Ethical Hacking : A Review on Tools,Techniques and Approaches

Pradeep Nagaraj *MSc.Computer Science*
Lakehead University
Thunder Bay, ON
nagarajp@lakeheadu.ca

***Abstract*—Security is a major concern in today's world, and everything should be done safely and securely. While communication technologies have brought the world closer together, they have also created uneasiness among system owners around the world. Hacking, specifically cracking computer systems, is the primary cause of this insecurity. Hacking is a procedure in which an individual or group exploits a system's flaw for personal gain or enjoyment. Hacking, specifically cracking computer systems, is the primary cause of this insecurity. Hacking is a procedure in which an individual or group exploits a system's flaw for personal gain or enjoyment. Ethical hacking is the technique of breaking into a network with good intentions and in an ethical manner to protect the system from being hacked. For organizations and governments, ethical hacking, also known as penetration testing or intrusion testing, has become a major concern. Companies are concerned about being "hacked", while potential customers are concerned about keeping control of their personal information. This main aim of this paper is to describes ethical hackers: tools and techniques, why do we need them and identifies the code of conduct for an Ethical Hacker and its need.**

***Keywords*—Hacking, Ethical Hacking, Penetration testing, Vulnerability analysis, Network security, Pen-testing tools, Ethics in hacking**

I. Introduction

The internet has accelerated the digitalization of several activities such as banking, online purchases, online financial transactions, collaborative computing, e-mail, and new avenues for advertising, information distribution, and data gathering. With the rapid development of the internet and the increasing number of users, the risk of data security is increasing, and the problem of information security is becoming extremely important. Because most technical advancements have made all information available online, some people use it to gain knowledge, while others use it to disrupt or steal information from websites or databases without the owner's knowledge. HACKING is the terminology used for this dark side.

A. Hacking

Hacking is the process of identifying and exploiting weak links or gaps in computer systems or networks in order to obtain unauthorized access to data or modify the features of the target computer systems or networks. Hacking is the alteration of computer hardware, software, or networks to achieve goals that are not aligned with the interests of the users. It's also known as breaching someone's security and capturing personal or confidential information such as contact information, credit card numbers, internet banking credentials, and so on. The methodology or the steps followed by the Hackers (See figure-1), as follows [1]

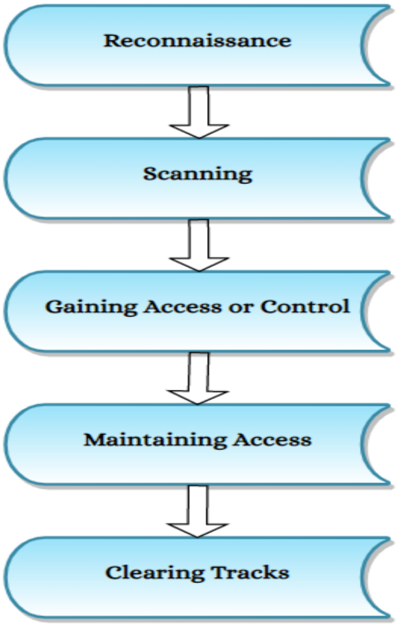


Fig. 1. Phases of Hacking

- **Reconnaissance:** Reconnaissance is the process of gathering information about a target system. This is also referred to as ”foot-printing.” The hacker gathers information on the company that will be hacked. The process requires locating vulnerabilities in the computer system, which entails determining which paths have been left open to attack. If the hacker can get access to the system, he or she will advance with the hacking process. The hacker has a lot of information at the end of the reconnaissance phase, and he can use it to build a viable attack on the target system.
- **Scanning:** The hacker wants to know which system is up, what programs are being utilized, and what versions of the programs are being utilized before launching an assault by creating a blueprint of the target network.

The actual IP addresses of the target network, as well as the services that are running on those systems, are all included in the blueprint. The information obtained during the reconnaissance phase is utilized to inspect the network in this phase, which includes the use of tools such as diallers and port scanners.
- **Gaining Access or Control:** The information obtained in the previous two phases is utilized to enter and take control of the target system over the network or physically in this phase. This is an actual hacking phase that gives the hacker entry to the hacker system. When it comes to system hacking, the first hacker will attempt to gain access to the system. This stage is often referred to as ”Owning the System.”
- **Maintaining Access:** Now that the hacker has gained access to the system, he begins uploading and downloading files. After acquiring access to the system in the previous stage, the hacker keeps it for future attacks and makes changes to it so that no other security personnel or hacker can acquire access to the compromised system. The attacked system is referred to as the ”Zombie System” in this situation.
- **Clearing Tracks:** It is the technique of erasing any remaining log files or other sorts of evidence on the hacked system that could lead to the hacker's capture. The hacker's login will be saved in the login log whenever he or she downloads a file or install the software. Hackers typically hide their tracks by removing log files, audit files, and registry files containing failed log-in attempts and suspicious network behavior.

In the 1960s, programmers at MIT invented the term ”hacker” to characterize someone who could understand and manipulate technology [2]. Hackers have moved beyond only manipulating technology to manipulating people, such as through phishing and a wider range of social engineering techniques. Although hackers continue to exploit technology, their position and nature have also progressed. Hackers are currently classified into three major categories based on their intentions: black-hat, white-hat, and gray-hat.

- **Black hat:** The black-hat hacker is the most well-known form of a hacker; they violate computer security for personal benefit. A ”Cracker,” a more advanced form of the black-hat hacker, is a computer hardware and software expert who breaks into someone's security with evil intent or bad intentions of stealing or damaging their important or secret information, compromising the security of large organizations, or shutting down or modifying the features of websites and networks. However, they are extremely difficult to locate because they are true experts in both the skills and understanding domains.
- **White Hat:** A white-hat hacker is a computer security expert who breaks into and finds security vulnerabilities in an organization's or company's protected networks or computer systems, then fixes them to improve security. With some certificates (CEC - Certified Ethical Hackers), White-Hat is characterized as the nice guys or ”ethical hackers”. White Hat Hackers utilize their talents and knowledge to protect an organization before malicious or bad hackers discover it and cause harm to it. White-hat or ethical hackers are hired by companies to secure their systems and prevent them from other hackers. Even though their methods are similar to those used by black-hat hackers, they have permission from the company or organization that hired them. Following the completion of the engagement, the ethical hacker will produce a report of findings, which will typically include recommendations for how to secure the systems.
- **Grey hat:** A grey-hat hacker is a hybrid of black-hat hackers who work with malicious intent to exploit computer systems and white-hat hackers who strive to keep systems secure. A grey hat hacker is a computer hacker or security expert who occasionally breaks the law but, unlike black hat hackers, has no bad intentions. Grey hat hackers are those who are sponsored to hack. Because they can quickly switch from black-hat to white-hat hacking and vice versa, grey-hat hackers are among the most dangerous types of hackers.

B. *Background*

Despite the fact that internet security is improving, hackers continue to find ways to breach systems. As a result, the need to protect systems from hackers necessitates the promotion of Ethical Hackers, who will fight back against illegal attacks on our computer systems. Ethical hacking is the process of examining security flaws and identifying prospective security vulnerabilities for an organization in charge of the information technology environment under attack [3]. Ethical hackers utilize the same methods to evaluate a security system as their less ethical counterparts, but instead of exploiting flaws, they report them. Ethical hacking and penetration testing are often used interchangeably since they are so closely related. There is, however, a narrow line of distinction between these two terms [4]. Penetration testing is a term that refers to the process of detecting vulnerabilities, dangers, and target environments in order to secure and take control of a system. Ethical hacking, on the other hand, is a broad concept that encompasses all hacking techniques as well as other computer attack strategies. So, in addition to identifying security flaws and vulnerabilities and verifying the target system's security, it goes beyond hacking the system but with authorization to protect the security for future purposes. In general, to carry out tasks, an ethical hacker will need access to each of an organization's systems, whereas a pentester simply needs access to the area of interest.

II. Methods

A. *Ethical Hacking aka Penetration testing*

Penetration testing, also known as intrusion testing or red teaming, is a process of evaluating computer and network security flaws and vulnerabilities [5]. Penetration testing is used to determine whether a system's security is effective or ineffective. The main objective of penetration testing is to find security holes in a controlled environment so that they may be fixed before hackers exploit the system. To find vulnerabilities, ethical hackers use their talents and conduct penetration testing. When making an assessment, special attention is given to data that is extremely sensitive. Penetration testing can be done from a business standpoint to protect the company from failure by preventing financial loss, or from an operational standpoint to discover risks and vulnerabilities.

Penetration testing provides comprehensive information about real-world security threats that can be exploited. We can quickly uncover the most crucial as well as the least significant vulnerabilities by doing penetration tests. Penetration testing can be done from a business standpoint to protect the company from failure by preventing financial loss, or from an operational standpoint to discover risks and vulnerabilities. Pen-testing is divided into three main types, namely, white box testing, grey box testing, and black-box testing. The type of penetration testing is based on the hacker's level of knowledge against its target and the situation of an organization that wants to test it, whether the scope is to simulate an attack by an insider or an external source [5].

- **White-Box Testing:** White-Box is known as Open box testing. It relies on a thorough understanding of the intended and targeted system, as well as all of its software and firmware components. White box testing is based on the attacker's ability to have a comprehensive understanding of how an organization functions. Because the system has already been fully understood, white-box testing takes less time. As a result, it's ideal for testing algorithms. It also assures that all logical statements are validated, as well as syntax checking for any potential design flaws.
- **Grey-Box Testing:** Grey box is also known as translucent testing. It is based on having limited information about the system from a secondary source. In other words, having only a partial understanding of a system. Because the internal programming is only partially known, it takes longer than white-box testing. It is not, however, appropriate for testing algorithms. In reality, it is non-intrusive and unbiased, with the lowest likelihood of tester-developer conflict.
- **Black-Box Testing:** Black box also known as Closed box testing. It is based upon the fact that testers are unfamiliar with the internal/external system, as well as the software and firmware structure. As a result, such a test is conducted from the perspective of the user rather than the designer. Even if the application used is unknown, a pen-tester can be an expert because testers rely on system inconsistencies. Due to the lack of prior knowledge of the tested system, this testing form takes the longest to complete. However, because many program routes are left untested, it is ineffective for testing algorithms or large parts of code.

B. *Ethical Hacking Methodology*

Before engaging in ethical hacking, all technological, administrative, and imperial considerations must be examined. The ethical hacking methodology or life-cycle is very similar to conventional hacking methodology, with the exception that ethical hackers, unlike black-hat hackers, attempt to cause no harm or damage to a given system. The ethical hacking process (See figure-2), on the other hand, is divided into six stages [7].

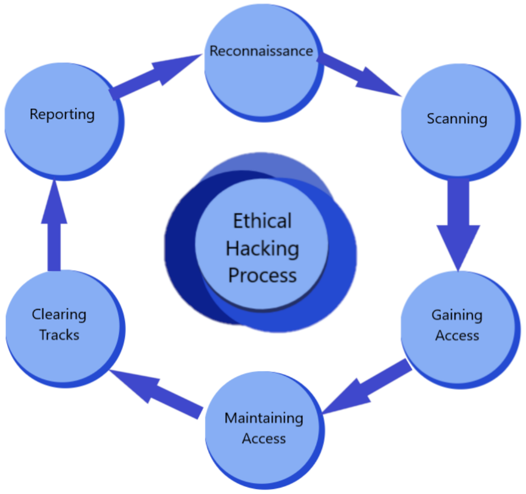


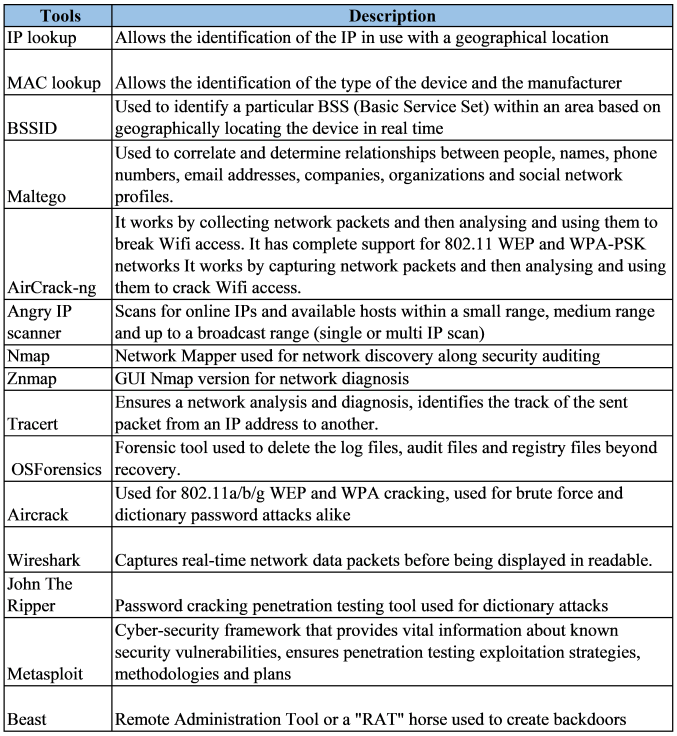
Fig. 2. Ethical Hacking Life-cycle

- **Reconnaissance:** The reconnaissance phase is based on the application of existing processes and techniques that can be utilised either intentionally or unintentionally to gather knowledge about systems or people. In this phase, ethical hackers use passive attacks to obtain network information over a lengthy period in a discreet manner.
- **Scanning:** Ethical hackers rely on simulated attacks during the scanning process to further exploit vulnerabilities. Scanning is based on pen testing to identify any security or vulnerability gaps that could be exploited to carry out an attack. This includes searching for open or underutilised open ports, live hosts, devices, systems, and, services, as well as security vulnerabilities in firewalls, routers, and switches. The second step of scanning, known as enumeration, is used to obtain information about a given target computer, device, system, or service after a complete picture of the system has been generated and the vulnerabilities have been found. This is accomplished by having a steady connection with it.
- **Gaining Access:** Ethical hackers will attempt to get access to the system, once vulnerabilities have been found and all necessary information has been gathered. This is accomplished by using a variety of pen-testing tools and techniques to virtually break into the system and bypass security protections. Passwords are recovered via cracking attempts in this step.
- **Maintaining Access:** After gaining access to a system, the system's resources can be exploited by looking for additional common vulnerable devices. This involves infecting them with a worm, or infecting them with malware or viruses, which can transform these machines into bots or ”zombies,” or implementing a rootkit. This secures remote access by granting administrative privileges at both the OS and application levels.

- **Clearing Tracks:** The attacker will attempt to erase his traces after achieving and maintaining a successful attack by employing forensic and anti-forensic tactics and tools. Hackers typically hide their traces by deleting log files, audit files, and registry files that include unsuccessful log-in attempts and unusual network behaviour, effectively removing any source of evidence.
- **Reporting:** In final stage, Ethical Hacker creates a report detailing his findings and the work he performed, including the tools he used, the success rate, vulnerabilities discovered, and exploit methods, as well as recommendations. This is what distinguishes a malicious hacker from an ethical hacker.

C. Ethical Hacking Tools

The cyber security business is a vast and active community, and there are several tools available to assist in Ethical hacking. It is critical to ensure that we are utilising the right tools for the ethical hacking process. Many tools focus on certain tests, but no single tool can test for everything; therefore, the more tools you have, the easier it will be to conduct ethical hacking. Before employing any ethical hacking technique, it's crucial to understand your personal and technical constraints. Figure-3 represents the important tools used for Ethical Hacking [8][9].



Tools	Description
IP lookup	Allows the identification of the IP in use with a geographical location
MAC lookup	Allows the identification of the type of the device and the manufacturer
BSSID	Used to identify a particular BSS (Basic Service Set) within an area based on geographically locating the device in real time
Maltego	Used to correlate and determine relationships between people, names, phone numbers, email addresses, companies, organizations and social network profiles.
AirCrack-ng	It works by collecting network packets and then analysing and using them to break Wifi access. It has complete support for 802.11 WEP and WPA-PSK networks It works by capturing network packets and then analysing and using them to crack Wifi access.
Angry IP scanner	Scans for online IPs and available hosts within a small range, medium range and up to a broadcast range (single or multi IP scan)
Nmap	Network Mapper used for network discovery along security auditing
Znmap	GUI Nmap version for network diagnosis
Tracert	Ensures a network analysis and diagnosis, identifies the track of the sent packet from an IP address to another.
OSForensics	Forensic tool used to delete the log files, audit files and registry files beyond recovery.
Aircrack	Used for 802.11a/b/g WEP and WPA cracking, used for brute force and dictionary password attacks alike
Wireshark	Captures real-time network data packets before being displayed in readable.
John The Ripper	Password cracking penetration testing tool used for dictionary attacks
Metasploit	Cyber-security framework that provides vital information about known security vulnerabilities, ensures penetration testing exploitation strategies, methodologies and plans
Beast	Remote Administration Tool or a "RAT" horse used to create backdoors

Fig. 3. Ethical Hacking Tools

D. Ethics in Ethical Hacking

The most significant downside of ethical hacking is the possibility of information exposure. As an outsider, the ethical hacker risks disclosing the company's secret information to others, either purposefully or unwittingly. With the growing demand for ethical hackers as part of a multi-layered security program, as well as the potentially sensitive and personal information that an ethical hacker may have access to, it's more important now to ensure proper ethical behaviour. Consider an ethical hacker hired to assess the security of a company that handles personal or highly sensitive information, such as a bank or law firm. Although this topic isn't limited to those types of businesses, such information in the wrong hands might be used for a variety of purposes. Several ethical problems should be explored in this situation, including: what do they do with the information and possible knowledge obtained? What safeguards are in place to ensure that the information is kept private? How does the attacker deal with a negative situation such as file corruption or disruption of the network?

Ethical hacking code of ethics or behaviour focuses on the ethical hacker's duties, responsibilities, and limitations when performing his profession. The ethical hacker ensures that the client's system or network has been thoroughly examined for security flaws and vulnerabilities. The ethical hacker's code of ethics must prioritize the protection of the client's system or network, as well as the ethical hacker's ability to accomplish his job effectively. As per the EC-Council code of ethics [10], an ethical hacker must ensure

- Before hacking, identify and determine the security and privacy of any organization's data, as well as any rules and regulations that may apply.
- By depending on your creativity and efforts to protect other people's intellectual property, you may ensure that all advantages go to the creator.
- Do not exceed the client's established boundaries when undertaking ethical hacking. It is feasible to have access beyond the target areas that the client signed up for in ethical hacking. Stay within the system or network's target areas as specified in the work agreement.
- Transparency guarantees that the client is aware of what is happening, and that the client can take the required steps to ensure the system's security. Potential threats to any e-commerce clients, the Internet community, or the public that you reasonably suspect are associated with a certain set or kind of electronic transactions, or related software or hardware should be disclosed to authorized persons or authorities.
- Do not share any of the private or confidential information discovered during the hacking with anyone. Ethical hacking is rendered useless when the client's confidential information is revealed.

III. Results and Discussion

Ethical hackers use many tools and techniques to find vulnerabilities in the system. Ethical hackers utilize the same methods as hackers to evaluate a security system as their less ethical counterparts, but instead of exploiting flaws, they report them. Ethical hacking and penetration testing are often used interchangeably since they are so closely related. To find vulnerabilities, ethical hackers use their talents and conduct penetration testing. When making an assessment, special attention is given to data that is extremely sensitive. Penetration testing can be done from a business standpoint to protect the company from failure by preventing financial loss, or from an operational standpoint to discover risks and vulnerabilities. Penetration testing provides comprehensive information about real-world security threats that can be exploited and can quickly uncover the most crucial as well as the least significant vulnerabilities by doing penetration tests.

Ethical hackers examine the security flaws and identifying prospective security vulnerabilities for an organization in charge of the information technology environment under attack. Every organization should be proactive rather than reactive to find the vulnerabilities in order to secure the system and protect from hackers. It is important to understand the types of Ethical Hacking and tools used. In assessing a system's security, an ethical hacker looks for answers to these basic questions: How intruder can gain access to the target system? Are they any weak link in the security system? On the target systems, what can an intruder see? What could an intruder do with that data? Is anyone at the target paying attention to the intruder's efforts or successes? It is important to understand about weak links and Vulnerabilities in the system and more important to understand if the organization can track the activities of the intruder, if the owners of the target systems are unaware that someone is attempting to break-in, the intruders can and will try for weeks or months before succeeding.

On the other hand, there is a lot of debate over ethical hacking. Many people consider that hacking is unethical. However, with the rise of cyber-crime, it is clear that businesses and governments must ensure their cybersecurity is flawless. That takes us to the value of ethical hacking and its application in the digital world. Ethical hacking codes of ethics or conducts focus on the ethical hacker's duties, responsibilities, and limitations when performing his profession. The ethical hacker ensures that the client's system or network has been thoroughly examined for security flaws and vulnerabilities.

IV. Conclusion

The entire world is moving toward technological advancements and increasing digitization of real-world activities, which increases the danger of security. Hacking, specifically cracking computer systems, is the primary cause of this insecurity. As a result, the need to protect systems from hackers necessitates the promotion of Ethical Hackers, who will fight back against illegal attacks on our computer systems. In this paper, I have concentrated on the importance and limitations of ethical hacking or penetration testing, tools used for penetration testing, and guidelines or the code of conduct to be followed by ethical hackers.

Internet security is more proactive, such as Ethical Hackers who attempt to hack into a corporation or organization prior to an 'attack' in order to discover any weak links. Companies engage ethical hackers to hack their own firm and find any flaws where an ill-intentioned hacker could cause damage so that the company can improve its security and cover the risks. Ethical hacking, when done correctly, aids in the discovery of security flaws. Penetration testing is more useful in identifying security flaws in a system. It is important to prevent data loss, financial loss, and the proactive reduction of recognized dangers. They put their creativity and expertise to work to make a company's digital world a reliable and secure environment for both owners and customers. These 'Cyber Cops' are in charge of preventing cybercrime and ensuring the safety of the internet. Hacking is important in the computer system since it deals with both good and bad sides and it attracts lots of debate about ethical hacking. This demands the guidelines or EC-council code of conduct for ethical hackers to focus on the ethical hacker's duties, responsibilities, and limitations when performing his profession.

V. Acknowledgment

I express my sincere gratitude to Dr. Trevor M. Tomesh for sharing his able guidance and amazing expertise throughout my project. The information provided in the project paper is true and, to the best of my knowledge, referring to different papers in different areas of Ethical Hacking.

References

[1] GeeksforGeeks, Methodology followed by the Hackers, https://www.geeksforgeeks.org/methodology-followed-by-the-hackers

[2] Hacker, ”SearchSecurity”, https://searchsecurity.techtarget.com/definition/hacker

[3] J. Metso, ”Penetration testing”, Bachelor's thesis - Oulu University of Applied Sciences, Autumn 2019

[4] Tutorialspoint, ”Penetration Testing Vs. Ethical Hacking”, https://www.tutorialspoint.com/penetration-testing/penetration-testing-vs-ethical-hacking.htm

[5] C. Lakshmi, P. Basarkod, ”BASICS OF ETHICAL HACKING”, International Journal of Engineering Sciences Emerging Technologies, Jan2015, ISSN:22316604 Volume 7, Issue 4, pp: 715-720

[6] Scott Cosentino, ”The Phases of Ethical Hacking”, https://scottc130.medium.com/the-phases-of-ethical-hacking-c1ecb60f6ddc

[7] Tutorialspoint, ”Ethical Hacking - Process”, https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_process.htm

[8] EC-Council, ”Code of Ethics”, https://www.eccouncil.org/code-of-ethics/

[9] Tuturialspoint, ”Ethical Hacking - Tools”, https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tools.htm

[10] w3schools, ”Scanning Techniques”, https://www.w3schools.in/ethical-hacking/scanning-techniques/

VI. Supporting Material

News on Ethical hacking and the importance or need of Ethical hacking. Below listed articles referred apart from the references listed

- ”How do you become an ethical hacker?”, https://www.itpro.co.uk/641470/so-you-want-to-be-an-ethical-hacker
- ”Metasploit”, https://www.metasploit.com/

- ”NMAP Security”, https://nmap.org/
- ”The proliferation of hacking as a service is giving cybersecurity experts nightmares ”, https://economictimes.indiatimes.com/tech/internet/the-proliferation-of-hacking-as-a-service-is-giving-cybersecurity-experts-nightmares/articleshow/76787932.cms
- ”Apple pays ethical hackers $288k for finding 55 vulnerabilities”, https://www.itpro.co.uk/security/ethical-hacking/357380/apple-pays-ethical-hackers-288k-for-finding-55-vulnerabilities
- ”Mobile banking apps are exposing user data to attackers”, https://www.itpro.co.uk/security/ethical-hacking/356252/poorly-secured-banking-apps-lead-to-cyber-threats
- ”Many BellTroxes: Delhi is now India’s hacker hub”, https://economictimes.indiatimes.com/tech/internet/many-belltroxes-delhi-is-now-indias-hacker-hub/articleshow/76304052.cms
- ”India’s Ethical Hackers Rewarded Abroad, Ignored at Home”, https://gadgets.ndtv.com/internet/features/indias-ethical-hackers-rewarded-abroad-ignored-at-home-1705103
- ”Decade-old Arcadyan Firmware Vulnerability Risks Millions Of Routers Attribution link”, https://latesthackingnews.com/2021/08/11/decade-old-arcadyan-firmware-vulnerability-risks-millions-of-routers/