

Forum:[Hack Forums](#)

Thread: [\[Idea\] using the POP protocol as a bruteforce attack vector?\[Idea\]](#)

?Criminal - October 5, 2014, 12:59 am

I was thinking of making a PoC of a gmail cracker that uses POP, normally SMTP is used to send mail and POP is used to retrieve mail, I was thinking keep cracking the auth untill you get a hit and when you get the right password it attempts to retrieve a random email from the victims gmail inbox any thoughts on this? if anyones wondering POP is the Post Office Protocol which is used to retrieve and download email from a server. Also since it's not using basic HTTP POST requests on the login form gmail most likely doesn't rate limit POP. I never really delved into the full specifications of it so just wondering.

ex:

pop.gmail.com

username

pass

port 995

Abdilo - October 5, 2014, 4:03 am

this is depressing.

really really depressing.

?Criminal - October 5, 2014, 3:10 pm

(Oct 5, 2014 04:03 AM)Grey Hat Mafias Bitch Wrote: [\[CITE\]](#) this is depressing.

really really depressing.

How is it depressing? another egotistical hotshot it seems. Im literally just curious about it at least you don't see me saying it's depressing over you trying to sell a csrf vuln for 3k then it getting released publically. If a SMTP based one is possible this should be as well. Do you normally try to harass everyone without yet again backing up your credibility? you could of at least told me why this wouldn't work out instead of being a douchebag and saying it's "depressing".

Abdilo - October 5, 2014, 3:38 pm

(Oct 5, 2014 03:10 PM)maybeBlue Wrote: [\[CITE\]](#) How is it depressing? another egotistical hotshot it seems. Im literally just curious about it at least you don't see me saying it's depressing over you trying to sell a csrf vuln for 3k then it getting released publically. If a SMTP based one is possible this should be as well. Do you normally try to harass everyone without yet again backing up your credibility? you could of at least told me why this wouldn't work out instead of being a douchebag and saying it's "depressing". I dont care a about credibility when i can fuck with people. pop3 btw not just pop.

And there are pop based brute forcers, goggle pop3 brute forcer.

and gmail would limit pop3, smtp, and thier webmail, shit thc-hydra can do this.

?Criminal - October 5, 2014, 3:41 pm

(Oct 5, 2014 03:38 PM)Grey Hat Mafias Bitch Wrote: [\[CITE\]](#) I dont care a about credibility when i can fuck with people. pop3 btw not just pop.

And there are pop based brute forcers, goggle pop3 brute forcer.

and gmail would limit pop3, smtp, and thier webmail, shit thc-hydra can do this. pop3 is just the third version of it same shit just more functionality and ah I figured no one thought of this before thanks for the reply though, but I doubt it's as limited as http look at ak47s gmail cracker im pretty sure his is SMTP based with proxy changing.

How bout using your brain - October 5, 2014, 3:43 pm

This method works fine as long as you don't bruteforce one account. I use it to check email/password combos.

But I have just run a quick test and you usually get disconnected after like 8-10 failed login attempts:

This is with IMAP, but same thign happened on POP protocol.

Although you can just directly reconnect and try again. I haven't been able to get myself IP blocked like this xD

However when you do find the right login, it will tell you to login through the webbrowser. But at that point you know you got the right logins at least, even though you can not dump the emails over POP then ?

Storm- - October 5, 2014, 3:43 pm

Been done before.

Not the best idea.

?Criminal - October 5, 2014, 3:51 pm

(Oct 5, 2014 03:43 PM)The Onion Router Wrote: [\[CITE\]](#) This method works fine as long as you don't bruteforce one account. I use it to check email/password combos.

But I have just run a quick test and you usually get disconnected after like 8-10 failed login attempts:

This is with IMAP, but same thign happened on POP protocol.

Although you can just directly reconnect and try again. I haven't been able to get myself IP blocked like this xD

However when you do find the right login, it will tell you to login through the webbrowser. But at that point you know you got the right logins at least, even though you can not dump the emails over POP then ?So do you personally think this is a more viable method then HTTP POST requests on the login form since I know for a fact after 5 trys gmail uses a global lockout system? I can just set up a loop to keep reconnecting after 8 trys and have it change IP's everytime.

How bout using your brain - October 6, 2014, 1:20 am

Yeah I don't know about HTTP requests as I have not tried. But from what I saw it will at least give you a captcha after trying a few times. On POP/IMAP you will get that captcha as well, but only if you actually put the right login details:

Spoiler [\(Click to View\)](#)

However, this captcha might also be asked because I was using Tor. But it still only gets asked when login is correct.

So when you do get that message, you know you got the right login.

You should do some more testing to actually find out. But yeah I believe it is easier than sending HTTP requests.

?Criminal - *October 6, 2014, 2:49 pm*

Alright ill play around with it some more and see what happens.

Decompress - *October 6, 2014, 7:12 pm*

This isn't a bad idea but I'm pretty sure Gmail would rate limit as people above have said.

Not many secure email providers would be stupid enough to let something like this go unnoticed.