

Lab14 Hydra Password Guessing

Lab Learning Objectives

- Use hydra to conduct password guessing attack on SSH and SMB

Lab Setup

In this lab, we will use Kali Linux and Windows 7 virtual machines.

Lab Instructions

1. Bring up a terminal at Kali Linux machine. Let's first review the password list we will use for this lab (the one comes with John the Ripper)

```
$ cat /usr/share/john/password.lst
```

We can count how many words are included in the list by running

```
$ cat /usr/share/john/password.lst | wc -l
```

We can also use the pw-inspector tool comes with the hydra to review the list at a fine-grained level. For example, we can see all the passwords with lower case letters and numbers by typing

```
$ cat /usr/share/john/password.lst | pw-inspector -n -l
```

2. Let's add an user account monk to the Kali Linux machine and set its password to **master1**

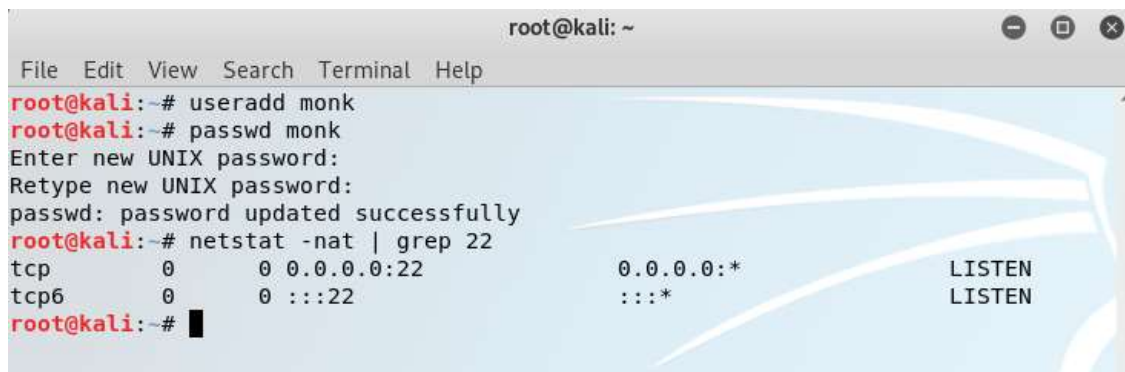
```
$ sudo useradd monk
```

```
$ sudo passwd monk
```

Next, we verify that sshd is listening on port 22 by running

```
$ sudo netstat -nat | grep 22
```

(if ssh is not working in Kali, install and start the service, "service sshd start")

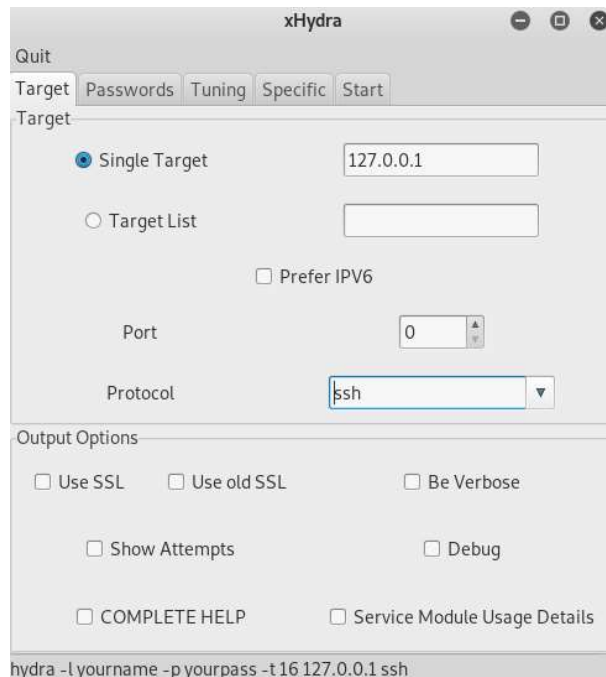


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# useradd monk  
root@kali:~# passwd monk  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
root@kali:~# netstat -nat | grep 22  
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN  
tcp6       0      0 :::22              :::*                LISTEN  
root@kali:~#
```

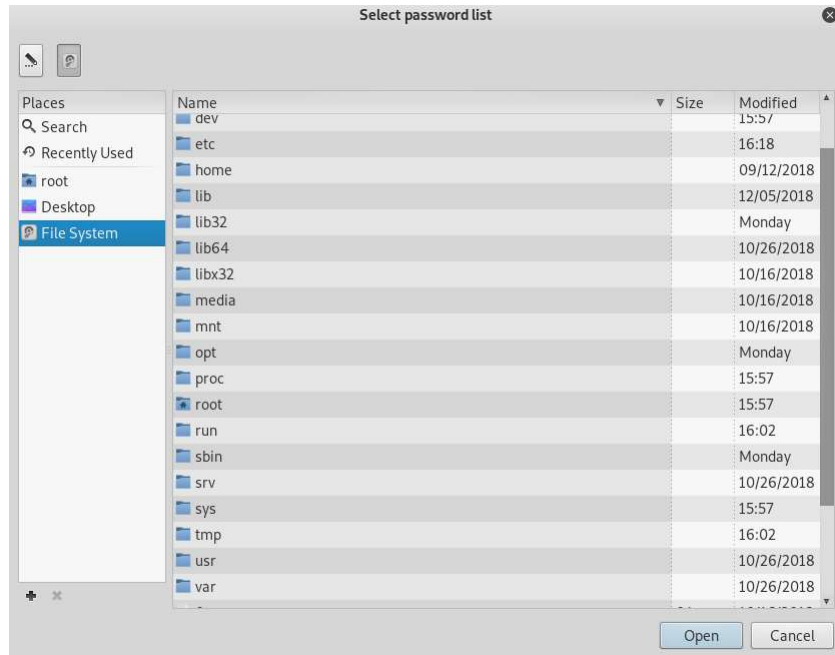
3. Bring up another terminal and start the xhydra

```
$ sudo xhydra
```

In the **Target** tab of xhydra windows. Let's enter Single Target field as 127.0.0.1 since we will attack the local host. Leave the Port field to 0 as xhydra will automatically choose the default port. Note that you have an option, though, of doing password guessing of services on non-standard ports, such as SSH on, say, TCP port 2222. Make sure the Protocol field is changed to ssh which indicates we will be password guessing using Secure Shell protocol.



Next, switch to the **Passwords** tab. Change Username to monk. Make sure that the radio button for **Password list** is selected. Click the blank box next to the Password list. On the next screen, click the File System on the left and navigate through usr → share → john to select the password.lst. You can also check the Try login as password and Try empty password options if you'd like at the bottom of the Passwords tab. You may already notice that xhydra automatically formulates the command at the bottom corresponding to the settings you choose which you could run at a command line hydra.

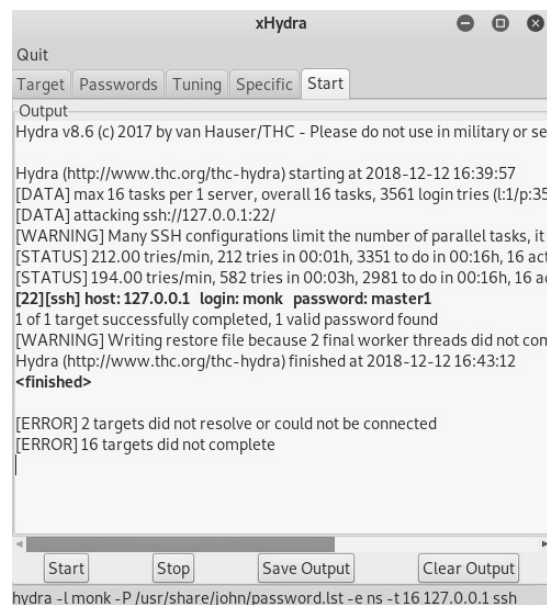


We'd like to find out how hydra might be logged at the target system when it performs the password guessing. Bring up a new terminal on Kali Linux machine and run the tail command. We configure the command with the `-f` option to update its output as items are appended to the main authentication log file `/var/log/auth.log`

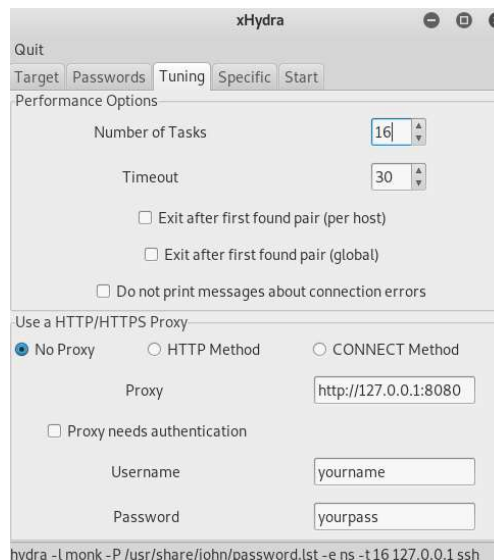
\$ sudo tail -f /var/log/auth.log

(if auth.log files doesn't exist on your system, run this first, 'sudo apt-get install rsyslog')

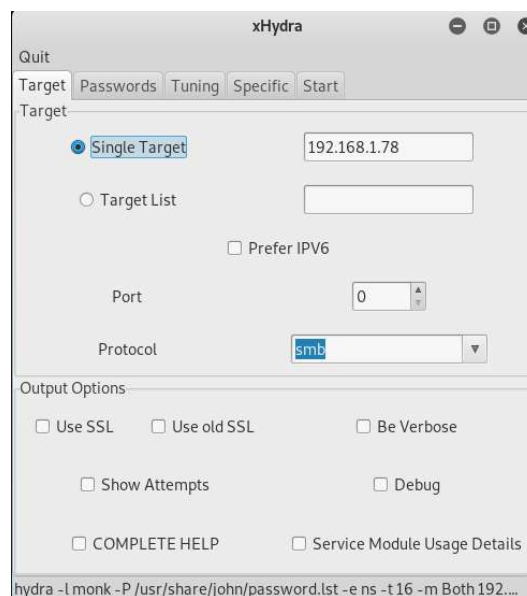
Next, let's move to the **Start** tab. Click the Start button at the bottom to start the attack. Wait for several minutes (could be long depending on your system), xhydra should successfully guess the password for monk. **(Screenshot #1)**



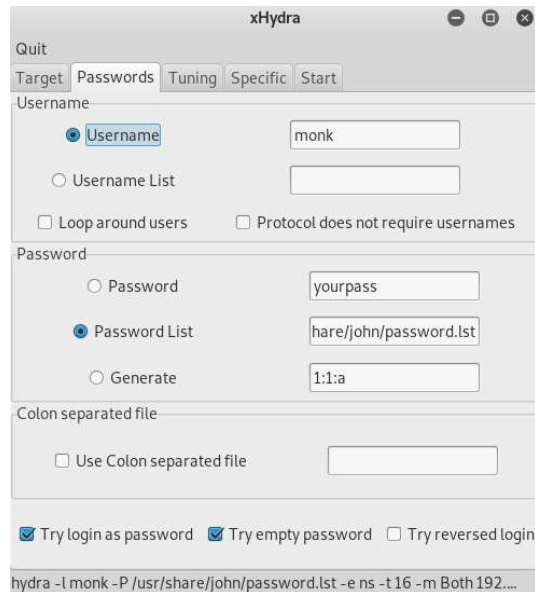
Also notice in the output that xhydra opens 16 threads (tasks) simultaneously when it performs the attack. If you click the **Tuning** tab, you can see the xhydra set the number of tasks to 16 by default.



4. Next, we will perform the password guessing for SMB over Windows 7 machine. In the **Target** tab, change the Single Target field to your *Window 7 IP address*. Leave Port field to 0 and Change the Protocol field to smb.



Click the **Passwords** tab. Change Username to monk. Make sure that the radio button for Password list is selected.



In a separate Kali terminal window, configure the tcpdump sniffer to look at all traffic going to and from your Windows 7 machine

\$ sudo tcpdump -nn host *Windows 7 IP_Address*

Next, let's move to the **Start** tab. Click the Start button at the bottom to start the attack. Wait for several minutes, xhydra should successfully guess the password for monk. **(Screenshot #2)** Also, in the terminal, check out if the packeting are going to the SMB port **(Screenshot #3)**



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# tcpdump -nn host 153.91.154.175
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:09:28.229571 ARP, Request who-has 153.91.154.175 tell 153.91.154.174, length 28
17:09:28.231420 ARP, Reply 153.91.154.175 is-at 00:0c:29:d5:08:7c, length 46
17:09:28.231443 IP 153.91.154.174.54622 > 153.91.154.175.445: Flags [S], seq 3997951610, win 29200, options [mss 1460,sackOK,TS val 3303151894 ecr 0,nop,wscale 7], length 0
17:09:28.232631 IP 153.91.154.175.445 > 153.91.154.174.54622: Flags [S.], seq 304572550, ack 3997951611, win 8192, options [mss 1460,nop,wscale 8,sackOK,TS val 20721 ecr 3303151894], length 0
17:09:28.232713 IP 153.91.154.174.54622 > 153.91.154.175.445: Flags [.], ack 1, win 229, options [nop,nop,TS val 3303151897 ecr 20721], length 0
17:09:28.232794 IP 153.91.154.174.54622 > 153.91.154.175.445: Flags [P.], seq 1:195, ack 1, win 229, options [nop,nop,TS val 3303151897 ecr 20721], length 194 S
MB PACKET: SMBnegprot (REQUEST)

17:09:28.273926 IP 153.91.154.175.445 > 153.91.154.174.54622: Flags [P.], seq 1:132, ack 195, win 260, options [nop,nop,TS val 20725 ecr 3303151897], length 131
SMB PACKET: SMBnegprot (REPLY)

17:09:28.274009 IP 153.91.154.174.54622 > 153.91.154.175.445: Flags [.], ack 132, win 237, options [nop,nop,TS val 3303151938 ecr 20725], length 0
```

Lab Report

- please include your name and 700# at the beginning of your report
 - please upload your report to the Blackboard by the due date
 - only word or pdf format is acceptable
1. Provide 3 screenshots (**Screenshot #1, #2, #3**, 5 point each).
 2. Provide screenshots with commands to show the number of passwords in password.lst which have a minimum length of 5 and meet at least two of the following criteria (5 point)
 - Have a lowercase letter
 - Have a number
 - Have a special character