

HACK FACEBOOK BY COOKIE STEALING

Facebook Authentication Cookies
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:
Cookie: datr=1276721606-b7f94f977295759399293c5b0767618dc02111ede159a827030fc;
How To Steal Facebook Session Cookies And Hijack An Account?
An attacker can 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 just needs to use a simple tool called firesheep in order to capture authentication cookie and gain access to victims account.
In the example below I will be explaining how an attacker can capture your authentication cookies and hack 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 right click on it and goto Copy - Bytes - Printable Text only.
Step 9 - 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 viola you are logged in to the victims facebook account.
Note: This Attack will only work if victim is on a http:// connection and even on https:// if end to end encryption is not enabled.

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

