SSH Password Testing With Hydra on Kali Linux

Introduction

Contents

Hail Hydra! Okay, so we're not talking about the Marvel villains here, but we are talking about a tool that can definitely do some damage. Hydra is a popular tool for launching brute force attacks on login credentials.

Hydra has options for attacking logins on a variety of different protocols, but in this instance, you will learn about testing the strength of your SSH passwords. SSH is present on any Linux or Unix server and is usually the primary way admins use to access and manage their systems. Sure, cPanel is a thing, but SSH is still there even when cPanel is being used.

This guide makes use of wordlists to provide Hydra with passwords to test. If you aren't familiar with wordlists yet, go check out our Crunch guide.

Warning: *Hydra is a tool for* ***attacking****. Only use it on your own systems and networks unless you have the written permission of the owner. Otherwise, it is* ***illegal****.*

Basic Syntax

Hydra is installed by default on Kali. There are both command line and graphical versions of Hydra, but this guide will use the command line.

Since, this guide is using the command line, you have to familiarize yourself with Hydra's syntax. Hydra has very specific syntax, so be sure to follow closely.

To start off, pick a machine on your network to test. It's probably best to use a virtual machine or something like a Raspberry Pi. This way, you aren't disrupting anything going on on your network. Find that machine's IP address, so you can point Hydra in its direction.

Once you have your target machine's IP, open up a terminal in Kali. The following linux command is very basic, and it will test the root user's SSH password.

```
# hydra -l root -p admin 192.168.1.105 -t 4 ssh
```

Okay, so the `-l` flag takes a single user parameter. The `-p` flag takes a single password. The IP is obviously the IP of the target machine. The `-t` specifies the number of threads used. Hydra suggests 4 for SSH. The last part just tells Hydra that it will be attacking SSH.

Using Word Lists

While this is good, it's not really practical to manually test every possible password. That's why Hydra takes wordlists. You can specify a wordlist instead of a single password by using `-P` instead of `-p`. A good wordlist already exists at `/usr/share/wordlists/rockyou.txt.gz`. Just decompress it, and it's ready for Hydra to use.

```
# hydra -l root -P /usr/share/wordlists/rockyou.txt
```

This will take a *long time*. There are literally millions of words in that list. If you want a quick one to test, spin up a short one with Crunch.

```
# crunch 4 4 012345abcdef -o Documents/pass.txt
# hydra -l root -P Documents/pass.txt 192.168.1.105
```

That should be fast enough for you to see it run through and complete.

Hydra also accepts wordlists for users and targets. They can be specified with the `-L` flag for users, and the `-M` flag for IPs.

```
# hydra -L /usr/share/wordlists.rockyou.txt -P /usr
```

More Flags

Like any good command line tool, Hydra has loads of flags to customize the way it runs. These flags range from more cosmetic in nature to actually altering the way it runs. Of course, since this guide focuses only on SSH, so do the explanations of these flags.

-s

Not every SSH server is running on port 22. Clever admins change them all of the time. If it's your server, you will know the port that you need to specify. If you've been hired to test someone else's server, you can use Nmap to discover which port SSH is running on.

To specify which port Hydra should attack, use the `-s` flag followed by the port number.

```
# hydra -s 22 -l root -P /usr/share/wordlists/rocky
```

-V

The `-V` just controls the verbosity of Hydra. If you would like to see each test that Hydra runs, use `-V`. If you would just like some more output but not everything, use `-v`.

```
# hydra -l root -P /usr/share/wordlists/rockyou.txt
```

-e nsr

The `-e` flag gives you more options to test with. Sometimes users have passwords that are so amazingly bad that you have to account for them outside the normal scope of your wordlist. The letters `nsr` after the `-e` flag correspond to more ways to test. `n` stands for "null," meaning that Hydra will test for a user not having a password. `s` stands for "same." Hydra will test the same password as the username, when using `s`. `r` stands for "reverse." If a user thought that they were clever and reversed their bad password, Hydra will catch that too.

```
# hydra -l root -P /usr/share/wordlists/rockyou.txt
```

Closing Thoughts

Hydra is an amazing tool for testing the strength of your SSH security. It is capable of running through massive lists of usernames, passwords, and targets to test if you or a user is using a potentially vulnerable password. It can also be tuned using its many flags to account for a number of additional situations and provide you with detailed output.

For any security tester, ensuring SSH passwords are secure should be a top priority.

ARE YOU LOOKING FOR A LINUX JOB?
Submit your RESUME, create a JOB ALERT or subscribe to RSS feed on LinuxCareers.com.

LINUX CAREER NEWSLETTER
Subscribe to NEWSLETTER and receive latest news, jobs, career advice and tutorials.

DO YOU NEED ADDITIONAL HELP?
Get extra help by visiting our LINUX FORUM or simply use comments below.

MORE ON LINUXCONFIG.ORG:

- Filtering Packets In Wireshark on Kali Linux
- Creating Wordlists with Crunch on Kali Linux
- Introduction to Nmap on Kali Linux
- Use Aircrack-ng To Test Your WiFi Password on Kali Linux

YOU MAY ALSO BE INTERESTED IN:

Comments and Discussions

3 replies

AutoPublisher Sep '18

xcxc

let me know were to get rockyou.txt file content ?

1 reply

AutoPublisher ▶ AutoPublisher Sep '18

erm3nda -> xcxc

I you where brave enough to read this content you'll be able to find rockyou.txt file over the internet… did you even typed it on any search engine?

AutoPublisher Sep '18

Mace Moneta

If you have the option, you shouldn't use (or even enable) password login with SSH. Use a 2048-bit RSA key with a passphrase. That way, for access you need something you have (the key installed on the client) and something you know (the passphrase which decrypts the key). Stealing the client provides no value without the passphrase, and knowing the passphrase without access to the key is useless.

NEWSLETTER

Subscribe to **Linux Career Newsletter** to receive latest news, jobs, career advice and featured configuration tutorials.

Full Name

Email

GDPR permission: I give my consent to be in touch with me via email using the information I have provided in this form for the purpose of news and updates.

WRITE FOR US

LinuxConfig is looking for a technical writer(s) geared towards GNU/Linux and FLOSS technologies. Your articles will feature various GNU/Linux configuration tutorials and FLOSS technologies used in combination with GNU/Linux operating system.

When writing your articles you will be expected to be able to keep up with a technological advancement regarding the

FEATURED LINUX TUTORIALS

- How To enable the EPEL Repository on RHEL 8 / CentOS 8 Linux
- Bash scripting Tutorial
- How to install VMware Tools on RHEL 8 / CentOS 8
- Howto mount USB drive in Linux
- How to install the NVIDIA drivers on Ubuntu 18.04 Bionic Beaver Linux
- How to update Kali Linux
- How to install apache tomcat

LATEST ARTICLES

- Hard drive shredding on Linux
- How to install Google Chrome web browser on Ubuntu 19.10 Eoan Ermine Linux
- Virtualbox: install guest additions on Ubuntu 19.10 Eoan Ermine
- How to install GIMP on CentOS 8 / RHEL 8 Linux
- How to install VLC Player on CentOS 8 / RHEL 8 Linux
- How to mount CD/DVD ROM

above mentioned technical area of expertise. You will work independently and be able to produce at minimum 2 technical articles a month.

APPLY NOW

CONTACT

web (at) linuxconfig (dot) org

on Linux RHEL 8 / CentOS 8
- How to install Apache on RHEL 8 / CentOS 8 Linux
- How to install node.js on RHEL 8 / CentOS 8 Linux
- How to check CentOS version
- How to Parse Data From JSON Into Python
- Check what Debian version you are running on your Linux system
- Bash Scripting Tutorial for Beginners
- Install ssh server on

on CentOS / RHEL Linux
- How to install Telegram messenger on CentOS 8 Linux
- How to install Skype on CentOS 8 Linux
- How to install VirtualBox on CentOS 8 Linux
- How to install the NVIDIA drivers on CentOS 8
- How to install telnet command in RHEL 8 / CentOS 8
- How to configure network interface bonding on RHEL 8 / CentOS 8 Linux

CentOS 8 / RHEL 8
- How to stop/start firewall on RHEL 8 / CentOS 8
- Install gnome on RHEL 8 / CentOS 8
- How to setup and use FTP Server in Ubuntu Linux
- How to Install Puppet on RHEL 8 / CentOS 8
- Enable SSH root login on Debian Linux Server
- How to install Redis server on RHEL 8 / CentOS 8 Linux
- How to install and configure Dropbear on Linux
- How to install WordPress on RHEL 8 / CentOS 88 Linux
- How to install mod_ssl on RHEL 8 / CentOS 8 with httpd Apache webserver
- Install nmap on RHEL 8 / CentOS 8
- Install python 2 on RHEL 8 / CentOS 8
- How to install netcat on RHEL

8 / CentOS 8 Linux
- How to configure NTP server on RHEL 8 / CentOS 8 Linux

Privacy Twitter