



Ethical Hacking

Done by: Syed Hammad, Muzzammil Paracha, Duc Anh, Emmanuel, Mohammad Zayat

Ethical Hacking

Ethical hacking, or white hat hacking, is the authorized and legitimate practice of using hacking techniques to find and address security vulnerabilities in computer systems, networks, or software. Ethical hackers conduct controlled tests to simulate potential attacks, assisting organizations in evaluating and fortifying their defenses. They operate with permission, adhere to strict legal and ethical standards, and play a critical role in safeguarding sensitive information and preventing unauthorized access. Their efforts are indispensable for maintaining strong cybersecurity measures amid ongoing threats. Their primary goals include:


1. Identifying Vulnerabilities: Discovering weaknesses in systems that malicious actors could exploit.
2. Testing Security Measures: Evaluating the effectiveness of existing security controls and defences.
3. Providing Recommendations: Offering guidance and recommendations to improve overall cybersecurity posture.
4. Preventing Attacks: Proactively mitigating risks and preventing potential breaches before they occur.
5. Compliance and Assurance: Helping organizations meet regulatory requirements and industry standards related to cybersecurity.



White Hat Hackers

A white hat hacker is a cybersecurity expert who uses their skills to find and fix security vulnerabilities in systems, with permission, to prevent malicious attacks. They work ethically to protect organizations from cyber threats.





Grey Hat Hackers

A grey hat hacker finds system vulnerabilities without malicious intent but often without explicit permission. They might exploit these findings for personal gain or notify owners to prompt fixes. Unlike white hat hackers, who operate with full authorization, grey hat hackers navigate a legal and ethical gray area, acting without approval but typically not with malicious intent like black hat hackers.



Black Hat Hackers

A black hat hacker uses technical skills to maliciously breach computer systems, networks, or software for personal gain, like data theft or spreading malware. They operate illegally, without permission, and ignore ethical standards, posing serious cybersecurity threats.

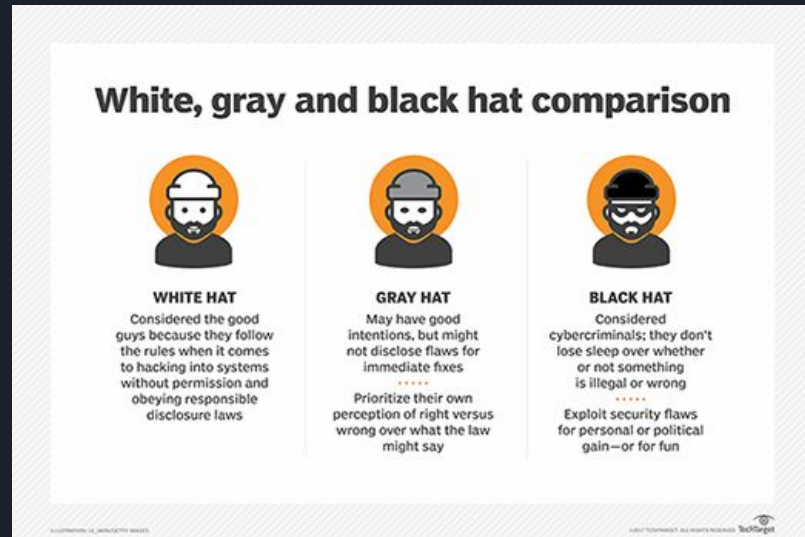


Difference between White, Grey and Black Hat Hackers

White hat hackers aim to improve cybersecurity by identifying and fixing vulnerabilities legally and ethically. They include penetration testers, security consultants, and cybersecurity professionals who operate with permission.

Black hat hackers exploit vulnerabilities illegally for personal gain or harm, engaging in cybercrime like data theft and malware development.

Grey hat hackers operate in a morally ambiguous space, sometimes finding and disclosing vulnerabilities without permission. They may transition to legitimate roles if they adhere to legal and ethical standards as bug bounty hunters or security researchers.



Malicious Hacking

Malicious hacking involves unauthorized exploitation of computer systems, networks, or software for harmful purposes. It is illegal, breaches ethical standards, and jeopardizes security, privacy, and operational integrity for individuals, businesses, and governments alike. The primary goals of malicious hacking include:

1. Unauthorized Access: Gaining entry into systems or networks without permission.
2. Data Theft: Stealing sensitive information, such as personal data, financial records, or intellectual property.
3. Damage or Disruption: Causing harm to systems, networks, or data through actions like deleting files, altering configurations, or disrupting services.
4. Financial Gain: Engaging in activities like identity theft, fraud, or ransom demands.
5. Espionage: Gathering intelligence or spying on individuals, organizations, or governments.
6. Malware Distribution: Spreading viruses, worms, ransomware, or other malicious software to infect and compromise systems.



Malicious Hacking vs Ethical Hacking

Ethical hackers improve cybersecurity by finding and fixing vulnerabilities in computer systems, networks, or software with permission and following ethical guidelines. They help protect systems from threats. In contrast, malicious hackers exploit vulnerabilities for personal gain, causing harm or disruption without permission, breaking laws and ethical standards. Ethical hackers strengthen security, while malicious hackers weaken safety and stability.



Ethical Hacking Phases

Types of Ethical Hacking Phases:

- 1) Reconnaissance: Gathering information about the target system.
- 2) Scanning: Identifying potential entry points.
- 3) Gaining Access: Exploiting vulnerabilities to enter the system.
- 4) Maintaining Access: Ensuring continuous access to the system.
- 5) Covering Tracks: Removing evidence of the intrusion.





Reconnaissance

The main goal of reconnaissance is to gather information about a target to understand its structure, vulnerabilities, and potential attack vectors. This helps in planning effective security assessments and improving overall security posture.

Types of Reconnaissance:

- Passive Reconnaissance
- Active Reconnaissance

Passive Reconnaissance:

Passive reconnaissance involves gathering data about a target system or organization from publicly accessible sources without directly engaging the target. It aims to collect standard information like employee names, IP addresses, domain names, and technology used without triggering security alerts. This initial phase helps ethical hackers understand the target's infrastructure and vulnerabilities before proceeding to more active testing or assessments.

Active Reconnaissance:

Active reconnaissance involves actively probing and interacting with a target system or network to gather specific and detailed information such as open ports, active services, network topology, and system configurations. This method contrasts with passive reconnaissance, which collects publicly available information without direct interaction. Active reconnaissance is essential for ethical hackers to assess security vulnerabilities comprehensively and plan effective security assessments or simulated attacks based on the acquired data.

Difference between Passive and Active Reconnaissance

Active reconnaissance involves direct interaction with a target system using tools such as port scanning, which generates traffic and potential security alerts. This method gathers detailed information about vulnerabilities. In contrast, passive reconnaissance gathers basic information from public sources like websites and social media without direct interaction or detection, offering foundational insights into the target's environment without raising security concerns.





Scanning: Identifying potential entry points

Scanning is a crucial step in ethical hacking, where hackers carefully study a target system or network to identify potential avenues of attack. Ethical hackers can assess a target's security posture and recommend steps to lower risks and fortify defences by examining the target's infrastructure and spotting potential weaknesses.


There are 3 types of scanning methods:

1. Port scanning: Identifies the target systems' open and active ports, exposing possible points of access.
2. Network Scanning: Identifies live IP addresses and the services they are connected to, laying out the architecture of the network.
3. Vulnerability Scanning: This technique helps to prioritise security configurations and fixes by identifying known vulnerabilities in systems or applications.

Difference between all the scanning methods

In ethical hacking, port scanning focuses on identifying open and active ports on target systems to uncover potential entry points. Network scanning aims to discover active devices and IP addresses within a network, mapping its structure and understanding system roles and communication patterns. Vulnerability scanning, on the other hand, seeks out known weaknesses in systems, applications, and network setups to prioritize security fixes and mitigate potential risks. Together, these methods provide ethical hackers with crucial insights into a target's infrastructure, helping them assess vulnerabilities comprehensively and recommend appropriate security measures to strengthen defenses.





Maintaining Access: Ensuring continuous access to the system

In hacking, maintaining access entails keeping control of a hacked system or network. Attackers accomplish this by creating covert entry points (backdoors), putting persistence mechanisms in place to avoid detection after system upgrades or reboots, using evasion strategies like encryption and log manipulation, and continuously tracking down and taking advantage of weaknesses. Attackers can maintain unauthorised access, alter data, increase privileges, or launch further attacks during this period, all while lowering the possibility of being discovered.

Covering Tracks: Removing evidence of the intrusion.

In the final phase of hacking, called clearing tasks, attackers aim to erase all traces of their presence from the compromised system to avoid detection. They use techniques like steganography to hide data, tunnelling protocols for covert connections, and alter log files to eliminate evidence of their activities. The objective is to restore the system to its initial condition to maintain unauthorized access without arousing suspicion or being identified.



Rules to Ethical Hacking

1. **Adherence to Ethical Guidelines:** Ethical hackers must strictly follow established rules to avoid harm to organizations they assess.
2. **Skill and Patience:** Ethical hackers rely on their expertise and perseverance to effectively identify and address security vulnerabilities.
3. **Clear Intentions:** Their primary objective should be to assist organizations by enhancing security, not causing harm.
4. **Privacy Preservation:** Respecting confidentiality is paramount; sensitive information obtained during assessments must be kept secure to prevent misuse or legal issues.





BENEFITS OF ETHICAL HACKING

- Ethical hacking assists in fighting cyber terrorism and national security breaches.
- It enables preventive actions against hackers.
- Ethical hacking helps in building secure systems that prevent unauthorized access.
- It provides enhanced security for banking and financial institutions.
- Ethical hacking identifies and closes vulnerabilities in computer systems and networks.



LIMITATIONS TO ETHICAL HACKING

- Ethical hacking involves navigating legal and ethical boundaries, which can be complex and sometimes unclear.
- Conducting thorough ethical hacking assessments requires significant resources, including skilled personnel and specialized tools.
- False positives in ethical hacking assessments may lead to wasted resources and unnecessary concerns about security vulnerabilities.
- Ethical hacking tests can potentially disrupt normal operations if not carefully planned and executed.
- Finding skilled ethical hackers with the necessary technical expertise can be challenging, and there is a dependency on third-party tools which can introduce vulnerabilities if not managed carefully.



Other types of Ethical Hackers

- Cyber Warrior: Hired to probe systems like malicious hackers, identifying vulnerabilities to help secure organizational data and websites.
- White Box Penetration Testers: Internal employees who ethically breach their organization's systems with full knowledge to uncover vulnerabilities and strengthen defenses.
- Certified Ethical Hacker (CEH): Certified professionals skilled in both black box (no prior knowledge) and white box (full knowledge) hacking techniques, essential for identifying and mitigating vulnerabilities in cybersecurity efforts. Requires recertification every three years.
- Hacktivists: Engage in unauthorized access to promote social or political causes through prominent website messages, aiming to influence public opinion digitally rather than for personal gain.

Types Of Hackers

-Hacking encompasses various forms of unauthorized computer access, involving diverse actors and intentions:

1-Criminal Hackers (Crackers): Maliciously attack or defraud systems for personal gain.

2-Script Kiddies: Typically young males who use pre-made hacking tools to vandalize or disrupt the Internet.

3-Hacktivists: Combine hacking with activism to perform acts of civil disobedience online, aiming to highlight political or social causes.





Hackers


Popular Perceptions: Hackers are seen as either heroes, activists, or criminals, often portrayed in media as lonely malicious criminals.

- Focus on Political Hacking: This type involves hacks driven by political or social agendas by private individuals, differing from hacks for personal profit, system testing, skill demonstration, chaos creation, or state-sponsored attacks.

- Examples of Political Hacking: Political hacking has targeted issues like nuclear disarmament and government actions, with notable instances including:

- Anti-nuclear hacking: The 1989 NASA and US Energy Department hack by the 'WANK' worm promoting anti-nuclear messages.

- State-Sponsored Hacks: Examples like Stuxnet, which targeted Iran's nuclear program, and cyber-espionage operations like 'Titan Rain' and 'Operation Aurora'.



Diverse political agendas and responses of hacker groups

- 1-Variety of Agendas: Hacker activities target issues like public protests, online freedom restrictions, court decisions, corruption, and online privacy.
- 2-Challenges in Evaluation: Anonymous and similar groups have no consistent ideology, making ethical evaluation difficult.
- 3-Ethical Framework: The framework evaluates hacking activities within their political context, focusing on the operation as a whole rather than individual motivations.
- 4-Examples of Political Hacks: Specific operations, such as Aaron Swartz's JSTOR hack and Anonymous' operations against ISIS and anti-piracy organizations, demonstrate the range of activities.
- 5-Evaluation Approach: The framework examines methods, targets, narratives, and outcomes to judge the ethicality of the hack, treating the operation as a collective effort.
- 6-Collective Responsibility: Ethical evaluation focuses on the collective action and its political agenda, assigning praise or condemnation to those most responsible, similar to evaluations in international ethics.

Ethical evaluation of political hacking by focusing on operations

Political hacking often targets fundamental human rights like integrity, autonomy, liberty, and privacy. Groups like Anonymous, rooted in early hacker principles of information freedom and authority distrust, attack organizations opposing their beliefs, such as anti-corporate sentiment and free speech. Despite diverse goals, hacker collectives share a common political ideology supporting values like opposing repressive regimes, free expression, and fighting corruption. Their actions are morally acceptable when they uphold fundamental rights like freedom of speech and privacy without harming others.





Political Violence (By Hackers)

Political hacking involves aggressive techniques like DDoS attacks, doxxing, and deploying malware and viruses, setting it apart from non-violent hacktivism aimed at promoting free speech and human rights. Hacktivism is viewed as civil disobedience within a noble tradition, utilizing non-violent, politically motivated actions to drive change. The essay critiques the moral legitimacy of political hackers' use of violence, contrasting it with the state's justified use of violence for political purposes based on a social contract sacrificing individual rights for societal safety and stability. Hackers, seen as threats to social order and the rule of law for operating outside this contract, are thus scrutinized for their use of political violence.

DDoS Attack:DDoS (Distributed Denial of Service) attacks involve overwhelming a targeted server, network, or website with a flood of internet traffic from multiple sources, rendering it unavailable to users. These attacks exploit multiple compromised systems to generate excessive traffic, disrupting normal service operations and causing significant downtime.

Doxxing: Doxxing is the act of publicly disclosing someone's private or personal information without their consent, typically to harass or intimidate them.

Ethical Justifications for Hacker Intervention Against State Failures

The state's authority is based on protecting vital interests and human rights, and it loses moral authority when it fails in this role. Hackers can be justified in upholding social norms and protecting rights where the state is negligent, incapable, or harmful. Their actions can highlight state failures and reinforce ethical standards. Good laws, even unenforced, guide hackers ethically, with universal human rights as a basis. Hackers should intervene when the state is the threat, unable to prevent harm, or unwilling to act, but should avoid acting on mere disagreements with just state decisions.



Ethical Justifications for Hacker Actions in Defense of Civil Rights

Hackers use the political justification of punishing wrongdoers and defending civil rights, especially information freedom, to justify their acts. They support the right to self-defense, which enables people and other parties to protect lives and important interests without the intervention of the government. This principle justifies a range of reactions from legal measures to more forceful acts, covering both physical and non-physical issues like autonomy and privacy. The appropriateness of their defensive tactics is contingent upon the gravity and urgency of the threat; threats that are less serious should be met with non-lethal methods, while those that are more serious should be met with immediate action. This may involve targeted hacking to fight certain risks, such as censorship or possible injury.



Ethical Justifications and Principles of Hacker Self-Defense

Hackers justify their actions based on diverse political motives, ranging from targeting wrongdoers like hate groups to defending civil rights such as freedom of information. They assert the right to protect lives and vital interests independently of state intervention, emphasizing the importance of safeguarding life, privacy, and autonomy. Responses vary from legal challenges to more forceful actions, depending on the severity and urgency of the threat. Immediate risks prompt swift responses, while preventive measures address potential future threats. Hacking as self-defense includes actions like circumventing censorship and using proportional tactics against serious threats, ensuring actions align with the perceived risk level.



Principles of Ethical Hacking and Responsible Action

The principles of ethical hacking emphasize proportionality and thoughtful assessment of consequences. Hackers should act only in response to significant failures of state mechanisms, ensuring any actions taken are justified by the positive impact and proportional to the situation at hand.





Sources

- Shivanshi Sinha. Dr. Yojna Arora. (May, 2020). Ethical Hacking: The Story of a White Hat Hacker
- Ross W. Bellaby. (12 February 2021). An Ethical Framework for Hacking Operations