

# Password authentication cracking!

by David Maciejak, 2011

This article will show how to use Hydra to check for weak passwords. Hydra tries all possible password combination against a server on the Internet until one valid one is found to log in to the server. It is a powerful tool for hackers and network administrators alike.



**Y**eah, again an article on how to choose secure passwords. Unbreakable, long and complicated so they are impossible to remember...

Not really! This article is different!

In this article I will talk from the attacker point of view. Why it is not trivial to brute force a password. I will explain how Hydra can help to test for weak passwords. Hydra is available from <http://www.thc.org/thc-hydra/>. It is supposedly the best network login cracking tool available today.

This article will only give you a broad overview of the potential of Hydra. You will figure out the rest by yourself.

First make your network as secure as you can. Make no mistakes: One small mistake by you, one giant leap for the attacker.

- Set up a test network

- Set up a test server
- Configuring services
- Configure ACL
- Choosing good passwords
- Use SSL
- Use cryptography
- Use an IDS.

...then let Hydra try to break into your own server!

## Setting up networks

The Internet is standardized. It will either be IPv4 or IPv6. Hydra can attack IPv4 and IPv6 networks alike. Use the -6 option to switch to IPv6.

## Configuring services and access controls

Common protocols for mail are SMTP, POP3 and IMAP4. They are used by small and large businesses alike, heck they are even used by gmail, hotmail and

other big players: Most of those biggies support one of those protocols beside the web based login known to most of you.

Your password is at risk even if you never ever used SMTP, POP3 or IMAP.

Use the -h option in Hydra to get a full list of supported protocols.

A common mistake of many new server installations is that they come with services like POP3, IMAP or SSH enabled by default. Access control and firewall are disabled by default. New default servers are an easy target for Hydra.

### Shell 1. Choosing IP version from command line

```
#!/hydra -l john -p doe imap://192.168.0.10:143
#!/hydra -l john -p doe imap://[::FFFF:192.168.0.10]:143 -6
```

### Shell 2. Bruteforce password generator option

```
#!/hydra -l john -x 5:8:A1 imap://192.168.0.10:143
```

### Shell 3. Set SASL method on command line

```
#!/hydra -l john -p doe imap://192.168.0.10/CRAM-MD5
```

## Choosing good passwords



Passwords are often chosen carelessly. 90% of all users pick one of the 10 most common passwords at some point on some system.

123456, password, secret, ... look familiar?

Might as well not use a password at all then!

Hydra also has a special command line option: Use “-e ns” to check for empty passwords and where the password is the username!

Hydra can work through list of common passwords or can mutate the passwords randomly.

Use the -x option for mutating the password.

For example use “-x 5:8:A1 “ to try all password of length 5 to 8 by using all possible combinations of all upper case characters and all numbers.

## Using SSL and cryptographic methods

Using encryption like SSL does not help. SSL is primarily used to encrypted the sessions between attacker and server. This is an advantage for the attacker as the attack is not picked up by a network Intrusion Detection System (IDS).

SSL is almost never used to authenticate a client. Client side authentication is done by traditional password authentication in almost all servers.

Research has shown that users using SSL chose weaker password for the SSL connection than for connections not using SSL. It appears there is some false sense of security lingering among all the good, bad and ugly things with SSL.

This is where Hydra attacks.

In cryptography if you do not understand it do not use it!

Beside SSL does Hydra also support SASL (CRAM-MD5, DIGEST-MD5 and SCRAM-SHA1).

The “Simple Authentication and Security Layer” (SASL) is a framework for authentication and data security in Internet protocols. It decouples authentication mechanisms from application protocols.

GNU project has implemented it through the GNU SASL Library called GSASL (see <http://www.gnu.org/software/gsas/>).

When the server is negotiating secure channel, secure method, Hydra just respond “ok let’s do it”, and generates valid credential based on the challenge sent.

The SASL method can be used as shown above. Use the -U option to get a full list of supported SASL options.

## Monitoring access and resources

More and more companies are buying SIEM (Security Information and Event Management) to centralized the event access logs. This could be useful to track abnormal events on the network, like for example many authentication failures on a given service. This kind of tool, is used to save your time, it could also automatically alerts you by using some correlated rules to detect malicious events.

No SIEM prevents the attack. They merely inform you after the event. After Hydra got in. After your data got stolen.

Sometimes the SIEM or the IAM (Identity and Access Management) can become the way of entry as well! These services are using LDAP. And guess what, Hydra also supports LDAP.

IPS (Intrusion Prevention System) is a must have in a corporate network, nowadays such kind of device always come with predefined signatures to detect password cracking attacks. However, they have a weak point, they are based on a defined rate. For example if there are 10 authentication failed in 5 seconds from the same source IP just block or quarantine the attacker for x seconds.

For this purpose Hydra comes with some features to plan how

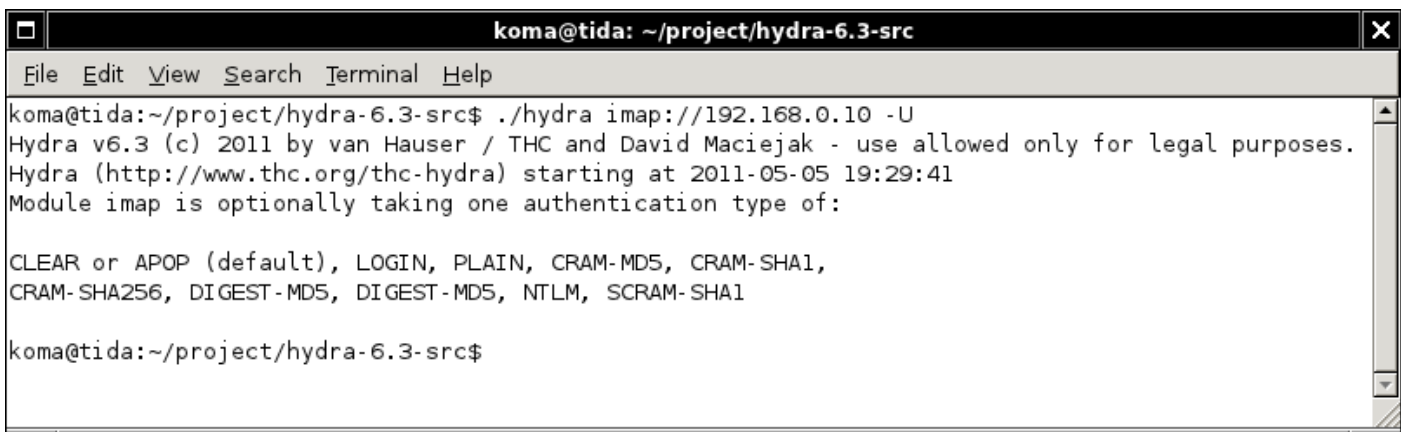
the attack is conducted. The `-t` option can be used to set the number of concurrent tasks (default is 16). Setting it to 1 and you will stay under the radar of any IDS.

## Conclusion

Chose your password wisely. Do not let IDS, IPS, SIEM, IAM or SSL lure you into a false sense of security.

Try Hydra. Make sure you are safe and secure.

The best tool against hacker attacks is a smart network administrator.



```
koma@tida: ~/project/hydra-6.3-src
File Edit View Search Terminal Help
koma@tida:~/project/hydra-6.3-src$ ./hydra imap://192.168.0.10 -U
Hydra v6.3 (c) 2011 by van Hauser / THC and David Maciejak - use allowed only for legal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2011-05-05 19:29:41
Module imap is optionally taking one authentication type of:

CLEAR or APOP (default), LOGIN, PLAIN, CRAM-MD5, CRAM-SHA1,
CRAM-SHA256, DIGEST-MD5, DIGEST-MD5, NTLM, SCRAM-SHA1

koma@tida:~/project/hydra-6.3-src$
```

Figure 1. Module usage, example using IMAP

## References

Hydra Home Project: <http://www.thc.org/thc-hydra>  
Wikipedia Page: [http://en.wikipedia.org/wiki/Hydra\\_\(software\)](http://en.wikipedia.org/wiki/Hydra_(software))

Special thanks goes to THC crew.