

Forum:[Hack Forums](#)

Thread: [how many types of hacking "hats" are there?](#)

mrhack - February 2, 2018, 1:49 pm

I've seen the "white hat", "black hat" and "red hat" terms. Are there more or only those 3 matter? What are the differences between those types of "hats" other than color?

virus - February 2, 2018, 1:52 pm

1: Script Kiddie

Script Kiddies normally don't care about hacking (if they did, they'd be Green Hats. See below.). They copy code and use it for a virus or an SQLi or something else. Script Kiddies will never hack for themselves; they'll just download overused software (LOIC or Metasploit, for example) and watch a YouTube video on how to use it. A common Script Kiddie attack is DoSing or DDoSing (Denial of Service and Distributed Denial of Service), in which they flood an IP with so much information it collapses under the strain. This attack is frequently used by the "hacker" group Anonymous, which doesn't help anyone's reputation.

2: White Hat

Also known as ethical hackers, White Hat hackers are the good guys of the hacker world. They'll help you remove a virus or PenTest a company. Most White Hat hackers hold a college degree in IT security or computer science and must be certified to pursue a career in hacking. The most popular certification is the CEH (Certified Ethical Hacker) from the EC-Council.

3: Green Hat

These are the hacker "n00bz," but unlike Script Kiddies, they care about hacking and strive to become full-blown hackers. They're often flamed by the hacker community for asking many basic questions. When their questions are answered, they'll listen with the intent and curiosity of a child listening to family stories.

4: Blue Hat

If a Script Kiddie took revenge, he/she might become a Blue Hat. Blue Hat hackers will seek vengeance on those who've them angry. Most Blue Hats are n00bz, but like the Script Kiddies, they have no desire to learn.

CyberStrike - February 3, 2018, 2:40 am

(Feb 2, 2018 02:49 PM)mrhack Wrote: [\[CITE\]](#) I've seen the "white hat", "black hat" and "red hat" terms. Are there more or only those 3 matter? What are the differences between those types of "hats" other than color?

Imagine the old cowboy days, at least according to the movies.. the good guys wore white hats and bad guys wore black hats, and the women usually wore the red hats...seriously though "red hat" is a distro of linux. There is considered to be a grey hat as well which is just kinda not really true.

And about " The most popular certification is the CEH (Certified Ethical Hacker) from the

EC-Council." it is far from what a professional actually needs they pretty much bottle feed everything to you, and it is based on very outdated material. If anything it's about as close to a legal scam as there can be. Whatever you guys do stay away from it, also you don't "need" a certificate to be a pentester or jr pentester, that is a requirement for the funny broken companies that don't have a clue on the baseline of what a pentesting job entails . These are the same companies that require a "pentester" to have a CS degree and all these great things such as CEH/SaST/DaST and about 3 years of previous pentesting experience, meanwhile they literally have logs that print shit like "alsadmin:alsadmin" in cleartext and public facing. The brilliant people who required all this are a large corporation worth over 34 billion dollars. Those CS degrees and a CEH and DaST/SaST experience for 3 years of pentesting was probably him watching porn because they are piss poor.

DemonCyclops - February 3, 2018, 2:42 am

There is the ultimate hacker which has the rainbow hat you need to be partly gay or lesbian to have it tho

SysAdmin - February 3, 2018, 9:50 am

(Feb 3, 2018 03:40 AM)sirru5h Wrote: [\[CITE\]](#) Imagine the old cowboy days, at least according to the movies.. the good guys wore white hats and bad guys wore black hats, and the women usually wore the red hats...seriously though "red hat" is a distro of linux. There is considered to be a grey hat as well which is just kinda not really true.

And about " The most popular certification is the CEH (Certified Ethical Hacker) from the EC-Council." it is far from what a professional actually needs they pretty much bottle feed everything to you, and it is based on very outdated material. If anything it's about as close to a legal scam as there can be. Whatever you guys do stay away from it, also you don't "need" a certificate to be a pentester or jr pentester, that is a requirement for the funny broken companies that don't have a clue on the baseline of what a pentesting job entails . These are the same companies that require a "pentester" to have a CS degree and all these great things such as CEH/SaST/DaST and about 3 years of previous pentesting experience, meanwhile they literally have logs that print shit like "alsadmin:alsadmin" in cleartext and public facing. The brilliant people who required all this are a large corporation worth over 34 billion dollars. Those CS degrees and a CEH and DaST/SaST experience for 3 years of pentesting was probably him watching porn because they are piss poor. CEH is a Go to if you want to get hired while starting in Pentesting, because companies actually think it's a great certification, which is not true. I'd much rather head onto OSCP, even if it is more expensive than the CEH.

CyberStrike - February 3, 2018, 6:04 pm

(Feb 3, 2018 10:50 AM)SysAdmin Wrote: [\[CITE\]](#) CEH is a Go to if you want to get hired while starting in Pentesting, because companies actually think it's a great certification, which is not true. I'd much rather head onto OSCP, even if it is more expensive than the CEH.

+1 I am not a fan of EC Council, there attitude and how they present themselves just turns me off. OSCP is a much more get you ready for the real world. Although yeah CEH is a "baseline" cert in many of these companies and especially internationally it is the cert to have I helped a guy in India with prepping for the OSCP and now he is having trouble finding a job .. recruiters in India (I checked with a few there which I know) pretty much never heard of it ? ?

Ben Shapiro - February 3, 2018, 6:07 pm

Red hat, is also referring to 'red wings'. It occurs when you eat out a women while she's on her period.

Black hat, also known as a fedora, is where a guy has never even eaten out a girl let alone earned his red wings/hat.

Baud - February 4, 2018, 4:59 am

(Feb 2, 2018 02:52 PM)YTCRACKER Wrote: [\[CITE\]](#) 3: Green Hat

These are the hacker “n00bz,” but unlike Script Kiddies, they care about hacking and strive to become full-blown hackers. They’re often flamed by the hacker community for asking many basic questions. When their questions are answered, they’ll listen with the intent and curiosity of a child listening to family stories.

4: Blue Hat

If a Script Kiddie took revenge, he/she might become a Blue Hat. Blue Hat hackers will seek vengeance on those who’ve them angry. Most Blue Hats are n00bz, but like the Script Kiddies, they have no desire to learn.

Never heard of these two definitions before. Both categories exist but they’re not as standardized as white, black, and grey hats. As far as my knowledge goes green hats are bug hunters, they find vulnerabilities to get paid. Blue hats on the other hand are those who have the job of keeping a network secure and have to take care of incident response. If white hats attack for good, blue hats build and maintain defences.

OP, red hats don't exist, Red Hat is a Linux distro. At least I hope they don't exist, there are so many hats now that we are only missing a pink, purple, and rainbow one.

Nomad.Null - February 4, 2018, 9:19 am

In hope of actually answering this question and setting aside all the sarcastic responses...

White Hat: Commonly refers to security administrators, network security, and ethical hackers. Specifically, it contrasts the definition of a black hat. White hat typically identifies penetration testers who attempt to improve the security of systems by identifying and exploiting vulnerabilities and responsibly reporting them to the owner of that system.

Black Hat: A criminal hacker or someone who engages in illegal computer crime. Simple as that.

Grey Hat: An ambiguous definition that can either refer to

a.) Someone who hacks as a hobby but engages in neither criminal nor professional, ethical hacking

b.) Someone pursues bug bounties and works freelance as a penetration tester.

Some may tell you that a grey hat is someone who does both criminal and professional hacking, but anyone that engages in criminal activity is a criminal and therefore a black hat. There is no gray area in that regard.

Red Hat: Also refers to security professionals, but typically focuses strictly on network security and domain administrators, especially those with experience in Linux.

Blue Hat: Not all that common to hear, but these are security professionals that focus on debugging, patching, and improving the security of existing controls and applications. As opposed to a white/red hat which will try to identify and exploit weaknesses in systems, blue hats focus entirely on actually fixing vulnerabilities.

In reality, very little of this matters and has no bearing on how much you learn. As long as you don't break into people's computers, and you learn in an ethical manner, you'll probably be fine. Don't worry about titles or labeling yourself.

[BLANK] - February 4, 2018, 10:26 am

Maybe some mixup between hats and teams. White hat hacks legally, black hat does illegal hacking. I don't really believe in Gray hat, because illegal is illegal regardless of intention.

Then there are security teams. Red team focus is offensive security, Blue team focus on defense security. Purple team combines both.

I also have found that the OSCP has become the baseline cert. Either you have it or are in the process of getting it. Either way it's standard for starting out. Now some positions that call themselves penetration testing but are really just vulnerability analysis may accept the CEH as baseline.

Mad76e - February 4, 2018, 10:33 am
Basically

Its the same set of tools youre using if youre white black or gray.. "The color of the hat" is just a way to describe how the practitioner implement morality, a conscience and how he/she understand right and wrong

Black Hat = 1
White Hat = 2
Grey Hat = 3

There are only 3, and they are blended together in a variety of color scales

Red hat = NO! Thats a linux distro

mrpizzahut - February 5, 2018, 2:38 am

I could have sworn that Blue Hats were Microsoft's internal security team.

Levi - February 5, 2018, 6:00 am

They're all fucking memes and it doesn't matter how you categorise yourself

mrhack - August 25, 2018, 6:51 pm

(Feb 3, 2018 03:40 AM) SilentWatch Wrote: [\[CITE\]](#) Imagine the old cowboy days, at least according to the movies.. the good guys wore white hats and bad guys wore black hats, and the women usually wore the red hats...seriously though "red hat" is a distro of linux. There is considered to be a grey hat as well which is just kinda not really true.

And about " The most popular certification is the CEH (Certified Ethical Hacker) from the EC-Council." it is far from what a professional actually needs they pretty much bottle feed everything to you, and it is based on very outdated material. If anything it's about as close to a legal scam as there can be. Whatever you guys do stay away from it, also you don't "need" a certificate to be a pentester or jr pentester, that is a requirement for the funny broken companies that don't have a clue on the baseline of what a pentesting job entails . These are the same companies that require a "pentester" to have a CS degree and all these great things such as CEH/SaST/DaST and about 3 years of previous pentesting experience, meanwhile they literally have logs that print shit like "alsadmin:alsadmin" in cleartext and public facing. The brilliant people who required all this are a large corporation worth over 34 billion dollars. Those CS degrees and a CEH and DaST/SaST experience for 3 years of pentesting was probably him watching porn because they are piss poor.

Speaking of the CEH, it's the one my local community college is either fond of or has a "deal" with so the school (for profit) can "run" the certification course and look legitimate (maybe they are?). Not sure if I should shell out over \$1K for a 6 week course?

Certification exam cost an additional \$950.

Publications required are:

Guide to Networking Essentials; Tomsho; ISBN1-305-10543-5; \$207.95

Certified Ethical Hacker (CEH); Gregg; ISBN 978-0-7897-5127-0; \$59.99

Couldn't I just self study these books (or other better books) and skip school and take the \$950 certification exam on my own or must I need to show the CEH that I went to a training facility for nothing?

Also, who sells these books for less?

vagabond - August 25, 2018, 6:54 pm

i wear an orange hat cuz i have swag

CyberStrike - August 25, 2018, 6:56 pm

(Aug 25, 2018 06:51 PM)mrhack Wrote: [\[CITE\]](#) Speaking of the CEH, it's the one my local community college is either fond of or has a "deal" with so the school (for profit) can "run" the certification course and look legitimate (maybe they are?). Not sure if I should shell out over \$1K for a 6 week course?

Certification exam cost an additional \$950.

Publications required are:

Guide to Networking Essentials; Tomsho; ISBN1-305-10543-5; \$207.95

Certified Ethical Hacker (CEH); Gregg; ISBN 978-0-7897-5127-0; \$59.99

Couldn't I just self study these books (or other better books) and skip school and take the \$950 certification exam on my own or must I need to show the CEH that I went to a training facility for nothing?

Also, who sells these books for less? You gotta have previous experience to just come in and take the test, I think in full with the voucher you are looking at like 1800 -1900.. generally EC council runs a "Boot camp" 5 days there are other courses which they hold I am familiar with the bootcamp option because at my previous employer an intern had just finished it. Check around a bit I'll post a few links just gotta find em .

mrhack - August 25, 2018, 7:40 pm

(Aug 25, 2018 06:56 PM)SilentWatch Wrote: [\[CITE\]](#) You gotta have previous experience to just come in and take the test, I think in full with the voucher you are looking at like 1800 -1900.. generally EC council runs a "Boot camp" 5 days there are other courses which they hold I am familiar with the bootcamp option because at my previous employer an intern had just finished it. Check around a bit I'll post a few links just gotta find em .

I guess the exam through the school is \$950...

Is this even a worthy certification that gets me hired or the pen testing one someone else suggested to me, like a 24 hour certification online. I think this one by CEH includes a lot of different things including pen testing?

CyberStrike - August 25, 2018, 7:50 pm

(Aug 25, 2018 07:40 PM)mrhack Wrote: [\[CITE\]](#) I guess the exam through the school is \$950...

Is this even a worthy certification that gets me hired or the pen testing one someone else suggested to me, like a 24 hour certification online. I think this one by CEH includes a lot of different things including pen testing?

I am biased I won't lie CEH is considered as "entry" level, like any other cert it will help get you interviews, of course if you are experienced and can do hands on stuff it will help your chances.

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>

<https://cert.eccouncil.org/certified-ethical-hacker.html>

Quote:To be eligible to apply to sit for the CEH (ANSI) Exam, a candidate must either:

Hold a CEH certification of version 1 to 7,

* (Prior to being ANSI accredited, EC-Council's certifications were named, based on versions – CEHV1, CEHV2 etc. During that time, candidates that attempted the certification exams were vetted for eligibility. In order to avoid "being double bill", the EC-Council Certification department shall issue a waiver of the application fee of any candidate that has a CEH V1- CEH V7 certification and wishes to attempt the CEH ANSI certification.)

or Have a minimum of 2 years work experience in InfoSec domain (You will need to pay USD100 as a non-refundable application fee);

Or Have attended an official EC-Council training (All candidates are required to pay the \$100 application fee, however your training fee shall include this fee)

Note:

As various consumer laws across the world to prohibit any type of "price fixing", EC-Council Certification department is unable to prescribe minimum pricing for its exams. This allows a free market approach which benefits our certification community.

As the price of an exam vouchers is many times bundled with official training by our accredited partners, the price may vary depending on the region, training facilities, training partner, the trainers experience, cost of proctoring the exam and even the mode of training of the partner.

It is imperative that we make it clear that no student shall be deemed to have any added advantage whatsoever from one mode of training to another in order to challenge the CEH ANSI exam as the exam is a standard exam for everyone, regardless of the method of training.

Should any training partner attempt to tell you otherwise, we ask that you lodge an official complaint with the EC-Council certification department so that the necessary action can be taken against the training partner.

mrhack - August 28, 2018, 4:23 pm

is CEH a good start then for me? Or is Kali Linux just better? Isn't certified ethical hacking the same as pen testing?

CyberStrike - August 28, 2018, 5:09 pm

(Aug 28, 2018 04:23 PM)mrhack Wrote: [\[CITE\]](#) is CEH a good start then for me? Or is Kali Linux just better? Isn't certified ethical hacking the same as pen testing?

CEH is pentesting at least hopefully that's what you will be doing. Let me say that if you live somewhere that CEH is like the go to certificate, for example a friend in India has a OSCP he is unable to get hired because they are unfamiliar with OSCP, and to the recruiters CEH is the only thing. The developers of Kali linux do have their own certifications, OSCP and a few others. It

depends honestly on what you are trying to do, if you are looking for work talk with recruiters in the country & company you are looking to work for. Check out job postings, see what is required and what actually gets results aka jobs.

Mr_Bot - August 28, 2018, 5:27 pm

Purple Hat bro.

It's a new hat which have be discover at around 2018-2017

mrhack - September 1, 2018, 1:34 am

I see. So I just need one or the other CEH/pentesting? This is why I had to ask how many types of hats are there or certifications. I guess my local community college preferred CEH due to it being what's sought after in the area? Whereas Kali Linux may be better off elsewhere?

(Aug 28, 2018 05:09 PM)SilentWatch Wrote: [\[CITE\]](#) CEH is pentesting at least hopefully that's what you will be doing. Let me say that if you live somewhere that CEH is like the go to certificate, for example a friend in India has a OSCP he is unable to get hired because they are unfamiliar with OSCP, and to the recruiters CEH is the only thing. The developers of Kali linux do have their own certifications, OSCP and a few others. It depends honestly on what you are trying to do, if you are looking for work talk with recruiters in the country & company you are looking to work for. Check out job postings, see what is required and what actually gets results aka jobs.

CyberStrike - September 1, 2018, 2:02 am

Certifications are not hats (the talk of hats only refers to your ethics, nothing more nothing less, they are just certifications has nothing what so ever to do with hats) .. There are several different certificates for pentesting each with their own certifying body. Colleges tend to be partnered with various corporate sponsors and certifying bodies.

daniterrer - September 4, 2018, 11:38 am

(Feb 2, 2018 02:49 PM)mrhack Wrote: [\[CITE\]](#) I've seen the "white hat", "black hat" and "red hat" terms. Are there more or only those 3 matter? What are the differences between those types of "hats" other than color?Black, white and grey.

I don't know more.