Forum Donate

Learn to code — free 3,000-hour curriculum

SEPTEMBER 16, 2022 / #ETHICAL HACKING

What are White Hat, Black Hat, and Red Hat Hackers? Different Types of Hacking Explained

Daniel Iwugo

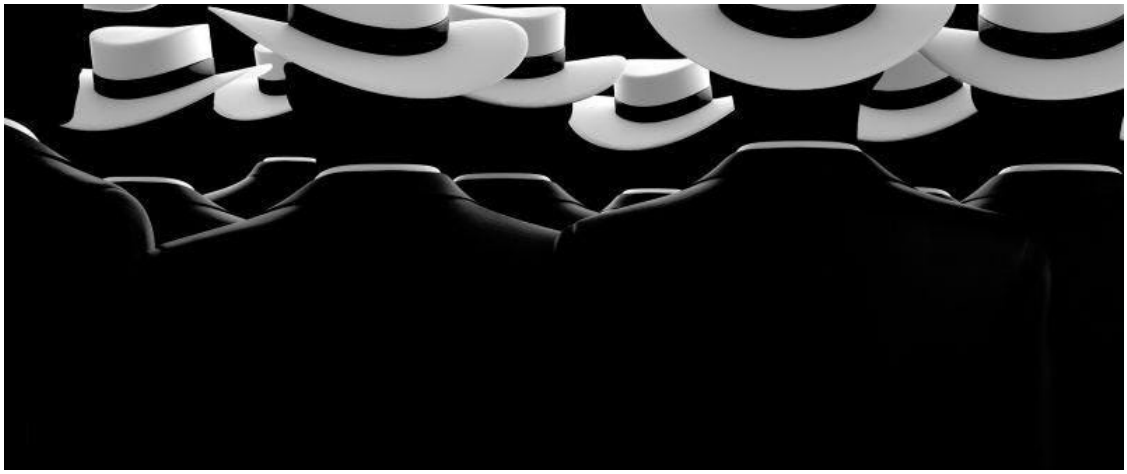
Welcome to the movies, everyone! 🍿 Have you ever heard the term white hat or black hat hacker, and wondered what it means?

Well, in this article, you will learn how hackers are classified by comparing them to a Marvel or DC hero that more or less represents them and what they do.

What is a Hacker?

Forum Donate

Learn to code — free 3,000-hour curriculum



Hats on Silhoettes | Credit: Wallpaperflare.com

A hacker is an individual who uses their skills to breach cybersecurity defences. In the world of Cybersecurity, hackers are typically classified by a 'hat' system. This system likely came from old cowboy film culture where the good characters typically wore white hats and the bad ones wore black hats.

There are 3 major hats in the cyberspace:

1. White Hats
2. Grey Hats
3. Black Hats

However, there are some others that have also cropped up over time such as:

1. Green Hats
2. Blue Hats
3. Red Hats

White Hat Hackers

Captain America | Credit: Wallpaperaccess.com

White hats are just like Marvel's Captain America 🛡️. No matter the day, time, or age, they always stand up for what's right and protect civilians and organizations at large by finding and reporting vulnerabilities in systems before the black hats do.

They usually work for organizations and take roles such as a Cybersecurity Engineer, Penetration Tester, Security Analyst, CISO (Chief Information Security Officer), and other security positions.

Under these organizations they perform tasks such as:

1. Scanning networks
2. Configuring IDSs (Intrusion Detection Systems)

Forum Donate

Learn to code — free 3,000-hour curriculum

4. Programming honeypots (Traps for the attackers 😼)
5. Monitoring network activity for suspicious activity

Famous examples of such hackers include:

1. Jeff Moss (DEF CON founder)
2. Richard Stallman (Founder of the GNU project)
3. Tim Burners-Lee (Creator of the World Wide Web)
4. Linus Torvalds (Creator of Linux)
5. Tsutomu Shimomura (The man that caught Kevin Mitnick)

And if you want to hear more from the founder of a cybersecurity company herself, check out this podcast featuring Rachel Tobac.

Grey Hat Hackers

Batman | Credit: Alphacoders.com

Forum Donate

Learn to code — free 3,000-hour curriculum

unconventional methods to do so.

Grey hat hackers are the balance between white hats and black hats. In contrast to white hats, they do not ask for permission to hack systems but do not perform any other illegal activities like black hat hackers.

Grey hats have quite a controversial history. This makes them hard to really classify, especially if their moral compass goes a little haywire down the line or what they did seems more black hat-ish than white hat-ish. Some even end up in jail for what they do.

But there are some that rise to be the heroes of the people and the enemy of the government and big organizations.

Some (in)famous examples of grey hat hackers are:

1. Anonymous (World famous hacktivist group)
2. HD Moore (Creator of Metasploit)
3. Adrian Lamo (aka the homeless hacker)
4. Khalil Shreateh (Hacked the facebook account of Mark Zuckerburg 🤣)

Black Hat Hackers

Forum Donate

Learn to code — free 3,000-hour curriculum

The Joker | Credit: Wallpapersden.com

Time to introduce the harmful lot 🃏. The Joker and Black Hats are like peas in a pod. They perform illegal activities for financial gain, the challenge, or simply for the fun of it.

They look for computers that are vulnerable over the internet, exploit them, and use them to whatever advantage they can.

Black Hats use techniques for getting into systems just like white hats. However, they don't use their defensive skills – rather, they up their game on the attack by doing things such as:

1. Installing backdoors
2. Maintaining access to compromised systems
3. Performing privilege escalation
4. Downloading private/sensitive/intellectual data
5. Installing malware such as ransomware
6. Creating phishing emails and links

Examples of infamous black hats include:

Forum Donate

Learn to code — free 3,000-hour curriculum

3. Hamza Bendelladj aka Bx1 (Latter owner of the ZeuS Banking Malware)
4. Kevin Poulsen (Dark Dante)
5. Robert Tappan Morris (Creator of the morris worm)

Mitnick, Poulsen, and Morris were criminally charged, served their sentences, and are good guys now. Mitnick founded a cybersecurity company. Poulsen created SecureDrop. And Morris became a professor at MIT (Don't you just love a happy ending? 😤).

Green Hat Hackers

Ms Marvel | Credit: Wallpapercave.com

Forum Donate

Learn to code — free 3,000-hour curriculum

that are new to the industry but are willing to learn to become great hackers.

Because of the availability and easy of use of hacking tools these days, it's pretty easy for a green hat to end up in trouble as they may not fully understand the full workings of the tool or target. But, they learn from their errors to gather experience.

Green hats may upgrade to White, Grey, or Black Hat hackers as they continue to move up the ranks.

Blue Hat Hackers

John Wick | Credit: Wallpaperswide.com

Okay, I know. John Wick isn't a part of either DC or Marvel but Dynamite Comics' greatest hitman is a favourite of any fan 🐶.

Forum Donate

Learn to code — free 3,000-hour curriculum

the gallows.

But due to what I can only guess to be cultural differences, a blue hat could also mean an external security professional brought in to test software for vulnerabilities prior to its release.

Red Hat Hackers

The Punisher | Credit: Wallpaperflare.com

I think the character says it all ☠. The Punisher is a ruthless anti-hero that stands up for what is right but is never ever (and I mean ever 😬) going to give criminals second chances.

Red hats are the same. They target cybercriminals and damage whatever they can to disable criminal activities, permanently.

Red hats are hackers no one wants to mess with, not even a black hat. Other hackers usually attack Microsoft Windows computers

Forum Donate

Learn to code — free 3,000-hour curriculum

rather severely for their crimes by taking justice into their hands. They do this by destroying all data and backups of their target, and usually render the system useless.

Conclusion

And on that terrifying note, we have come to the end of this article. I hope you enjoyed it. And as I always say, Happy hacking! 🙃

Acknowledgements

Thanks to Chinaza Nwukwa, Holumidey Mercy, Georgina Awani, and my family for the inspiration, support and knowledge used put this post together. You guys are amazing.

Helpful Resources

1. What is a honeypot?
2. Many more classifications of hats

Daniel Iwugo

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet

---

If you read this far, tweet to the author to show them you care.

Tweet a thanks