Forum:Hack Forums

Thread: what are the most useful areas of hacking to study?

raggaescience - *April 18, 2019, 10:37 pm*

So which areas do you consider the most useful:

web/database hacking
network hacking
browser hacking
hacking into an actual box (like Hack the Box, etc.)
python hacking
C++ hacking
mobile app hacking
cryptography
exploit development
other (please list)

The reason I ask is I cannot do all of them. I have to specialize so I can actually get good.

What would the most useful set of hacking skills be to you and what do you recommend? Any other area that is on HF counts besides IoT, Electronics, etc. I am interested in that but I am truncating it because I want to pick the most useful hacking skills and learn that so I can actually get good more quickly.

Please advise.

Also, please give a recommendation as to how many areas I should specialize in to get good because if I don't have a focus I will get scattered and spread myself thin like I do in other areas. I am going to become too interested in everything and it will cause me not to learn anything and I am hoping this will help me with structure.

And how many areas do you recommend to have as primary ones since I am going to get too interested and become a jack of all trades and master of none if I don't have a specific goal is what I'm scared of.

Thanks.

shelled - *April 18, 2019, 10:39 pm*

web application for bug bounties and the future of anything related to actual hacking because it'll often be an API test and the way you think will be transferable to iot testing as well

raggaescience - *April 18, 2019, 10:51 pm*

(Apr 18, 2019 10:39 PM)shelled Wrote: *[CITE]* web application for bug bounties and the future of anything related to actual hacking because it'll often be an API test and the way you think will be transferable to iot testing as well

Define "actual hacking." And yes I want to do bug bounties the most so I know one of my specialties is gonna be web hacking. My question is just is that it or how many and which additional areas do you recommend for usefulness?

shelled - *April 18, 2019, 10:54 pm*

(Apr 18, 2019 10:51 PM)raggaescience Wrote: [CITE] Define "actual hacking." And yes I want to do bug bounties the most so I know one of my specialties is gonna be web hacking. My question is just is that it or how many and which additional areas do you recommend for usefulness?

define actual hacking? can't.

means different things to different people on this forum apparently.

apparently ewhoring is "actual hacking" to some elites here https://hackforums.net/showthread.php?tid=5961381 so idk what it is anymore.

I say that's good enough if you u can pick up webapps u can pick the rest up no problem

Faith Connors - *April 19, 2019, 8:44 am*

the ones you're interested in.

/thread

raggaescience - *April 21, 2019, 10:01 pm*

(Apr 19, 2019 08:44 AM)Faith Connors Wrote: [CITE] the ones you're interested in.

/thread

I'm interested in all of the above + skype, IRC, etc. hacking. I will spread myself thin if I do too many right?

But I see your point.

realsunjester - *April 22, 2019, 1:27 am*

web/database hacking

network hacking

browser hacking

hacking into an actual box (like Hack the Box, etc.)

python hacking

C++ hacking

mobile app hacking

cryptography

exploit development

other (please list)

1. you need to first understand and know how to create and maintain a database.

2. you need to know what a network is, "network hacking" isn't anything since it's just too general. a network is just a group of computers connected through a common connection. so "network hacking" is nothing more than computer hacking. maybe you mean network device hacking like routers?

3. do you mean persistent xss? i am confused about what you mean.

4. all the above (and below probably) are hacking into "actual" boxes.

5. hacking python? do you mean learning python?

6. hacking c++? do you mean learning c++ or reverse engineering c++ applications?

7. do you mean reversing java applications? almost all mobile apps are created in java.

8. cryptography isn't really a hacking thing, it's more of a use case thing.

9. you will need to know programming quite a bit, plus many different hacking techniques.

Pawnhub - *April 22, 2019, 7:25 am*
The first two you listed are most important and you should study those.

Omniscient - *April 22, 2019, 9:17 am*
Some of those need each other for development of skills. I'd say learn a language first and foremost.

raggaescience - *April 22, 2019, 9:47 am*
(Apr 22, 2019 01:27 AM)realsunjester Wrote: *[CITE]*
web/database hacking

network hacking

browser hacking

hacking into an actual box (like Hack the Box, etc.)

python hacking

C++ hacking

mobile app hacking

cryptography

exploit development

other (please list)

1. you need to first understand and know how to create and maintain a database.

2. you need to know what a network is, "network hacking" isn't anything since it's just too general. a

network is just a group of computers connected through a common connection. so "network hacking" is nothing more than computer hacking. maybe you mean network device hacking like routers?

3. do you mean persistent xss? i am confused about what you mean.

4. all the above (and below probably) are hacking into "actual" boxes.

5. hacking python? do you mean learning python?

6. hacking c++? do you mean learning c++ or reverse engineering c++ applications?

7. do you mean reversing java applications? almost all mobile apps are created in java.

8. cryptography isn't really a hacking thing, it's more of a use case thing.

9. you will need to know programming quite a bit, plus many different hacking techniques.
1. I know. I'm going to build a full-stack website after I complete some IT certs.
2. WiFi hacking, moving laterally on a company's network, hacking CISCO devices, VoIP, etc.
3. exploiting Firefox or Chrome code, etc.
4. You've never heard of HTB? I mean logging in as a normal user and gaining root privileges on a device, reverse shells, etc.
5. learning python and using it to write hacking tools, exploit development, reverse engineering, etc.
6. learning c++ and using it to write hacking tools, exploit development, reverse engineering, etc.
7. No, I mean plugging the phone into the computer and exploiting code in the mobile apps. There are ways to get usernames and passwords from the GMail App. It's a real thing. Look it up.
8. Yes, wouldn't it be appropriate for a hacker to know?
9. so you would recommend being well-rounded but how do I do that and retain the skills? How well-rounded should I realistically get?

realsunjester - *April 22, 2019, 9:57 am*

(Apr 22, 2019 09:47 AM)raggaescience Wrote: *[CITE]* 1. I know. I'm going to build a full-stack website after I complete some IT certs.
2. WiFi hacking, moving laterally on a company's network, hacking CISCO devices, VoIP, etc.
3. exploiting Firefox or Chrome code, etc.
4. You've never heard of HTB? I mean logging in as a normal user and gaining root privileges on a device, reverse shells, etc.
5. learning python and using it to write hacking tools, exploit development, reverse engineering, etc.
6. learning c++ and using it to write hacking tools, exploit development, reverse engineering, etc.
7. No, I mean plugging the phone into the computer and exploiting code in the mobile apps. There are ways to get usernames and passwords from the GMail App. It's a real thing. Look it up.
8. Yes, wouldn't it be appropriate for a hacker to know?
9. so you would recommend being well-rounded but how do I do that and retain the skills? How well-rounded should I realistically get?
1. IT !== full stack development
2. knowing how networks work will help you greatly, also, learning linux is going to be the best way to do this since most of the hardware and servers will be linux based.
3. both of these are open source browsers, i'd start there.
4. yes, i am regular on htb. i suggest looking for writeups (https://0x00sec.org/t/htb-shell-affect-access-writeup/13085/2)
5. https://docs.python.org/3/
6. https://devdocs.io/cpp/
7. if you have physical access to a phone, there isn't much need

8. knowing the math behind algorithms probably isn't going to help you much.
9. phrack, pocorgtfo, read.

Faith Connors - *April 22, 2019, 11:05 am*
the more you explore the fields you selected, you'll find out their actual limitations in what you can/can't do and how similar they actually are to each other. for instance, web hacking an mobile hacking to some degree are identical for the reasons that most apps use some sort of webview or at the very least send http requests to connect to the servers on the backend. and because of that, you can theoretically do mobile hacking over wifi, ie. network hacking. and because most sites use ssl, there is some applied use of cryptography here, at least to the level that you want to try and downgrade requests to either not use any cryptographic implementation or use weaker keys to make it more easily crackable. to do that, you might write your own python script or something, using some programming knowledge. and once you find a vulnerability in the app, you'll write yourself an exploit (or a pyaload) for it, so you'll have some exploit development going on there too.

everything is connected, and everything has limitations. there's no use focusing on a field when they're all so similar. focusing on a field just means learning about all the nuances between the fields and learning how to work around (or with) them.

raggaescience - *April 22, 2019, 12:44 pm*
(Apr 22, 2019 11:05 AM)Faith Connors Wrote: [CITE] the more you explore the fields you selected, you'll find out their actual limitations in what you can/can't do and how similar they actually are to each other. for instance, web hacking an mobile hacking to some degree are identical for the reasons that most apps use some sort of webview or at the very least send http requests to connect to the servers on the backend. and because of that, you can theoretically do mobile hacking over wifi, ie. network hacking. and because most sites use ssl, there is some applied use of cryptography here, at least to the level that you want to try and downgrade requests to either not use any cryptographic implementation or use weaker keys to make it more easily crackable. to do that, you might write your own python script or something, using some programming knowledge. and once you find a vulnerability in the app, you'll write yourself an exploit (or a pyaload) for it, so you'll have some exploit development going on there too.

everything is connected, and everything has limitations. there's no use focusing on a field when they're all so similar. focusing on a field just means learning about all the nuances between the fields and learning how to work around (or with) them.
Ok so how long should I spend with web hacking before I add in another area in your view?

Faith Connors - *April 22, 2019, 4:30 pm*
(Apr 22, 2019 12:44 PM)raggaescience Wrote: [CITE] Ok so how long should I spend with web hacking before I add in another area in your view?
however long makes you feel comfortable with what you know
for most people that becomes never, since things are always constantly changing.
but maybe you just want to learn about doing a few cool things and move onto something else so you can be more wellrounded

there's no answer that can satisfy your question.

edit:
observe the following as to why this question can't be answered:

there's a book on my desk here, introduction to philosophy: classic and contemporary readings, fourth ed. by louis p pojman and james fieser
it's about 700 pages long, filled with essays by every major or semi-famous philosopher since plato

(or socrates, if you count platos works as socratic.)

i can tell you that reading this book will give you a really good introduction to the world of philsophy. that's definitely true.
then, you subsequently ask 'how long should i spend reading it?'

if you spend five minutes scanning through and saying you 'completed' it, you might have been introduced to a few concepts but have not put in any thought, as philosophy requires. same goes for reading for an hour, or two, or however long you spend.

if you simply go through the book, think about the questions posed by the book's editors (as well as the questions/subject matter of the essays,) then it'll take you way longer. but you will actually get yourself a really good foundation in terms of philosophy as a whole across millenia.

but maybe you don't want to know about medieval and modern philosophy, just sticking to the basics like aristotle, epictetus and plato. you'll spend like 10x less time getting through this section than the whole book, but your foundation on those subjects in particular will still be good, letting you move onto something else that interests you and might still be related (ie. how aquinas took aristotilian virtue to create aquinian christianity or whatever.)

it's just not a good question to ask. focus on what you like, if you don't like it move on. if you just want to scan through stuff to do it quickly, then by all means do it, but don't expect it to be as good as if you spent hours upon hours studying something.

raggaescience - *April 22, 2019, 5:49 pm*
(Apr 22, 2019 04:30 PM)Faith Connors Wrote: [CITE] however long makes you feel comfortable with what you know
for most people that becomes never, since things are always constantly changing.
but maybe you just want to learn about doing a few cool things and move onto something else so you can be more wellrounded

there's no answer that can satisfy your question.

edit:
observe the following as to why this question can't be answered:

there's a book on my desk here, introduction to philosophy: classic and contemporary readings, fourth ed. by louis p pojman and james fieser
it's about 700 pages long, filled with essays by every major or semi-famous philosopher since plato
(or socrates, if you count platos works as socratic.)

i can tell you that reading this book will give you a really good introduction to the world of philsophy. that's definitely true.
then, you subsequently ask 'how long should i spend reading it?'

if you spend five minutes scanning through and saying you 'completed' it, you might have been introduced to a few concepts but have not put in any thought, as philosophy requires. same goes for reading for an hour, or two, or however long you spend.

if you simply go through the book, think about the questions posed by the book's editors (as well as the questions/subject matter of the essays,) then it'll take you way longer. but you will actually get yourself a really good foundation in terms of philosophy as a whole across millenia.

but maybe you don't want to know about medieval and modern philosophy, just sticking to the basics like aristotle, epictetus and plato. you'll spend like 10x less time getting through this section than the whole book, but your foundation on those subjects in particular will still be good, letting you move onto something else that interests you and might still be related (ie. how aquinas took aristotilian virtue to create aquinian christianity or whatever.)

it's just not a good question to ask. focus on what you like, if you don't like it move on. if you just want to scan through stuff to do it quickly, then by all means do it, but don't expect it to be as good as if you spent hours upon hours studying something.
Right but I actually want to be good at hacking. Maybe even good in a few areas and that’s it. I see your point.

I’ll just see what interests me and stick to that. I want to get good so probably I will just stick with web hacking. I think I see your point. So your saying being good at everything is a stupid goal.

I think I see your point.

What if I want to be especially good at three things and just know basics of the rest?

Faith Connors - *April 22, 2019, 6:14 pm*
(Apr 22, 2019 05:49 PM)raggaescience Wrote: [CITE] Right but I actually want to be good at hacking. Maybe even good in a few areas and that’s it. I see your point.

I’ll just see what interests me and stick to that. I want to get good so probably I will just stick with web hacking. I think I see your point. So your saying being good at everything is a stupid goal.

I think I see your point.

What if I want to be especially good at three things and just know basics of the rest?
my point isn't that you should stick to one thing. my point is that you should do things as you feel fit. there's no right path, and there's no wrong path. there are only paths, and your path can follow someone else's path if you really want, but it doesn't have to, since it's very unlikely that someone else's path will be exactly what you want and what you're looking at doing.

if you want to stick to one thing, stick to one thing. if you want to stick to three things and have a general understanding of others, then do that. my point isn't that one of these is inherently worse than any other, since they really aren't that different as long as you're still learning something. you clearly already have a set of goals in mind as i'm writing this out. so follow those goals instead of worrying about the path you 'need' to take.

raggaescience - *April 22, 2019, 7:10 pm*
(Apr 22, 2019 06:14 PM)Faith Connors Wrote: [CITE] my point isn't that you should stick to one thing. my point is that you should do things as you feel fit. there's no right path, and there's no wrong path. there are only paths, and your path can follow someone else's path if you really want, but it doesn't have to, since it's very unlikely that someone else's path will be exactly what you want and what you're looking at doing.

if you want to stick to one thing, stick to one thing. if you want to stick to three things and have a general understanding of others, then do that. my point isn't that one of these is inherently worse than any other, since they really aren't that different as long as you're still learning something. you clearly already have a set of goals in mind as i'm writing this out. so follow those goals instead of worrying about the path you 'need' to take.
So if my goal was to be good at these three, so I could be good for bug bounties and hacking on

the web:

hacking Skype, IRC, etc. and other chat rooms
web/database hacking
browser hacking

And that's it for specialities and then I would want to know the basics of:

Hack the Box
network hacking

Would that be a realistic goal to be good at those five things but be more skilled in the first three, especially web hacking? Then I just want to be up to date in the other two and know what I'm doing with them.

Gbulla - *April 22, 2019, 7:20 pm*

(Apr 18, 2019 10:37 PM)raggaescience Wrote: [CITE] python hacking
C++ hacking
what exactly is this?

Faith Connors - *April 22, 2019, 7:40 pm*

(Apr 22, 2019 07:10 PM)raggaescience Wrote: [CITE] So if my goal was to be good at these three, so I could be good for bug bounties and hacking on the web:

hacking Skype, IRC, etc. and other chat rooms
web/database hacking
browser hacking

And that's it for specialities and then I would want to know the basics of:

Hack the Box
network hacking

Would that be a realistic goal to be good at those five things but be more skilled in the first three, especially web hacking? Then I just want to be up to date in the other two and know what I'm doing with them.
anything is a realistic goal as long as what you want to do is realistic

raggaescience - *April 22, 2019, 9:46 pm*

(Apr 22, 2019 07:40 PM)Faith Connors Wrote: [CITE] anything is a realistic goal as long as what you want to do is realistic
But is learning all five of those things a realistic thing to do in a few years? I think I can do it, I just have to work really hard. Do you agree?

Faith Connors - *April 22, 2019, 9:50 pm*

(Apr 22, 2019 09:46 PM)raggaescience Wrote: [CITE] But is learning all five of those things a realistic thing to do in a few years? I think I can do it, I just have to work really hard. Do you agree?
is it possible to learn five things? yes
therefore, learning five things is a realistic goal, yes

it's really not that deep. you're overthinking things.

raggaescience - *April 22, 2019, 9:52 pm*

(Apr 22, 2019 09:50 PM)Faith Connors Wrote: [CITE] is it possible to learn five things? yes therefore, learning five things is a realistic goal, yes

it's really not that deep. you're overthinking things.
But to actually be good at all five is a different story right?

Faith Connors - *April 23, 2019, 8:34 am*

(Apr 22, 2019 09:52 PM)raggaescience Wrote: [CITE] But to actually be good at all five is a different story right?
no different than being good at five subfields of any other subject (ie. understanding five programming languages at a high level for compsci)

and ik some absolutely idiotic putrid cunt will try and counter with 'but lerning languages is ezpz once u kno one" so i'll counter now
the logic remains over the course of learning all languages as a fundamental. the problem solving remains over the course of learning how to program. occasionally you forget things and look them up as reference. same thing goes for fields of hacking in which nothing is truly 'exclusive' aside from a few nuanced things but there are lots of fundamentals (ie. networking) that remain no matter what field you study.

BestFwend - *April 24, 2019, 5:32 am*

(Apr 18, 2019 10:51 PM)raggaescience Wrote: [CITE] Define "actual hacking." And yes I want to do bug bounties the most so I know one of my specialties is gonna be web hacking. My question is just is that it or how many and which additional areas do you recommend for usefulness?
Hey if you are interested in buying a course from Sans I will definitely give one more to you.

sans.org

They charge like 2k for this stuff but I'll give it to you for much cheaper. Just PM me if interested.

It definitely has SUPER USEFUL INFO. Anyway it helped me find some of my first bugs.

And yes I'm desperate for money

Sitrep - *April 25, 2019, 3:45 pm*

I would say all of them, but I really tend to stick to web applications since that's a way to earn money in the end too with bug bounties.

raggaescience - *April 25, 2019, 7:28 pm*

(Apr 25, 2019 03:45 PM)Sitrep Wrote: [CITE] I would say all of them, but I really tend to stick to web applications since that's a way to earn money in the end too with bug bounties.
Yeah, ok. So then I will probably learn web hacking first.

I really think the WiFi Pineapple is cool. But yeah I agree that web hacking is probably a lot more fun.

So yeah, I am going to probably start by learning web hacking.

Its a good idea.

Thanks for letting me know that.

Probably WiFi hacking will be the one I learn after I get through web hacking first. I just need to

become proficient in web hacking first thing.

Thanks for the advice.

Is there money to be made browser hacking or mobile app hacking?

Sitrep - *April 25, 2019, 7:34 pm*

(Apr 25, 2019 07:28 PM)raggaescience Wrote: [CITE] Yeah, ok. So then I will probably learn web hacking first.

I really think the WiFi Pineapple is cool. But yeah I agree that web hacking is probably a lot more fun.

So yeah, I am going to probably start by learning web hacking.

Its a good idea.

Thanks for letting me know that.

Probably WiFi hacking will be the one I learn after I get through web hacking first. I just need to become proficient in web hacking first thing.

Thanks for the advice.

Is there money to be made browser hacking or mobile app hacking?

To be honest, the main thing is that you personally have fun when you hack. That's the best way to learn! So go for the Pineapple first if that's what you want!

raggaescience - *April 25, 2019, 7:54 pm*

(Apr 25, 2019 07:34 PM)Sitrep Wrote: [CITE] To be honest, the main thing is that you personally have fun when you hack. That's the best way to learn! So go for the Pineapple first if that's what you want!

I really would rather learn wifi hacking before the pineapple but I really do think web hacking is the thing to learn first because I want to do bug hunting.

But I strongly believe no one should use the Pineapple unless they can already hack WiFi the basic way.