

Forum: [Hack Forums](#)

Thread: [rename pentesting and forensics](#)

apt1337 - December 12, 2020, 1:17 am

Hi, I'm making this suggestion in hopes to wake up that section a little bit and make it more high quality, I think you should consider renaming pentesting & forensics to "information security" or "Infosec" as both of these fields are fields within infosec, I think giving it this name would deter some of the low quality "looking for ddos" or "hiring hacker for deface" posts and attract the people that are actually in these two fields. There is a lack of soc analysts and pentesters in that section, there is a few that are genuine posts but there is alot that are just entirely unrelated, I think calling it "informaiton security" is accurate and would wake it up abit, just a suggestion.

I found this thread actually and I agree with the OP of this thread, it seems other posters also agree.

<https://hackforums.net/showthread.php?tid=6093919>

Also this one, <https://hackforums.net/showthread.php?tid=6084952>

A second suggestion but still related, is to move it from "advanced hacking" to it's own sub-forum under the "hacking" section called "Information Security", and then move bug bounty and whitehat into it as these are also fields within InfoSec.

Features - December 12, 2020, 3:57 am

Just trying to understand, how will this wakeup the legitimate serious users? I don't think it would increase the amount of HQ users there by changing that name.

Would it? why?

apt1337 - December 12, 2020, 4:58 am

(Dec 12, 2020 04:57 AM)Features Wrote: [\[CITE\]](#) Just trying to understand, how will this wakeup the legitimate serious users? I don't think it would increase the amount of HQ users there by changing that name.

Would it? why?

Because first of all, information security isn't a name that will attract skids, it's too boring and it has "security" in the name, that will deter the LQ posters because they just want to do illegal stuff and say stupid things like "how to hack ip" or "how to deface website".

That isn't what these fields are about, there is no grey area, penetration testing is a legal and very advanced security field within infosec, and I didn't actually say the words "HQ users" I think that's too generalizing, not just any "HQ users", I meant it will attract information security professionals and information security related posts because that's the field their lives revolve around.

Also pentesting and forensics are literally fields within infosec, infosec is the correct term for the field, so it makes sense. Most people think these fields are just things within "cyber security", but infact information security is an advanced field within cyber security, and penetration testing is an advanced field within information security. Their names currently attract alot of people that don't actually know that these are security fields, which is why we get posts like "paying hacker to hack

chinese casiono \$10,000" and then you view the post and its someone with 3 posts that clearly just wants to do illegal stuff.

Features - December 12, 2020, 6:20 am

(Dec 12, 2020 05:58 AM)size_t Wrote: [\[CITE\]](#) Because first of all, information security isn't a name that will attract skids, it's too boring and it has "security" in the name, that will deter the LQ posters because they just want to do illegal stuff and say stupid things like "how to hack ip" or "how to deface website".

That isn't what these fields are about, there is no grey area, penetration testing is a legal and very advanced security field within infosec, and I didn't actually say the words "HQ users" I think that's too generalizing, not just any "HQ users", I meant it will attract information security professionals and information security related posts because that's the field their lives revolve around.

Also pentesting and forensics are literally fields within infosec, infosec is the correct term for the field, so it makes sense. Most people think these fields are just things within "cyber security", but infact information security is an advanced field within cyber security, and penetration testing is an advanced field within information security. Their names currently attract alot of people that don't actually know that these are security fields, which is why we get posts like "paying hacker to hack chinese casiono \$10,000" and then you view the post and its someone with 3 posts that clearly just wants to do illegal stuff.

I kinda thought so just curious. Yes that is annoying.

Poet - December 12, 2020, 6:34 am

People will post low quality anywhere on the forums and changing the name will do no good.

Features - December 12, 2020, 6:48 am

(Dec 12, 2020 07:34 AM)WhiteHack Wrote: [\[CITE\]](#) People will post low quality anywhere on the forums and changing the name will do no good.
Thats unfortunate.

tsuki - December 12, 2020, 7:53 am

(Dec 12, 2020 05:58 AM)size_t Wrote: [\[CITE\]](#) Because first of all, information security isn't a name that will attract skids, it's too boring and it has "security" in the name, that will deter the LQ posters because they just want to do illegal stuff and say stupid things like "how to hack ip" or "how to deface website".
It will.

Pentesting & Forensics founds far less "skiddish" than infosec, particularly since it's more specific.

(Dec 12, 2020 05:58 AM)size_t Wrote: [\[CITE\]](#) infact information security is an advanced field within cyber security

You mean the other way around. Information security encompasses the area of physical security too, which is unrelated to cyber security.

webdev77 - December 12, 2020, 9:51 am

This doesn't even make sense to me. Information security is not the same as digital forensics.

apt1337 - December 12, 2020, 12:30 pm

(Dec 12, 2020 10:51 AM)webdev77 Wrote: [\[CITE\]](#) This doesn't even make sense to me. Information security is not the same as digital forensics.

So information security is a category name that is used to group multiple fields of work, cyber security is the same it's another category and refers to a group of different types of fields that are

related but fall within the cyber security, digital forensics and penetration testing are two fields that fall within information security. The reason they're both within "information security" is because they revolve around securing information, digital forensics for example is not just reviewing security breaches and looking for evidence, it also involves securing digital crime scenes and helping put protections in place in order to prevent further attacks / future attacks.

https://en.wikipedia.org/wiki/Information_security

(Dec 12, 2020 08:53 AM)tsuki Wrote: [\[CITE\]](#) It will.

Pentesting & Forensics sounds far less "skiddish" than infosec, particularly since it's more specific.

You mean the other way around. Information security encompasses the area of physical security too, which is unrelated to cyber security.

I never said pentesting and forensics sound skiddish, I said it attracts people that are not in either fields, you failed to address why there are dumb threads in there, if it's not related to the name of the section then can you explain it for us? I would say the word "security" would deter people looking for crime specifically, do you not agree with that logic? Explain why you disagree. I think it will make a difference personally, even if it's not massive.

No I didn't mean the other way around, while you might be right with cybersecurity being a subset of information security, both pentesting and forensics are within information security, these terms are fluid, and I fully disagree that all physical engagements are unrelated to cyber security, specifically when the physical security assessment is a penetration test.

<https://www.redteamsecure.com/services/penetration-testing/physical-penetration-testing/> but I agree that physical security at least where it overlaps with the protection of information and business assets falls under InfoSec. Regardless of whether information security is within cyber security - some people would argue that infosec and cybersec are the same thing - that's not the point at all, both penetration testing and digital forensics are fields of work within the information security field, I'm sure we both agree on that.

Kriptik - December 12, 2020, 1:35 pm

This will not change much imo, people with good skills in infosec will not come to HF already knowing it's reputation (by this I mean that they know there are a lot of skids around here) why would they want to share their knowledge knowing it might end up in the wrong hands (all those skids around here).

Also people who are serious about getting into infosec will learn on their own and not share information they learned, why? Because that is what infosec is about, you do your own research and find the information you need. Nobody is willing to feed you, you gotta go out there and do your due diligence.

There is no easy way to become a real hacker and I think people should stop immediately if they are looking for easy ways, there is no easy way. period.

apt1337 - December 12, 2020, 1:59 pm

(Dec 12, 2020 02:35 PM)RedPillMTX Wrote: [\[CITE\]](#) This will not change much imo, people with good skills in infosec will not come to HF already knowing it's reputation (by this I mean that they know there are a lot of skids around here) why would they want to share their knowledge knowing it might end up in the wrong hands (all those skids around here).

Also people who are serious about getting into infosec will learn on their own and not share information they learned, why? Because that is what infosec is about, you do your own research and

find the information you need. Nobody is willing to feed you, you gotta go out there and do your self diligence.

There is no easy way to become a real hacker and I think people should stop immediately if they are looking for easy ways, there is no easy way. period.

I disagree there are pentesters on here, I'm a junior pentester myself, and I'm more than willing to share and discuss things within the field, because there are probably people way more experienced than me on here that I can learn from, and because what I know might also help others, infact I'm going to do a writeup series on exploit development in that section soon. Not only for others but also explaining concepts to other people helps me learn that subject alot more.

You're wrong about this for a few reasons:

1. Skids are unable to comprehend what we're talking about without a good enough technical foundation to understand, if a skid can understand a writeup on kernel exploit development then I would say he's not really a skid. Infact I would say if a skid can follow along with a writeup like that, then that's great, he will learn something valuable from it.
2. Why won't they use it for bad things? The amount of security mitigations will prevent them from replicating exploit development writeups in the real world, they will have to bypass DEP, KASLR, CFG to name a few. This isn't something a skid can do, infact even the majority of professionals within infosec (including myself) would seriously struggle bypassing the modern mitigations (not DEP or ASLR but things like CFG) unless they're specializing in this kind of security research.
3. People who are serious and in infosec do their own research, but you're wrong again here because there are thousands and thousands of research papers on vulnerabilities, thousands of blogs and writeups, you won't be spoonfed information you're right, but that doesn't mean you don't discuss anything you learnt. Why do you think things like defcon and blackhat conference exist?
4. Writeups, discussion, blogs, etc. all help in the learning process.
5. If people didn't share the information they learned, can you explain how people do there own research without any resources to learn from? There would be no infosec at all if that was the case.

There is no easy way that's probably the only thing I agree with, it's an advanced field, but that doesn't mean conversation is closed, I'm in plenty of groups and have lots of friends within this field that I talk to everyday.

Kriptik - December 12, 2020, 2:20 pm

(Dec 12, 2020 02:59 PM)size_t Wrote: [\[CITE\]](#) I disagree there are pentesters on here, I'm a junior pentester myself, and I'm more than willing to share and discuss things within the field with beginners, infact I'm going to do a writeup series on exploit development in that section soon.

You're wrong about this for a few reasons:

1. Skids are unable to comprehend what we're talking about without a good enough technical foundation to understand, a skid can understand a writeup on kernel exploit development then he's not really a skid. Infact I would say if a skid can follow along with a writeup like that, then that's great, he will learn something valuable from it.
2. Why won't they use it for bad things? The amount of security mitigations will prevent them from replicating exploit development writeups in the real world, they will have to bypass DEP, KASLR, CFG. This isn't something a skid can do, infact it isn't something the majority of professionals within

infosec can do.

3. People who are serious and in infosec do their own research, but you're wrong again here because there are thousands and thousands of research papers on vulnerabilities, thousands of blogs and writeups, you won't be spoonfed information but that doesn't mean you don't discuss anything you learnt. Why do you think things like defcon and blackhat conference exist?

4. Writeups, discussion, blogs, etc. all help in the learning process.

5. If people didn't share the information they learned, can you explain how people do their own research without any resources to learn from? There would be no infosec at all if that was the case.

There is no easy way that's probably the only thing I agree with, it's an advanced field, but that doesn't mean conversation is closed, I'm in plenty of groups and have lots of friends within this field that I talk to everyday.

Don't get me wrong but I didn't really mean to say people in the infosec field won't/should not discuss what they learned, just saying that they won't be sharing it on forums like HF knowing the amount of people that are not serious about it. They rather share this information on Defcon conferences and other sites.

Now I am not completely against sharing information with people, it's just that some people will use that knowledge for illegal activities and I think that's why such information should be hard to find. Nowadays you could find this information very easy on the internet and I think (this is my own opinion) it should not be the case. It's okay to give an explanation at a high level, but don't share every detail. Don't simplify the life of every John Doe around the internet, is all I'm saying.

apt1337 - December 12, 2020, 2:49 pm

(Dec 12, 2020 03:20 PM)RedPillMTX Wrote: [\[CITE\]](#) Don't get me wrong but I didn't really mean to say people in the infosec field won't/should not discuss what they learned, just saying that they won't be sharing it on forums like HF knowing the amount of people that are not serious about it. They rather share this information on Defcon conferences and other sites.

I understand what you mean, which is one of the reasons I've taken the time to write this thread because I wanted to help improve that section because I know that people that know what they're doing are more likely to post there if there is less of the trollish posts, I mean it's not going to solve the problem 100% but I think having a name like cyber security or information security would atleast help.

I don't think people that are not in the field will understand a word we're saying, for example, even with the most simple basic EIP overflow it will just be another language to the majority of people lol, "first we send a bunch of incrementing bytes to overflow the input functions buffer to write data onto the stack, then we need to find the EIP offset and take control of the EIP register, then we need to follow dump in ESP and find bad chars in memory, then we need to overwrite the EIP register with a specific controlled address so we can control what gets executed within the program, then we need add a nop sled to prevent some bytes of the shellcode being mangled on the stack." etc. they're not going to understand what any of that means, and even if they do, all that is going to happen is they will learn what a simple buffer overflow is, probably learn alot about memory which is a good thing.

My final words to the mods / admins, I don't think that changing the name is the absolute solution, just a suggestion that could look more appealing to people in these fields of work, and to deter the people that have no actual interest in those topics, especially people looking to do illegal things because they're probably scared of anything related to "cyber security" if they're criminals.

Consider grouping these topics into another subforum titled "cyber security" or "information

security", "ethical hacking" etc whichever you prefer, and then have "pentesting", "forensics", "Bug bounty", "whitehat", under this subforum to keep tsuki happy with specific names ;) finally, if there were more people active in that section I think it would actually have a really good influence on people that are leaning towards bad things on here, and it could also be very educational for people that are genuinely interested in this stuff.

tsuki - December 12, 2020, 4:27 pm

(Dec 12, 2020 01:30 PM)size_t Wrote: [\[CITE\]](#) you failed to address why there are dumb threads in there, if it's not related to the name of the section then can you explain it for us?

If we want to attract higher quality members to HF, we need to specialize and rename threads like "Malware & Viruses" to "Malware Research & Analysis", rather than generalize as you suggest. Competent infosec people will search "malware research" on google, but they're not going to search "best rat crypter", for example.

I also think it would be a good idea to have a "Frequently asked questions" stickied thread in each section and to restrict all new users with less than 50 posts from creating threads, until they read the sticky or something.

This would at least prevent all of the trash threads made by people with only 1 post who never show up on HF again after making their thread.

(Dec 12, 2020 01:30 PM)size_t Wrote: [\[CITE\]](#) I would say the word "security" would deter people looking for crime specifically, do you not agree with that logic? Explain why you disagree. I think it will make a difference personally, even if it's not massive.

Since you mentioned being a junior pentester, I'm sure you've heard of the OSCP certification. OS in it stands for "offensive security", which is a common term too. So security doesn't necessarily imply ethical.

apt1337 - December 12, 2020, 4:37 pm

(Dec 12, 2020 05:27 PM)tsuki Wrote: [\[CITE\]](#) If we want to attract higher quality members to HF, we need to specialize and rename threads like "Malware & Viruses" to "Malware Research & Analysis", rather than generalize as you suggest. Competent infosec people will search "malware research" on google, but they're not going to search "best rat crypter", for example.

I also think it would be a good idea to have a "Frequently asked questions" stickied thread in each section and to restrict all new users with less than 50 posts from creating threads, until they read the sticky or something.

This would at least prevent all of the trash threads made by people with only 1 post who never show up on HF again after making their thread.

Since you mentioned being a junior pentester, I'm sure you've heard of the OSCP certification. OS in it stands for "offensive security", which is a common term too. So security doesn't necessarily imply ethical.

Yea I definitely agree with that, I still think they should actually have a dedicated section to all of these topics under the name "Information security" or "cyber security", like the "whitehat" section is under "tech" I'm not really sure why that's there, if they make a subforum with one of these titles they can throw a bunch of other stuff in there like "malware research" and other interesting things, I think that's a really good idea. The ideas you suggested are amazing especially the frequently asked questions thread, this will definitely clean up the forum and make things high quality along with the extra topics, I guess your thinking is that they will be indexed on search engines and attract traffic from the infosec field, these would be pretty big changes and I think they will attract alot of high quality people.

Yea ofcourse I know offsec, actually I'm a student at offsec and plan on taking the new "Offensive Security Exploit Developer" course when it comes out I'm pretty excited for that, I intend to take that as a stepping stone to OSEE. I know exploit development is abit of a grey area for jobs unless 0day research but it's just something I'm passionate about :_