

Forum:[Hack Forums](#)

Thread: [HACK FACEBOOK ACCOUNTS USING \(COOKIE STEALING\)](#)

Byt3Door - January 2, 2016, 7:10 am

WARNING:- This is only for EDUCATIONAL purposes to make you aware of how your FACEBOOK account may get HACKED so that you may PREVENT it from getting hacked,,,,!!! The person posting this or the this blog is not responsible for any type malicious activities performed by anyone who is reading this,,,,!!!

? Hey there,,,,!!! Many of them have been reuesting me to post about FACEBOOK HACKING,,,,!!! Well here it is for you,,,,!!!

? Authentication Cookies used by Facebook :

? The cookie which facebook uses to authenticate it's users is called "Datr", If an attacker can get hold of your authentication cookies, All he needs to do is to inject those cookies in his browser and he will gain access to your account. This is how a facebook authentication cookie looks like:

```
datr=1276721606- b7f94f977295759399293c5b0767618dc02111 ede159a827030fc;
```

? An attacker may use variety of methods in order to steal your facebook authentication cookies depending upon the network he is on, If an attacker is on a hub based network he would just sniff traffic with any ****Packet Sniffer**** and gain access to victims account.

? If an attacker is on a Switch based network he would use an ****ARP Poisoning**** request to capture authentication cookies, If an attacker is on a wireless network he uses a tool called ****FIRESHEEP**** in order to capture authentication cookie and gain access to victims account.

? Here in the example below I will be explaining in simple STEPS how an attacker can capture your authentication cookies and hack into your Facebook account with ****Wireshark****.

? Step 1 - First of all download wireshark from the official website and install it.

? Step 2 - Next open up wireshark click on analyze and then click on interfaces.

? Step 3 - Next choose the appropriate interface and click on start.

? Step 4 - Continue sniffing for around 10 minutes.

? Step 5 - After 10minutes stop the packet sniffing by going to the capture menu and clicking on Stop.

? Step 6 - Next set the filter to http.cookie contains "datr" at top left, This filter will search for all the http cookies with the name datr, And datr as we know is the name of the facebook authentication cookie.

? Step 7 - Next right click on it and goto Copy - Bytes - Printable Text only.

? Step 8 - Next you'll want to open up firefox. You'll need both Greasemonkey and the

cookieinjector script. Now open up Facebook.com and make sure that you are not logged in.

? Step 9- Press Alt C to bring up the cookie injector, Simply paste in the cookie value into it.

? Step 10 - Now refresh your page and *****BINGO***** You are logged in to the victims facebook account.*****

? Now comes the important part,,,,,!!!

[b]HOW TO PROTECT YOUR ACCOUNT ??[/b]

? Well, the best way to protect yourself against a session hijacking attack is to use " h.t.t.p.s:// " connection each and every time you login to any of your accounts in Facebook, Gmail, Yahoo or any other email account. As your cookies would be encrypted so even if an attacker manages to capture your session cookies he won't be able to do any thing with your cookies. Also avoid using unwanted apps that you use in FACEBOOK. Keep changing your password frequently. Use tough passwords which are hard to guess with a combination of uppercase and lowercase characters with symbols in between to make the password very strong.

. TRY FRM YOURSELF N CMNT YOUR PRBLM HERE ?

Byt3Door

tyrone913 - January 2, 2016, 7:12 am

Posting so i can try it out later

Humour - January 2, 2016, 7:14 am

How would this work if I wanted to hack a pacific acc and their not in my region.

zeaun - January 2, 2016, 7:17 am

i will check this out and let you know

Michael - January 2, 2016, 7:18 am

Atleast give credits tho.

<http://www.rafayhackingarticles.net/2011/07/facebook-cookie-stealing-and-session.html>

How2Hacks - January 2, 2016, 12:38 pm

This truly one of the best copy and pasted from another blog posts I have ever seen.

10/10 OP, you the real mvp.

@Humour , it wouldn't work you would need to be on the same network as them.
Maybe brute force there password.