5/4/2025

INTRODUCTION TO ETHICAL HACKING

RESEARCH REPORT

Balaji Varaprasad
CYBER SAPIENS

INTRODUCTION:

Ethical hacking is the authorized practice of deliberately probing computer systems, networks, and applications to identify and fix security vulnerabilities before malicious hackers can exploit them. Often carried out by cybersecurity professionals known as "white hat" hackers, ethical hacking helps organizations strengthen their defence, comply with security standards, and safeguard sensitive data. Unlike illegal hacking, ethical hacking is conducted with proper permission and follows a structured, responsible approach to ensure no harm is done to the systems being tested.

In today's digital world, where cyber threats are becoming more advanced and frequent, ethical hacking plays a crucial role in keeping businesses and individuals safe. It's not just about finding flaws, it's about building trust, preventing data breaches, and ensuring that technology works for people, not against them. By simulating real-world attacks in a controlled environment, ethical hackers help organizations stay one step ahead of cybercriminals.

FUNDAMENTAL SECURITY CONCEPTS:

CIA TRIAD:

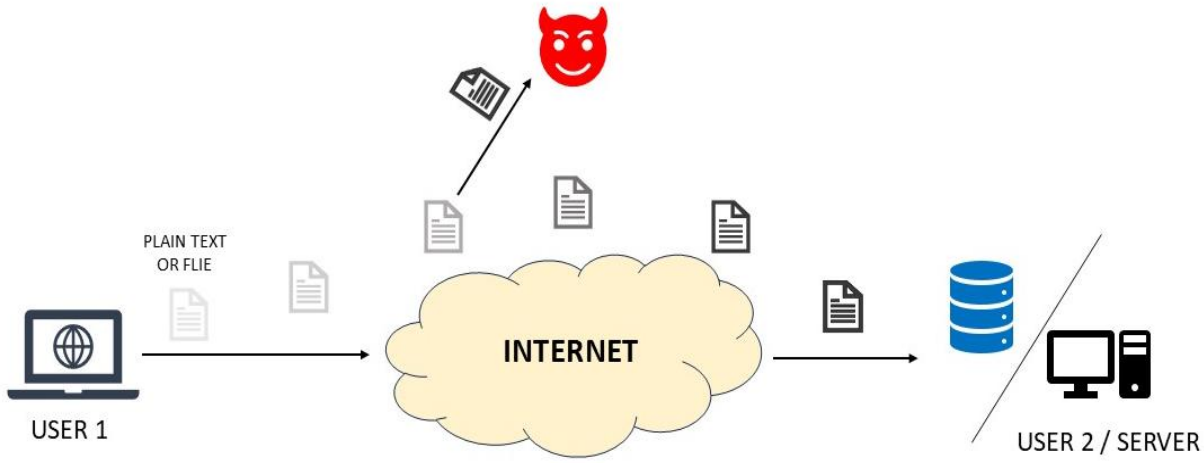
The CIA Triad is a fundamental model in cybersecurity that represents the core principles for securing information systems. It stands for Confidentiality, Integrity, and Availability. Confidentiality ensures that sensitive information is accessible only to authorized users, protecting it from unauthorized access or disclosure. Techniques such as encryption, access controls, and authentication are commonly used to maintain confidentiality. Integrity refers to the accuracy and

trustworthiness of data. It ensures that information is not altered or tampered with by unauthorized individuals. Hash functions, checksums, and digital signatures help preserve integrity. Availability means that data and systems are accessible to authorized users whenever needed. This involves maintaining reliable hardware, minimizing downtime, and protecting against denial-of-service (DoS) attacks. Together, these three principles form the foundation of a secure information environment and guide the development of cybersecurity policies and practices.

Confidentiality:

- Ensuring data is hidden, only visible to authorized users.
- Enforced through encryption.
- Violations: Packet sniffing, Breaking encryption, unintentional human error.

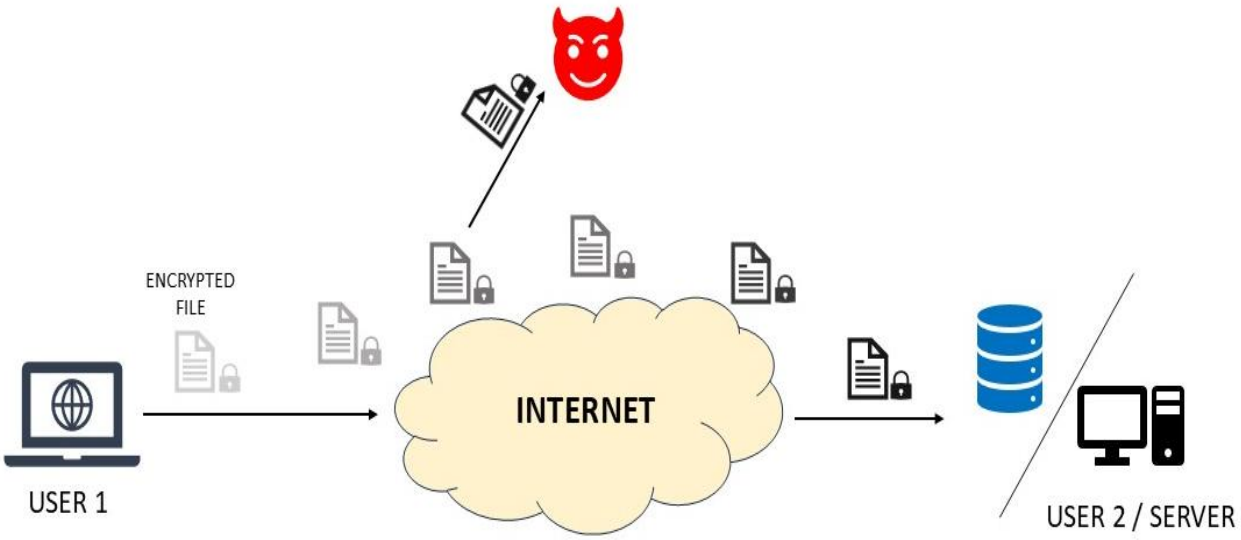
Without encryption:



In this scenario, User 1 sends a document or file over the internet in plain text, meaning it is not protected by any encryption. As the file travels through the public network, it becomes vulnerable to interception. A malicious cyber actor is able to eavesdrop on the communication and capture the unprotected file. Since the file is not encrypted, the attacker can easily read or steal its contents without detection. This represents a classic case where the Confidentiality

aspect of the CIA Triad is compromised. Sensitive information is exposed to unauthorized parties, which can lead to data leaks, identity theft, or further cyber attacks. To prevent this, encryption methods such as SSL/TLS, VPNs, or end-to-end encryption should be used to ensure that data remains confidential during transmission.

With encryption:

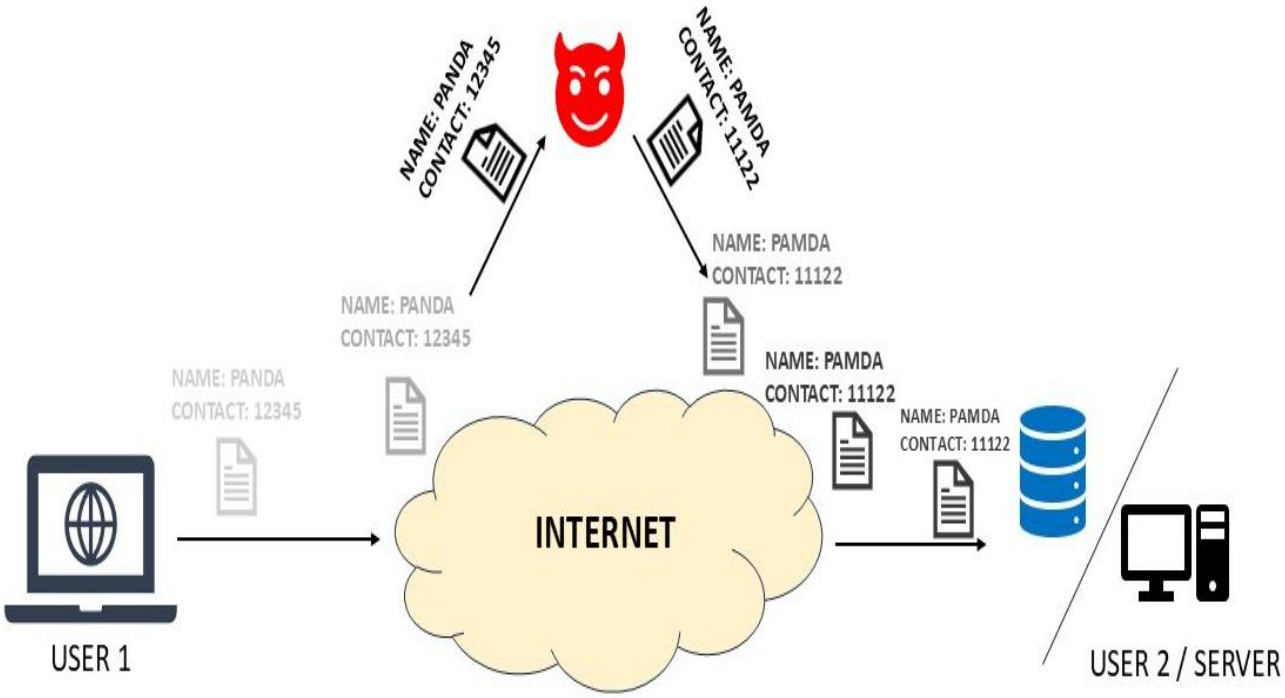


In this scenario, User 1 sends a file over the internet, but unlike before, the file is now encrypted before transmission. As it travels through the public network (Internet), the data remains protected through encryption. Even though a cyber attacker attempts to intercept the file, the encrypted content is unreadable and useless without the decryption key. This prevents unauthorized access and ensures that the file reaches User 2 or the server securely and without compromise. This scene effectively demonstrates how encryption preserves the Confidentiality component of the CIA Triad, ensuring that sensitive information remains private, even when transmitted across potentially insecure channels. Confidentiality means keeping sensitive data private and accessible only to authorized users. It is protected using methods like encryption, strong passwords, access controls, and secure communication channels, ensuring that information is not exposed to unauthorized individuals or cyber attackers.

Integrity:

- Accuracy and completeness of data, assurance that data has not been modified or omitted.
- Enforced through hashes.
- Violations: Modification of data during transit.

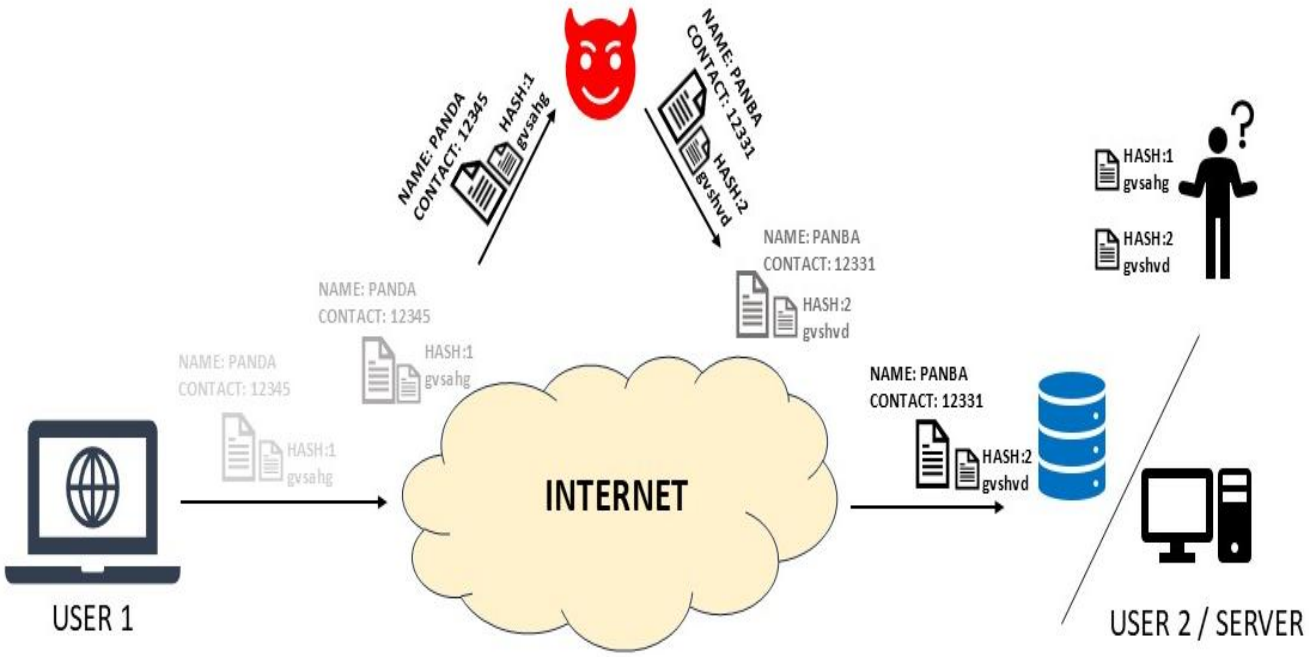
Without hash:



This image illustrates a scenario where data integrity is violated. User 1 sends a file containing sensitive information (e.g., Name: Panda, Contact: 12345) over the internet. During transmission, a cyber attacker intercepts the file, alters the content to "Name: Pamda, Contact: 11122", and then forwards the modified data to User 2 or the server.

Although the file reaches its destination, the content has been tampered with, leading to incorrect or potentially harmful data being processed. This demonstrates a compromise in integrity, where unauthorized changes to the data occur during transit, making it unreliable and untrustworthy.

With hash:



This image demonstrates a scenario how integrity can be protected using cryptographic hashing. User 1 sends a file along with its hash value (Hash:1) over the internet. During transmission, a cyber attacker alters the original file data (e.g., changes “PANDA” to “PANBA” and contact number), resulting in a new hash (Hash:2) that does not match the original.

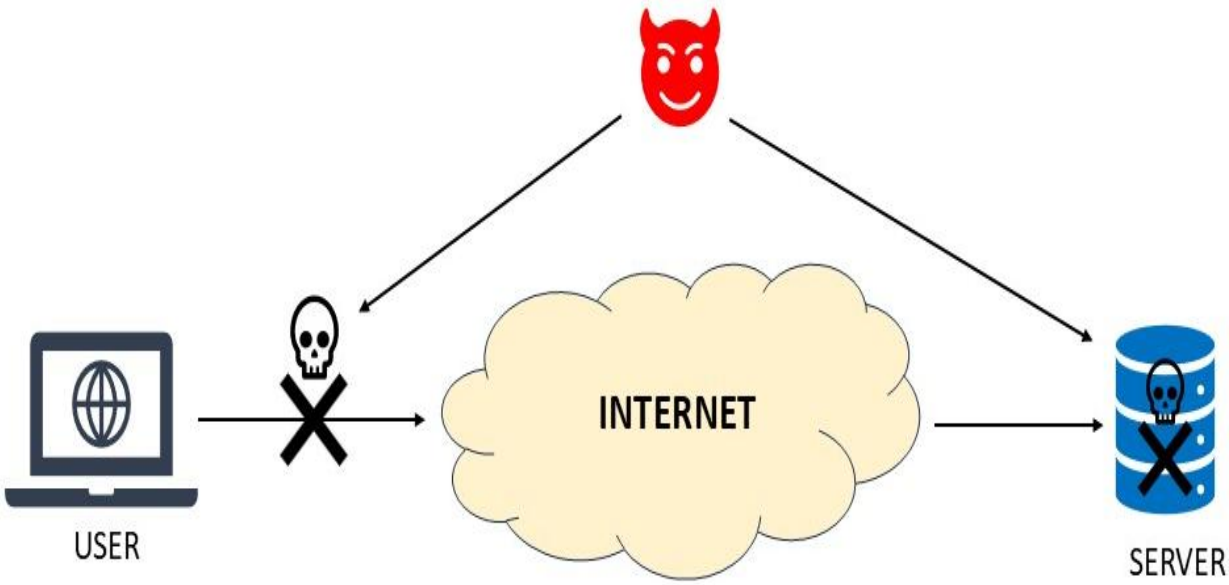
When User 2 or the server receives the data and recomputes the hash, it detects a mismatch between Hash:1 and Hash:2, indicating that the file was tampered. With this process helps in verifying data integrity and ensuring that the received information has not been altered during transmission.

This clearly illustrate the importance of maintaining data integrity during transmission. Without proper protection mechanisms like cryptographic hashing, attackers can tamper with the data in transit modifying names, contact details, or other sensitive information without detection. By comparing the original hash sent by the sender with the hash computed by the receiver, any unauthorized changes can be quickly identified. This process ensures that the information received is authentic, unaltered, and trustworthy, which is vital for secure communication, especially in environments involving financial transactions, medical data, or legal documents.

Availability:

- Data is available when required.
- Enforced through redundancy.
- Violations: hardware damage, DoS.

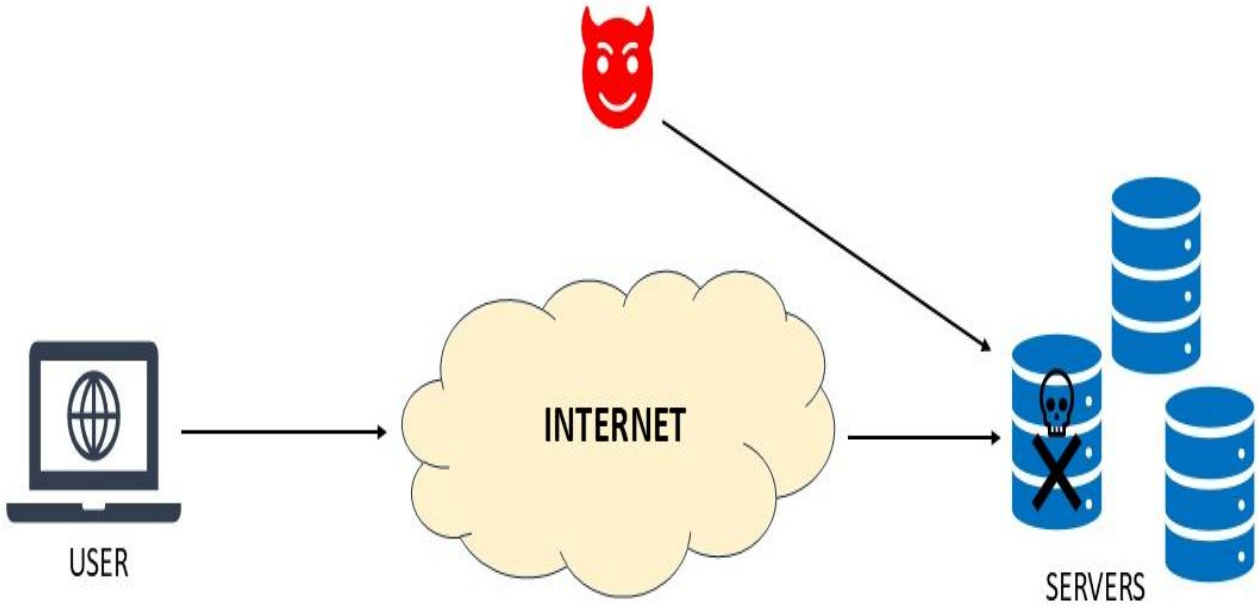
With single server and network:



This image illustrates the cybersecurity principle of Availability, one of the three pillars of the CIA triad. In the above scenario, a malicious attacker disrupts communication between the user and the server through the internet. Both the user and server are unable to access or provide services due to the attack, which could be a Denial of Service (DoS) or other form of disruption. As a result, even though the data may still exist, it becomes inaccessible, rendering systems unusable and operations halted.

In real-life terms, imagine needing to access your bank account online during an emergency, but the website is down because an attacker has overwhelmed the system. That's an availability attack. It impacts not just technology, but people's lives, businesses, and even emergency services. Ensuring availability means keeping systems operational, resilient, and responsive especially when people need them most.

With multiple servers and networks:



This scenario involving multiple servers. While one server has been compromised by a malicious attacker, the other servers remain unaffected and operational. This highlights an essential cybersecurity defense mechanism called redundancy. By distributing services across multiple servers, organizations ensure that even if one system is taken down, users can still access services through others, thereby maintaining availability.

In practical terms, this setup is like having backup power during a blackout. Imagine trying to make an emergency call, but your network provider is under attack. Thanks to backup servers, your call still goes through. For humans, this means uninterrupted access to vital services such as healthcare, banking, or communication, even during cyber incidents. This resilience not only protects business continuity but also builds trust and reliability in digital infrastructures.

In conclusion, How systems must remain accessible and operational even in the face of cyber threats. Whether it's a single server under attack or a distributed infrastructure handling failures gracefully, ensuring availability means that users can rely on continuous access to services and data. In the IT field, this translates to implementing failover mechanisms, redundancy, and robust network defenses to minimize downtime and maintain trust in digital systems.

Note: In addition, other properties, such as authenticity, accountability, nonrepudiation and reliability can also be involved. (ISO/IEC 27000:2009)

Auditing & Accountability:

Basically keep tracking of everthing, like, who's been logging in when are they loggin in whose access this data.

Non-Repudiation:

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

TYPES OF HACKERS:

White Hat hacker:

A white hat hacker is an ethical cybersecurity expert who uses their hacking skills to help organizations identify and fix security vulnerabilities. Unlike malicious hackers, white hat hackers have permission to test systems, often through penetration testing or vulnerability assessments, to strengthen defences and prevent cyberattacks. Their goal is to protect systems, data, and networks from unauthorized access or harm.

Black Hat hacker:

A black hat hacker is a malicious individual who exploits vulnerabilities in computer systems, networks, or software without authorization. Their goal is often to steal data, disrupt operations, install malware, or gain financial or personal advantage. Unlike ethical hackers, black hat hackers operate illegally and pose significant threats to cybersecurity and privacy.

Grey Hat hacker:

A grey hat hacker is someone who operates in the middle ground between ethical (white hat) and malicious (black hat) hacking. They may access systems or networks without explicit permission, but unlike black hat hackers, they do not intend to cause harm or steal information. Instead, they often look for vulnerabilities to expose weaknesses and, in some cases, inform the organization. Sometime even requesting compensation or recognition afterward.

However, despite their seemingly good intentions, grey hat hackers still violate laws and ethical standards by bypassing security without authorization. Their actions can be unpredictable and may still put systems at risk. While they might help organizations discover and fix security flaws, doing so without consent makes their activities legally questionable. As a result, grey hat hacking raises important debates in cybersecurity ethics about whether the ends can justify the means.

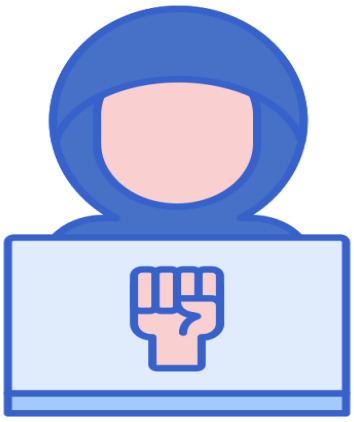
Script Kiddie / Skiddies:

A Script Kiddie is someone who uses pre-written scripts or hacking tools developed by others to carry out cyberattacks, without truly understanding how they work. Unlike skilled hackers, script kiddies lack deep technical knowledge and rely on basic methods to exploit vulnerabilities in systems. Their goal is often to show off, cause disruption, or gain unauthorized access just for fun or attention, rather than for serious criminal or ethical reasons. While they may seem harmless, the damage they can cause, like website defacement or minor data breaches can still be significant, especially for smaller or poorly protected systems.

State-Sponsored Hacker:

A State-Sponsored Hacker is a cybercriminal funded or supported by a government to carry out attacks against other nations, organizations, or individuals. Their goals often include espionage, stealing sensitive data, disrupting infrastructure, or influencing political events. These hackers are usually highly skilled and work as part of organized cyber units.

Hacktivist:



A Hacktivist is a hacker who uses their skills to promote a political, social, or ideological cause. Instead of seeking personal gain, hacktivists often target government websites, corporations, or institutions to protest, expose wrongdoing, or raise awareness, usually through defacement, data leaks, or denial-of-service attacks.

Suicide Hackers:

Suicide Hackers are individuals who carry out cyberattacks knowing they will likely be caught or face serious consequences. Their goal is often to cause maximum damage, disruption, or make a bold statement, without concern for their own safety or anonymity. These hackers may act for ideological, political, or extremist reasons, and are willing to sacrifice themselves for their cause.

Cyberterrorist:

Cyberterrorist is someone who uses technology to conduct violent or disruptive attacks intended to cause fear, harm, or chaos often for political, religious, or ideological reasons. Their targets can include governments, critical infrastructure and the public. Cyberterrorism aims to intimidate or coerce by damaging systems, stealing sensitive data, or spreading fear through digital means.

DIFFERENCES BETWEEN HACKERS:

Type of Hacker	Motivation	Skills	Targets	Legal Status
White Hat Hacker	Improve security, protect against attacks	High (in-depth security knowledge)	Client-authorized systems and networks	Legal (acts with explicit permission)
Black Hat Hacker	Personal or financial gain, disruption, malice	Moderate to high	Any vulnerable systems (corporate, government, personal)	Illegal (unauthorized and malicious)
Grey Hat Hacker	Expose vulnerabilities, sometimes request rewards, mixed intent	Moderate to high	Systems without prior consent (often large organizations)	Illegal (no authorization despite good intent)
Script Kiddie	Show off, cause disruption, attention	Low	Small websites, individual PCs	Illegal (amateur, but lacks deep intent)
Hacktivist	Political, social or ideological protest	Moderate	Government sites, corporations, public institutions	Illegal (viewed as activism)
State-Sponsored Hacker	Espionage, cyber warfare, political influence	Very high (government-backed)	Foreign governments, critical infrastructure, rivals	Illegal (but backed or tolerated by state)
Suicide Hacker	Maximum disruption or statement, self-sacrificial	Varies (often skilled)	High-value targets (financial systems, power grids)	Illegal (willing to be caught)
Cyberterrorist	fear, ideological violence, widespread chaos	Very high	Critical infrastructure (power, healthcare), public	Illegal (terrorism via digital means)

STAGES OF ETHICAL HACKING:

Ethical hacking follows a systematic process of five phases. Each phase has specific objectives, tools, and techniques:

1. Reconnaissance (Information Gathering):

- **Objective & Activities**: Gather as much information as possible about the target (network, systems, people) to plan attack. This footprinting phase may involve identifying IP ranges, domain names, employee email addresses, DNS records, network topology, and other public data. Reconnaissance can be active (probing systems directly) or passive (collecting data without touching the target).

- **Example Tool:** Nmap – an open-source network mapper/port scanner that discovers live hosts, open ports, and services. (Other examples: Maltego, theHarvester, whois.)

- **Technique:** OSINT and Footprinting – using public sources (search engines, social media, company websites) and simple commands (e.g. whois, DNS queries) to enumerate information. For example, Google dorking or LinkedIn searches can reveal staff names and email addresses.

2. Scanning:

- **Objective & Activities:** Use technical tools to identify open ports, services, and vulnerabilities on discovered hosts. Scanning pinpoints potential entry points (e.g. exposed servers or outdated software). This phase often includes: port scanning (finding open ports/services), vulnerability scanning (checking for known security flaws), and network mapping.

- **Example Tool:** Nmap for port/service scanning. Other tools: Nessus or OpenVAS (vulnerability scanners), Netcat (for banner grabbing), Masscan (fast port scanning).

- **Technique:** Port and Vulnerability Scans, e.g. running Nmap to detect open ports and then using a vulnerability scanner to check software versions. Attackers may also run automated scripts or use traceroute to map routers and firewalls.

3. Gaining Access (Exploitation):

- **Objective & Activities:** Exploit identified vulnerabilities to enter the system or network. At this stage, the tester uses the information gathered to breach a system and obtain a foothold (usually a shell or admin-level account). Common approaches include SQL injection, buffer overflows, password attacks, or social engineering. After initial breach, the attacker may escalate privileges to gain full control.

- **Example Tool:** Metasploit Framework, a popular exploit framework for penetration testing. (It provides ready-made exploits for many vulnerabilities.) Other examples: SQLmap (automates SQL injection attacks), Hydra (brute-force password cracker), custom scripts.

- **Technique:** Exploitation, for instance, using Metasploit to deliver a reverse shell via a known buffer overflow, or crafting a phishing email to capture credentials. Once inside, methods like privilege escalation are used to elevate access.

4. Maintaining Access (Post-Exploitation):

- **Objective & Activities:** Ensure continued access to the compromised systems for as long as needed. The attacker may install backdoors, rootkits, or create hidden administrator accounts to return later. This phase is about persistence, making it hard for defenders to remove the intruder. Maintaining access can also involve pivoting (using the compromised host to launch further attacks deeper into the network).

- **Example Tool:** Netcat, often used as a lightweight backdoor (e.g. listening shell) or to set up reverse connections. Meterpreter (part of Metasploit) is another common payload that provides stealthy remote control. Empire and Ncat also serve similar post-exploit purposes.

- **Technique:** Backdoors and Privilege Escalation, e.g. deploying a persistent backdoor program or malicious scheduled task, installing a rootkit to hide processes, creating new user accounts with admin rights. These actions allow the attacker to "blend in" and return even if the original vulnerability is patched.

5. Clearing Tracks:

- **Objective & Activities:** Erase evidence of the intrusion so that detection and attribution become difficult. An intelligent attacker will modify or delete log files, clear command history, and remove any tools or files they uploaded. They may also change network identifiers (e.g. spoof their MAC address) or disable security logging.

- **Example Tool:** Audit Viewer or other log-review tools (though rarely needed by skilled attackers, who often manipulate files manually). Attack scripts may simply truncate log files or remove logs from security systems.

- **Technique:** Log Tampering and Stealth Practices, for example, using commands like history -c to clear shell history or editing /var/log/syslog to erase login entries. Other tactics include encrypting malicious files so they appear benign, cleaning up temporary files, and disconnecting via anonymizing networks (VPN/Tor) to hide one's source. The goal is that forensic investigators find no clear trail leading back to the hacker.

CONCLUSION:

Conclusion

Ethical hacking plays a crucial role in modern cybersecurity by proactively identifying vulnerabilities before malicious actors can exploit them. Understanding the differences between black hat, grey hat, and white hat hackers helps highlight the importance of intent and legality in cybersecurity activities. While all hacker types may use similar tools and techniques, it is the white hat hacker's ethical commitment and legal boundaries that transform hacking into a constructive, protective force for individuals, organizations, and governments alike.

The structured methodology followed in ethical hacking, from reconnaissance to clearing tracks, ensures a comprehensive evaluation of a system's security posture. Each phase is designed to mimic real-world attack scenarios so that organizations can understand and fortify their weak points. Tools like Nmap, Metasploit, and Netcat are not just hacking instruments, they are diagnostic tools in the hands of ethical hackers, used to build resilience and trust in digital infrastructure.

As cyber threats continue to grow in complexity and frequency, ethical hacking remains more relevant than ever. It is not just a technical discipline but a responsibility that requiring a deep understanding of systems, a strong moral compass, and a clear respect for legal frameworks. Through responsible practices, continuous learning, and collaboration, ethical hackers contribute to a safer digital world for everyone.

REFERENCES:

https://usa.kaspersky.com/resource-center/definitions/hacker-hat-types?srsltid=AfmBOooUzRIzF0fqw05tRlvAGp8MOixXjlGoE7degi-fjSYse6JfT63M#:~:text=Black%20hat%20hackers%20are%20criminals,numbers%2C%20and%20other%20personal%20information

https://www.techtarget.com/searchsecurity/definition/white-hat#:~:text=Where%20white%20hat%20hackers%20disclose,exploits%20to%20the%20highest%20bidder

https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/#:~:text=1

https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking#:~:text=Active%3A%20Directly%20interacting%20with%20the,tool%20to%20scan%20the%20target

https://www.geeksforgeeks.org/5-phases-hacking/#:~:text=1,names%2C%20positions%2C%20and%20email%20addresses

THANK YOU