

Forum:[Hack Forums](#)

Thread: [Starting point \[MISSING\]](#)

Caliber44 - November 29, 2017, 9:31 am

Im'm looking for a starting point of my learning proccess. I know it will take years of work, and studies, i dont mind, i just want to do it. I have some knowledge but its so small that ill probably should start over just to be sure. So my real question here is:

From what i should start to learn to get into hack world. Id like some websites/tutorials/books to read/lessons to follow/what studies i should do?

Im 20, ive done the Electronics School, and my dream was always to be part of that world so badly that now im ready. Every suggestion will be a gr8 suggestion.

Faith Connors - November 29, 2017, 9:36 am

pick a field and learn about it. literally nothing else. you can be a jack of all trades and a master of none but it's generally better to just focus on one area and get really good at it.

Asdethprime - November 29, 2017, 4:38 pm

This will obviously depend on what you want to achieve. If vulnerability discovery and exploit development of executable binary is what you are interested in then this might help (I am not an expert, I am learning this myself though I may be a bit ahead of you on the materials).

- 1) follow a simple computer science course. CS50 video on YouTube is good. This will get u started on C programming language and Python for scripting.
- 2) then start with assembly language. If you want to understand how a program really works and use that to figure out what you could do to hack it (provided it's possible) you need to look into assembly because that's all you get. Get a book, search for online free courses whatever suits u.

3) find tools that will help u take apart a program and let u view how it works. This will be operating system specific. I use Linux and use objdump (it's a program that comes pre-installed) to see a programs assembly output. Also a simple tip create a very basic program on C (hello world for example) turn it into an executable (I. E. Compile and link it) and use objdump on it. You will see a huge amount of sections are added by the compiler / OS. whatever program u are trying to understand and find weakness for, you can ignore these sections as they are not directly related to the program at hand.

Linux provides a treasure trove of free programs for reversing , though above all else GDB which is installed by default is a hugely useful. I use radare2 framework but u can use whatever u like. Framework doesn't affect your result your patience does.

Look for the assembly code you get. Try to understand it. Keep a txt file to store information you discover and if possible try and covert the code into a programming language of your choice (c for example). It helps u keep track of what u discover. You will need it because few months to fully understand a small real world program isn't uncommon (some will take even longer).

If there is particular section you don't understand post then here (sadly hackforums is pretty lame for getting answers as no one seem interested to help) or on other websites (stackoverflow and garage4hackers) are more helpful.

Try it. You will get stuck at places but you will know exactly what u don't understand and what u would need to learn.

You also want to look at what hacking techniques are out there : buffer overflow, integer overflow, race condition etc.

The internet is your library to explore and challenge yourself to how far you can go.

CyberStrike - November 29, 2017, 5:14 pm

Now a days with VirtualBox and VMware it is very easy there is no reason to just hack some website or network.

You want to make a free account on Cybrary where you can learn about many different subjects. You want to focus on networking and then OSs such as Windows and Linux. From there check out the Ethical Hacking and Pentesting course then the Advanced Pentesting course then check out the WebApp Pentesting course.. Don't just watch videos or just read books actually practice and learn by using the virtual pentesting lab which you create.

<https://www.cybrary.it>

Also don't be scared to Google up things, that is going to be something you do during any pentest.

Step 2 make yourself a hacking/pentesting lab

[http://resources.infosecinstitute\[.\]com/building-your-own-pentesting-environment/](http://resources.infosecinstitute[.]com/building-your-own-pentesting-environment/)

Vulnerable VMs

<https://www.vulnhub.com/>

Windows Server & VMs

<https://www.microsoft.com/en-us/evalcent...erver-2016>

<https://developer.microsoft.com/en-us/mi...tools/vms/>

So always practice safely.

Caliber44 - December 3, 2017, 4:48 am

(Nov 29, 2017 05:38 PM)Asdethprime Wrote: [\[CITE\]](#) This will obviously depend on what you want to achieve. If vulnerability discovery and exploit development of executable binary is what you are interested in then this might help (I am not an expert, I am learning this myself though I may be a bit ahead of you on the materials).

1) follow a simple computer science course. CS50 video on YouTube is good. This will get u started on C programming language and Python for scripting.

2) then start with assembly language. If you want to understand how a program really works and use that to figure out what you could do to hack it (provided it's possible) you need to look into assembly because that's all you get. Get a book, search for online free courses whatever suits u.

3) find tools that will help u take apart a program and let u view how it works. This will be operating system specific. I use Linux and use objdump (it's a program that comes pre-installed) to see a program's assembly output. Also a simple tip create a very basic program on C (hello world for example) turn it into an executable (I. E. Compile and link it) and use objdump on it. You will see a huge amount of sections are added by the compiler / OS. whatever program u are trying to understand and find weakness for, you can ignore these sections as they are not directly related to the program at hand.

Linux provides a treasure trove of free programs for reversing, though above all else GDB which is installed by default is a hugely useful. I use radare2 framework but u can use whatever u like.

Framework doesn't affect your result your patience does.

Look for the assembly code you get. Try to understand it. Keep a txt file to store information you discover and if possible try and covert the code into a programming language of your choice (c for example). It helps u keep track of what u discover. You will need it because few months to fully understand a small real world program isn't uncommon (some will take even longer).

If there is particular section you don't understand post then here (sadly hackforums is pretty lame for getting answers as no one seem interested to help) or on other websites (stackoverflow and garage4hackers) are more helpful.

Try it. You will get stuck at places but you will know exactly what u don't understand and what u would need to learn.

You also want to look at what hacking techniques are out there : buffer overflow, integer overflow, race condition etc.

The internet is your library to explore and challenge yourself to how far you can go.

I really appreciate your answer, thank you so much this is really usefull, i think its the best starting point that someone has given to me. Ill for sure try to make my way in this world now, im very happy thank you so much.

sirru5h thank you so much, i didn't know i can actually create a Lab for pentesting eand training with VWmare despite i use it a lot in school. Thanks also for the links you provided to me they are a great starting point. You are the best guys

Nomad.Null - December 3, 2017, 7:37 am

I've always been in favor of reading books. I've used Cybrary.it as well, and vulnhub has some great sources as well. Similarly to the answers everyone else has given you, it's going to depend on where you want to go and what you want to learn because hacking is a broad topic of many subjects. You never really master any one of them, and you will never learn it all, but you eventually find your niche, the speciality that fits your style and the technology you gravitate most towards. Web application hacking, exploit development, network exploitation, phishing and social engineering, wireless penetration testing, physical security, even forensics. I wrote a book for beginners that was designed to introduce you to the first inch of all of these topics and get you started down a path towards becoming an ethical hacker. If you're interested in something like that, there is a free sample copy on google books that you can find in my signature. The paperback/ebook versions are the only complete ones though.

Good luck on your journey ?

Caliber44 - December 3, 2017, 10:18 am

(Nov 29, 2017 05:38 PM)Asdethprime Wrote: [\[CITE\]](#) This will obviously depend on what you want to achieve. If vulnerability discovery and exploit development of executable binary is what you are interested in then this might help (I am not an expert, I am learning this myself though I may be a bit ahead of you on the materials).

1) follow a simple computer science course. CS50 video on YouTube is good. This will get u started on C programming language and Python for scripting.

2) then start with assembly language. If you want to understand how a program really works and use that to figure out what you could do to hack it (provided it's possible) you need to look into assembly because that's all you get. Get a book, search for online free courses whatever suits u.

3) find tools that will help u take apart a program and let u view how it works. This will be operating system specific. I use Linux and use objdump (it's a program that comes pre-installed) to see a programs assembly output. Also a simple tip create a very basic program on C (hello world for example) turn it into an executable (I. E. Compile and link it) and use objdump on it. You will see a huge amount of sections are added by the compiler / OS. whatever program u are trying to understand and find weakness for, you can ignore these sections as they are not directly related to the program at hand.

Linux provides a treasure trove of free programs for reversing , though above all else GDB which is installed by default is a hugely useful. I use radare2 framework but u can use whatever u like.

Framework doesn't affect your result your patience does.

Look for the assembly code you get. Try to understand it. Keep a txt file to store information you discover and if possible try and covert the code into a programming language of your choice (c for example). It helps u keep track of what u discover. You will need it because few months to fully understand a small real world program isn't uncommon (some will take even longer).

If there is particular section you don't understand post then here (sadly hackforums is pretty lame for getting answers as no one seem interested to help) or on other websites (stackoverflow and garage4hackers) are more helpful.

Try it. You will get stuck at places but you will know exactly what u don't understand and what u would need to learn.

You also want to look at what hacking techniques are out there : buffer overflow, integer overflow, race condition etc.

The internet is your library to explore and challenge yourself to how far you can go.

(Dec 3, 2017 08:37 AM)True Demon Wrote: [\[CITE\]](#) I've always been in favor of reading books. I've used Cybrary.it as well, and vulnhub has some great sources as well. Similarly to the answers everyone else has given you, it's going to depend on where you want to go and what you want to learn because hacking is a broad topic of many subjects. You never really master any one of them, and you will never learn it all, but you eventually find your niche, the speciality that fits your style and the technology you gravitate most towards. Web application hacking, exploit development, network exploitation, phishing and social engineering, wireless penetration testing, physical security, even forensics. I wrote a book for beginners that was designed to introduce you to the first inch of all of these topics and get you started down a path towards becoming an ethical hacker. If you're interested in something like that, there is a free sample copy on google books that you can find in my signature. The paperback/ebook versions are the only complete ones though.

Good luck on your journey ?Thank you so much, ill use it for sure, good luck with your work ?

Dimeblade - January 9, 2018, 10:48 am

(Nov 29, 2017 06:14 PM)sirru5h Wrote: [\[CITE\]](#) Now a days with VirtualBox and VMware it is very easy there is no reason to just hack some website or network.

You want to make a free account on Cybrary where you can learn about many different subjects. You want to focus on networking and then OSs such as Windows and Linux. From there check out the Ethical Hacking and Pentesting course then the Advanced Pentesting course then check out the WebApp Pentesting course.. Don't just watch videos or just read books actually practice and learn by using the virtual pentesting lab which you create.

<https://www.cybrary.it>

Also don't be scared to Google up things, that is going to be something you do during any pentest.

Step 2 make yourself a hacking/pentesting lab

[http://resources.infosecinstitute\[.\]com/building-your-own-pentesting-environment/](http://resources.infosecinstitute[.]com/building-your-own-pentesting-environment/)

Vulnerable VMs

<https://www.vulnhub.com/>

Windows Server & VMs

<https://www.microsoft.com/en-us/evalcent...erver-2016>

<https://developer.microsoft.com/en-us/mi...tools/vms/>

So always practice safely.

Cant argue with that ? ? ?