# Research Paper on Ethical Hacking

**Harsh Jain[1], Joshi Javan[2], Kavya Shah[3], Madhvi Bera[4]**

[1,2,3] B-Tech Student, Computer Science and Engineering, Indus Institute of Technology and Engineering, Ahmedabad – 382115

[4] B-Tech Professor, Computer Science and Engineering, Indus Institute of Technology and Engineering, Ahmedabad – 382115

## Abstract:

This paper explores the significance of ethical hacking in safeguarding the security of the contemporary digital landscape. It delves into the definition of ethical hacking, addressing the legal considerations associated with this practice. Furthermore, it elucidates the essential skills and capabilities required by ethical hackers. The paper also scrutinizes the ethical hacking process, highlighting the protective measures implemented to mitigate legal risks for ethical hackers. The conclusion provides an insight into the challenges encountered by ethical hackers in their profession, along with suggested solutions to foster ethical hacking.

## Introduction:

The heightened prevalence of digital technology and the growing complexity of online threats present a substantial peril to the security and privacy of both organizations and individuals. Consequently, safeguarding digital systems requires more than merely relying on firewalls and antivirus software. In response to this challenge, organizations can enlist the expertise of ethical hackers. These professionals leverage their specialized skills to simulate system attacks, aiming to pinpoint and rectify vulnerabilities. By doing so, they enhance system security and contribute to the development of robust security protocols.

## Defining Ethical Hacking:

Ethical hacking involves conducting penetration tests on an organization's digital systems to uncover security vulnerabilities and assess the effectiveness of system defences. What distinguishes ethical hacking from its illicit counterpart is its emphasis on testing and enhancing system defences. Ethical hackers are dedicated to fortifying security measures and addressing identified vulnerabilities. Typically, organizations engage ethical hackers to simulate attacks on their systems, uncovering potential vulnerabilities that might elude non-expert staff.

## History of Ethical Hacking:

The term "ethical hacking" was coined in the 1990s by IBM employee John Patrick, but the practice itself predates this period. In the 1960s and 1970s, the U.S. government pioneered the hiring of computer experts to hack into their own systems—a group known as "red teams." These teams simulated attacks to uncover weaknesses and enhance security.

As computer networks expanded in the 1980s and 1990s, businesses and organizations followed suit by employing "white hat" hackers to identify and rectify security vulnerabilities. The term "white hat" denotes the ethical use of their skills for the greater good rather than personal gain.

Today, ethical hacking plays a pivotal role in cybersecurity. Professional organizations offer certifications and training programs for ethical hackers, reflecting its importance. Ethical hacking is instrumental in identifying vulnerabilities across computer systems, networks, and applications, aiding organizations in fortifying their overall security posture.

## Types of Ethical Hacker:

The different types of Ethical Hackers are mentioned below:

- **Black Hat Hacker:** Black hat hackers are individuals who engage in malicious activities within the digital realm for personal gain, financial profit, or to cause harm. Their intent involves unauthorized actions, such as stealing sensitive data, spreading malware, or disrupting computer systems. Unlike ethical hackers, black hat hackers operate outside legal and ethical boundaries, utilizing their skills for nefarious purposes. Motivations often revolve around financial incentives or a desire to create chaos. These individuals pose a significant threat to cybersecurity, exploiting vulnerabilities for their benefit and representing a constant challenge for organizations and individuals seeking to protect their digital assets.

- **White Hat Hacker:** White hat hackers, also known as ethical hackers, are individuals who engage in hacking activities with the explicit goal of enhancing cybersecurity. Unlike their black hat counterparts, white hat hackers operate within legal and ethical boundaries. Their primary intent is to identify and rectify vulnerabilities within computer systems, networks, and applications. Motivated by a sense of responsibility, they use their skills to improve overall security, protecting organizations and individuals from potential threats and cyberattacks. White hat hackers play a crucial role in the field of cybersecurity, working to fortify defences, conduct penetration testing, and contribute to the development of robust security protocols. Their actions align with ethical standards, making them valuable assets in the ongoing effort to create a more secure digital environment.

- **Grey Hat Hacker:** Grey hat hackers occupy a middle ground in the hacking spectrum, operating between black hat and white hat practices. These individuals engage in hacking activities without explicit authorization but lack malicious intent. Instead, they often uncover and disclose vulnerabilities to highlight security flaws.

Grey hat hackers might bring attention to weaknesses in systems, networks, or applications without adhering strictly to legal standards. Motivations for grey hat hackers can vary, with some driven by a desire to assist organizations in improving their security posture. While their actions may be beneficial in exposing vulnerabilities, the ethical ambiguity of their methods distinguishes them from both white hat and black hat hackers.

- **Script Kiddies:** Script kiddies are individuals with limited technical skills who engage in hacking activities using pre-written scripts or tools created by others, rather than developing their own. Unlike more sophisticated hackers, script kiddies lack in-depth knowledge of programming or cybersecurity principles. Their motivation often revolves around curiosity, a desire for recognition, or the thrill of causing disruption. While they may attempt to engage in hacking for entertainment or experimentation, script kiddies typically rely on the work of others, making them less skilled and more reliant on easily accessible tools. Their activities are often less targeted and more opportunistic, lacking the strategic intent of more experienced hackers.

- **Hacktivists:** Hacktivists are individuals or groups who employ hacking techniques to advance political or social causes. Unlike traditional hackers driven by personal gain, hacktivists use their skills as a form of activism, seeking to promote ideologies, challenge perceived injustices, or advocate for specific social or political issues. Their actions may involve website defacement, data leaks, or denial-of-service attacks, often aiming to influence public opinion or bring attention to their cause. The term "hacktivist" is a combination of "hacker" and "activist," reflecting their commitment to using digital tools to further their socio-political objectives. While motivations vary, hacktivists share a common goal of leveraging technology for advocacy, sometimes blurring the lines between online activism and cyber disruption.

- **Phreakers:** Phreakers are individuals with expertise in manipulating and exploiting telecommunication systems, especially during the early days of technology. Originating in the 1960s and 1970s, phreakers focused on exploring and manipulating phone lines and networks. Their activities included methods to make free phone calls, manipulate billing systems, or gain unauthorized access to telecommunications infrastructure. The term "phreaking" is a portmanteau of "phone" and "freaking," highlighting their fascination with the intricacies of telephone systems. While the prominence of phreaking
has diminished with advancements in technology, it remains a historical precursor to modern cybersecurity concerns, emphasizing the early exploration and exploitation of communication networks.

- **Cyber Espionage:** Cyber espionage involves the use of hacking techniques, often by state-sponsored actors, to conduct intelligence gathering or cyber warfare. In this form of cyber activity, governments or other entities aim to acquire sensitive information, gain a strategic advantage, or monitor the activities of other nations or organizations. Cyber espionage can encompass various tactics, including sophisticated malware, phishing campaigns, and other cyber infiltration methods. Motivations for cyber espionage often revolve around national interests, political advantage, or military strategies. The perpetrators seek to gain valuable insights, steal classified information, or disrupt the operations of their targets, making it a significant concern in the realm of cybersecurity and international relations.

- **Malware Authors:** Malware authors are individuals or groups responsible for creating and distributing malicious software, commonly known as malware. This software is designed to compromise computer systems, steal sensitive data, or cause damage to digital infrastructure. Motivations for malware authors vary, and they may include financial gain, data theft, or advancing a particular agenda. Malware can take various forms, such as viruses, worms, trojans, ransomware, and spyware, each with its specific malicious intent. Malware authors leverage their programming skills to exploit vulnerabilities in computer systems and networks, posing a continuous challenge for cybersecurity professionals seeking to protect against these digital threats.

- **Social Engineers:** Social engineers are individuals who specialize in exploiting human psychology to manipulate and deceive others into divulging sensitive information, granting unauthorized access, or performing actions that compromise security. Unlike traditional hackers who target technical vulnerabilities, social engineers rely on interpersonal skills and psychological tactics to achieve their objectives. Their methods may involve impersonation, pretexting, or other forms of deception to gain the trust of individuals and extract valuable information. Social engineering attacks can take various forms, including phishing, pretext calls, and impersonation in person or online. The primary motivation behind social engineering is often data theft, unauthorized access, or the acquisition of confidential information for malicious purposes. As technology advances, social engineering remains a prevalent and significant threat to cybersecurity.

- **Hacktivist Groups:** Hacktivist groups are collective entities that utilize hacking techniques as a means of advancing political, social, or ideological causes. These groups distinguish themselves by combining digital skills with activist principles, employing various cyber tactics to promote their agenda. Notable examples include Anonymous and Lizard Squad. Hacktivist activities may involve website defacement, distributed denialof-service (DDoS) attacks, or the release of sensitive information to draw attention to perceived injustices. Motivations vary widely, encompassing political activism, social justice advocacy, or resistance against institutions they view as oppressive or corrupt. The term "hacktivist" underscores their commitment to leveraging digital tools to influence public opinion or bring about change, blurring the lines between online activism and disruptive cyber actions.

**Legal Issues Related to Ethical Hacker:**

With the escalating prevalence of internet usage in India, the specter of cyber-attacks has emerged as a substantial threat to the security of computer networks. In response, India embraced the model law on electronic commerce, sanctioned by the United Nations Commission on
International Trade Law. This initiative culminated in the enactment of the Information
Technology Act of 2000. The primary thrust of this legislation is to confer legal recognition upon transactions conducted through electronic data interchange, commonly referred to as "electronic commerce." This shift involves a departure from traditional paper-based communication and information storage methods.

Section 84 of the Act discerns a nuanced demarcation between black hat hackers and white hat hackers. It accentuates the protection afforded to the government, controllers, or their duly authorized representatives acting in good faith. The provision extends a shield to ethical hackers appointed by the government or a controller, ensuring their protection when operating in compliance with the act, rules, or regulations.

Section 43 of the Act specifically addresses unauthorized access to computers, systems, or networks. Individuals who modify, damage, disrupt a computer network, or access data without permission may incur penalties for damages. The provision introduces a caveat that absolves individuals acting under authority or in good faith from liability for damages.

Section 43-A holds individuals accountable for compensation if they fail to protect data. Notably, if an ethical hacker, functioning as a body corporate, neglects to secure the data they handle, they may be held liable under this section.

Section 66 of the IT Act is dedicated to computer-related offenses, penalizing those who engage dishonestly and fraudulently in acts mentioned in Section 43. The maximum penalty for such offenses is three years.

Government agencies, including the CBI, Army, law enforcement bodies, Intelligence Bureau, and the Ministry of Communication and Information Technology, wield the authority to establish agencies under Section 70-A and Section 70-B for Critical Information Infrastructure Protection. These agencies are empowered to enlist cybersecurity experts to counter cyber terrorism, as stipulated in Section 66-F, which addresses acts performed without authorization or that exceed authorized access.

While the Information Technology law in India imposes penalties on hackers without proper authorization, the explicit protection for ethical hackers is contingent upon their employment by the government under Section 84. Recognizing the pivotal role ethical hackers play in fortifying computer networks against cyber terrorism and attacks, their contribution is indispensable to the overarching goal of cybersecurity.

### Skills of an Ethical Hacker:

#### 1) Technical Proficiency:

a. **Networking Skills:** Ethical hackers must understand network protocols (TCP/IP, UDP), network configurations, and overall network architecture. Proficiency in analysing network traffic is crucial for identifying vulnerabilities.

b. **Programming Knowledge:** Knowledge of programming languages, such as Python, C, or Java, allows ethical hackers to script their tools, analyze code for vulnerabilities, and automate tasks during assessments.

c. **Operating Systems Knowledge:** Familiarity with operating systems like Windows, Linux, and Unix is essential. Ethical hackers need to navigate and understand various environments to identify system weaknesses.

2) **Cybersecurity Fundamentals:**

a. **Security Protocols:** A deep understanding of security protocols, encryption algorithms, and cryptographic techniques is fundamental. This knowledge helps in securing communication and protecting sensitive data.

b. **Vulnerability Assessment:** Ethical hackers should be adept at identifying and assessing vulnerabilities in systems, networks, and applications. This involves using tools and methodologies to discover potential weaknesses.

3) **Web Application Security:**

a. **Web Technologies:** Understanding web technologies, such as HTML, CSS, and JavaScript, is crucial for assessing and securing web applications. Knowledge of how web applications function aids in identifying and addressing vulnerabilities.

b. **Web Security Tools:** Proficiency in using tools like Burp Suite, OWASP Zap, and others is essential for testing web applications. These tools assist in identifying and mitigating security risks.

4) **Penetration Testing:**

a. **Penetration Testing Tools:** Ethical hackers should be familiar with tools like Metasploit, Nmap, and Wireshark for simulating cyberattacks. These tools aid in identifying weaknesses and assessing the security posture of systems.

b. **Exploitation Techniques:** Understanding ethical exploitation techniques is critical. Ethical hackers need to comprehend how attackers might exploit vulnerabilities to gain unauthorized access.

5) **Security Frameworks and Standards:**

a. **Compliance Knowledge:** Ethical hackers need to understand security standards and compliance frameworks (ISO 27001, NIST, etc.) to align their security practices with industry standards. Compliance ensures a structured and secure approach.

b. **Risk Management:** Evaluating and managing risks is a key skill. Ethical hackers should be able to assess the potential impact of vulnerabilities and prioritize security efforts accordingly.

6) **Forensic Skills:**

a. **Incident Response:** Ethical hackers must be skilled in incident response, involving the ability to respond to security incidents effectively, contain threats, and implement corrective measures.

b. **Digital Forensics:** Knowledge of forensic tools and techniques is essential for analysing digital evidence. Ethical hackers may be involved in investigating breaches and collecting evidence.

7) **Soft Skills:**

a. **Communication Skills:** Effective communication is crucial for ethical hackers. They need to articulate complex technical concepts in a clear manner and convey security findings and recommendations to both technical and non-technical stakeholders.

b. **Problem-Solving:** Ethical hackers encounter intricate problems regularly. Strong problem-solving skills enable them to analyse complex systems, identify vulnerabilities, and propose effective solutions.

8) **Continuous Learning:**

a. **Curiosity and Learning Mindset:** The dynamic nature of cybersecurity requires a curious mindset and a commitment to continuous learning. Ethical hackers need to stay informed about the latest threats, vulnerabilities, and security trends.

b. **Stay Updated:** Regularly updating knowledge about emerging threats, new vulnerabilities, and evolving security technologies is crucial for an ethical hacker to remain effective in their role.

9) **Legal and Ethical Understanding:**

a. **Legal Knowledge:** Ethical hackers need familiarity with laws and regulations related to cybersecurity to ensure their activities are within legal boundaries.

b. **Ethical Conduct:** Upholding ethical standards and maintaining integrity is critical. Ethical hackers should operate transparently, respecting privacy and adhering to professional ethical guidelines.

10) **Certifications:**

a. **Industry Certifications:** Certifications such as Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), and others are recognized benchmarks in the industry. They validate an ethical hacker's skills and expertise.

**Ethical Hacking Process:**

Following is the process for Ethical Hacking:

1) Planning and Reconnaissance
2) Scanning
3) Gaining Access
4) Maintaining Access
5) Analysis and WAF Configuration

A perpetrator or an ethical hacker both adhere to a similar five-step hacking process when attempting to infiltrate a network or system. The ethical hacking process initiates with the exploration of diverse methods to breach the system, exploiting vulnerabilities, establishing consistent access to the system, and ultimately, covering one's tracks. The five phases of ethical hacking are:

### 1) Reconnaissance

The initial step in the ethical hacking methodology is reconnaissance, also termed as the footprint or information gathering phase. The primary objective during this preparatory phase is to amass comprehensive information. Prior to launching any attack, the attacker or ethical hacker meticulously gathers all essential details about the target.
This data may encompass passwords, crucial employee information, and more. Tools such as HTTP Track facilitate the download of entire websites to extract pertinent details about an individual. Similarly, search engines like Maltego aid in researching an individual through various links, job profiles, news, etc.

Reconnaissance holds paramount importance in ethical hacking as it identifies potential attacks and assesses the vulnerability of an organization's systems. Footprinting, within the reconnaissance phase, involves data collection from various areas, including TCP and UDP services, vulnerabilities, specific IP addresses, and the host of a network. In ethical hacking, footprinting manifests in two forms:

a) **Active Footprinting:** This method entails gathering information directly from the target using tools like Nmap to scan the target's network.

b) **Passive Footprinting:** The alternative method involves collecting information without directly accessing the target. Attackers or ethical hackers can obtain reports through sources like social media accounts and public websites.

### 2) Scanning

The second stage in the hacking methodology is scanning, a process where attackers seek diverse avenues to acquire the target's information. In this phase, the attacker aims to identify information such as user accounts, credentials, and IP addresses. Ethical hacking involves searching for efficient and rapid methods to access the network and retrieve information. Tools employed during the scanning phase include dialers, port scanners, network mappers, sweepers, and vulnerability scanners, which are crucial for examining data and records. In the ethical hacking methodology, four distinct types of scanning practices are employed:

a) **Vulnerability Scanning:** This practice focuses on identifying vulnerabilities and weak points within a target, exploring various methods to exploit these weaknesses. Automated tools like Netsparker, OpenVAS, and Nmap are commonly used for vulnerability scanning.

b) **Port Scanning:** Port scanning involves the utilization of port scanners, dialers, and other data-gathering tools to observe open TCP and UDP ports, running services, and live systems on the target host. Ethical hackers leverage port scanning to discover accessible entry points to an organization's systems.

c) **Network Scanning:** This practice is employed to detect active devices on a network and ascertain potential ways to exploit it. It can be applied to organizational networks where all employee systems are interconnected. Ethical hackers utilize network scanning to fortify a company's network by identifying vulnerabilities and potential access points.

d) **System Scanning:** In this type of scanning, ethical hackers examine individual systems for vulnerabilities and weaknesses. This targeted approach allows for a more granular assessment of security within the network.

These scanning practices are integral to the ethical hacking process, enabling security professionals to proactively identify and address vulnerabilities, ultimately fortifying the security posture of the targeted systems or networks.

### 3) Gaining Access

The subsequent phase in hacking involves the attacker employing all available means to gain unauthorized access to the target's systems, applications, or networks. Utilizing various tools and methods, the attacker endeavours to infiltrate the system with the aim of exploiting it—whether by downloading malicious software or applications, pilfering sensitive information, attaining unauthorized access, or making ransom demands. Metasploit stands out as one of the most frequently utilized tools for gaining access, while social engineering remains a prevalent method for exploiting a target.

Ethical hackers and penetration testers play a crucial role in fortifying potential entry points. They ensure that all systems and applications are safeguarded with robust passwords and secure the network infrastructure through the implementation of firewalls. In a proactive approach, they may simulate social engineering attacks, including the creation of deceptive emails, to discern which employees might be susceptible to cyberattacks. This enables them to identify vulnerabilities and fortify the organization's defences against unauthorized access and potential exploitation.

### 4) Maintaining Access

Upon successfully accessing the target's system, the attacker endeavours to persist in maintaining that access. During this stage, the hacker systematically exploits the system, orchestrates Distributed Denial of Service (DDoS) attacks, utilizes the compromised system as a launching point for further attacks, or exfiltrates the entire database. Tools such as backdoors and Trojans are employed to exploit vulnerable systems, pilfer credentials, essential records, and more. The objective in this phase is for the attacker to sustain their unauthorized access covertly, ensuring that their malicious activities go undetected by the user.

Ethical hackers and penetration testers can leverage this phase by conducting a comprehensive scan of the entire organization's infrastructure. This enables them to identify and apprehend any malicious activities, trace their root causes, and implement preventive measures to mitigate the risk of systems being exploited. Through proactive measures in this stage, ethical hackers contribute to fortifying the organization's defences and thwarting potential unauthorized access or malicious activities.

### 5) Clearing Track

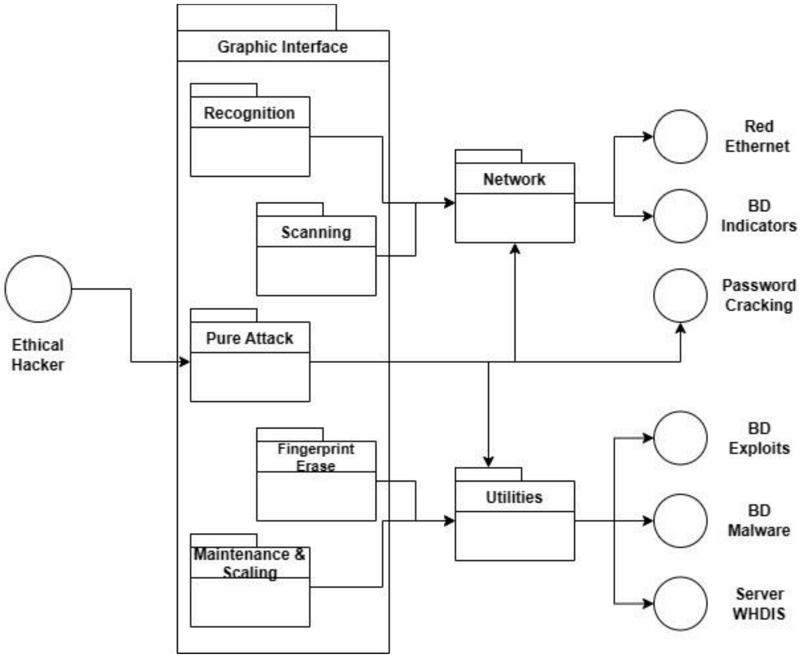
The final phase of ethical hacking necessitates hackers to meticulously clear their tracks, as no attacker desires to be apprehended. This critical step ensures that attackers leave no discernible clues or evidence that could be traced back to their activities. It holds particular significance for ethical hackers, who need to maintain their connection within the system without being identified by incident response or forensic teams. Techniques employed in this phase may involve editing, corrupting, or deleting logs and registry values. Additionally, attackers may delete or uninstall folders, applications, and software or manipulate changed files to revert to their original values. In ethical hacking, practitioners can utilize various methods to erase their tracks, including:

a) **Reverse HTTP Shells:** Employing reverse HTTP shells allows ethical hackers to obscure their activities and evade detection.

b) **Deleting Cache and History:** Clearing the digital footprint by deleting cache and browsing history helps in covering tracks effectively.

c) **Using ICMP (Internet Control Message Protocol) Tunnels:** Leveraging ICMP tunnels provides a covert means of communication, aiding in maintaining anonymity.

These five phases encapsulate the Certified Ethical Hacking (CEH) methodology, empowering ethical hackers and penetration testers to detect vulnerabilities, identify potential entry points for cyberattacks, and mitigate security breaches to enhance organizational security. For those seeking in-depth knowledge on analysing and enhancing security policies and network infrastructure, pursuing an ethical hacking certification, such as Certified Ethical Hacking (CEH v12) offered by EC-Council, can provide comprehensive training on understanding and utilizing hacking tools and technologies within legal and ethical frameworks.



**What is CVE:**

CVE, which stands for Common Vulnerabilities and Exposures, functions as a compendium that categorizes vulnerabilities. This glossary scrutinizes vulnerabilities and employs the Common Vulnerability Scoring System (CVSS) to assess the severity of each vulnerability. The CVE score is frequently employed to prioritize the mitigation of security vulnerabilities.

The CVE glossary represents an initiative dedicated to monitoring and documenting vulnerabilities in both consumer software and hardware. Managed by the MITRE Corporation and supported by funding from the US Division of Homeland Security, this project utilizes the Security Content Automation Protocol (SCAP) to accumulate and organize vulnerability data.
SCAP assesses vulnerability information and assigns a distinctive identifier to each vulnerability.

For a vulnerability to be classified as a CVE, it must satisfy specific criteria, including:

1. **Independence from other issues:** The vulnerability should be capable of being addressed independently of other issues.

2. **Vendor acknowledgment:** The vendor must be aware of the vulnerability and acknowledge its potential to pose a security risk.

3. **Proven security risk:** Submission of the vulnerability should be accompanied by evidence demonstrating its security impact, thereby contravening the vendor's security policies.

4. **Affecting a singular codebase:** Each product vulnerability is assigned a distinct CVE. If vulnerabilities arise from shared protocols, standards, or libraries, a separate CVE is designated for each affected vendor. An exception is made when using the shared component is unavoidable without incorporating the vulnerability.

### What is CVSS:

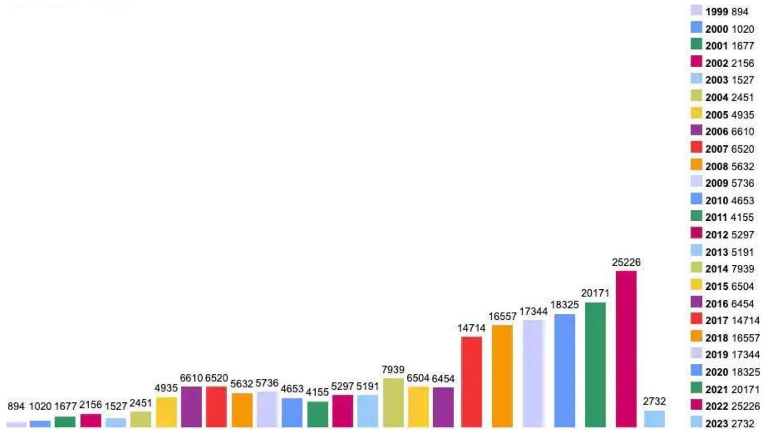
The CVSS is among various methods employed to gauge the significance of vulnerabilities, commonly referred to as the CVE score. It operates as an open set of standards designed for evaluating vulnerabilities and assigning a severity level on a scale ranging from 0 to 10. The present version of CVSS is v3.1, and the scale is delineated as follows:

| **Severity** | **Base Score** |
|---|---|
| None | 0 |
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

The CVSS standard is adopted by numerous well-established organizations, such as NVD, IBM, and Oracle. For those interested in understanding the calculation of CVSS or converting scores assigned by entities not employing CVSS, the NVD calculator is a valuable resource.

### Essential Penetration Testing Statistics:

The continuously expanding threat landscape persists in its global impact on companies, influencing their critical infrastructure. In the year 2022, there was a remarkable surge in CVE data, reaching over 25,000 publications, marking it as a record-breaking growth year. On a daily average, there were 68.75 CVEs published during this period. Hence, it is crucial to delve into the statistics of these vulnerabilities and comprehend their impact:



- In 2022, there were 404 high-risk vulnerabilities featuring CVSSv3 scores of 10.00 and RCE access, surpassing the 363 recorded in 2021.
- The tech ecosystem witnessed the emergence of 860 vulnerabilities in 2022, with CVSSv3 scores ranging from 9.0 to 10.0, in contrast to the 1165 vulnerabilities reported in 2021.
- A total of over 13,000 vulnerabilities were published in 2022, with 3,238 flagged with CVSSv2 scores between 7.0 and 10.0. This represents a 40% reduction compared to 2021, which documented around 21,000 vulnerabilities.
- Cobalt's State of Pentesting 2022 highlights the top 5 most prevalent vulnerability categories identified by the pentesting community: Server Security Misconfigurations (38%), Cross-Site Scripting (13%), Broken Access Control (11%), Sensitive Data Exposure (10%), and Authentication and Sessions (8%).
- In 2021, a minimum of 66 zero-day vulnerabilities surfaced. The rapid proliferation of hacking tools globally is cited as a contributing factor to this growth rate.

**References:**

1. https://www.knowledgehut.com/blog/security/types-of-ethical-hacking#what-are-theimportance-and-the-key-concepts-of-ethical-hacking?%C2%A0
2. https://www.knowledgehut.com/blog/security/history-of-ethical-hackers#the-origins-ofthe-hacker%C2%A0
3. https://images.app.goo.gl/rsAgG35nneyoyXdr9
4. https://blog.ipleaders.in/legality-of-ethical-hacking-in-india/
5. https://www.eccouncil.org/cybersecurity/what-is-ethical-hacking/
6. https://pentest-tools.com/blog/penetration-testing-statistics
7. https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/