

Forum:[Hack Forums](#)

Thread: [How do find usernames and passwords in Wireshark!](#)

Erwin Schrödinger - May 7, 2013, 9:43 pm

Hello!

Today I'm gonna tell you how to find Usernames and Passwords with Wireshark. This method works aslong as the other person you will hack is on the same network as you are.

Step 1. In Wireshark select your internet card, and press start.

Step 2. When you are here you must apply http to the filters.

Step 3. After you have applied that filter you can now stop searching for packets.
This is the buttton:

Step 4. When you know when the person is logging it to whatever it is. Maby a http based browser game, you start searching for packets agian.
This is the button to restart the searching:

Step 5. When the person is logged in you will see some new packets come up. (Remember to use the http filter.) If you look at the info tab you are looking for the one that starts with "post".

Step 6. Right click on that and press "Follow TCP stream".

Step 7. In here you will se red text and blue text. The red text is your request, and the blue text is the servers "awnser". If you look your first request at it's last line you will see the username and password.

Thank you for reading it all! Did you like it? Did it help you? Tell me bellow!

Here is a video on how to do it. [Video: <http://www.youtube.com/watch?v=jcN7CnIN23w>]

on-silo - May 7, 2013, 10:35 pm

was short sweet and to the point, well done for those who dont wanna really dive into wireshark for whatever reason.

efinitix - May 8, 2013, 12:53 am

cheers for the tutorial needed to use wireshark to test some "things" :P

Endonium - May 8, 2013, 1:29 am

Wireshark can also be used to recover the passwords from loggers, stealers, even some bots/rats.

When you execute the virus (do it is sandboxie dont be an idiot, or even better on a VM) it will attempt to connect to whatever email/server it sends info it collects to.

You can find that string of data and get login/pass.

Doesn't work for everything, quite. Few encrypt the data packets.

Erwin Schrödinger - May 8, 2013, 5:53 am

I'm glad everyone liked it! :D

(May 8, 2013 01:29 AM)Endonium Wrote: [\[CITE\]](#) Wireshark can also be used to recover the passwords from loggers, stealers, even some bots/rats.

When you execute the virus (do it is sandboxie dont be an idiot, or even better on a VM) it will attempt to connect to whatever email/server it sends info it collects to.

You can find that string of data and get login/pass.

Doesn't work for everything, quite. Few encrypt the data packets.

Cool, I didn't know that! Maby it will help me one day? =)

Creatiivitiy. - May 8, 2013, 6:16 am

Good Tut and very well explained. Thanks

Altijd Bezig - October 10, 2013, 2:46 pm

Real sweet.

I'm sure that this is helpful to me.

I just went ahead and tested this on my own account.

Could not find any usernames or passwords.

Hope one of you can help me out.

Erwin Schrödinger - October 11, 2013, 12:28 am

(Oct 10, 2013 02:46 PM)Altijd Bezig Wrote: [\[CITE\]](#) Real sweet.

I'm sure that this is helpful to me.

I just went ahead and tested this on my own account.

Could not find any usernames or passwords.

Hope one of you can help me out. When you're trying to take passwords from Wireshark it need to be on HTTP severs not HTTPS servers. A https means that it's crypted.

You could try it on the browser game "Tribal wars". They're servers are not crypted.

(You don't need a real username and pass to make it work. As long at you get the "Wrong login" it's enough.)

Altijd Bezig - October 11, 2013, 12:32 am

I tried it on the game Tribal Wars and Grepolis.

Both with actual accounts.

I was using mobile to login on the Web version.

I don't think that's the problem because I was using the normal Web version and not the mobile version.

Erwin Schrödinger - October 11, 2013, 12:38 am

(Oct 11, 2013 12:32 AM)Altijd Bezig Wrote: [\[CITE\]](#) I tried it on the game Tribal Wars and Grepolis.

Both with actual accounts.
Hmm, I can probably help you later today!

Altijd Bezig - October 11, 2013, 12:58 am
Ok.
Thanks.

With a bit off luck I'm online around 21:00 local time.
Thats is 11 hours from now.

Cyprella - October 11, 2013, 5:57 am
Great tutorial, small spelling mistake on answer.

ORK24 - October 11, 2013, 6:28 am
Thanks mate, will be quite useful (:

Erwin Schrödinger - October 11, 2013, 8:18 am
Thanks for the great feedback! :)
(Oct 11, 2013 05:57 AM)MLGL33TPRO Wrote: [\[CITE\]](#) Great tutorial, small spelling mistake on answer.Yeah, I see. I'm not a native English speaker.

Smexy - October 11, 2013, 8:31 am
So does anyone know this works trough hamachi because then i can steal ALOT.
Please someone anwser quick.

Erwin Schrödinger - October 11, 2013, 8:32 am
(Oct 11, 2013 08:31 AM)Smexy. Wrote: [\[CITE\]](#) So does anyone know this works trough hamachi because then i can steal ALOT.
Please someone anwser quick.
I don't know.
You should try it! :)
(It was a really good idea.)

Smexy - October 11, 2013, 8:35 am
(Oct 11, 2013 08:32 AM)Racego Wrote: [\[CITE\]](#) I don't know.
You should try it! :)
(It was a really good idea.)
How can i try something like this? i mean like omg.

Altijd Bezig - October 11, 2013, 9:27 am
(Oct 11, 2013 08:18 AM)Racego Wrote: [\[CITE\]](#) Yeah, I see. I'm not a native English speaker.
Just being curious what is your native language?
And do you have Skype?
(Oct 11, 2013 08:18 AM)Racego Wrote: [\[CITE\]](#) Yeah, I see. I'm not a native English speaker.
Just being curious what is your native language?
And do you have Skype?

HbananF - October 11, 2013, 9:43 am
There's no "POST" packets for me, plus, I can't find the stop/resume button.

Erwin Schrödinger - October 11, 2013, 10:08 am
(Oct 11, 2013 09:27 AM)Altijd Bezig Wrote: [\[CITE\]](#) Just being curious what is your native language?
And do you have Skype?

Just being curious what is your native language?

And do you have Skype? My native language is Norewgian.

And I prefer don't to give my Skype out to random members.

(Oct 11, 2013 09:43 AM)HbananF Wrote: [\[CITE\]](#) There's no "POST" packets for me, plus, I can't find the stop/resume button.

Do you have the newest version of WireShark?

HbananF - October 11, 2013, 10:22 am

I guess, I have 1.10.2. Do you have Skype?

Altijd Bezig - October 11, 2013, 11:40 am

(Oct 11, 2013 10:08 AM)Racego Wrote: [\[CITE\]](#) My native language is Norewgian.

And I prefer don't to give my Skype out to random members.

Do you have the newest version of WireShark?

Ok.

I can understand why you don't wanna give your Skype to random members.

I'm using Wireshark Version 1.10.2

Noxite - October 11, 2013, 12:08 pm

Nice tutorial. Though, if the username and password was used within a https connection, shouldn't it then be encrypted?

?Jax - October 11, 2013, 12:24 pm

(Oct 11, 2013 11:40 AM)Altijd Bezig Wrote: [\[CITE\]](#) Ok.

I can understand why you don't wanna give your Skype to random members.

I'm using Wireshark Version 1.10.2

Do you think he want to get skype resolved, stupid noob

Minimal - October 11, 2013, 12:28 pm

So you're saying this works, without ARP poisoning?

Why would the victims computer be sending packets designated to the router to your computer?

Altijd Bezig - October 11, 2013, 12:30 pm

(Oct 11, 2013 12:24 PM)Demoniz Wrote: [\[CITE\]](#) Do you think he want to get skype resolved, stupid noob

I like to think that the most people here now how to spoof there ip.

And there is no need to state the obvious.

The fact that i'm asking for help is proof enough.

So yes i'm a noob and you no what i'm proud of it.

Can you say the same???

?Jax - October 11, 2013, 12:35 pm

(Oct 11, 2013 12:30 PM)Altijd Bezig Wrote: [\[CITE\]](#) I like to think that the most people here now how to spoof there ip.

And there is no need to state the obvious.

The fact that i'm asking for help is proof enough.

So yes i'm a noob and you no what i'm proud of it.

Can you say the same???

Sorry man, I'm a noob to hacking, but advanced to codeing ;)

Erwin Schrödinger - October 11, 2013, 1:12 pm

Please, stop fighting.

If you want to discuss Wire Shark or things around it feel free to.

Fighting fire with fire won't work.

Werto - October 11, 2013, 4:59 pm

Uhm, I cant find no "Post" packets, I've got the newest version of Wireshark.

Can you help me? :l

Altijd Bezig - October 11, 2013, 11:21 pm

I've got the post packets but no UN or PW

Are you online tonight?

Erwin Schrödinger - October 11, 2013, 11:51 pm

Here!

I made a video demonstrating how to do it! :)

<http://www.youtube.com/watch?v=jcN7CnIN23w>

Werto - October 12, 2013, 8:38 am

(Oct 11, 2013 11:51 PM)Racego Wrote: [\[CITE\]](#) Here!

I made a video demonstrating how to do it! :)

<http://www.youtube.com/watch?v=jcN7CnIN23w>

Thats exactly what im doing. Im still not getting any "GET" packets. D:

He B TeMy - October 12, 2013, 10:13 am

(Oct 12, 2013 08:38 AM)Werto Wrote: [\[CITE\]](#) Thats exactly what im doing. Im still not getting any "GET" packets. D:

Perhaps because this isn't 2000's year anymore?

One question, are you trying with specific websites? If yes, which ones?

Erwin Schrödinger - October 12, 2013, 10:16 am

(Oct 12, 2013 08:38 AM)Werto Wrote: [\[CITE\]](#) Thats exactly what im doing. Im still not getting any "GET" packets. D:

Please try to do it on the same website I'm suding. (Tribalwars.net).

He B TeMy - October 12, 2013, 10:44 am

(Oct 12, 2013 10:16 AM)Racego Wrote: [\[CITE\]](#) Please try to do it on the same website I'm suding. (Tribalwars.net).

It must be plain http... or somewhat decrypted as that website uses jquery or javascript.

Altijd Bezig - October 12, 2013, 11:34 am

I'll try .net tonight.

Perhaps there's a difference between the .net en .nl version.

Erwin Schrödinger - October 12, 2013, 12:17 pm

(Oct 12, 2013 11:34 AM)Altijd Bezig Wrote: [\[CITE\]](#) I'll try .net tonight.

Perhaps there's a difference between the .net en .nl version.

I really doubt that, but you could try.

Altijd Bezig - October 12, 2013, 1:43 pm

It works from my own computer.
now waiting for some one on our wifi to log in :)

Erwin Schrödinger - October 12, 2013, 1:48 pm

(Oct 12, 2013 01:43 PM)Altijd Bezig Wrote: [\[CITE\]](#) It works from my own computer.
now waiting for some one on our wifi to log in :)
Remember that you need to be in "recive" mode if you have a laptop.
If you have a desktop you have to buy something like [this](#).

Altijd Bezig - October 12, 2013, 1:51 pm

I'm using a laptop.

Maybe a dumb question but how do I put it in receive mode?

jimcar - October 12, 2013, 1:51 pm

I going to try this out to see if it work.

Erwin Schrödinger - October 12, 2013, 1:53 pm

(Oct 12, 2013 01:51 PM)Altijd Bezig Wrote: [\[CITE\]](#) I'm using a laptop.

Maybe a dumb question but how do I put it in receive mode?
I think it's automaticly set to this. Because you need to recive data wirelesly, and not though cable.

Altijd Bezig - October 12, 2013, 1:57 pm

Oke.
i'll give it a try in a few minutes.
Lets hope that the misses logs in then ;)

She did log in on [Grepolis](#)
when i tried to get her UN en PW using wireshark i got this:

[img]http://i39.[censored].com/70eruh.gif[/img]

I hope one of you guys/girls can help me solve this.

Exposweg - October 12, 2013, 5:56 pm

pretty dope tut bro thnx for helpin me out!?

mafiaanonymous - October 13, 2013, 5:51 am

Wow Work username and password is working ;) I no know plasse send skype : mafiaanonymous :)
add me Thank you bro ;)