

Forum:[Hack Forums](#)

Thread: [is brute force really outdated?](#)

v740612 - August 17, 2017, 3:17 pm

is there any possibly way for it to work? I'm just trying to find my old email, not hack anybody. Yahoo and gmail are absolute SHIT and don't provide any customer service. I have been struggling for 6 years trying to find my old email accounts.

Can you use burp suite pro + hydra for brute forcing to really work? I saw this in a youtube video and it was legit.

Plus, adding a wait time between attempts to avoid captcha/lock out. Or if fails, use an auto captcha solver. Has anyone tried this to see if it works?

The reason i'm asking is cause i'm still waiting for my free trial of burp suite pro to be sent to my email. It has pretty much everything you need to hack like a professional...I can't wait to try it.

Hydra alone sucks. I tried using it on an email that I already know, created a word list with the password in it, and it said all the passwords are invalid, WTF?!?

bananasouce - August 17, 2017, 3:23 pm

I can tell you already that this is not going to work..

With brute forcing you are trying to find a hay in a needle factory.

Vana - August 17, 2017, 3:24 pm

With connection times, account locking, and captchas, you're not going to get anywhere attempting this.

Elitas - August 17, 2017, 3:26 pm

Brute forcing has been out of date since people started using stronger passwords.

Dictionary attacks (ie educated wordlists) are still useful and extremely relevant in many fields of hacking such as hash cracking or even targeted attacks on websites.

v740612 - August 17, 2017, 3:26 pm

(Aug 17, 2017 03:23 PM)bananasouce Wrote: [\[CITE\]](#) I can tell you already that this is not going to work..

With brute forcing you are trying to find a hay in a needle factory.
Pretty sure it's the other way around...

A needle in haystack

???

Elitas - August 17, 2017, 3:27 pm

(Aug 17, 2017 03:24 PM)Vana Wrote: [\[CITE\]](#) With connection times, account locking, and captchas, you're not going to get anywhere attempting this.

You're forgetting that there are many ways to get the header response from a website to verify

whether you have the correct username/password.

Take APIs for example, they sometimes require authentication in order to gather specific API information. These can be manipulated in the form of a GET request which can respond with either a successful authentication or an invalid authentication.

Sometimes this doesn't even require proxies.

(Aug 17, 2017 03:17 PM)v740612 Wrote: [\[CITE\]](#) is there any possibly way for it to work? I'm just trying to find my old email, not hack anybody. Yahoo and gmail are absolute SHIT and don't provide any customer service. I have been struggling for 6 years trying to find my old email accounts.

Can you use burp suite pro + hydra for brute forcing to really work? I saw this in a youtube video and it was legit.

Plus, adding a wait time between attempts to avoid captcha/lock out. Or if fails, use an auto captcha solver. Has anyone tried this to see if it works?

The reason i'm asking is cause i'm still waiting for my free trial of burp suite pro to be sent to my email. It has pretty much everything you need to hack like a professional...I can't wait to try it.

Hydra alone sucks. I tried using it on an email that I already know, created a word list with the password in it, and it said all the passwords are invalid, WTF?!?

I mean Hydra is a little outdated and I haven't used it successfully in years. There are new tools out now which works. I've been looking at ways of preventing them. It's all about websites being tight on the information which they serve to users be it from an API or a response to a specific POST request. API keys and captchas are good ways of limiting brute force attempts but they aren't perfect.

bananasouce - August 17, 2017, 3:30 pm

(Aug 17, 2017 03:26 PM)v740612 Wrote: [\[CITE\]](#) Pretty sure it's the other way around...

A needle in haystack

???

No, cuz it is way harder that just that.

Vana - August 17, 2017, 3:31 pm

(Aug 17, 2017 03:27 PM)Elitas Wrote: [\[CITE\]](#) You're forgetting that there are many ways to get the header response from a website to verify whether you have the correct username/password.

Take APIs for example, they sometimes require authentication in order to gather specific API information. These can be manipulated in the form of a GET request which can respond with either a successful authentication or an invalid authentication.

Sometimes this doesn't even require proxies.

Most APIs don't take username:password authentication, usually OAuth or API keys. Along with that, rate limiting will more than likely impede on how many API requests you can make.

v740612 - August 17, 2017, 3:39 pm

(Aug 17, 2017 03:27 PM)Elitas Wrote: [\[CITE\]](#) I mean Hydra is a little outdated and I haven't used it successfully in years. There are new tools out now which works. I've been looking at ways of preventing them. It's all about websites being tight on the information which they serve to users be it from an API or a response to a specific POST request. API keys and captchas are good ways of

limiting brute force attempts but they aren't perfect.

You mean better alternatives, like Medusa or nCrack, plus using botnets?

Nomad.Null - August 17, 2017, 3:59 pm

It's possible if you have a pretty good idea what password might be being used by a list of accounts, but spraying a single account with thousands of passwords is not feasible anymore over HTTP/HTTPS requests unless literally no security has been built into the system. There is no way to get around account lockout thresholds and rate limits. If you have been trying to get back this account for 6 years, shouldn't you have moved on by now anyway?

Long time ago, bro. Cut the cord.

?Criminal - August 17, 2017, 5:37 pm

Expanding on what Vana said in the future all websites will enable username based lockout policies by default very few currently do this due to user experience hindering, most sites use IP based lockout systems which are trivial to bypass with optic fiber socks5 which supersede traditional proxies because you get really nice speed out(better HTTP r/s) of it compared to public proxy lists. But once this happens bruteforcing and dictionary attacks will completely die out however in this day and age barely anyone does this, most people do what's known as a credential stuffing attack where they SQL inject another site crack the hashes and then run the leaked credentials on various other sites checking for password reuse so we can say it's pretty much already dead since so few people actually crack most people just check credentials hacked from other sites and sell the accounts obtained.

Mr.Zzz - August 17, 2017, 7:17 pm

According to me Hydra is not so inefficient (I found several passwords with it) mostly combined with Crunch. The main point is that several providers have implemented cracking protection system (i.e. gmail and Yahoo).

Cheers!

?Criminal - August 17, 2017, 7:19 pm

(Aug 17, 2017 07:17 PM)Mr.Zzz Wrote: [\[CITE\]](#) According to me Hydra is not so inefficient (I found several passwords with it) mostly combined with Crunch. The main point is that several providers have implemented cracking protection system (i.e. gmail and Yahoo).

Cheers!

you must be bruteforcing some random chinese wordpress blog running wordpress 2 which is years old for hydra to still work in 2017, because all sites have some sort of rate limiting in place and hydras not designed for bypassing rate limits, it doesn't even support proxies it only supports one proxy and that's pretty much useless.

G3yb01 - August 17, 2017, 7:57 pm

AI Bruteforcing.

ITs more alive than ever.

v740612 - August 17, 2017, 8:38 pm

(Aug 17, 2017 07:19 PM)?Criminal Wrote: [\[CITE\]](#) you must be bruteforcing some random chinese wordpress blog running wordpress 2 which is years old for hydra to still work in 2017, because all sites have some sort of rate limiting in place and hydras not designed for bypassing rate limits, it doesn't even support proxies it only supports one proxy and that's pretty much useless.

Did you not read my post? Hydra is designed to avoid rate limits, using -w / -W to indicate wait time for responses. Of course, that would make the process much more slower.

It's impossible to bypass rate limits unless you hack the server.

and why would you need to use more than one proxy?

Faith Connors - August 17, 2017, 8:45 pm

(Aug 17, 2017 08:38 PM)v740612 Wrote: [\[CITE\]](#) Did you not read my post? Hydra is designed to avoid rate limits, using -w / -W to indicate wait time for responses. Of course, that would make the process much more slower.

It's impossible to bypass rate limits unless you hack the server.

and why would you need to use more than one proxy?

wow how long have u been out of the game that you dont know why multiple proxies are needed

oh idk maybe because servers will blacklist ips that make too many attempts in a short span of time

/*i know technically using the wait system can keep it active for longer, but still, using a bunch of transparent proxies will help you make more requests before they all eventually get banned*/

v740612 - August 17, 2017, 8:54 pm

(Aug 17, 2017 08:45 PM)Faith Connors Wrote: [\[CITE\]](#) wow how long have u been out of the game that you dont know why multiple proxies are needed

oh idk maybe because servers will blacklist ips that make too many attempts in a short span of time

/*i know technically using the wait system can keep it active for longer, but still, using a bunch of transparent proxies will help you make more requests before they all eventually get banned*/

I wouldn't have asked if i wasn't a beginner :P

Like how many proxies for a large wordlist? Wouldn't i need to separate the word list into smaller lists, since hydra won't tell me when the server has blacklisted me or locked me out?

Faith Connors - August 17, 2017, 9:04 pm

(Aug 17, 2017 08:54 PM)v740612 Wrote: [\[CITE\]](#) I wouldn't have asked if i wasn't a beginner :P

Like how many proxies for a large wordlist? Wouldn't i need to separate the word list into smaller lists, since hydra won't tell me when the server has blacklisted me or locked me out?

nah u just dont use hydra and you wont have an issue

senry is ok if ur on windows, just run hydra or ur fave bruteforcer through proxychains if on linux

v740612 - August 17, 2017, 9:09 pm

(Aug 17, 2017 09:04 PM)Faith Connors Wrote: [\[CITE\]](#) nah u just dont use hydra and you wont have an issue

senry is ok if ur on windows, just run hydra or ur fave bruteforcer through proxychains if on linux

i'm a mac user, what about for us?

Vana - August 17, 2017, 9:22 pm

(Aug 17, 2017 09:09 PM)v740612 Wrote: [\[CITE\]](#) i'm a mac user, what about for us?

Hydra supports MacOS: <https://github.com/vanhauser-thc/thc-hydra>

Faith Connors - August 17, 2017, 9:24 pm

(Aug 17, 2017 09:09 PM)v740612 Wrote: [\[CITE\]](#) i'm a mac user, what about for us?

given (almost) anything for linux compiles for mac, you just need hydra, proxychains and the gcc (and make)

v740612 - August 17, 2017, 9:26 pm

(Aug 17, 2017 09:24 PM)Faith Connors Wrote: [\[CITE\]](#) given (almost) anything for linux compiles for mac, you just need hydra, proxychains and the gcc (and make)
thanks, your info is very helpful ?