

Forum:[Hack Forums](#)

Thread: [The White-Hat vs Black-Hat Narrative is Wrong](#)

soatok - July 9, 2014, 8:51 pm

The conventional definitions of hackers often separate us into two camps. Hacker versus cracker, white-hat versus black-hat, and so on. If someone claims to be a White Hat, they are saying that they perform penetration tests and vulnerability research for the express purpose of securing systems. They will decry the activities of Black Hat hackers, whom they define as the bad guys who want your credit card numbers and secret futanari porn stash. These dichotomies are not only false, but the descriptions employed are actually harmful to growing as a technologist.

Simply put, hackers are people, and people are far too complex and interesting to compress to a single bit of classification. Most hackers should wear gray.

Let's say you discover a remotely exploitable vulnerability in every operating system on the planet. What do you do?

Keep it to yourself; exploit it for fun and profit.

Sell it to an exploit broker.

Tell Microsoft, Apple, Google, and only large companies, to win their bug bounties.

Discretely report it (via GPG encryption) to people who maintain the vulnerable component, including a PoC and patch. Then, after the fix is rolled out, email the PoC to Full Disclosure.

Discretely report it (via GPG encryption) to people who maintain the vulnerable component, then publish a vague advisory (but not the PoC) to Full Disclosure.

Classically, these practices are labelled respectively:

Black-hat.

Gray-hat, but you're acting in good faith that this exploit will end up in the right hands, so it might as well be white!

White-hat.

White-hat.

White-hat.

The ambiguity in the last three (arguably four) points is precisely the problem I have with the white-hat dichotomy. In reality, these hackers can be described as:

Black-hat.

Money-hungry.

Siding with the rich and powerful.

Reckless attention-whoring.

White-hat.

Furthermore, the dichotomy implies that whitehats and blackhats are enemies. While there is obviously an ideological disagreement between the two camps, the main adversary of a blackhat hacker is a system administrator. Sysadmins assume a defensive posture, but that says nothing about their ethics or arsenal.

In closing, before you call yourself a whitehat, grayhat, or blackhat, think long and hard about what you do and the context you do it in, and maybe consider not labelling yourself as such?

tibia_paly151 - July 9, 2014, 9:30 pm

wow you really thought hard about this haha.. very interesting post though. i get wat ya mean

soatok - July 17, 2014, 10:33 am

(Jul 9, 2014 09:30 PM)tibia_paly151 Wrote: [\[CITE\]](#) wow you really thought hard about this haha.. very interesting post though. i get wat ya mean

Actually, this was a bit of shooting from the hip. I read a lot on the subject in my "youth" :)

Th3PonyWizard - July 17, 2014, 1:08 pm

You're confusing ethics with motives.

soatok - July 17, 2014, 2:23 pm

(Jul 17, 2014 01:08 PM)Th3PonyWizard Wrote: [\[CITE\]](#) You're confusing ethics with motives. That may be true, but it is a historically accurate conflation of the terms.

<http://dsr.segfault.es/stuff/website-mirrors/pHC/old/texts/hack3.txt>

Mad76e - July 22, 2014, 2:31 pm

(Jul 17, 2014 02:23 PM)soatok Wrote: [\[CITE\]](#) ...

(Jul 17, 2014 01:08 PM)Th3PonyWizard Wrote: [\[CITE\]](#) ...

You're both right. Its a question of morale AND greed. there both walking hand in hand

However soatok, there must be more than 5 levels. I see myself as a grayhat, and the reason i think you should add more than 5 in to this is how you see a grayhat. Example. I do 90% whitehat stuff, but i can do if i feel hack the neighbors Wifi and use that instead (and i do once a while), as i can retaliate with just the right amount of force (not DDoS skiddish shit) if someone hurts my closest.

Now I wont touch some of the areas that a black hat does, not even with a fork, even if someone paid me. However im not quite white either and I can penetrate a system and leave it just as it is, just for the thrill of it or like "Yeah, i can still do this shit".

soatok - July 22, 2014, 5:54 pm

(Jul 22, 2014 02:31 PM)mad76e™ Wrote: [\[CITE\]](#) You're both right. Its a question of morale AND greed. there both walking hand in hand

However soatok, there must be more than 5 levels. I see myself as a grayhat, and the reason i think you should add more than 5 in to this is how you see a grayhat. Example. I do 90% whitehat stuff, but i can do if i feel hack the neighbors Wifi and use that instead (and i do once a while), as i can retaliate with just the right amount of force (not DDoS skiddish shit) if someone hurts my closest.

Now I wont touch some of the areas that a black hat does, not even with a fork, even if someone paid me. However im not quite white either and I can penetrate a system and leave it just as it is, just for the thrill of it or like "Yeah, i can still do this shit".The examples I gave are points along a spectrum. As there are infinitely many frequencies in the visible light spectrum and we simplify them down to 5-7 (red, yellow, green, blue, purple-- with the potential addition of {orange,cyan} & indigo), I was expressing significant mile-markers.

Every hacker is a person, every person is subtly different from other people. I wouldn't ever be so arrogant as to believe I can summarize all people with a simple metric derived from my experiences. :)

crazyycast13 - July 22, 2014, 6:31 pm

>GPG encryption

Pretty sure that you meant to say PGP which stands for Pretty Good Privacy

Either way black hats and white hats do a lot of the same things, its just a matter of who they are working for and why they are doing it, which is kinda what you said.

soatok - July 22, 2014, 6:34 pm

(Jul 22, 2014 06:31 PM)crazyycast13 Wrote: [\[CITE\]](#) >GPG encryption

Pretty sure that you meant to say PGP which stands for Pretty Good Privacy

Either way black hats and white hats do a lot of the same things, its just a matter of who they are working for and why they are doing it, which is kinda what you said.I meant the Gnu Privacy Guard (command line: gpg), which is compatible with Pretty Good Privacy. I use the two interchangeably as a consequence of this compatibility.