**Ethical Hacking Tools and Techniques: Cyber Security Implications**

RajendraPrasad M\*1, Sourabh Jain2, Bhoopesh Singh Bhati3R Lakshman Naik4

Dept. of CSE, Indian Institute of Information Technology, Sonepat, Haryana, India

**Abstract:** Ethical hacking is a crucial and sensitive aspect of cyber security, enabling organizations to test their defenses and identify security weaknesses. It involves detecting and remediating vulnerabilities in systems, networks, and applications. The dailydave mailing list highlights the latest tools and trends in ethical hacking techniques and tools. The key stages include network reconnaissance, vulnerability testing, exploitation, social engineering, web application tests, and wireless security testing. These tools and techniques use specialized techniques like port scanning, penetration tests, and phishing simulations to identify vulnerabilities in a company's security posture. It explains the various phases of ethical hacking, for effective implementation of the tools and techniques to work on organizations security, so it is essential to identify. And by applying these methods and framework solutions, the ethical hackers factor into identifying and fixing security flaws ahead of attackers, and help companies in mitigating cyber risks and overall elevate cyber security preparedness.

**Keywords:** Ethical Hacking,Hackers, Hacking Phases, Cyber security, Tools, Techniques.

1. **INTRODUCTION**

The growth of the cyber technology world and the advancement of computer security has led to a heightened evolution of security for governments and business peoples where getting hacked is relative to how well their infrastructure is secured. Ethical hackers are professionals who use the same methods and techniques that hackers use to discover security weaknesses and vulnerabilities, only in a lawful and legitimate manner to assess the security posture of a target system and without causing any damage to the target systems. When the ethical process has been finalized, the owners will receive all the detailed report of the vulnerabilities they have discovered, as well as the details of how to fix find the malicious code they have uncovered.

Ethical hacking is also called “Penetration Hacking” or “Intrusion Testing” or “Red Teaming”. Hacking without evil is also known as ethical hacking. Ethical Hackers vs Malicious Hackers-The ethical hackers and the malicious are not the same and are just playing different roles in security. Palmer (2004, cited by Pashel, 2006 ) says: "Ethical hackers use the same tools and methods of intruders, but they don't damage the third systems or steal information. They don’t damage servers or delete files; they assess the service-like security of the target systems, and feed that information back to the owners of the target systems, so owners can address any weaknesses found in the course of that normal back-and-forth relationship. The massive expansion of the Internet has brought a wave of good slate of things with it. Electronic commerce, email, vast reserves of reference material and many other wonderful things. Like, you know, all good things in technology, there’s a flip side: criminal hackers who will surreptitiously rip off the organization’s data and blast it out to the open internet. They are known as black hat hackers. Then, to escape from such critical factors we got another type of hackers and they are termed as Ethical hackers or white hat hackers.

Ethical hacking is one form of a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack does not mean there are no security issues. The output of an ethical hack is a detailed report of the findings and a statement that a particular hacker with a specific amount of time and skill would or would not be able to do some damage or gain some access. Ethical hacking is a security assessment, a form of training, the testing of an information technology environment for weakness. An ethical hack demonstrates the security risks of an information technology environment and reccomendations can be made to mitigate the risk to some extend or to accept it. Ethical hacking fits well into the security life cycle shown in the below figure.

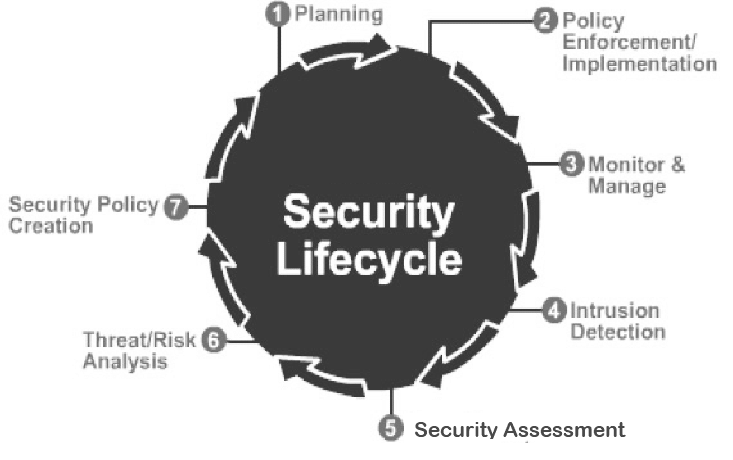


Fig. 1 Security Life Cycle

1. **HACKING**

Hacking is the spawn of curiosity. The hacker wants to know more, depending on his/her taste, out of curiosity. The hacker is one who enjoys the intellectual challenge of creatively overcoming and circumventing limitations of programming systems and who tries to extend his/her facilities for doing so. He/She is a computer fan and a good programmer, skillful in programming language, computer and network. Mostly you hear to the term hackers for someone who breaks the computer network security systems. Internet and making www work, were developed by the hackers. The same goes for the UNIX operating system. Hacking -- Originally meaning- "A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the basics that let them do what they need." A slogan introduced by Peter Landin meaning "One who likes programming, or training, or influence, or even one who believes that everyone should learn to program."

They are not hackers who break into systems; they are the ones who protect a company’s networks. They penetrate systems of the organizations to find, if any, flaw in the security within their legal allowance. Ethical hacking is also called as “Penetration Hacking” or “Intrusion Testing” or “Red Teaming”. Cracking and malicious hacking is defined as the unauthorized use of computer and network resources. When you get Hackers malicious application to gain access to other users email or account numbers and passwords. spyware to infiltrate a corporate network to steal key information. It can lead to identity theft, information theft, work hours waste, utilization of network resources like over use of bandwidth, mail flooding, deception with regards to transactions made, misuse of credit card / debit card numbers, and sale of the user”s personal information like addresses, account numbers, phone numbers etc. To the public at large, they are the “Thugs of the Cyber Space”, who just want to mess up and damage someone else’s network and data. Crackers are also referred to as “Hackers”, they are the bad ones. Like the good, the bad hackers focus deep inside their skill set, the only difference is the intension.

White-hat hackers are extremely persistent. All they require is time, and the will do find gaps in the security to work their way into the system. This essential element of patience can also be find on the attacking side, as the malicious hacker would have, the patience level at least, if not, and would watch the victim closely, for weeks, or could be, for months, waiting a chance to make the attempt. The difference is that a white hat hacker would have the patience to investigate the target for any security flaw against which to attack, while the black hat would have patience to investigate and find some opportunity to attack as relevant the target system. It can be seen that all the methods and skills applied for the ethical hackers and the malicious hackers were the same. But for the intention of the hackers, they are one and the same. Once the ethical hackers gain these techniques and skills, they would always target the system and try to find the vulnerabilities and how to counter it against any of the malicious attacks, but in opposing to this, the malicious hackers would always try to get use of these techniques and skills to attack on the system of the target in order to destroy or harm it for the personal interested (for example, money). The same can be said of these good hackers (who are, I agree are a bit of a different beast to the nefarious ones). This is because an Ethical hacker would now need to learn and understand the changes made in the network by the malicious hacker.

1. **TYPES OF HACKING / HACKERS**

The hacking systems can be distinguished with three types as per the colors of the “Hat”. The term Hat comes from old western movies, where the Hero’s’ cap color was “White” and the villains was “Black”. Again it may be said, the lighter the color, the less purpose to injure. White Hat Hackers are the good guys, working for companies, authorized and paid on the work they do. They are also called “IT Technicians”. They protect the Internet, companies, computer systems and networks from crackers. Some firms pay a fee to IT professionals to try to hack their servers and computers to see how secure they are. They do hacking in the service of the company. They’re hacking into their own security software. The white Hat Hacker is also known as an Ethical Hacker. Unlike the white hat hackers, the Black hat hackers are the one who exploit the computer systems and network with the malicious intent. The compromise the security, trespass on the network and damage and destroy data to render the network unusable. They vandalize the websites, swipe the data and break through the security. The \*h4><3r$ break into their programs and password to break in the unauthorized network or system. They are doing things for their own selfish own loves like $$. They’re commonly referred to as “Crackers,” or Malicious Hackers.

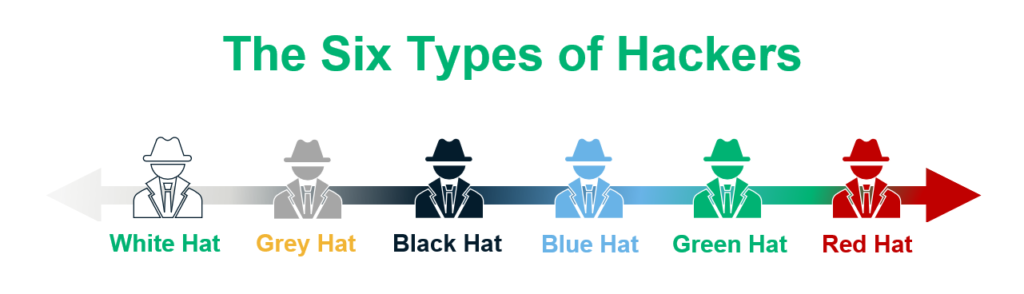


Fig. 2 Types of Hackers

In addition to white hats and black hats, a third type of hacker is a Grey Hat. Even just like inheritance, entire properties of the base class/not necessarily of the both are inherited by the derived classes, same goes here a grey hat hacker have the properties of both black hat and white our case as well. They’re the ones with ethics. Grey Hat Hacker- This is where a hacker only has access into a system and tries to find a way to inform the security administrators of a break in the security of the system. Then the cure, perhaps, could be their own. They already know what’s right and what’s wrong, sometimes they just don’t act positively. He/She would be more accurately designated as a Gray Hat, since he is effectively violating the computer security of the organizations, and using and defacing it. But in general, they are changing what were already programmed general units that can be fixed. Well, eventually they come and tell the administrator some of the ways the organization is weak in security. They hack or enter unauthorized into the network just for the sake of fun and with no intention of destroying the Organizations’ network. During hacking a system, either it is ethical hacking (white hat hacking) or malicious hacking (black hat hacking), the hacker has to do some steps to get into a computer system that can be described as five phases.

**Phase 1: Reconnaissance can be Active or Passive:**

In Passive Reconnaissance, The Information is collected about the target in the absence of knowledge about target company or individual. This can be done by just for searching information of the target on Internet or bribing an employee of targeted company who would do this and provide useful for you. This process is also known as “Information Gathering”. In this method, hacker doesn’t use to hack the system or network of the company to get the information. In active reconnaissance on the other hand, the hacker goes inside the network in order to find out specific hosts, IP addresses and network services. This method is also known as “Rattling the Doorknobs”. There is a higher change in getting caught in this approach than passive reconnaissance.

**Phase 2: Scanning:** The information from Phase 1 helps analyze the network. Hackers use tools like dialers and port scanners to explore and access the company’s system and network.

**Phase 3: Owning the System:** The hacking phase involves the hacker using information from earlier phases to attack and access the local area network, local PCs, internet, or offline systems, known as "owning the system.”

**Phase 4: Zombie System:** Once a hacker gains access to a system or network, they keep that access for future attacks by altering the system so others cannot enter. This compromised system is then called a "Zombie System."

**Phase 5: Evidence Removal:** In this phase, the hacker eliminates all evidence of the hack, like log files and alarms, to avoid being caught and facing legal issues. After hacking, there are methods called penetration testing to identify the hacker and cracker.

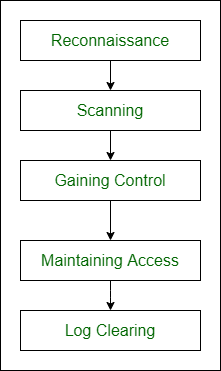


Fig. 3 Hacking Phases

**4. ETHICAL HACKING APPROACHES AND PRACTICES**

Ethical hacking involves finding and exploiting security flaws using various methods. This section reviews key techniques such as network hacking, vulnerability scanning, penetration testing, social engineering, and online application hacking, discussing their advantages, disadvantages, and use in different organizations.

* **Vulnerability Scanning:** An automated procedure called vulnerability scanning is used to find possible security holes in networks or systems. To find problems like open ports, missing security updates, and out-of-date software, this approach uses specialist tools. Despite being successful in identifying known vulnerabilities, it frequently generates a sizable number of false positives.
* **Penetration Testing:** This testing checks a system's security by simulating attacks. It assesses how well an organization can detect and respond to threats by exploiting weaknesses. There are three testing methods: black box, white box, and gray box.
* **Social Engineering:** Human brain research is used in social engineering to deceive people into sharing sensitive information or taking risky actions. Techniques include phishing, pretexting, and baiting. Awareness training and strong security can help reduce its impact.
* **Web Application Hacking:** Web application hacking involves SQL injection, XSS, CSRF, and session hijacking. To protect online applications, use secure coding, input validation, and conduct regular security audits.
* **Network Hacking:** Network hacking exploits weaknesses in hardware like firewalls and routers. Techniques include spoofing, sniffing, and DoS attacks. Countermeasures are intrusion detection systems, firewalls, and segmentation.

**5. ETHICAL HACKING TOOLS**

Automatic tools have transformed penetration testing and ethical hacking, making the process faster, more reliable, and easier. It summarizes the best tools currently used in the hacking field.

* **Nmap:** It is a top tool used in ethical hacking for port scanning. Originally a command-line tool for Unix or Linux operating systems, it now has a Windows version, making it easier to use. It also helps in operating system fingerprinting.
* **Nessus:** The most well-known vulnerability scanner in the world, Nessus was created by Tenable Network Security and is free for home users and non-business environments. It may be used to identify serious flaws in a system and is a network vulnerability scanner.
* **Nikto:** It is a free and open-source tool, detects the default files and applications on over 270 servers and looks for version-specific issues and outdated versions on over 1000 servers. It is the greatest tool for testing the penetration of web servers.
* **Kismet:** There is a market for WLAN hacking, and companies hire penetration testers to test wireless networks. Kismet is a suitable tool for this, as it passively collects packets and detects both hidden and non-beaconing networks through data traffic, potentially revealing their identities over time.
* **MetaSploit:** It is a powerful tool used to run exploit code on computers. It is user-friendly and has a database of available exploits, making it ideal for penetration testing.
* **NetStumbler:** It works with Windows operating systems and can find WiFi networks using IEEE 802.11b, 802.11g, and 802.11a. MiniStumbler is compatible with Windows CE.

**6. ETHICAL HACKING TECHNIQUES**

* **Information Gathering**: In this step, testers collect information about the web application to understand its logic better. A deeper understanding will lead to more successful penetration testing. Testers should gather all information, even if it seems unrelated, since it may be useful later. This can be done using public tools like search engines, scanners, sending simple or crafted HTTP requests, or walking through the application.
* **Vulnerability Analysis:** Testers use the gathered information to scan for vulnerabilities in the web application. They test areas like configuration management, business logic, authentication, session management, and data validation, examining various types of vulnerabilities in the process.
* **Exploitation:** Testers analyze vulnerabilities to identify target areas for exploits. They then exploited the two applications based on this list.
* **Test Analysis Phase:** This phase involves the results, testers, and the target entity. The target must understand the common methods, techniques, tools used by attackers, and any unnecessary data exposure they face.

**7. CONCLUSION**

Ethical hacking has become an essential part of sophisticated cybersecurity. In order to shield enterprises from the constantly changing threat landscape, ethical hackers play a critical role in proactively detecting and fixing vulnerabilities. The various facets of ethical hacking have been emphasized in this analysis, including its methods, development, use in penetration testing and vulnerability assessment, and wider effects on corporate security. Despite all of its benefits, ethical hacking has drawbacks and moral conundrums. Policymakers, business leaders, and researchers will need to work together to overcome these challenges. Ethical hacking is predicted to become more important as technology develops, therefore continuing study and development is essential to avoiding emerging risks. Ethical hacking is not only a defensive tactic but also a strategic requirement for businesses looking to protect their digital assets. Organizations may ensure a safer digital future and significantly increase their resistance against cyberattacks by investing in qualified ethical hackers and fostering a security-conscious culture.

**REFERENCES**

1. [Soumik Ghosh](https://www.csoonline.com/profile/soumik-ghosh/), The biggest data breaches in India, https://www.csoonline.com/article/569325/the-biggest-data-breaches-in-india.html
2. [Soumik Ghosh](https://www.csoonline.com/profile/soumik-ghosh/), The 15 biggest data breaches of the 21st century https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html
3. https://www.statista.com/statistics/1196721/india-internet-connections-in-rural-and-urban-areas/ India: number of internet connections in rural and urban areas
4. Bishop, M. (2003). Introduction to Computer Security. Addison-Wesley
5. Kizza, J. M. (2020). Ethical and Social Issues in the Information Age, Springer
6. DomainKeys Identified Mail (DKIM), https://threatcop.com/blog/dkim, 2021
7. Sender Policy Framework (SPF): https://threatcop.com/blog/spf-authentication, 2021
8. Fink, G. A. et al. (2009) ‘Visualizing cyber security: Usable workspaces’, in 6th International Workshop on Visualization for Cyber Security 2009, VizSec 2009 - Proceedings. doi: 10.1109/VIZSEC.2009.5375542.
9. Hámornik, B. P. and Krasznay, C. (2018) ‘A team-level perspective of human factors in cyber security: Security operations centers’, Advances in Intelligent Systems and Computing, 593, pp. 224–236. doi: 10.1007/978-3-319-60585-2\_21
10. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson
11. Sutherland, I., & Crocker, A. (2019). Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication. McFarland & Company.
12. Whitman, M. E., & Mattord, H. J. (2017). Principles of Information Security (6th ed.). Cengage Learning.
13. Kaur, R., & Kaur, S. (2017). Ethical hacking: The need for cyber security. International Journal of Engineering and Computer Science, 6(7), 21972-21975.
14. Allen, J., & Frye, C. (2015). The Ethical Hacker's Handbook: Conducting Penetration Tests (2nd ed.). McGraw-Hill Education.
15. Peltier, T. R. (2016). Information Security Risk Analysis (3rd ed.). CRC Press.
16. Andress, J. (2019). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (3rd ed.). Syngress.