Concours Blanc 2023 – LVA – PT V

En vous appuyant uniquement sur les documents du dossier thématique qui vous est proposé, vous rédigerez une synthèse répondant à la question suivante :

What is at stake with ethical hacking today?

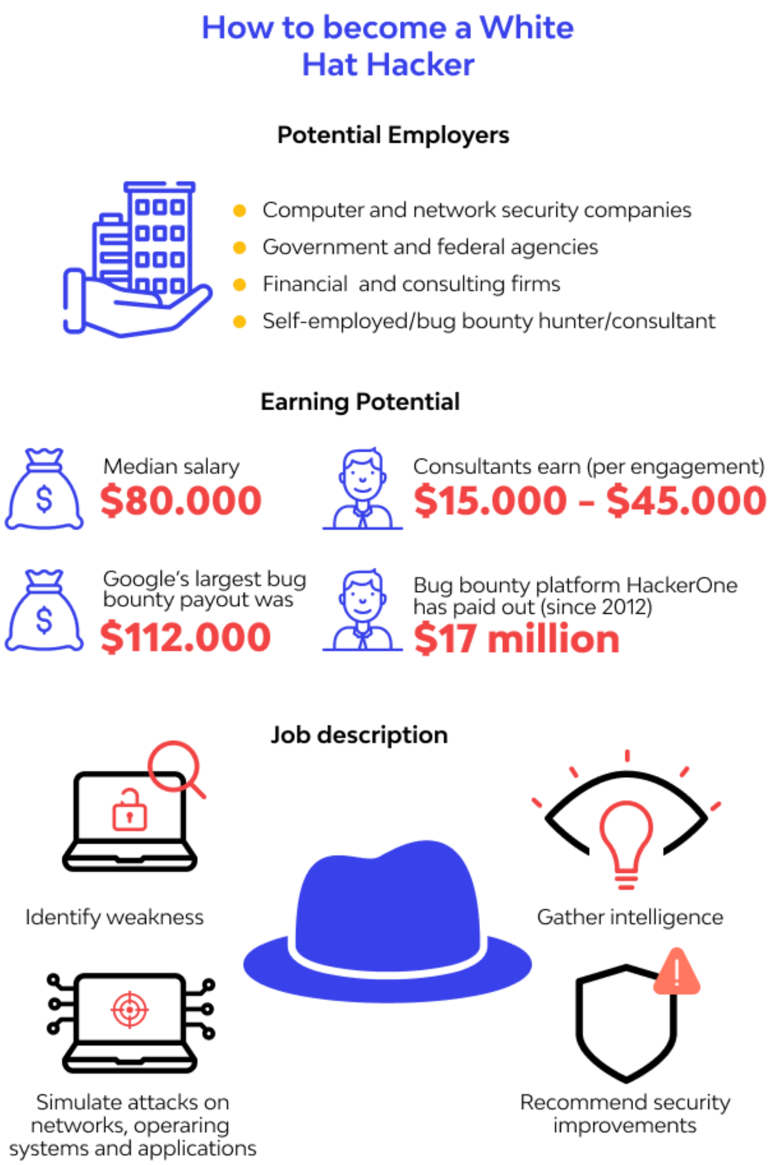
Votre synthèse comportera entre 450 et 500 mots. La synthèse devra être précédée d'un titre et les candidats devront indiquer le nombre de mots comptés en fin de copie.

Liste des documents:

- “White hat hacker”, *www.wallarm.com*,
- “Teenage hackers motivated by morality not money, study finds”, *The Guardian*, by Matthew Weaver, April 21, 2017
- “The Cybersecurity 202: The government's relationship with ethical hackers has improved, security experts say”, *The Washington Post*, By Joseph Marks, August 6, 2019
- “How one Ukrainian ethical hacker is training ‘cyber warriors’ in the fight against Russia”, *www.therecord.media*, by Daryna Antoniuk, July 11, 2022
- Ethical and unethical hacking, Extract from *The Ethics of Cybersecurity*, by David-Olivier Jaquet Chiffelle & Michele Loi, 2020

Document 1 – White hat hacker

https://www.wallarm.com/what/white-hat-hacker



How to become a White Hat Hacker

Potential Employers

- Computer and network security companies
- Government and federal agencies
- Financial and consulting firms
- Self-employed/bug bounty hunter/consultant

Earning Potential

Median salary
$80.000

Consultants earn (per engagement)
$15.000 – $45.000

Google's largest bug bounty payout was
$112.000

Bug bounty platform HackerOne has paid out (since 2012)
$17 million

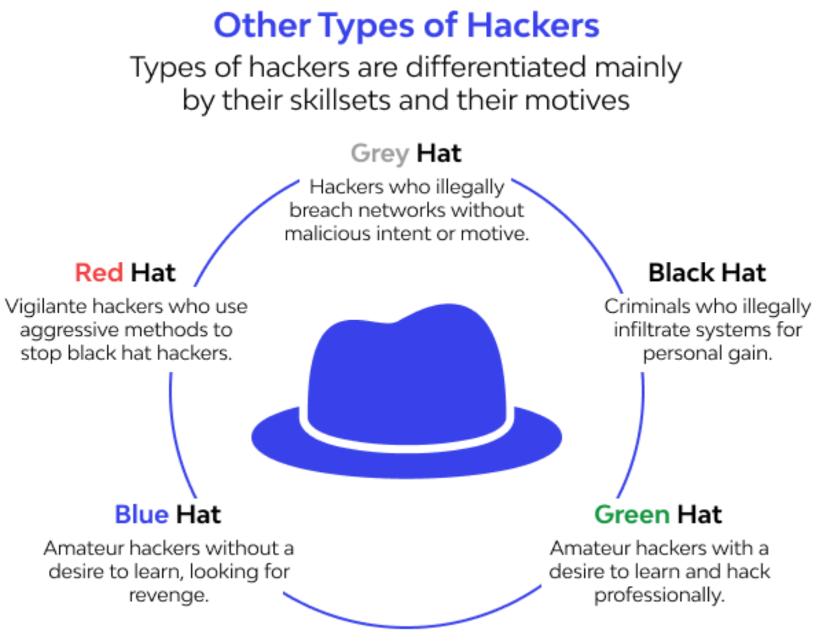
Job description

Identify weakness

Gather intelligence

Simulate attacks on networks, operaring systems and applications

Recommend security improvements



Other Types of Hackers

Types of hackers are differentiated mainly by their skillsets and their motives

Grey Hat
Hackers who illegally breach networks without malicious intent or motive.

Red Hat
Vigilante hackers who use aggressive methods to stop black hat hackers.

Black Hat
Criminals who illegally infiltrate systems for personal gain.

Blue Hat
Amateur hackers without a desire to learn, looking for revenge.

Green Hat
Amateur hackers with a desire to learn and hack professionally.

Document 2 - Teenage hackers motivated by morality not money, study finds

The Guardian, by Matthew Weaver, April 21, 2017

Young people attack computer networks to impress friends and challenge political system, crime research shows

Teenage hackers are motivated by idealism and impressing their mates rather than money, according to a study by the National Crime Agency.

The law enforcement organisation interviewed teenagers and children as young as 12 who had been arrested or cautioned for computer-based crimes.

It found that those interviewed, who had an average age of 17, were unlikely to be involved in theft, fraud or harassment. Instead they saw hacking as a "moral crusade", said Paul Hoare, senior manager at the NCA's cybercrime unit, who led the research.

Others were motivated by a desire to tackle technical problems and prove themselves to friends, the report found.

Speaking to BBC Radio 4's Today programme, Hoare said: "They don't understand the implications on business, government websites and individuals."

Young hackers could profit from their skills if they avoided cybercrime, he said. "A lot of the skill sets these people have are hugely marketable. The world has a lack of cybersecurity and there are lucrative careers to be had, but [they] are much harder to come by if you already have a criminal conviction."

The report said: "Conquering the challenge, proving oneself to the group and intellectual satisfaction are more important motivations than financial gain."

Jake Davis, a former member of the Anonymous hacking collective who was arrested aged 18 in 2011 for attacking government websites, said he had no desire to profit from his crimes but wanted to challenge secrecy.

He said: "It was not financially motivated at all, as the NCA report says, it was mostly politically motivated. I was motivated as a teenager by the idea that this internet was this utopian space that shouldn’t be controlled or filtered or segmented or chopped up into little blocks and distributed out, and that it should be open and free, and anyone in the world should be able to use it.”

Davis, who served time in a young offender institution and was banned from the internet for two years, said he had not lost his idealism. “There is still a place for that kind of idea of freedom online, but we got a little bit out of hand,” he said.

There were more opportunities to get involved in “ethical hacking”, he suggested. “Companies and governments love hiring hackers. There are systems in place called bug bounties. You get to hack to prevent them being hacked. Companies will put out a message to say: ‘This is within scope, if you hack us responsibly, tell us about it, we will patch it up and then we will pay you.’“The hackers will message the company saying: ‘I’ve found this bug in your system, here is what damage it can cause.’ If you take a company like Twitter they have paid over $800,000 [£625,000] to hackers over the last few years.”

Document 3 - The Cybersecurity 202: The government's relationship with ethical hackers has improved, security experts say

The Washington Post, By Joseph Marks, August 6, 2019

The relationship between ethical hackers and the federal government is better now than it was in 2013, when then-National Security Agency chief Keith Alexander first spoke at the Black Hat cybersecurity conference — not long after Edward Snowden revealed the government's sweeping surveillance programs.

That’s the conclusion of 72 percent of experts who responded to an informal survey by The Cybersecurity 202 before the kickoff of this year’s conference in Las Vegas.

The experts are part of the The Network, an ongoing survey of more than 100 cybersecurity experts from government, academia and the private sector. (…)

When Alexander spoke in 2013, many security researchers were enraged about the newly disclosed surveillance programs, which they said ran roughshod over Americans’ privacy rights and made their jobs harder. Alexander's defense of the programs fell especially flat, many survey respondents said, since at that time the U.S. government often failed to distinguish between ethical hackers, who tried to make the Internet safer by finding and patching computer bugs, and criminal hackers who tried to exploit those bugs to steal people’s money and information.

But over the past six years, the U.S. government has made a greater effort to work with ethical hackers and to shield them from legal jeopardy, most respondents said. (…)

One of the biggest ways the federal government has helped ethical hackers in recent years is by shielding them from copyright lawsuits brought by companies after they point out hackable vulnerabilities in their computer code, said Harley Geiger, director of public policy at the cybersecurity firm Rapid 7.

The Library of Congress first approved those protections in 2016 — “with the full-throated support of the Department of Justice,” Geiger noted — and renewed them in 2018. Before the protections, companies frequently used copyright law to punish researchers who found bugs in their products and to scare off other researchers from looking for those flaws.

The government has also embraced bug bounties, contests pioneered in the private sector in which hackers get cash or other prizes for finding and disclosing bugs in federal agency websites and online tools, noted Betsy Cooper, director of the Aspen Institute’s Tech Policy Hub. “The U.S. government not only sees the value of engaging ethical hackers, but increasingly borrows their tools,” Cooper said.

“Government agencies operating bug bounty programs has helped build trust between the government and the security community after it fell off a cliff from the Snowden revelations,” noted Chris Wysopal, chief technology officer at the cybersecurity company Veracode. (…)

However, (some) said the relationship between government and the ethical hacking community was no better now than in 2013 at the height of the Snowden drama.

One big reason they cited was the government's continued demands that tech companies allow law enforcement to access encrypted communication systems — which cybersecurity experts say would result in all digital communications being less secure. (…)

Others criticized Congress and the Justice Department for failing to update the government’s main anti-hacking law, the 1986 Computer Fraud and Abuse Act — which most cybersecurity experts say is far too vague to govern what’s legal and illegal in the modern Internet. (…)

Document 4 - How one Ukrainian ethical hacker is training ‘cyber warriors’ in the fight against Russia

www.therecord.media, by Daryna Antoniuk, July 11, 2022

In the Ukrainian hacker community, Nikita Knysh is a household name. The 31-year-old former employee of Ukraine’s Security Service (SBU) founded cybersecurity consulting company HackControl in 2017 and launched a YouTube channel about internet security and digital literacy. It has about 8,000 subscribers.

When the war broke out in Ukraine, Knysh took up a weapon — his computer — and began fighting back against Russia in cyberspace. (…) “I realized that we should take control of the situation,” Knysh told The Record. “Our government didn’t have a ‘cyber army’, so we built it ourselves.”

To teach Ukrainians the basics of digital guerrilla war, Knysh launched a website called “HackYourMom Academy,” a guide to hacking. The website is free to use and is available in Ukrainian, Russian and English.

Some lessons are simple: how to install an antivirus program, connect to a VPN, or use a virtual machine. Others are more advanced, such as how to conduct distributed denial-of-service (DDoS) attacks or hack Russian cameras and WiFi routers. (…)

Global demand for cybersecurity specialists has increased by more than 40% in the past year, driven by businesses reacting to ransomware attacks and phishing campaigns. To expand the talent pool and train more young workers, cybersecurity activists are creating their own courses and training programs, including HackYourMom.

Days after Russia’s full-scale invasion, Ukrainian hacktivists flocked to Telegram — one of the country’s most popular messaging apps — to discuss how to access Russian cyberspace. Their main goals were to tell Russians the truth about the war in Ukraine (…).

The most famous group of hacktivists — IT Army — now has almost 250,000 followers on Telegram. One of its favorite tools are DDoS attacks, which flood Russian websites with junk traffic to knock them offline.

International experts are concerned about the potential consequences of these attacks. (…) A senior researcher with the Zurich-based think tank Center for Security Studies, said that the IT Army violates “the existing legal frameworks” for state behavior in cyberspace. (He) refuses to treat IT Army as “random volunteers” and argues that it largely consists of Ukrainian defense and intelligence services — a claim that the Ukrainian government and cybersecurity specialists have repeatedly denied. (…)

HackYourMom has an entire section dedicated to cyber warfare. For example, it explains how students can learn how to find Russian soldiers responsible for atrocities in Ukraine on the internet with the help of open-source intelligence (OSINT) or how to install software for DDoS attacks.

“We don’t encourage people to attack — we give them the tools. They decide themselves what to do with them,” Knysh said. (…)

Now is a unique time when Ukrainian hacktivists can join so-called red teams that break into defenses. “When they have learned to attack, it will be easier for them to learn to defend better in the future,” Knysh said.

Document 5 – Ethical and unethical hacking

https://link.springer.com/chapter/10.1007/978-3-030-29053-5_9

Extract from *The Ethics of Cybersecurity,* by David-Olivier Jaquet Chiffelle & Michele Loi, 2020