

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Hack Facebook & Youtube via Session Hijacking \[Tutorial\]](#)

Carl Elias - November 25, 2012, 2:20 pm

Well hello, this is my first tutorial so give me some slack.

There are probably a few of these methods on this site. It may not be hackers favorite because the victim must be on FB and the hacker must be in the same network. This may work on other site, you just have to test it out. I have tested FB and Youtube, and BOTH work with this method!!

Now first you need a few pieces of software:

[Cain And Abel](#)

[WireShark](#)

Cookie Manager:

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

[Chrome Edit This Cookie](#)

[Firefox Cookie Manager](#)

Now you have all the required software, we can start hijacking.

--

Step 1:

Open up Cain and Abel and click on Sniffer, then activate the sniffer by clicking the button the arrow points to.

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

[IMG]<http://imageshack.us/a/img819/7475/41061672.jpg>[/IMG]

Then you have to add the host to your list. To do this click the cross in the top of the program and hit ok. After this you should get All the IP's in the network. If you wish you can right click them and select "Resolve HostName" to get the computers name so it is easier to tell which computer is which. It does not always work but can be helpful in targeted attacks.

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

[IMG]<http://imageshack.us/a/img694/7142/42484793.jpg>[/IMG]

--

Step 2:

Now that we have the IP's you can start APR Poisoning. To do this in the bottom of the sniffer page select "APR" with the radiation symbol. Click in the top box then hit the same cross you hit earlier. This time a new window opens up. Now in the first box in the left select the Routers IP or default Gateway. In the second box on the Right select the computer that you wanted to get the Facebook from.

[IMG]<http://imageshack.us/a/img231/9303/23399294.jpg>[/IMG]

Then click the Radiation symbol at the top right next to the same button you clicked to activate the sniffer. This will activate the poisoning, you should now see it saying "Poisoning" next to the IP.

--

Step 3:

Now on to taking the cookies. This is where the WireShark starts so open WireShark. Now up in the tool bar in the top of the window click the first Icon to select the correct interface. This will list multiple interfaces on the computer, select the IP that is your IP and usually the one with higher packets in and out and click "Start".

[IMG]<http://imageshack.us/a/img841/8413/37518345.jpg>[/IMG]

Now it will start monitoring all packets going through your computer. This is good, but try not to use your computer during this or you may end up using your own computers session instead of the victims. Now there is not really any time set that you need to do this. You just need to wait for them to refresh the website. Once you think they have refreshed the page continue to Step 4!

--

Step 4:

Now that you have the packets, you can stop both the APR Poisoning and the WireShark (DO NOT CLOSE WIRESHARK). In WireShark you now can filter out the cookies to make it easier to find what we need. To do this in the textbox near the top of the page on the left type in "http.cookie" and hit apply or enter.

[IMG]<http://imageshack.us/a/img811/6246/97828660.jpg>[/IMG]

Here is the tricky part. Now you need to find the packet with the login cookie. This for me was the last one because I stopped it as soon as the page reloaded. To get to the cookie what you need to do is select the packet and in the window at the bottom click the plus sign by the "HyperText Transfer Protocol" and look in that section for the word "Cookie: " (Usually it has the word "[truncated]" at the beginning). Now right click this line and select "Copy" then "Value" and paste it into Notepad. This is because everything is in one line and confusing. To make it easier what you do is every time there is a "; " hit enter. The "; " means the end of that section of the cookie.

Now you will have something like this

Quote:user=25425420;

pass=14254520;

id=205001; Now the first part before the "=" is the name. The second part after the "=" is the content. And if you want to you can remove the "; " because this will need to be removed anyway. This is important to know for later on!!

Each site uses a different cookie layout. I have a small table below.

Youtube:

Spoiler ([Click to View](#))

wide_exp=

VISITOR_INFO1_LIVE=

use_hitbox=

__utma=

__utmb=

__utmc=

__utmz=

SID=

HSID=

APISID=

LOGIN_INFO=
PREF=

Facebook:

Spoiler ([Click to View](#))

(Feb 15, 2015 12:45 PM)Krew Wrote: [\[CITE\]](#) Facebook cookie example btw;

lsd=
display=
enable_profile_selector=
legacy_return=
profile_selector_ids=
trynum=
timezone=-
lgnrnd=
lgnjs=
email=
pass=
default_persistent=
qsstamp=

After all of it is formatted for easy use continue.

--

Step 5:

Now depending on what browser you have it may differ a little. I will go through both browsers I have.

FireFox:

Spoiler ([Click to View](#))

Here is where you use the addon you were supposed to install earlier. Now open up "Cookie Manager+". Now add each line from the text document from earlier. For the End use "End at Session" instead of "Date".

If the name already exist change what is in it into what was in the text document.

Chrome:

Spoiler ([Click to View](#))

To Come

--

Step 6:

Now just refresh the page and if it worked you should now be logged into the users account. Now you can do anything you want, Change email/pass and take over the account, or what ever you want. This can be a pretty good way to spread your virus and links, by doing this to multiple account it can give you a lot of people that will see your links thinking it is the real owner of the account.

--

OK Well there you go. I hope you liked this and it helped you out. This is really good, but only down

side is no password is given, just the account and that you need to be in their network. What I have done is just WEP crack all the WiFi's in my area and do this attack.

If i missed something tell me so I can fix it. Also if you liked it please post a Thanks!! I will be getting new better pics, these were just made quickly.

I found this video using this same method, It was not my video.

[Video: <http://www.youtube.com/watch?v=gWNF0NHIs-Q>]

-Ty

BladeZ201 - November 26, 2012, 7:06 am

Nice one! I am going to try this after someone connected to my free wifi!

Carl Elias - November 26, 2012, 3:11 pm

Well I mean you can go to school, have anyone pay say 1-5 dollars for a wifi hotspot for so many hours (1 class period = 2\$) and find a way to do this from your phone, and you are set to get as many facebook's as they log in :D

Thats a good idea BladeZ201

j4rkill - November 26, 2012, 3:37 pm

is a Tutorial for LOCAL Accounts (from PC) not from another User :D

Carl Elias - November 26, 2012, 4:15 pm

(Nov 26, 2012 04:37 PM)j4rkill Wrote: [\[CITE\]](#) is a Tutorial for LOCAL Accounts (from PC) not from another User :D

This is a Tutorial for NETWORK LOCAL PC's, This works with any computer on the same network (WiFi). This was said in the tutorial.

mikesbeast123 - November 26, 2012, 5:55 pm

Thanks for spending your time to make this tutorial!!

MikoulFR - November 27, 2012, 10:30 am

Thanks you for tutoriel ;) good job

Carl Elias - November 28, 2012, 3:31 pm

Thanks everyone, This should work with most if not all websites that store logins with cookies!!!

Once you are in, just change the email, and passwords and you should be good with that account!

-Ty

Zacchariah - November 29, 2012, 12:55 am

thanks! Great tutorial,. I appreciate it:)

hackergeorge - November 29, 2012, 1:28 am

nice tutorial buddy...really liked it...:)

Ps3k0dz - December 1, 2012, 7:27 am

Nice tuto buddy

I am going to try this after someone connected to my free wifi

alexlandonflicksss - December 1, 2012, 9:27 am

nice tutorial...you're awesome...:-)

torturer33 - December 1, 2012, 12:54 pm

its working bro thank u sooo muchhh

Carl Elias - December 3, 2012, 11:56 am

I will add the Facebook and other layouts of the cookies and do one for chrome later this week!!

Thanks everyone

-Ty

REALTOR - December 3, 2012, 12:30 pm

Not OP, but here's a note in case you use a different browser: Opera has it's own cookie manager.

Press CTRL + SHIFT + I and you'll start Opera Firefly. Opera Firefly is pretty handy for cookie editing, and to access cookies, go to the "Storage" tab in the tool bar that pops up. From there you can modify cookies without having to install plugins/extensions! :)

preetam.kondekar - December 3, 2012, 8:38 pm

Thanks for sharing this to HF buddy, I have one question, is it only for who is getting connected to free wi fi ?? I am using my internet connection from my home..is it possible to get userid/pass details for other facebook account???

Carl Elias - December 13, 2012, 12:12 pm

(Dec 3, 2012 09:38 PM)preetam.kondekar Wrote: [\[CITE\]](#) Thanks for sharing this to HF buddy, I have one question, is it only for who is getting connected to free wi fi ?? I am using my internet connection from my home..is it possible to get userid/pass details for other facebook account???

Sorry for the delay, school stuff. This works with any network, as long as YOU and the victims facebook is open on the SAME WiFi/LAN, it should work. it will not work on remote IP's.

ink- - December 16, 2012, 8:36 pm

Thanks! Great tutorial, I appreciate it.

Carl Elias - December 17, 2012, 8:25 am

(Dec 16, 2012 09:36 PM)ink- Wrote: [\[CITE\]](#) Thanks! Great tutorial, I appreciate it.

No problem. If you liked this look at my methods of making money, and bitcoins.

KingJulien - December 17, 2012, 8:39 am

Great tutorial man ! good work bro <3 !

AnonymousPerson101 - December 17, 2012, 2:22 pm

Thanks it was really helpful, please keep making tutorials i like them they are very interesting

Carl Elias - December 19, 2012, 12:39 pm

Thanks everyone. I also have post on how to get bitcoins and money if you are interested. I am working on another, but am unsure of when I will be able to finish.

ramoncito24 - December 19, 2012, 8:03 pm

bookmarked this. will try later. thank you so much

d0oo0dle - December 20, 2012, 3:25 am

This seems a good tutorial , im gonna try . Thanks

Carl Elias - December 22, 2012, 5:48 pm

Thanks everyone. Have a nice holiday, and be sure to check other threads of mine.

Molonlabe - December 22, 2012, 7:08 pm

Thanks for uploading this video... Very interesting!

Lartsch - December 22, 2012, 7:32 pm

It's a very good tut but a bit useless...

methsmoker323 - December 23, 2012, 1:05 am

Thanks bro It is very Cool! Thanks!

december24 - December 24, 2012, 8:55 am

thanks good tutorial) will use it soon

BottomNotch - December 26, 2012, 10:32 pm

:Random Orgasm: Omg dude... I can't wait to try this

Carl Elias - December 28, 2012, 10:33 am

(Dec 22, 2012 08:32 PM)Lartsch Wrote: [\[CITE\]](#) It's a very good tut but a bit useless...

Yes you are kind of right, it is. This was meant for beginners who only feel like accessing neighbors and family members facebook. But if you can drive then you can do this at friends houses if you can get there and hide close enough to the house to get a connection.

bastianwolf - December 29, 2012, 12:35 am

Can you add the facebook and chrome instructions? Thanks :)

soacool - December 29, 2012, 4:39 am

thanks! Great tutorial,
i will try it next time ...:)

Carl Elias - December 29, 2012, 1:32 pm

(Dec 29, 2012 01:35 AM)bastianwolf Wrote: [\[CITE\]](#) Can you add the facebook and chrome instructions? Thanks :)

Yeah, The chrome is very similar to the Firefox, just uses a different program, when I have time I will add that, Just been busy on another project. If you need it now search "Facebook Session Hijacking Chrome" that should get you somewhere (The app is in the thread you will need that still)

-Ty

Kids Wish - December 28, 2013, 12:06 pm

Thanks for the tutorial m8 :) Definitely going to try this out.

hehiho - December 28, 2013, 1:40 pm

Nice tutorial but this work only work for home connection?

Carl Elias - December 28, 2013, 4:27 pm

Wow I forgot I even posted about this. Yes you must be in the same network as the person you want to hijack. As far as I know there is no way to do it remotely without some other program. Sorry.

-Ty

afexmillion - February 8, 2015, 7:31 am

A very detail tutorial and I hope to try it soon. Thank you

Carl Elias - February 8, 2015, 3:42 pm

Nice gravedig. Unfortunately, I have a feeling this method has be patched but who knows.

-Ty

zav1995 - February 15, 2015, 9:23 am

I suppose this works only for http or https as well? Thanks

tsaad - February 15, 2015, 11:43 am

Thanks for the excellent tutorial

Regards

Krew - February 15, 2015, 11:45 am

Facebook cookie example btw;

lsd=
display=
enable_profile_selector=
legacy_return=
profile_selector_ids=
trynum=
timezone=-
lgnrnd=
lgnjs=
email=
pass=
default_persistent=
qsstamp=

Shiroe - February 15, 2015, 11:58 am

Dam son going to be takig my laptop to open networks and gettin accounts thanks op

KoolTubeHD - February 21, 2015, 10:44 pm

great tutorial man! Looking forward to trying it

dadada12 - February 22, 2015, 4:56 am

Thanks man, now i know what to do, Great tutorial :)

Carl Elias - February 22, 2015, 8:47 pm

I am not sure if this still is possible, but I assume it is because of the replies. I updated the OP with the data you posted as well Krew, Thanks. I would be so surprised if this was still an issue

-Ty

Nalgun - March 2, 2015, 9:18 am

Nice tutorial, really enjoyed it, appreciate your job, thanks

Carl Elias - March 6, 2015, 5:49 pm

(Mar 2, 2015 10:18 AM)Nalgun Wrote: [\[CITE\]](#) Nice tutorial, really enjoyed it, appreciate your job, thanks

Thanks! I believe this is the first and probably only tutorial that I have ever posted on HF, so that means a lot

-Ty

fozzygang - March 6, 2015, 8:19 pm

intresting i like what isee and red

tko - March 7, 2015, 5:51 am

too bad not working anymore because https

ubermensch511 - March 15, 2015, 9:27 am

You really try man, thanks for the tutorial

Carl Elias - March 17, 2015, 11:36 am

(Mar 15, 2015 09:27 AM)ubermensch511 Wrote: [\[CITE\]](#) You really try man, thanks for the tutorial
No problem! I will try to create more some time soon.

-Ty

itoxiik - July 30, 2015, 1:22 pm

cool tutorial.. Ill give this a shot. I appreciate it!

x3meQ - July 31, 2015, 7:24 pm

you can also use droidsheep on android... but facebook/gmail and many others does not work because of https

thezohanxxx - July 31, 2015, 8:16 pm

noice lol I love to learn stuff I don't use but I love to learn :D

FearFactory - January 9, 2017, 11:14 am

Good job mate :) Appreciate the tutorial :)

amirkhan0 - January 10, 2017, 5:14 am

youtube link is not working

Mrcad1 - January 12, 2017, 4:36 pm

Thanks for Tutorial, but I've the cookie but I don't know how to use it ?
Can you help me please ?

camarazon100 - February 8, 2017, 10:28 am

thanks! Great tutorial,. I appreciate it:)..

weirdo1987 - February 17, 2017, 4:16 am

is this still working? Its what i am looking for! Will try it anyway! THANK YOU!

Wilkassek - February 17, 2017, 4:43 am

Thank you really much, very very good tutorial, I like it!