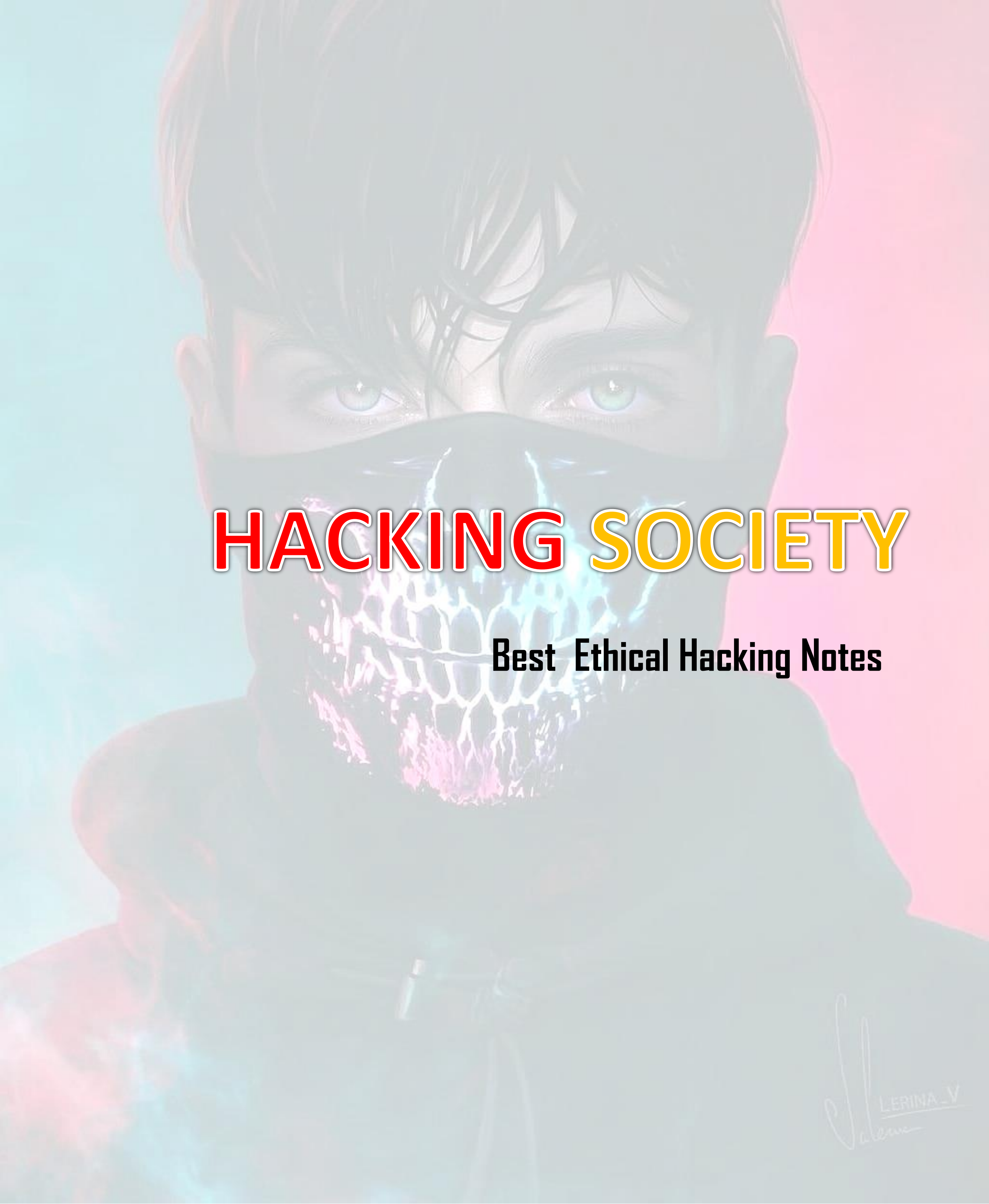
HackitTech

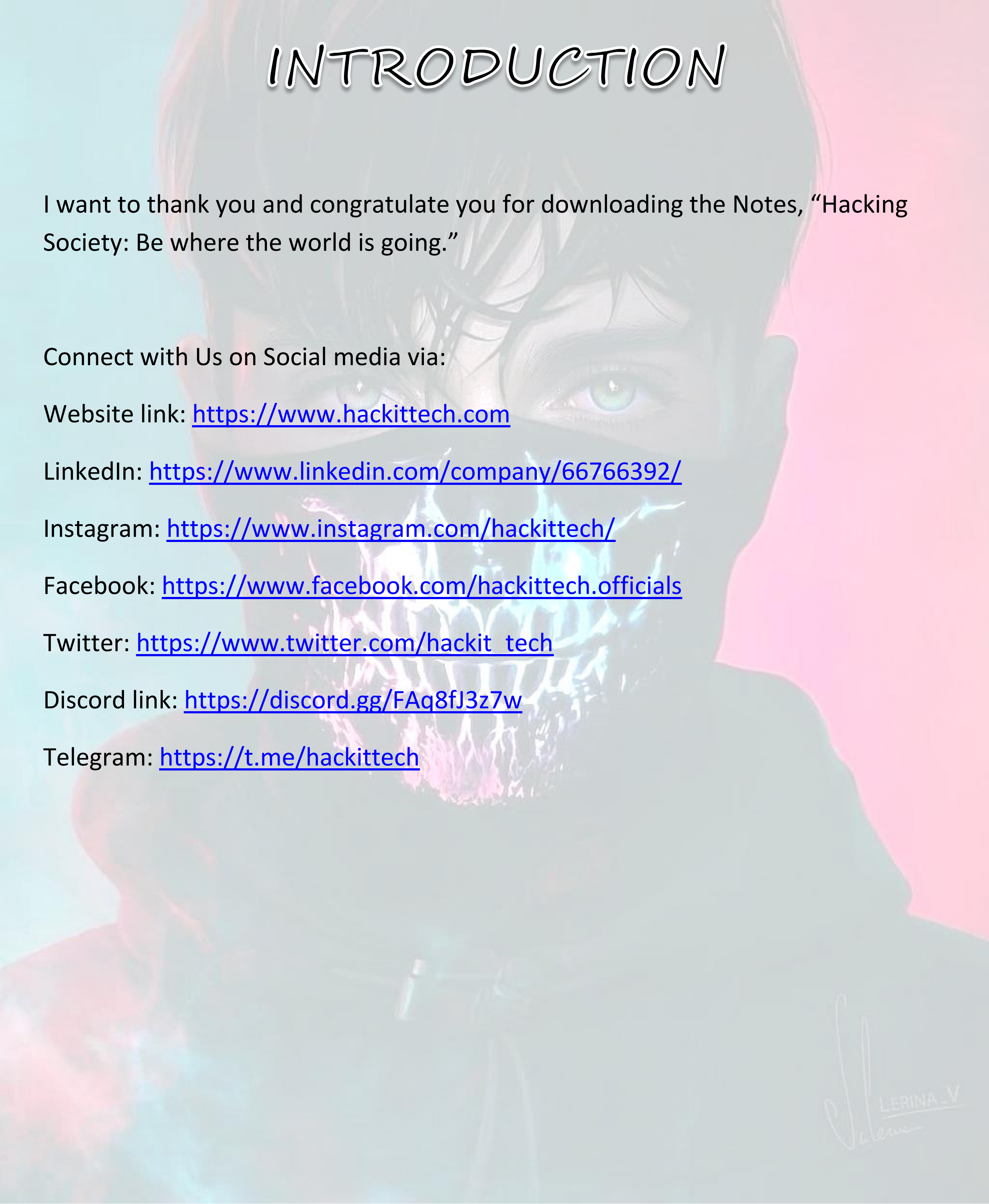
HACKING SOCIETY

Best Ethical Hacking Notes



By Sandeep Kumar

Insta **@admirerr_20**



INTRODUCTION

I want to thank you and congratulate you for downloading the Notes, “Hacking Society: Be where the world is going.”

Connect with Us on Social media via:

Website link: https://www.hackittech.com

LinkedIn: https://www.linkedin.com/company/66766392/

Instagram: https://www.instagram.com/hackittech/

Facebook: https://www.facebook.com/hackittech.officials

Twitter: https://www.twitter.com/hackit_tech

Discord link: https://discord.gg/FAq8fJ3z7w

Telegram: https://t.me/hackittech

By Sandeep Kumar

Insta @admirerr_20

Module 1

What is Hacking

- Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized access to the system.

Eg:- Stealing, disclosure of Sensitive information

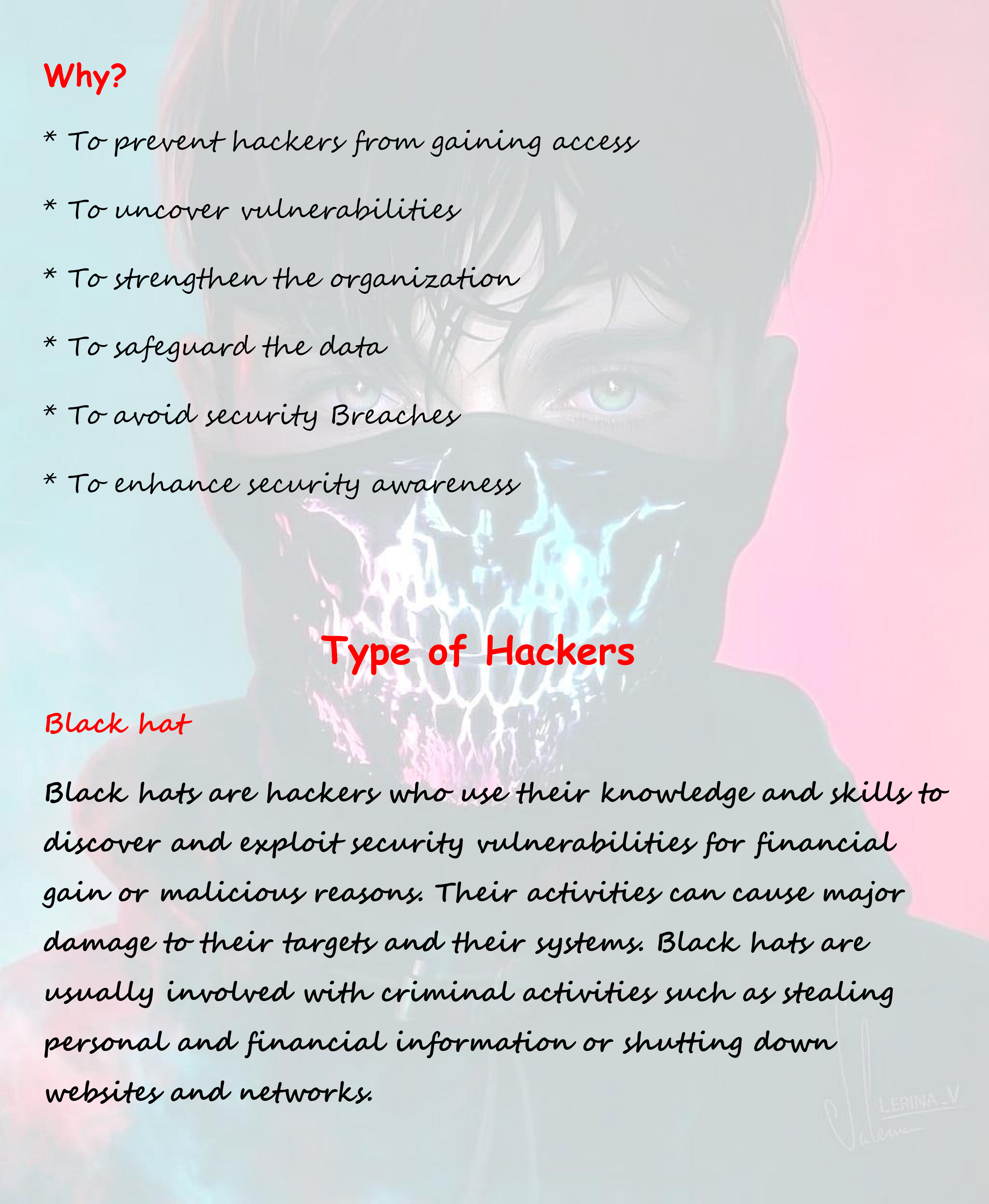
Why Hack Happens?

- ATTACKS = MOTIVE (GOAL) + METHOD + VULNERABILITY
- MOTIVE: - Information theft, manipulating data, Financial loss, Revenge, Ransom, Damaging Reputation.

Ethical Hacking

- Ethical Hacking involves the use of hacking tools, tricks, and techniques to identify vulnerability so as to ensure system security.
- Ethical Hackers performs security assessment of their organization with the permission of concerned authorities

In simple - Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. … Also known as "white hats," ethical hackers are security experts that perform these assessments



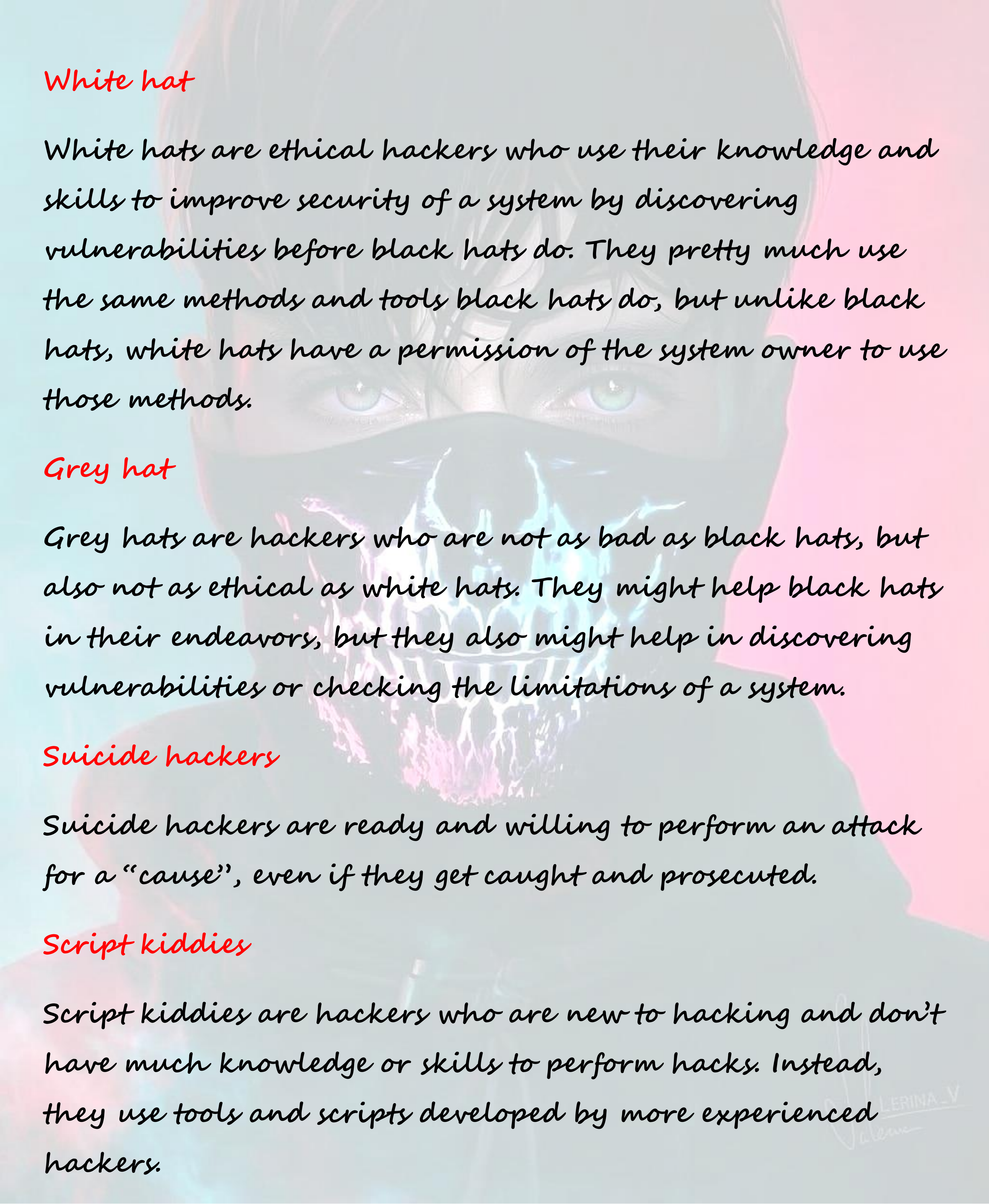
Why?

- To prevent hackers from gaining access
- To uncover vulnerabilities
- To strengthen the organization
- To safeguard the data
- To avoid security Breaches
- To enhance security awareness

Type of Hackers

Black hat

Black hats are hackers who use their knowledge and skills to discover and exploit security vulnerabilities for financial gain or malicious reasons. Their activities can cause major damage to their targets and their systems. Black hats are usually involved with criminal activities such as stealing personal and financial information or shutting down websites and networks.



White hat

White hats are ethical hackers who use their knowledge and skills to improve security of a system by discovering vulnerabilities before black hats do. They pretty much use the same methods and tools black hats do, but unlike black hats, white hats have a permission of the system owner to use those methods.

Grey hat

Grey hats are hackers who are not as bad as black hats, but also not as ethical as white hats. They might help black hats in their endeavors, but they also might help in discovering vulnerabilities or checking the limitations of a system.

Suicide hackers

Suicide hackers are ready and willing to perform an attack for a "cause", even if they get caught and prosecuted.

Script kiddies

Script kiddies are hackers who are new to hacking and don't have much knowledge or skills to perform hacks. Instead, they use tools and scripts developed by more experienced hackers.

Cyber terrorists

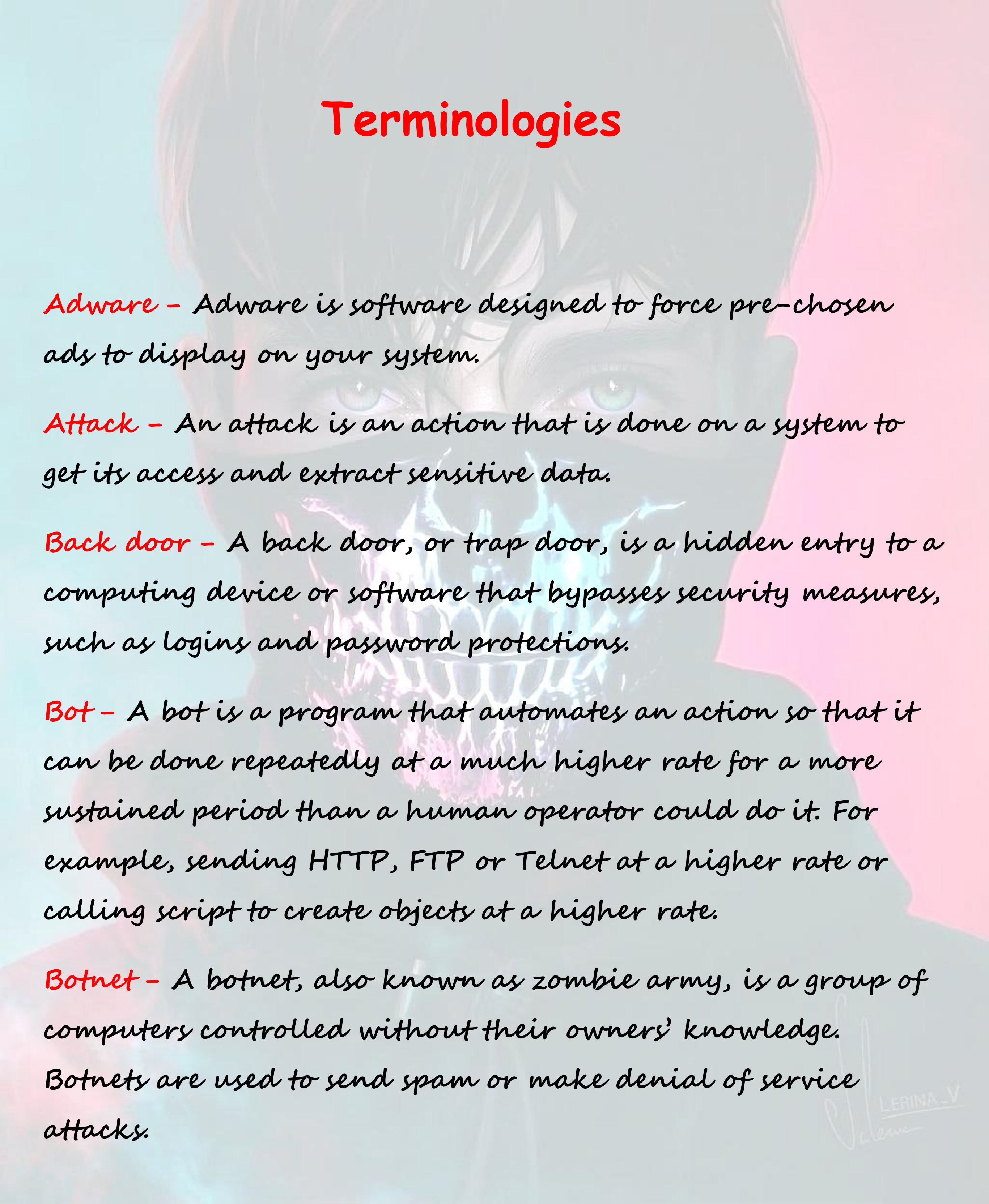
Cyber terrorists are hackers who are influenced by certain religious or political beliefs. They work to cause fear and disruption of systems and networks.

State sponsored hackers

State sponsored hackers are recruited by governments to gain access to secret information of other governments.

Hacktivists

Hacktivists break into government or corporate systems out of protest. They use their skills to promote a political or social agenda. Targets are usually government agencies or big corporations.



Terminologies

Adware – Adware is software designed to force pre-chosen ads to display on your system.

Attack – An attack is an action that is done on a system to get its access and extract sensitive data.

Back door – A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.

Bot – A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.

Botnet – A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.

Brute force attack – A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.

Buffer Overflow – Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.

Clone phishing – Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

Cracker – A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.

Denial of service attack (DoS) – A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

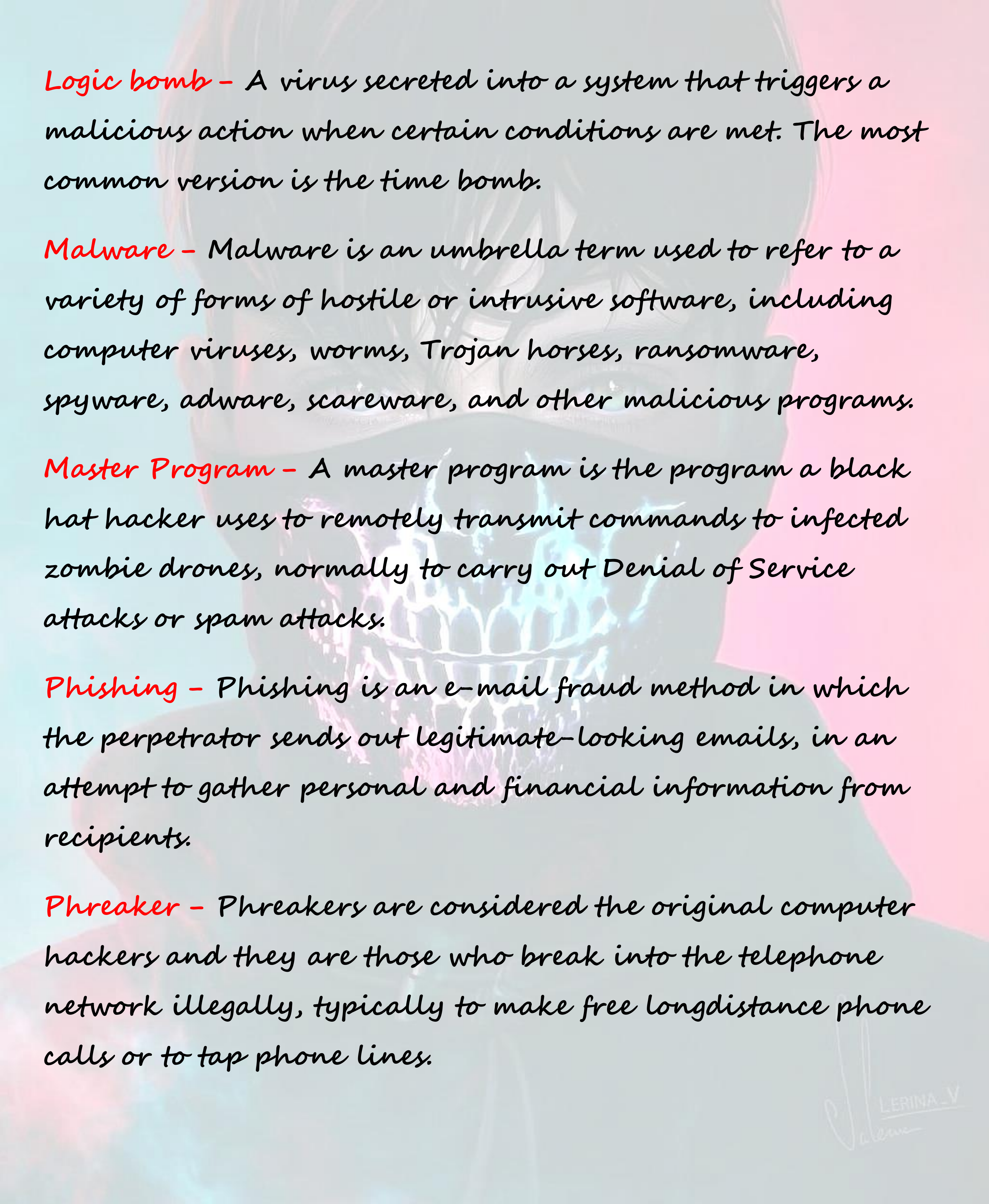
DDoS – Distributed denial of service attack.

Exploit Kit – An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.

Exploit – Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.

Firewall – A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.

Keystroke logging – Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.



Logic bomb – A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.

Malware – Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

Master Program – A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.

Phishing – Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.

Phreaker – Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free longdistance phone calls or to tap phone lines.

Rootkit – Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Shrink Wrap code – A Shrink Wrap code attack is an act of exploiting holes in unpatched or poorly configured software.

Social engineering – Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.

Spam – A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.

Spoofing – Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

Spyware – Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another

By Sandeep Kumar
Insta @admirerr_20

entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

SQL Injection – SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

Threat – A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.

Trojan – A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other information.

Virus – A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

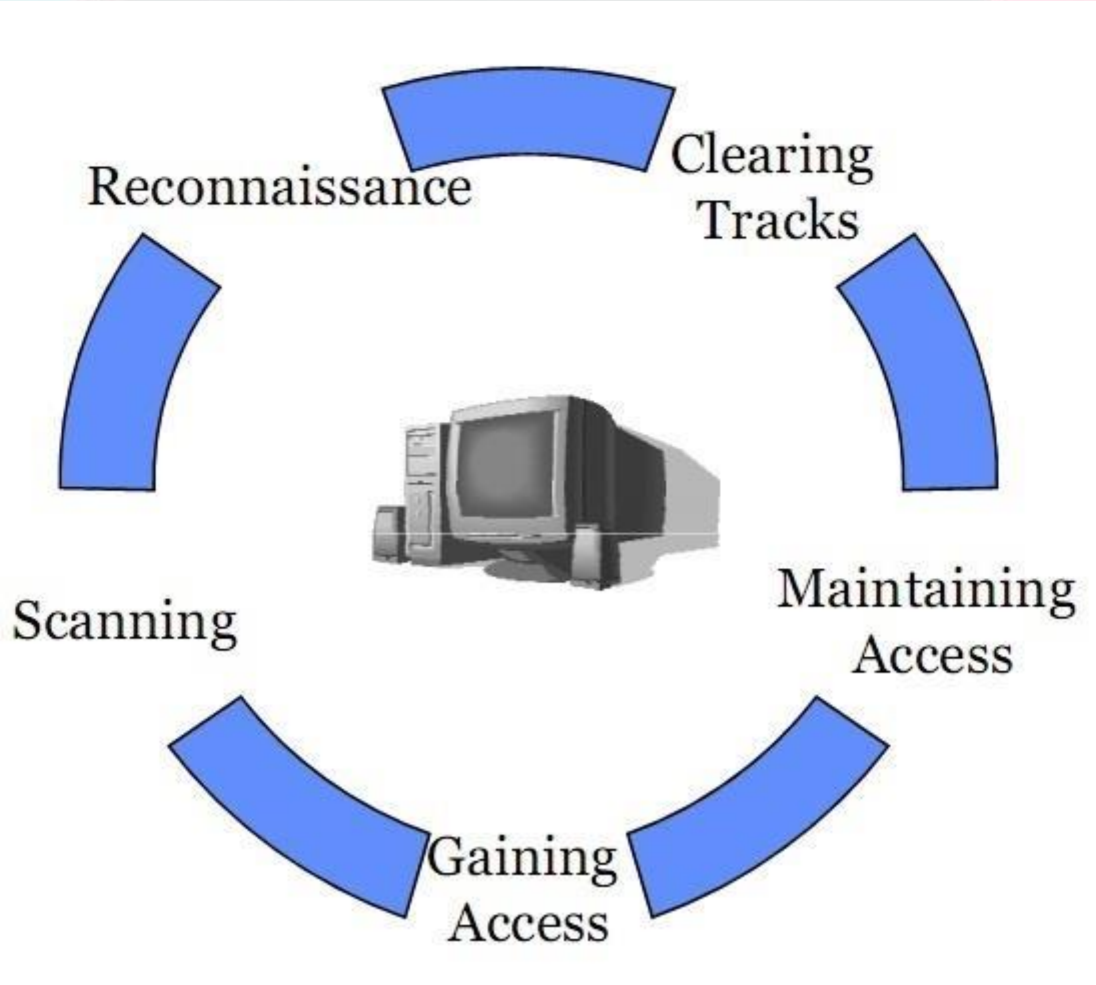
Vulnerability – A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.

Worms – A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Cross-site Scripting – Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.

Zombie Drone – A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

Phases of Hacking


Reconnaissance
Clearing Tracks
Maintaining Access
Gaining Access
Scanning

Reconnaissance:- This is the primary phase where the Hacker tries to collect as much information as possible about the target. It includes Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc.

Scanning:- It involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include dialers, port scanners, network mappers, sweepers, and vulnerability scanners. Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

Gaining Access:- After scanning, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. Examples include stack based buffer overflows, denial of service (DoS), and session hijacking. These topics will be discussed in later chapters. Gaining access is known in the hacker world as owning the system.

Maintaining Access:- Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Covering Tracks:- Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include steganography, the use of tunneling protocols, and altering log files.

Security Policies

Access Control Policy

Information is a valuable asset and access to it must be managed with care to ensure that confidentiality, integrity and availability are maintained.

The University of Sheffield provides access to information assets, accounts, systems and resources based on the principle of least privilege (see Information Security Glossary for explanation).

This policy outlines the rules relating to authorising, monitoring and controlling access to University accounts, information and information systems.

firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies

password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training..

email policy is to set proper expectations with your employees. What are the rules and guidelines regarding email and what happens if you ignore the rules? The email policy should be written and reviewed with the employee at the time of employmento

Information protection policy is a document which provides guidelines to users on the processing, storage and transmission of sensitive information. Main goal is to ensure information is appropriately protected from modification or disclosure. … It should define sensitivity levels of information.

user account policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, typically within an organization. It is very important for large sites where users typically have accounts on many systems.

Physical security

Is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

1. Security Controls

Computer security is often divided into three distinct master categories, commonly referred to as controls:

- Physical
- Technical
- Administrative

These three broad categories define the main objectives of proper security implementation. Within these controls are sub-categories that further detail the controls and how to implement them.

2. Physical Controls

Physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. Examples of physical controls are:

- Closed-circuit surveillance cameras
- Motion or thermal alarm systems
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors

Biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals)

3. Technical Controls

Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Technical controls are far-reaching in scope and encompass such technologies as:

- Encryption
- Smart cards
- Network authentication
- Access control lists (ACLs)
- File integrity auditing software

4. Administrative Controls

Administrative controls define the human factors of security. It involves all levels of personnel within an organization and determines which users have access to what resources and information by such means as:

- Training and awareness
- Disaster preparedness and recovery plans
- Personnel recruitment and separation strategies
- Personnel registration and accounting

Penetration Testing

• Penetration Testing is a method of evaluating the security of an information system or network by simulating an attack to

• find vulnerability

• Security Measures

• Documentation and Report Preparation

Need?

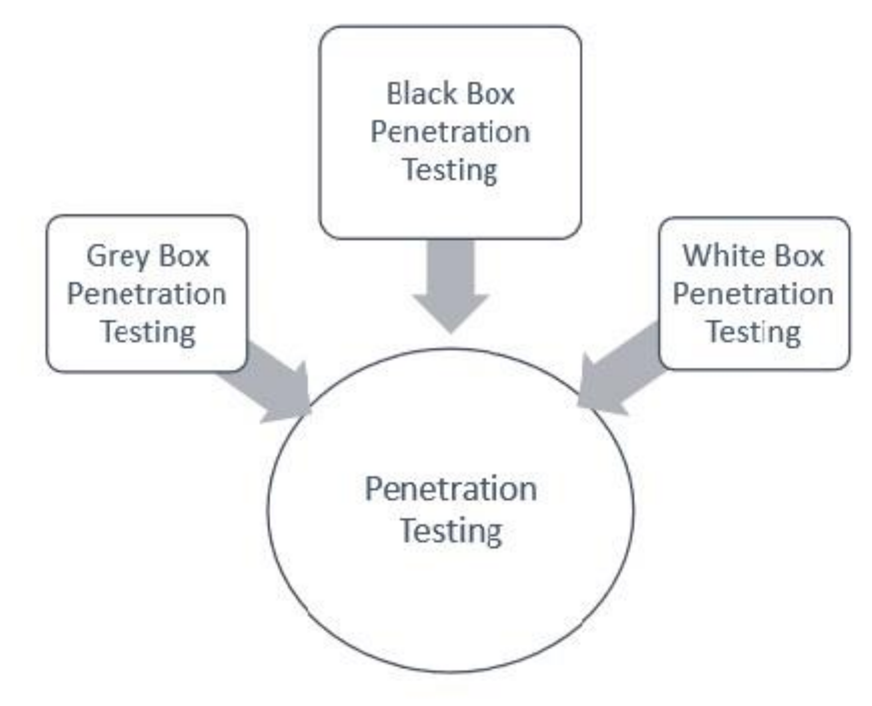
1)Identification of threats

2)Security Protections and controls

3)Assessment of Organization's Security

4)Evaluation of Network Security 5)Upgradation of Infrastructure

Types of Pentesting:


Black Box Penetration Testing
Grey Box Penetration Testing
White Box Penetration Testing
Penetration Testing

Black Box Penetration Testing

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.

Advantages of Black Box Penetration Testing

It has the following advantages −

- Tester need not necessarily be an expert, as it does not demand specific language knowledge
- Tester verifies contradictions in the actual system and the specifications
- Test is generally conducted with the perspective of a user, not the designer

Disadvantages of Black Box Penetration Testing

Its disadvantages are −

- Particularly, these kinds of test cases are difficult to design.
- Possibly, it is not worth, incase designer has already conducted a test case.
- It does not conduct everything.

White Box Penetration Testing

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

Advantages of White Box Penetration Testing

It carries the following advantages −

- It ensures that all independent paths of a module have been exercised.
- It ensures that all logical decisions have been verified along with their true and false value.
- It discovers the typographical errors and does syntax checking.
- It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

Grey Box Penetration Testing

In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Advantages of Grey Box Penetration Testing

It has the following advantages −

- As the tester does not require the access of source code, it is non-intrusive and unbiased
- As there is clear difference between a developer and a tester, so there is least risk of personal conflict
- You don't need to provide the internal information about the program functions and other operations

Standards and Compliances

1) Payment Card Data Security Standard (PCI DSS)

2) ISO/IEC 27001:2013

3) Health Insurance Portability and Accountability Act(HIPPA)

4) Sarbanes Oxley Act(SOX) – To prevent fraudulent Financial Activities(shares)

5) The Digital Millennium Copyright Act(DMCA) – Copyrights

6) Federal Information Security Management Act(FISMA) – Natural and Man Made threats

7) Governance, Risk Management and Compliance (GRC)

8) General Data Protection Regulation (GDPR) – EU and Transfer outside EUCyber Laws

- Section 43 - Damage to computer System
- Section 65 – Tampering of Computer Source Documents
- Section 66 – Computer Related Offences
- SECTION 66 A – Sending offensive Messages

By Sandeep Kumar
Insta @admirerr_20

- SECTION 66 B – Smuggling goods
- SECTION 66 C – Identity theft
- SECTION 66 D – False Personation(Telecallers)
- SECTION 66 E – Violation of Privacy
- SECTION 66 F – Cyber TerrorismCyber Laws – Cont'd
- SECTION 67 – Transmitting Obscene Material
- SECTION 71 - Misrepresentation
- SECTION 72 – Breaching of Confidentiality and Privacy
- SECTION 73 – Publishing Electronic Signatures

Hello Everyone I hope you like the course content … but the thing is if you want to do something great you need to learn more and more everyday … This training is totally FREE of Cost the only thing I want from you guys is your time and efforts towards this training. I wish you the best in your future endeavors, Happy Hacking

Do follow me on Instagram - https://www.instagram.com/admirerr_20/

By Sandeep Kumar
Insta @admirerr_20