

Forum:[Hack Forums](#)

Thread: [WAYS TO GET A PASSWORD](#)

coocochi - July 30, 2017, 3:17 pm

I will like to know, asides, phishing and RATting, what other ways are available to get someones password remotely?. Thats is with the email available.

THC - July 31, 2017, 12:58 am

Try searching through leaked databases to find a password hash matching the email. Sites such as leakbase offer such services.

Boolean type - July 31, 2017, 4:58 am

Social engineering. If your target is dumb enough you can get what you want very easily ;)

Bouzazi - July 31, 2017, 6:03 am

Social engineering. That's how I'd do it if I had his email. Be sure your mail doesn't go to SPAM Box.

People often represent the weakest link in the security chain.. -- Bruce Schneier.

coocochi - August 1, 2017, 7:45 am

(Jul 31, 2017 12:58 AM)M.D. Wrote: [\[CITE\]](#) Try searching through leaked databases to find a password hash matching the email. Sites such as leakbase offer such services. Thanks, but i have searched and that didn't quite work.

(Jul 31, 2017 04:58 AM)stdbool.h_____ Wrote: [\[CITE\]](#) Social engineering. If your target is dumb enough you can get what you want very easily ;) I think this also involves phishing of some sort, innit?

GhostKarate - August 1, 2017, 8:42 am

You could look into stealing password hashes from a target and then crack them offline. Like the windows SAM file or Linux Shadow file. Or you could steal some cookies and use them to access web accounts.

Zork - August 1, 2017, 11:25 am

Another cool idea would be to SSL-Strip traffic and try to get some cleartext passwords. Although this might not always work as SSL is forced nowadays on most sites.

coocochi - August 2, 2017, 3:31 am

(Aug 1, 2017 08:42 AM)GhostKarate Wrote: [\[CITE\]](#) You could look into stealing password hashes from a target and then crack them offline. Like the windows SAM file or Linux Shadow file. Or you could steal some cookies and use them to access web accounts. This sound really interesting, but stealing the cookies, i guess the only way to do that is by RAT or Logger. Please correct me if i am wrong

(Aug 1, 2017 11:25 AM)Zork Wrote: [\[CITE\]](#) Another cool idea would be to SSL-Strip traffic and try to get some cleartext passwords. Although this might not always work as SSL is forced nowadays on most sites. I am not sure, I know anything about this.

GhostKarate - August 2, 2017, 11:21 am

Quote: This sounds really interesting, but stealing the cookies, I guess the only way to do that is by RAT or Logger. Please correct me if I am wrong

Start looking into msfconsole, SEtoolkit and reverse_tcp meterpreter sessions. Like a Rat it creates a back door into someone's system. They normally have the functionality built in to just dump say all of the windows/linux password files onto your computer. Or all of the cookie files.

I can't post links but youtube Lesson 48 : Backdoor Gaining Access

It's the first part of 5 videos on the subject so make sure you watch them all. They are only a few minutes long each.

Marsuves - August 2, 2017, 4:28 pm

(Aug 2, 2017 11:21 AM) GhostKarate Wrote: [\[CITE\]](#) Start looking into msfconsole, SEtoolkit and reverse_tcp meterpreter sessions. Like a Rat it creates a back door into someone's system. They normally have the functionality built in to just dump say all of the windows/linux password files onto your computer. Or all of the cookie files.

I can't post links but youtube Lesson 48 : Backdoor Gaining Access

It's the first part of 5 videos on the subject so make sure you watch them all. They are only a few minutes long each.

This is the best advice I have seen so far on the topic; there are many ways to do what you are trying to do but using these tools is much better than just running a RAT/logger.

A fun way to do this would be to get the target's physical address, mail them a malduino with a script to download and run a metasploit script

DaRealDeal - August 3, 2017, 6:51 am

(Aug 2, 2017 11:21 AM) GhostKarate Wrote: [\[CITE\]](#) Start looking into msfconsole, SEtoolkit and reverse_tcp meterpreter sessions. Like a Rat it creates a back door into someone's system. They normally have the functionality built in to just dump say all of the windows/linux password files onto your computer. Or all of the cookie files.

I can't post links but youtube Lesson 48 : Backdoor Gaining Access

It's the first part of 5 videos on the subject so make sure you watch them all. They are only a few minutes long each.

This is some great info. I appreciate it!

coocochoi - August 4, 2017, 7:19 am

(Aug 2, 2017 11:21 AM) GhostKarate Wrote: [\[CITE\]](#) Start looking into msfconsole, SEtoolkit and reverse_tcp meterpreter sessions. Like a Rat it creates a back door into someone's system. They normally have the functionality built in to just dump say all of the windows/linux password files onto your computer. Or all of the cookie files.

I can't post links but youtube Lesson 48 : Backdoor Gaining Access

It's the first part of 5 videos on the subject so make sure you watch them all. They are only a few minutes long each. Wow, really appreciate the info, and I got the videos. They are really something. Thanks once again.

Prom?nent - August 4, 2017, 9:57 am

Social engineering or dictionary attack?

coocochoi - August 7, 2017, 6:42 am

(Aug 4, 2017 09:57 AM)Prom?nent Wrote: [\[CITE\]](#) Social engineering or dictionary attack?I dont think Dictionary attack still works, with captcha and all this verifications when several attempts has been made on an account.

Delphinus - August 7, 2017, 7:12 am

Minor nitpick, but Meterpreter is a RAT, just a text-based one.

It's also one of the best. Learn it. Password dumps are pretty much the first thing you learn with it.