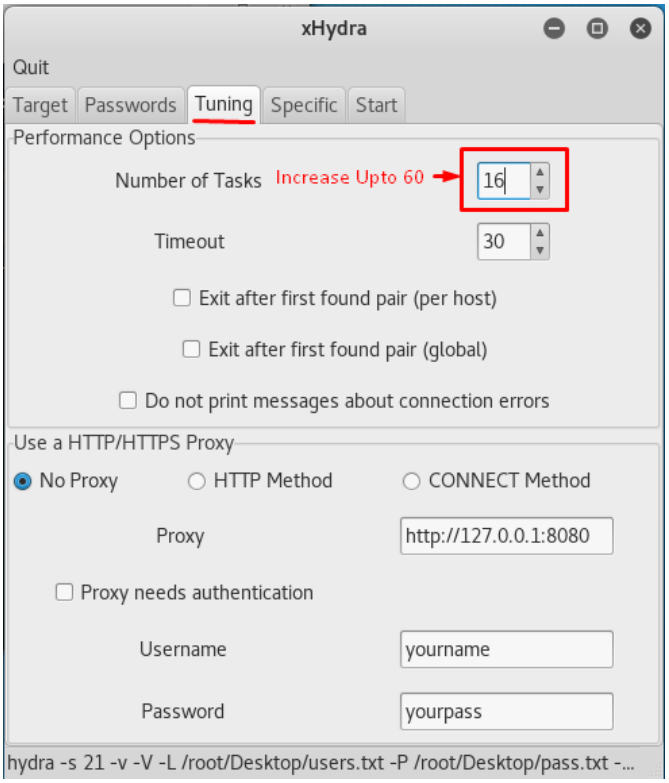

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Target
Single Target
192.168.0.103
1
Target List
Prefer IPV6
Port
21
2
Protocol
3
ftp
Output Options
Use SSL
Use old SSL
4
Be Verbose
5
Show Attempts
Debug
COMPLETE HELP
Service Module Usage Details
hydra -s 21 -v -V -L /root/Desktop/users.txt -P /root/Desktop/pass.txt -...

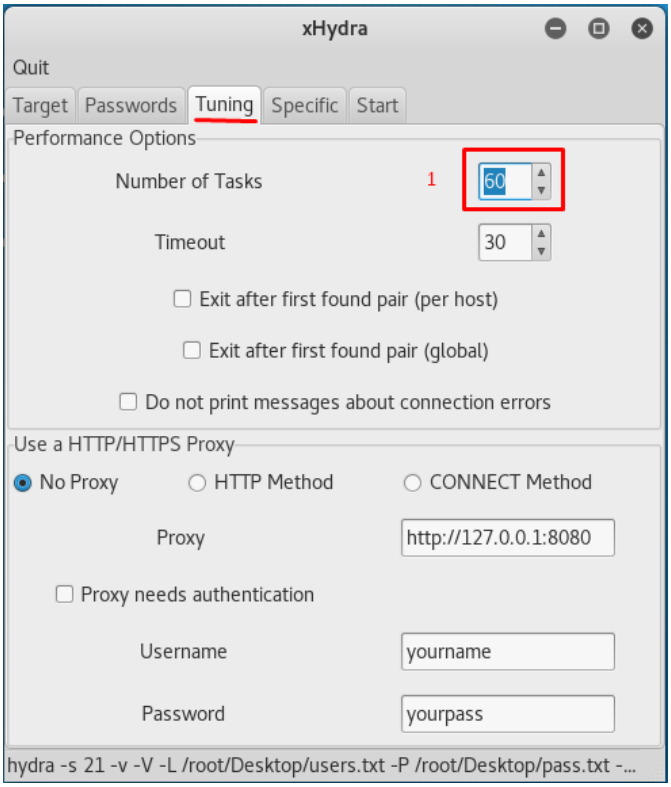

Open
users.txt
~/Desktop
Save
admin
administrator
user
test
root
cisco
windows
ftp
anonymous

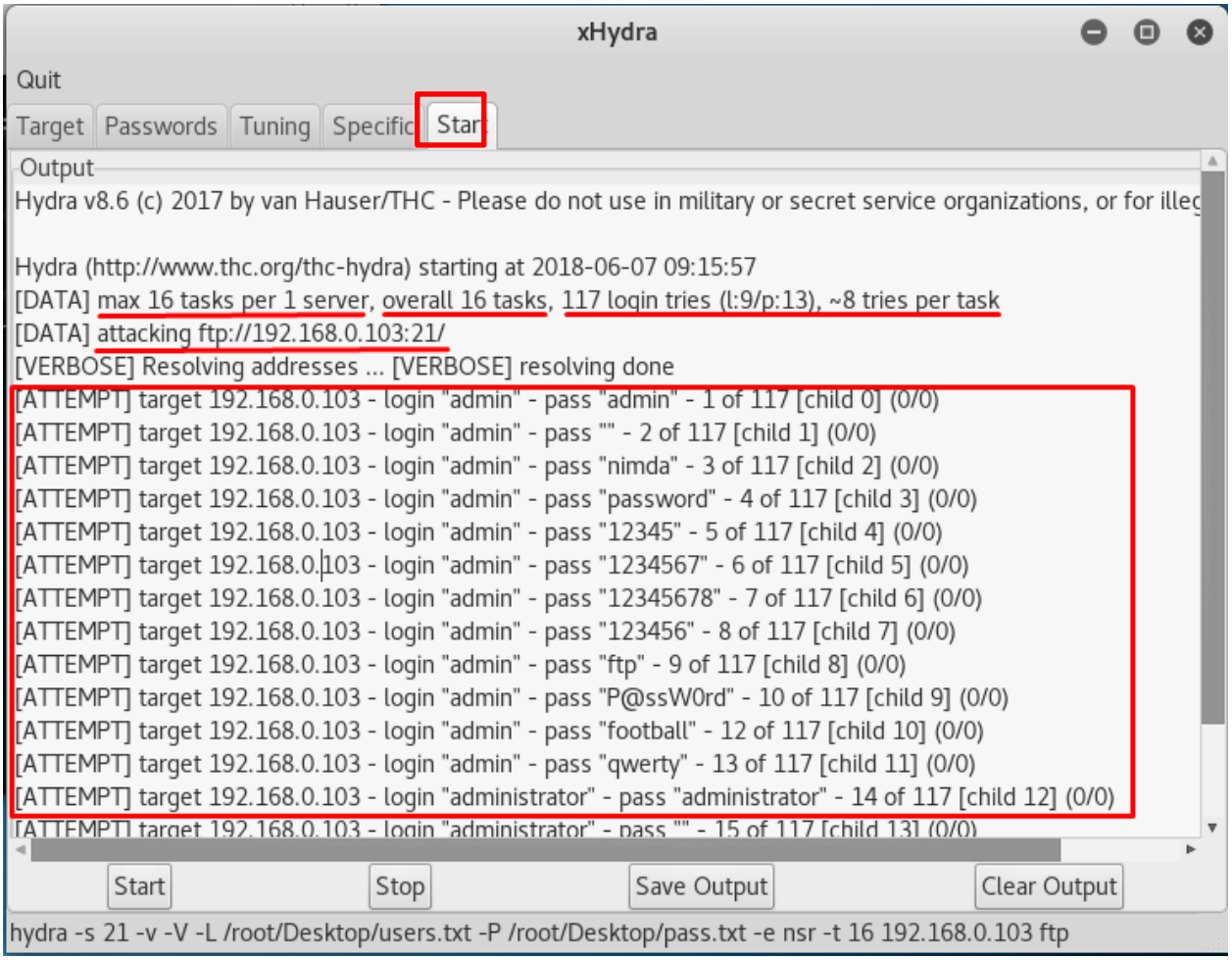

Open
pass.txt
~/Desktop
Save
password
12345
1234567
12345678
123456
ftp
P@ssW0rd
admin
football
qwerty

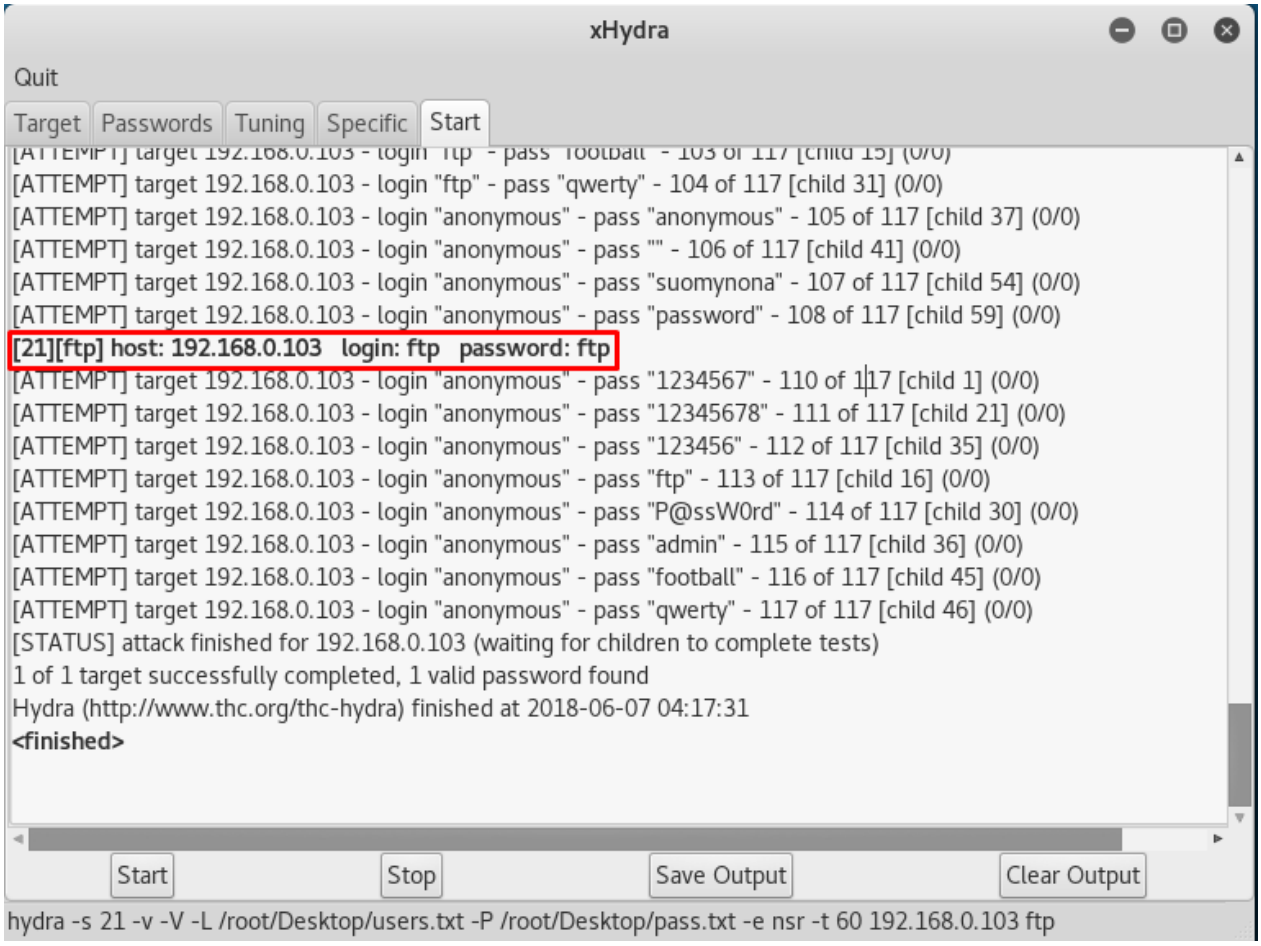

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
yourname
Username List
/root/Desktop/users.txt
Loop around users
Protocol does not require usernames
Password
Password
yourpass
2
1
Password List
Generate
1:1:a
Colon separated file
Use Colon separated file
Try login as password
Try empty password
Try reversed login
hydra -s 21 -v -V -L /root/Desktop/users.txt -P -e nsr -t 60 192.168.0....

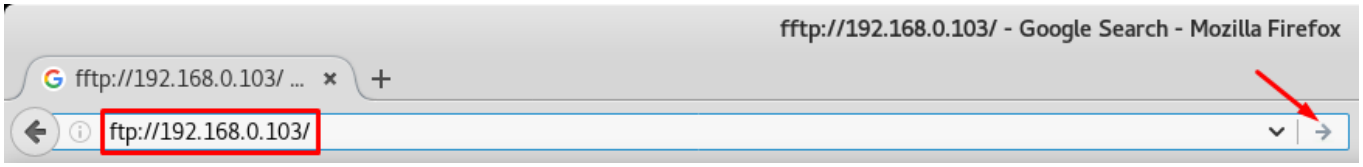

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
yourname
Username List
/root/Desktop/users.txt
Loop around users
Protocol does not require usernames
Password
Password
yourpass
Password List
/root/Desktop/pass.txt
Generate
1:1:a
Colon separated file
Use Colon separated file
CHECK ALL THESE 3 BOXES
Try login as password
Try empty password
Try reversed login
hydra -s 21 -v -V -L /root/Desktop/users.txt -P /root/Desktop/pass.txt -...

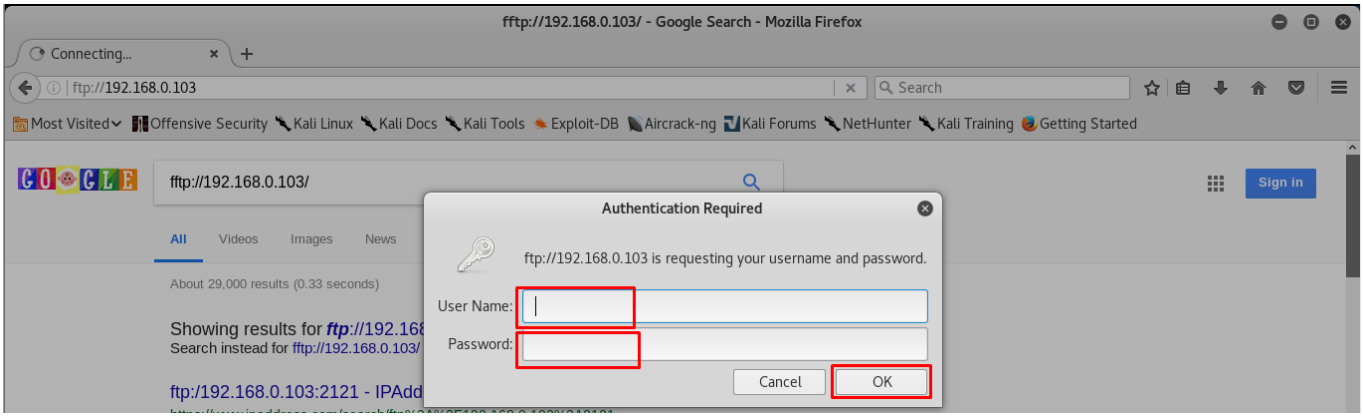

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Performance Options
Number of Tasks
Increase Upto 60
16
Timeout
30
Exit after first found pair (per host)
Exit after first found pair (global)
Do not print messages about connection errors
Use a HTTP/HTTPS Proxy
No Proxy
HTTP Method
CONNECT Method
Proxy
http://127.0.0.1:8080
Proxy needs authentication
Username
yourname
Password
yourpass
hydra -s 21 -v -V -L /root/Desktop/users.txt -P /root/Desktop/pass.txt -...

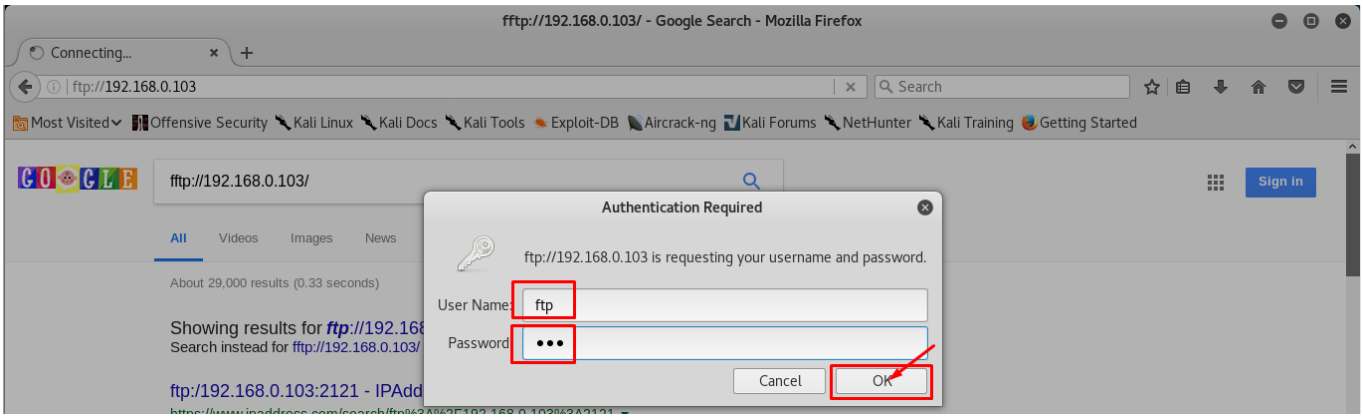

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Performance Options
Number of Tasks
1
60
Timeout
30
Exit after first found pair (per host)
Exit after first found pair (global)
Do not print messages about connection errors
Use a HTTP/HTTPS Proxy
No Proxy
HTTP Method
CONNECT Method
Proxy
http://127.0.0.1:8080
Proxy needs authentication
Username
yourname
Password
yourpass
hydra -s 21 -v -V -L /root/Desktop/users.txt -P /root/Desktop/pass.txt -...

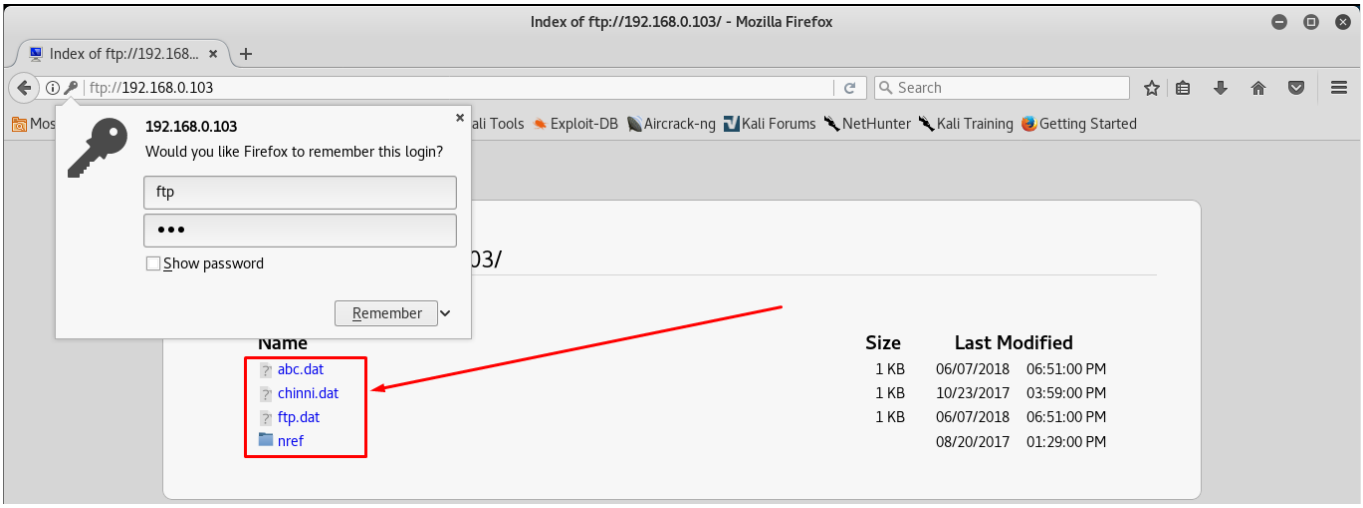

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Output
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illeg
Hydra (http://www.thc.org/thc-hydra) starting at 2018-06-07 09:15:57
[DATA] max 16 tasks per 1 server, overall 16 tasks, 117 login tries (l:9/p:13), ~8 tries per task
[DATA] attacking ftp://192.168.0.103:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "admin" - 1 of 117 [child 0] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "" - 2 of 117 [child 1] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "nimda" - 3 of 117 [child 2] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "password" - 4 of 117 [child 3] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "12345" - 5 of 117 [child 4] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "1234567" - 6 of 117 [child 5] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "12345678" - 7 of 117 [child 6] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "123456" - 8 of 117 [child 7] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "ftp" - 9 of 117 [child 8] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "P@ssW0rd" - 10 of 117 [child 9] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "football" - 12 of 117 [child 10] (0/0)
[ATTEMPT] target 192.168.0.103 - login "admin" - pass "qwerty" - 13 of 117 [child 11] (0/0)
[ATTEMPT] target 192.168.0.103 - login "administrator" - pass "administrator" - 14 of 117 [child 12] (0/0)
Start
Stop
Save Output
Clear Output
hydra -s 21 -v -V -L /root/Desktop/users.txt -P /root/Desktop/pass.txt -e nsr -t 16 192.168.0.103 ftp


xHydra
Quit
Target
Passwords
Tuning
Specific
Start
[ATTEMPT] target 192.168.0.103 - login "ftp" - pass "qwerty" - 104 of 117 [child 31] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "anonymous" - 105 of 117 [child 37] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "" - 106 of 117 [child 41] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "suomynona" - 107 of 117 [child 54] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "password" - 108 of 117 [child 59] (0/0)
[21][ftp] host: 192.168.0.103 login: ftp password: ftp
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "1234567" - 110 of 117 [child 1] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "12345678" - 111 of 117 [child 21] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "123456" - 112 of 117 [child 35] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "ftp" - 113 of 117 [child 16] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "P@ssW0rd" - 114 of 117 [child 30] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "admin" - 115 of 117 [child 36] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "football" - 116 of 117 [child 45] (0/0)
[ATTEMPT] target 192.168.0.103 - login "anonymous" - pass "qwerty" - 117 of 117 [child 46] (0/0)
[STATUS] attack finished for 192.168.0.103 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-06-07 04:17:31
<finished>
Start
Stop
Save Output
Clear Output
hydra -s 21 -v -V -L /root/Desktop/users.txt -P /root/Desktop/pass.txt -e nsr -t 60 192.168.0.103 ftp


fftp://192.168.0.103/ - Google Search - Mozilla Firefox
fftp://192.168.0.103/ ...
ftp://192.168.0.103/


fftp://192.168.0.103/ - Google Search - Mozilla Firefox
Connecting...
ftp://192.168.0.103
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
fftp://192.168.0.103/
Sign in
All
Videos
Images
News
About 29,000 results (0.33 seconds)
Showing results for ftp://192.168
Search instead for fftp://192.168.0.103/
ftp:/192.168.0.103:2121 - IPAdd
Authentication Required
ftp://192.168.0.103 is requesting your username and password.
User Name:
Password:
Cancel
OK


fftp://192.168.0.103/ - Google Search - Mozilla Firefox
Connecting...
ftp://192.168.0.103
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
fftp://192.168.0.103/
Sign in
All
Videos
Images
News
About 29,000 results (0.33 seconds)
Showing results for ftp://192.168
Search instead for fftp://192.168.0.103/
ftp:/192.168.0.103:2121 - IPAdd
Authentication Required
ftp://192.168.0.103 is requesting your username and password.
User Name:
ftp
Password:
Cancel
OK


Index of ftp://192.168.0.103/ - Mozilla Firefox
Index of ftp://192.168...
ftp://192.168.0.103
Search
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
192.168.0.103
Would you like Firefox to remember this login?
ftp
Show password
Remember
03/
Name
Size
Last Modified
abc.dat
1 KB
06/07/2018 06:51:00 PM
chinni.dat
1 KB
10/23/2017 03:59:00 PM
ftp.dat
1 KB
06/07/2018 06:51:00 PM
nref
08/20/2017 01:29:00 PM