

Forum:[Hack Forums](#)

Thread: [Biggest Beginners Guide To Become A Successful Hacker {whitehat}](#)

|||||| - May 5, 2016, 7:02 am

So after I Looked trough HF, I didn't see any fast and good way to learn to hack. So I cooked together a little sample for you.

MORE INFO

But before we start, read trough this softwares and ebooks to get started.

[How The Hack Is Made](#) - RECCOMENDED

Best ebook for beginners. It helps you getting started with every hacking method out there today.

Sololearn

These apps will learn you the basics in JavaScript and SQL. They are avaiable in google play.

[Violent Python](#)

This ebook will help you use python in a really good way.

RATS

Rats is something everyone should know how to use and how it works. When you start with pentesting or just fun hacking using metasploit (or similar), you will discover something called "meterpreter" which reminds about a rat, plus that it's just really good to know it.

So everyone have heard about Dark Comet. This is the most used RAT since it's stable, simple to use and is the most known and used. However, this is not the most stable RAT, mot because you are just going to learn, this free rat is the best one right now. Since this is and old RAT, there is tons of downloadlinks here at HF, just look trough the uploaders REP before downloading.

Later when you've learned how a rat works, you should buy a rat. I highly reccomend that you buy [LuminosityLink](#).

It's the top ranked (in my opinion).

The creator is very friendly and experienced. It has all functions that you can wish for so yeah, just do that.

Sometimes you will discover some problems with RATs, so let me give you some mentors and some quick info.

1. Always portforward
 2. Make sure that your firewall is 100% disabled (open the firewalls "advanced options" and make sure that they all have a green mark before shutting down the firewall)
 3. Make sure that the AV haven't removed it.
- And those are the biggest reasons why RATs don't work.

The top mentor are ofcourse: [xVulnerable](#)

And yes, it costs, but it's not free to learn to hack, nothing comes free.

KEYLOGGERS Something else that's good to know is keyloggers. These softwares are widely used for alot of reasons, like - Infection on yourself to never forget about your passwords, infect your computers to make sure no one does something you don't want on them. And ofcourse we got a

bunch of idiots, stealing private info with them. I use them on my pcs that i share with others so I can keep an eye on what they are doing on my PC.

There are actually a lot of free good keyloggers. But this is the ones I recommend.

*[Dracula Logger](#) RECOMMENDED

*[Agent Tesla](#)

REMEMBER: You don't need a mentor for keyloggers, if you want help with them, you can ask any mentor here and they should be able to help you!.

SOCIAL ENGINEERING

Social engineering - Manipulate a person instead of a server/device.

A lot of people think that SE is only used for blackhat, but nope. I've been using this when I sell things online, working as a phone salesman, buying things.

You can actually use it to just sell your car for more money than the buyer wants to give, buy things for less than it's worth. The best way here at HF to learn it, is to become a e-whorer.

So let's give you a good e-whore mentor and a good tutorial.

MENTOR

[dopepizza](#) RECOMMENDED

STARTER LINKS

[Boxxys Guide](#)[/align]

Let me give you a few things that you will ask later anyway!

1. Saturated packets will be unsaturated again, look for old packs
2. You won't make a single cent your first few days, stay patient
3. Yes, Kik method is still the best way to make money
4. No, Your computer is not fcked up, You need an older version of manycam for this to work

Let's get into some more advanced hacking!

XSS/CROSS-SITE SCRIPTING

Cross-site scripting is what it sounds, it's scripting over the site, that is not yours, or that you don't have access to (It can be yours, but if you go into it as a regular user to just test this)

xss is built on JavaScript, which is why you should learn some JavaScript before starting.

One of the simplest ways to test for xss is to find a website with either a "search" function or a "post" function. Then you try to enter a basic js to if the site is vulnerable. Like this example:
Go to YOURSITE.com and click on the search button, then write a script with "alert(123)" between the script command

If you get an alert message saying "123", the site is vulnerable.

Best site to read more on this is: [OWASPS XSS TUTORIAL](#) For more info, read the javascript section in "More Info" in the beginning.

SQLi SQL injections is an old hacking method that sadly works today. It's quite similar to xss in one way, but totally different because you are attacking the database instead of the website (in most occasions). Some people are saying that manual sqli is better than softwares. When I hear that, it's like they never discovered sqlmap. One of the best ways to see if a website could be vulnerable, is

to look for a "?" followed by something similar like "id=8" or something. Let me give you an example.

www.YOURWEBSITE.com/section/login.php - Probably not vulnerable

www.YOURWEBSITE.COM/login?id=1'.php - Could be vulnerable

If you would like to read more, look into this members "tests" and read more:

[lgrotesque](#)

Read more in the "sql" section in "more info"

DOX

You are probably wondering why I didn't pick "dox" before all the others, well.. the reason is pretty simple. It's much simpler to DOX someone when you understand sqli and xss. I'm not saying that you should do a sqli just to find out who someone is, but it's still good to know some ways to hack before you start with DOX.

I'm guessing that some of you are asking 1 question now.

What is doxing?

Dox is simply "stalking" but in the techs world, so no, it's not "stalking". We who do it are just trying to find info about someone. Like IP, real name, real number, real country and so on.

If you are good at social engineering, it's pretty simple to find someone's IP by just make them click on a link. By doing so, you will also find out what country they are in and what state/city they are in.

Remember that the state and city won't always be 100% accurate. So here is a good list of websites for your doxing:

*[Market Visual](#) - Find important info about workers and CEOs

*[TinEye](#) - Reverse Image Search

*[ip-adress](#) - My favorite site for locating IPs

*[iplogger](#) - My favorite site for finding someone's IP

*[My Ip Neighbors](#) - Reverse IP lookup

*[NameCHK](#) - Reverse Username/Domain search

*[PasteLert](#) - Reverse Pastebin Search

*[CheckUsernames](#) - Username Reverse Search

*[Who's talkin](#) - Search For Social Medias Tags and similar

*[Tweetarchivist](#) - Reverse Twitter Search

*[Whois Lookup](#) - Advanced Whois Lookup

*[LeakedIn](#) - Leaked Info

*[echosec.net](#) - Reverse Location Search

It's a long list but you need it. If you need any more help in this, I suggest you read [Legends Help Desk](#)

VULNERABLE SCANS

This is fun, REALLY fun actually. This is how security companies do their work when they are searching for vulnerable points in websites and servers. There is a lot of ways to do this on. But I will give you my top ways.

There are some top softwares that I want you to check in before starting here:

*[VEGA](#) - Application Scanner

*[WMAP](#) - Web scanner

*[Nessus](#) - Vulnerability Scanner

All these softwares are really simple to use, and you can find info about them online.

I once asked myself, "How do I test this on deep web sites". So here is a short explanation.

A deep web site only has a url, they don't have a special ip to test anything on so first of all, stop

thinking about your softwares that requires a IP to be able to work. The deep web sites are only available if you are behind the tor proxy. So if the software does not have access to a proxy, you can use it either (you can but it's a bit more advanced). So when your software is behind a proxy and you can insert a url in the textfield, you can test the site.

Remember that you will get a lot of negative positives and positive negatives. Make sure that you read all the explanations to why the server is vulnerable and what's REALLY vulnerable in the point you found. Something that a lot of people are believing is the usual problem found called "password over cleartext" which only means that they don't have an "SSL". With other words, you need to be on the same network (or hack their internet provider) and do a MITM to read their passwords.

I'm sorry for being selfish here, but I recommend [ME](#) for as a mentor for this, since I haven't heard anything about another mentor in pentesting and vulnerable scans.

PENETRATION TESTING

Before we go any further, you need to know what "Penetration testing" is. Have you ever wondered how someone could hack into FBI's servers, the pentagon and all of those. They don't have vulnerable SQL servers, they don't have a simple "search field" for xss. No, they got what we really mean with "Hacked". This is what penetration testing is all about. Pentesting is when you inject malicious codes into their network/servers/websites and so on.

This is usually done by metasploit, but there is a lot of other softwares like "armitage" which gives you a GUI experience, and of course the "core impact" which is (from what i've heard, never really used it) an expensive but the most powerful tool out there today.

To get more info, go to the "advanced hacking" tab here at HF and look through the threads, ask [Me](#) to mentor you through it. EDIT: Currently fixing a new thread that fits our members more, stop commenting in hope to get a few "rep" because you seem to know better.

Cxdde3990xc - May 5, 2016, 7:06 am

Your thread is wrong on so many levels TBH
Just straight saying it

SysAdmin - May 5, 2016, 7:38 am

Most of these are not whitehat, Social Engineering cannot be discussed on the forums and i wouldn't bother typing this out again as it is mostly wrong.

SkinX - May 5, 2016, 7:41 am

I think you need to learn what the white/grey/black hats mean sir. Good on you for posting this mind, but I'd just edit it and sort it out as a lot of it is grey/blackhat imo.

?Xe - May 5, 2016, 8:05 am

I don't think a whitehat would ever be using a keylogger, never even heard of a case where that happens.

JesusBallz - May 5, 2016, 8:13 am

"Let's get into some more advanced hacking"

>SQLi

>XSS

?

Can i ask why you're mentioning web hacking and pentesting in the same thread? It's a whole different subject which doesn't relate to web hacking.

If you're going to explain it, please explain it in detail. What am i going to do after running metasploit? How am i going to deliver a payload then root?

Personally i don't even think you know yourself. Also on this subjecting why don't you mention Nmap as it's a necessity?

where's ponywizard to teach these tards ???

Not trashing but w/e. gl.

0x7FFDF000 - May 5, 2016, 8:16 am

(May 5, 2016 08:13 AM)JesusBallz Wrote: [\[CITE\]](#) where's ponywizard to teach these tards ??? I think that dude is still around. ?

||||| - May 5, 2016, 8:44 am

I said "beginners guide" not "master of the hacking".

It's for when you're STARTING, not when you know. If a RAT is simple, what do you call sqlmap? it's more advanced. Not mentioning nmap since i ran out of words. (most 12000).

Yes, social engineering can be used as whitehat, Social engineering is ONLY used to manipulate a real person instead of a system. Since when is it illegal to do that? E-whoring is social engineering, still illegal but it's on the forum. When you're buying a car, you use social engineering to lower the price, when you're mad at an idiot and wanna hurt him the most, you use social engineering, when you publish your ebook and want as many as possible to buy it, you write a good review, which is social engineering, when you love someone and wanna make them feel as good as possible, guess what? YOU'RE USING SOCIAL ENGINEERING!. All of these are used by IT security companies.

If you would like to start with hacking, you should know some about keylogging, or how should it sound like later?

customer - Hello sir, I'm having some troubles with my pc

you - Okay, what's the problem?

customer - I downloaded a file, then my facebook got hacked, and my AV can't find any virus

you - Oh, I think it's some kind of keylogger, but i don't know how they work...

Good job! ?

JesusBallz - May 5, 2016, 8:56 am

(May 5, 2016 08:44 AM)k4rm4 Wrote: [\[CITE\]](#) I said "beginners guide" not "master of the hacking".

It's for when you're STARTING, not when you know. If a RAT is simple, what do you call sqlmap? it's more advanced. Not mentioning nmap since i ran out of words. (most 12000).

Yes, social engineering can be used as whitehat, Social engineering is ONLY used to manipulate a real person instead of a system. Since when is it illegal to do that? E-whoring is social engineering, still illegal but it's on the forum. When you're buying a car, you use social engineering to lower the price, when you're mad at an idiot and wanna hurt him the most, you use social engineering, when you publish your ebook and want as many as possible to buy it, you write a good review, which is social engineering, when you love someone and wanna make them feel as good as possible, guess what? YOU'RE USING SOCIAL ENGINEERING!. All of these are used by IT security companies.

If you would like to start with hacking, you should know some about keylogging, or how should it sound like later?

customer - Hello sir, I'm having some troubles with my pc

you - Okay, what's the problem?

customer - I downloaded a file, then my facebook got hacked, and my AV can't find any virus

you - Oh, I think it's some kind of keylogger, but i don't know how they work...

Good job! ?

Who tf would want to work in IT support/troubleshooting anyway? The fuck.

No one's going to hire a person in the example you said above.

Make lock the thread then make a second post with the rest of the stuff.

You seriously have no clue. Dumb guy.

Learn yourself before you teach.

0x7FFDF000 - May 5, 2016, 10:18 am

(May 5, 2016 08:44 AM)k4rm4 Wrote: [\[CITE\]](#) I said "beginners guide" not "master of the hacking". It's for when you're STARTING, not when you know. If a RAT is simple, what do you call sqli? it's more advanced. Not mentioning nmap since i ran out of words. (most 12000).

Yes, social engineering can be used as whitehat, Social engineering is ONLY used to manipulate a real person instead of a system. Since when is it illegal to do that? E-whoring is social engineering, still illegal but it's on the forum. When you're buying a car, you use social engineering to lower the price, when you're mad at an idiot and wanna hurt him the most, you use social engineering, when you publish your ebook and want as many as possible to buy it, you write a good review, which is social engineering, when you love someone and wanna make them feel as good as possible, guess what? YOU'RE USING SOCIAL ENGINEERING!. All of these are used by IT security companys.

If you would like to start with hacking, you should know some about keylogging, or how should it sounds like later?

customer - Hello sir, I'm having some troubles with my pc

you - Okay, what's the problem?

customer - I downloaded a file, then my facebook got hacked, and my AV can't find any virus

you - Oh, I think it's some kind of keylogger, but i don't know how they work...

Good job! ?Can you please edit this entire thread to link to this one?

<https://hackforums.net/showthread.php?tid=4976270>

IIIIII - May 5, 2016, 11:08 am

(May 5, 2016 10:18 AM)0x7FFDF000 Wrote: [\[CITE\]](#) Can you please edit this entire thread to link to this one?

<https://hackforums.net/showthread.php?tid=4976270>

1. Ra4w vpn is better than [censored] since ra4w vpn is the cheapest and have portforwarding. 143vpn is more expensive but also good.

2. Oday does not mean "not known" it means "no known fix for problem"

3. "For choosing a language, I'd recommend C++. It's a killer." but he doesn't telling anything about "java" which is compatible with every OS, yes c++ is the most powerful, but he should still mention JAVA.

And alot of more, His guide is to travel trough hacking, mine is a "think about, what do you want"

0x7FFDF000 - May 5, 2016, 11:14 am

(May 5, 2016 11:08 AM)k4rm4 Wrote: [\[CITE\]](#) 1. Ra4w vpn is better than [censored] since ra4w vpn is the cheapest and have portforwarding. 143vpn is more expensive but also good.

2. Oday does not mean "not known" it means "no known fix for problem"

3. "For choosing a language, I'd recommend C++. It's a killer." but he doesn't telling anything about "java" which is compatible with every OS, yes c++ is the most powerful, but he should still mention JAVA.

And alot of more, His guide is to travel trough hacking, mine is a "think about, what do you want"His

tutorial is also about thinking what do you want, because it offered all practical routes for hacking. Anything worthwhile you said in this tutorial (Close to nothing btw) is mentioned there. Why not cut the chase and link?

1. All VPNs on HF are trash. Utter trash. Nobody gives a shit about whatever you use.
2. Bullshit. Oday means not currently known widely and to the vendor. As soon as it is known it gets patched. No such thing as a software having "No known fix". If there is, give me 3 examples.
3. Java is a joke. Nobody needs to mention a shit language.

skelly76 - May 5, 2016, 1:38 pm

What is that shitty ass ebook you linked? I hope nobody bought that lmfao. TrueDemon's ebook is the only one you really need and it's like \$5. Hell it's leaked online if you're too poor for it.

Overall this was a horrible "tutorial". You just told people what stuff is and not how to do anything. This isn't even the "biggest guide". Bad grammar on top of it all. 2.2/10

Deathiant - May 5, 2016, 1:44 pm

I understand you are trying to help, and you posted this to teach people a few things, but you need to go over it first a few times for contradictions and actual writing, this reads more like someone talking than actual writing. Also you might wanna sort out your hats there, this is mostly grey. Not flaming or anything, just giving you my 2 cents on this thread since everyone else is so negative about it. Don't let this deter you, just fix up your thread and labels and writing and your good to go!