

Forum:[Hack Forums](#)

Thread: [Advice from a White hat.](#)

Trinity - January 20, 2017, 2:28 pm

i deleted this, it was crap. a more detailed guide will come in a couple of weeks, wich will be a guide on how to get into cyber secuurity among tother things.

Regards EngLen?

wit - January 20, 2017, 2:33 pm

This is very helpful, i appreciate the time you took to type this out!

Trinity - January 20, 2017, 2:35 pm

(Jan 20, 2017 03:33 PM)CryptoZeus Wrote: [\[CITE\]](#) This is very helpful, i appreciate the time you took to type this out!

thank you ? This is just a start tho, it will grow and get more organised. Maybe throw some graphic in there and "order" it a bit more so it's nice for the eye...

Kind regards EngLen ?

UnknownDog - January 20, 2017, 3:08 pm

Good guide. I hope it will help people out. While on the topic about staying safe online; should be noted that using the same password on different places is the worst thing you can do, and should be reminded not to do so.

Infamia - January 20, 2017, 3:11 pm

Great tutorial dude, but as you said- you should probably add some art because you'know, people would think your tutorial is more legitimate if it looks so from a glimpse.

Trinity - January 20, 2017, 3:13 pm

(Jan 20, 2017 04:08 PM)UnknownDog Wrote: [\[CITE\]](#) Good guide. I hope it will help people out. While on the topic about staying safe online; should be noted that using the same password on different places is the worst thing you can do, and should be reminded not to do so.

Yep will do Unknown, and Shuld add "use Commen Sense" too.

(Jan 20, 2017 04:11 PM)Infamia Wrote: [\[CITE\]](#) Great tutorial dude, but as you said- you should probably add some art because you'know, people would think your tutorial is more legitimate if it looks so from a glimpse.

Thanks Infamia ? yeah ill gte ma hands on some art as soon as possible.

Gizmo - January 21, 2017, 12:37 pm

Got some very interesting links included. Thanks for sharing this!

Very useful information. Keep up the good work.

imperlin - January 21, 2017, 1:24 pm

Damn... This is some HQ shit you posted right here. There are some very interesting stuff and it's an amazing detailed guide.

Markl - January 24, 2017, 6:25 pm

Good post! This is very helpful! Some of the programs that you list are difficult to install. Can someone add FAQ's?

? Quick ? - January 24, 2017, 6:27 pm

Really well put together. +1

skelly76 - January 24, 2017, 6:56 pm

Can I be frank? I don't know how everyone thinks this is a good tutorial thread...

I mean you don't go into detail about anything, you don't know what proxies are, and you just skip around topics like it's hopskotch. Take a look at these and improve yours.

<https://hackforums.net/showthread.php?tid=4329505>

<https://hackforums.net/showthread.php?tid=4178212>

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

Someone had to say it man, but at least you tried I guess. Just add more stuff that actually TEACHES. There is no point in knowing a name of an attack if you don't explain what it is or how to do it.

Faith Connors - January 24, 2017, 7:42 pm

(Jan 24, 2017 07:56 PM)Aerial Wrote: [CITE](#) Can I be frank? I don't know how everyone thinks this is a good tutorial thread...

I mean you don't go into detail about anything, you don't know what proxies are, and you just skip around topics like it's hopskotch. Take a look at these and improve yours.

<https://hackforums.net/showthread.php?tid=4329505>

<https://hackforums.net/showthread.php?tid=4178212>

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

Someone had to say it man, but at least you tried I guess. Just add more stuff that actually TEACHES. There is no point in knowing a name of an attack if you don't explain what it is or how to do it.

Its good that you said it because i would have. And i would have written a 3 post essay on why this is a bad guide and everything wrong with it, from grammar/spelling, incorrect terminology, incorrect explanations, and other downright wrong information.

So thank you for saving me some time.

EDIT: Although it was a valiant attempt, I'm going to write that essay out of spite. Thank you for trying though.

My self control is weak when I see threads like this.

Logical Flaws in "Advice from a White hat."

By: Faith Connors

Released under GPLv3

The Good:

I'll start off with everything good I've seen in this guide, then get down and dirty with the bad. It's my way of showing that I'm looking at both sides of this. I would also like you to note that I am sometimes wrong as well, and although I may come off as arrogant or annoying or whatever, have a look at my other guides and surely you will see corrections made by other users. If anyone sees something wrong with this, please correct me.

First of all, I like how you color coded things. Not only does it help you organize your ideas but you also chose bright colors that would be easy to read. Well, kind of. I'd actually use some kind of brighter (whiter) shade of red, because if you're like me and you have a shitty monitor or if your monitor is really bright like most gamers, then it'll be hard to read. Also brown, maybe something like beige?

I also appreciated how you cited some sources. Although not full citations like you would write in an English class, it's good that you included them. Also how throughout the post you quoted sites instead of either paraphrasing or even worse, straight copy/pasting and claiming as your own. I appreciate that and I'm sure most uni professors would too. As well as anyone else that would be ready to call you out (like me, again.)

It's also cool how you linked some other threads, but you probably missed a ton that are exponentially better, like Aerial mentioned. I'll get into some of those later.

The Bad:

Here we are, the entire guts of this.

Title:

Okay, part one. Your title is misleading, claiming you are a "whitehat." Your disclaimer claims that you aren't an expert and that's fine. But the whitehat buzzword throws people off. Also I get the impression you don't actually know what you're talking about. But whatever, buzzwords get people's attention, like you tried to do and you succeeded. People read your thread and responded. Sadly, you also got the attention of people like me, who are going to dig their nails in and rip it open.

XMPP:

Cool that you included that people can message you over that if they can't PM for whatever reason, or they can't discuss a topic on this forum. That's nice. Except for one thing. You didn't actually include your XMPP address anywhere in the thread. Oh well. Also, I find that people who set up XMPP for the first time have a bit of trouble, so linking them to Cynical's thread on setting it up would be nice too. I believe he even owned a server for some time until it got taken down.

Cybersec:

Your first section. Although only a few lines long, there's a lot wrong with this.

First, it's cool that you included a Wikipedia definition on it, I appreciate that, like I mentioned earlier. But now, paraphrase it, put it into your own words, a way that people will actually understand it. Because that definition is just a million buzzwords thrown around to make it sound smart (although mostly correct nonetheless.)

Now, your "vulnerabilities and attacks one can perform."

This is the first thing that is downright wrong. You say "vulnerabilities" in the sentence/header, but none of these are vulnerabilities. True they can arguably be attacks but still, not necessarily. Specify what tampering is, what do you mean by tampering? Like tampering with data on a server? Tampering with server sided code to help you make a backdoor? Tampering with hardware? Specify. This one isn't even necessarily an attack, just something that someone could do, with malicious or non-malicious intent.

Next up, Phishing.

Oh, actually, while we're at it, let's include Social Engineering. Because these are the exact same fucking thing.

Social Engineering is neither an attack nor a vulnerability. It is a concept which includes sociology/psychology to help you get someone to do something for you. I could social engineer my friend to let me have a slice of the pizza he just bought. I could also social engineer a multimillion dollar company to install a backdoor onto their main database servers. It can be used for an attack, but it's not an attack unto itself.

Phishing is a subset of social engineering. Instead of getting my friend to let me have a slice of pizza, I'm trying to get a user to give me their login credentials. I'm not going to go into it as it's a bit of a taboo subject on these forums, but whatever. It's still social engineering, and it's piss easy.

Now, again, next thing that's wrong. The way you noted whether something is whitehat or blackhat.

This tells me right away that you have zero clue what you're talking about. I want you to think about this for a second. How are whitehat hacking and blackhat hacking any different from one another? Protip: There is literally none. Blackhats don't use some kind of secret tools that whitehats can't. Whitehats aren't in any way inferior to blackhats. Greyhats are just people that have weird motives. The hat is only the motive. Green hats go where the money is. Redhats are biased towards only hacking linux systems (okay that was a shitty joke.) But you get the idea. A whitehat might use phishing to get an employees credentials while performing a pentest, as long as the employer gives them permission. Everything applies to everything, hats don't matter with techniques used.

Now, your link to a wikipedia page for a list of vulns/attacks is extremely shitty. And while I'm talking about it, I'm going to mention your "where to learn" sites, which you described as spoonfeeding.

First of all, giving a link to lmgty and cybrary isn't spoonfeeding. It's still up to the user to learn about stuff. It's not like you're giving them a script they can use, putting it in their hand and giving them an exact command to let them do what they want. That's spoonfeeding. Telling someone to go learn from cybrary is not.

Now, back to wikipedia. Clearly you haven't heard of OWASP. Here:

https://www.owasp.org/index.php/Main_Page

Look at the sidebar, there's even a hotlink to finding a list of all common/uncommon attacks in the last 40yrs or whatever.

Wikipedia is literal shit-tier, I don't want you using it or linking it ever again.

I'm only like a tenth of the way into this and I'm already doubting any credibility you had.

Staying Safe:

Okay, okay. Second line, already a problem. Telling people to make sure a VPN doesn't keep logs is kinda memey again, because all VPNs keep logs. Wait, what's that, they don't? Really? Well how would they debug their services or ever do maintenance on the servers if they didn't log any errors/timestamps for start/stop/whatever? Exactly, you're wrong again. ALL VPNS LOG. MAKE SURE THEY DON'T LOG ACTIVITY!!! Also, make sure they don't comply with DMCA and other takedown requests and are based offshore, so outside America.

Given the fact that you still haven't actually explained anything yourself so far, I don't think you know anything about anything, let alone proxies.

Okay, rest of the list is fine, nothing wrong with that, now, your VPN recommendations:

PIA may seem like a good choice because it's a low cost, has decent encryption and claims to not log activity (you can never be 100% sure) but the main problem I have with them lies in their ToS. They do respond to law enforcement and cooperate heavily with them. I don't like that. I would stay away. As for Dicta, never personally used them and I'm not going to read through their entire PP and ToS just for this, but they might be alright. I personally use [censored], they're really good, mailing address is in Panama for christ's sake. Mullvad and nvpn are both good options as well.

You shouldn't have to recommend proxies, especially since many of them die within hours. Educate yourself on that though, definitely more to it than most people think, it's much deeper than "hurr durr, hide my ip im a hack3r"

Veracrypt, I'm glad you just linked the official documentation. It's pretty solid and straightforward. But I would probably create a container for any sensitive files, rather than encrypt your drive with it. For your drive, if you're on Windows, bitlocker will be more than enough. Although sure, Vera is pretty damn good too, also since they went through the audit.

Firefox is good too because open source and all that bullshit, but Icecat is a fork of it that's much better. I would suggest putting that up there too. Also thanks for citing PKA... for the flags in the config. Damn, you know how to cite people, I've seen so many people just blatantly copy/paste. Fuck it, you're getting +3 from me anyway just for all those citations, even if this guide is terribad.

It's good that you included some plugins, but yeah, you missed a lot. Don't worry, the ones you listed are fine, but there are some other good ones.

Tools:

Oh man, you're just listing common ones from Kali or whatever. Although they're good, at least give a brief description of what it does/what it's for. Come on, explain something in this damn guide.

ESET is a good AV but there are other good ones too, bitdefender, mwb, the list goes on. Maybe add some free ones too (specify that they're free) for people that are on a budget.

For firewalls, that's pretty good. Honestly it doesn't get much better than those two, but I'd also like to include Peerblock. Open source, blocks everything, it's not really for anonymity, but you'd be surprised how much shit is constantly trying to connect to your PC at all time. Give it a shot, it's worth your time.

Programming:

Oh god no, make it stop. Delete this right now. This is almost insulting to me. Just kidding, but you did horribly for this section. Hint hint: Look at the guide I wrote for this, link it if you want.

<https://hackforums.net/showthread.php?tid=5468505>

Niches?:

I'm 99.99% sure tutorial writing and ebook writing has absolutely nothing to do with hacking. Also graphic design and SEO (even blackhat SEO)

This section is just about useless, remove it.

It's more of a finding an HF niche rather than the entire point of your guide. Would have been better to have listed fields of hacking at the end, like webpen, system pen, exploit development, reverse

engineering, etc.

In Conclusion:

Please stop. It hurts.

It's past midnight, I should sleep.

I didn't even go through all the spelling/grammar mistakes.

There are much better guides, no need to rewrite anything, especially if it's gonna be this bad in comparison. Better to just bump the other threads.

Have a nice day.

Trinity - January 25, 2017, 3:49 am

(Jan 24, 2017 08:42 PM)Faith Connors Wrote: [\[CITE\]](#) Please stop. It hurts.

It's past midnight, I should sleep.

I didn't even go through all the spelling/grammar mistakes.

There are much better guides, no need to rewrite anything, especially if it's gonna be this bad in comparison. Better to just bump the other threads.

Have a nice day.

Thank you for this, i will edit the thread. However, I am Here to learn as the rest of you... all you insult me over and over again, i fail to see how this would improve my thread or confidence in what im doing, for that matter? you do however also give me a small amount of credit, thank you... yes my english writeing is horrible i know, unfortunately i was not so lucky to end up on the bus that said "fit for school" so i have learned what i have by teaching my self. Wich is pretty impressive if you think about it.

EDIT: i like to get postive feedback, and not saying anything bad about previous comments, but this is actually more inspireing to read, since it dosent just says "good tutorial" or something like that.

Regards EngLen ?

yayimamember - January 25, 2017, 4:32 am

Your hat seems rather blue

zSecurity - January 26, 2017, 3:18 am

(Jan 25, 2017 05:32 AM)yayimamember Wrote: [\[CITE\]](#) Your hat seems rather blueyou mean gray?