
How
HACKERS
operate
@cybervalkryies

Before diving into specialised cybersecurity technologies and methods, it's always a good idea to recognize who a hacker is and what they do.

@cybervalkryies

Who and why?

A hacker is simply defined as any person who uses computers to gain unauthorized access to data.

Unfortunately, popular media in recent years has often blurred the definition of the word to immediately make many imagine anonymous cyber criminals that live in their terminals upon hearing the word "hacker".

The reality is, however, that hacking is a very vast world, and hackers are diverse in their types and motifs. While other classifications do exist, the main three types include:

1. White Hat Hackers

A white hat hacker refers to anyone with permission or certification to break into or hack a system. Often, they act as skilled professionals hired to find vulnerabilities and expose flaws so that these security gaps can be filled in later on. They operate in an entirely ethical manner and follow the necessary guidelines and regulations.

So, white hats include most offensive security jobs like penetration testers and red teamers, but also includes hackers who take on personal initiatives to hack ethically, namely through the means of bug bounty hunting.

Many organizations today sign themselves up for different crowd-sourced bug bounty programs, in which anyone can make attempts to find vulnerabilities in their technologies, and upon reporting them, can receive compensations (sometimes in the form of monetary rewards) If that sounds interesting to you, you can visit platforms like Bugcrowd and Hackerone's bug bounty opportunities (https://www.hackerone.com/bug-bounty-programs) to figure out more about operating as a bug bounty hunter as well as which organizations have signed up.

2. Black Hat Hackers

@cybervalkryies

A black hat refers to cybercriminals who hack with malicious intentions, gaining access to computer networks and systems often with the aims of financial gain (by holding organizations ransom, selling sensitive data to other cybercriminals, or selling hacking services or tools) or generally, the disruption of services and networks.

3. Gray Hat Hackers

*On both the legality and ethical spectrums of hacking, grey hat hackers lie somewhere in between **black and white hats**. While they do not have malicious intent like black hats, they still operate by violating laws or acceptable standards by exploiting security vulnerabilities without permission, often for a "good" cause.*

<u>This may include:</u>

- attempts to find vulnerabilities in a system without consulting its owner or gaining permission, but alerting the owner afterwards
- Or more generally, hacktivism, which is hacking as a form of civil disobedience for a political or social cause.

Ethics in Cyb3r

@cybervalkryies

Properly categorizing hackers is important, because it allows us to evaluate our ethical and legal standpoints during our journey of studying cybersecurity.

Using your information security knowledge to attack systems you don't have the authority or permission to is a significant crime, many of the time regardless of intentions. And because we don't want you swapping out your hats for orange jumpsuits, this is a reminder that any tools or technologies discussed moving forward are entirely for educational and ethical purposes and are intended to be used in safe, legal environments.

Studying and operating in this field often comes with complex ethical decisions you must navigate, often balancing integrity, confidentiality, and the defense of individual rights and needs alongside systems.

Nonetheless, there are plenty of (legal) ways you can tinker around with tools or use your knowledge for the good, which we'll be highlighting more and more as we come across them.

Cybersecurity Attacks & Hacker Methods

Whether you're an aspiring cybersecurity expert or just anyone who uses technology, it's important to be able to recognize different cybersecurity attacks and understand what it means for the targeted individual or organization. Knowing the different types of attacks also means you can take further steps to protect yourself and those around you.

We'll be highlighting the attack type from both a brief offensive and defensive perspective, as well as their effects.

Malware is likely the most well-known type of cybersecurity attack. The word is a portmanteau of the words "malicious" and "software" and is a general term to refer to any software installed on a system deliberately designed to disrupt operations, destroy data, or spy on its user. Malware comes in many forms, but most commonly include:

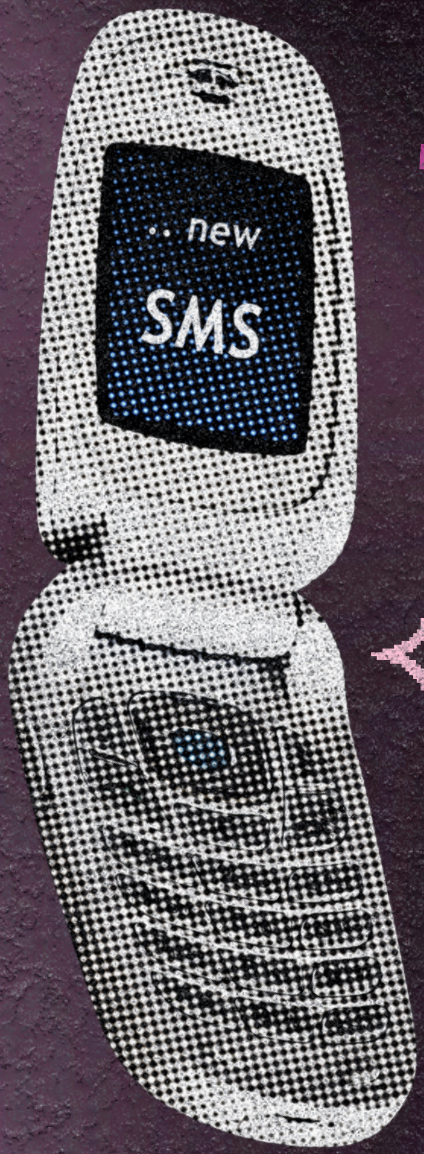
Virus

Malicious programs that require a "host". They attach themselves to files or other programs on a device, replicate, and spread across different systems.

Worms

@cybervalkryies

Malware that self-replicates and spreads across networks, exploiting system vulnerabilities without needing a host file like a traditional virus, often consuming large amounts of bandwidth and slowing operations. Infamously includes the ILOVEYOU worm, one of the most destructive malwares in computing history, which originally started as a university project, and the Morris Worm, one of the first documented worms spread via the internet in history.



Trojans / Trojan Horses

Malware that disguises itself as a legitimate program, but creates backdoors upon execution. Cleverly named after the Greek mythology Trojan Horse. Today, trojan horses often present themselves to be "cracked" versions of popular software.

Ransomware

A type of malware that encrypts (locks away) a user's files and holds them up for ransom, only providing the decryption key when the malware author is sent payment. Some well-known ransomware attacks are the WANNACRY attacks of 2017 and the variants of the PETYA malware attacks between 2016 and 2017.

Common methods to defend against malware include constructing firewalls responsible for controlling traffic and blocking unauthorized access attempts or using good anti-virus software.

However, in order for malware to operate, it must be installed on a target device. This means that it deliberately requires an unknowing user to be involved in its installation. This often means that the best countermeasure against malware is awareness and education of individuals and organizations to prevent its installation at all.

@cybervalkryies

2 Phishing

Phishing is one of the most common types of social engineering.

Social engineering (SE) is when a hacker doesn't target systems, but instead, targets people. It's when hackers use manipulation techniques to incentivize an individual to make a security error (even if they wouldn't in normal circumstances) which can lead them to revealing sensitive details or granting unauthorized access to their systems

Phishing uses SE techniques by sending out emails, text messages, or phone calls to trick users. Common examples include scam emails from fake companies, or "gift" surveys attached to chain messages. With phishing being reported as the most common type of cybercrime today, it has developed intensely in recent years, often to the point where mirrors of legitimate company websites are used to further fool the user.

There are several indications that can help anyone with a keen eye notice when they have come across a phishing attempt, which include:

1. Impersonation/Fake identity: attackers may act as people, organizations, or services to increase their credibility and lure users in

2. Incorrect domains or links: attackers may use free, personal domains (such as @gmail.com) when posing as corporations.

They may use spoofing techniques in which the emails they use present themselves as legit, but fail security checks like SPF and DMARC

They use typosquatting and punycode, in which links or emails are misspelled deliberately in a way that isn't outwardly obvious at first glance. (i.e facebook.com, or glthub.com)

3. They create a sense of urgency, either by frightening the receiver (i.e, fake unauthorized logins to their social media accounts or large transactions made with their banking accounts) or by attracting them (i.e, promises of winning raffles or giveaways and that they MUST claim their rewards)

4. They entice you to do something a real company wouldn't, such as emailing back your credentials/entering them in a survey, or downloading and executing suspicious files.

@cybervalkryies

DoS and DDoS attacks 3

@cybervalkryies

DoS

DoS (Denial of Service) refers to a type of cyberattack that is constructed with the intention of making a service or system unavailable to its intended, regular users. It is carried out by overwhelming the system with fraudulent requests until it is unable to respond to genuine ones. Often, it leads to an entire shutdown of a system or service until it can resume service normally again.

DDoS

Similarly, a DDoS attack (Distributed Denial of Service) uses this same method of overflooding servers with traffic, but from several sources rather than just one, typically through the use of botnets (a network of connected systems/computers that have been compromised and can be controlled by a cybercriminal, often without the knowledge of the system's actual owner.) .

Common defense mechanisms against these type of attacks include rate limiting (when limits are placed on the amount of requests a server will accept from a specific ip address within a given time frame), content-delivery network systems (CDN) (when a system's data that is being accessed is spread across several servers rather than one, leading to traffic by DoS attacks being split and easier to mitigate), as well as developing a proper incident-response plan.

4- Man in The Middle (MiTM) attacks

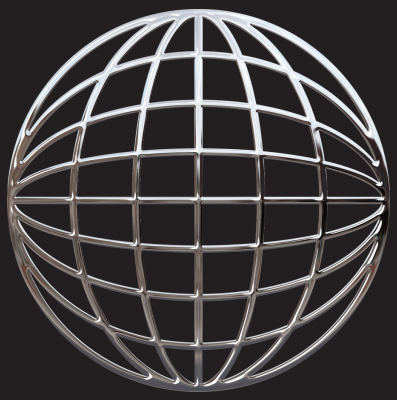
These are a type of cyberattack in which an attacker can relay or even alter communications between two parties. While each party (either two clients or a client and server) believes they are directly communicating with each other, the entire process is underneath an attacker's control.

MITM attacks come in many different forms, including but not limited to: HTTPs spoofing (fake SSL/TLS certificates), Wifi MITM also known as evil twin attacks (creating fake wifi hotspots to intercept user activities) or DNS spoofing (redirection of users into fraudulent websites).

MITM attacks are prevented by modern authentication techniques (like the use of cryptographic keys) and can be detected via discrepancies in expected response times.

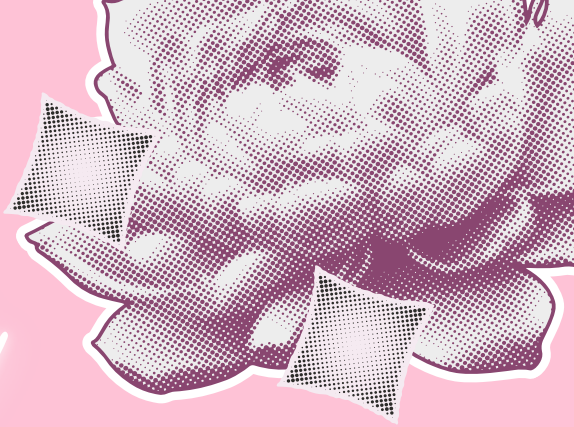
@cybervalkryies

original connection



new connection

anonymous proxy, phiser, man in the middle



Code injections

@cybervalkryies

Code Injection refers to any type of attack that involves an attacker "injecting" code into a program/system that is then interpreted/executed by the application, including:

1

XSS attacks (cross-site-scripting): Injecting malicious scripts into an application/system so that they are executed by a regular user's device on visit, with web pages (using Javascript) being common targets of these types of injections but not the only ones. Often used to hijack user sessions and steal sensitive data, deface websites, or redirect victims to downloading/executing malware.

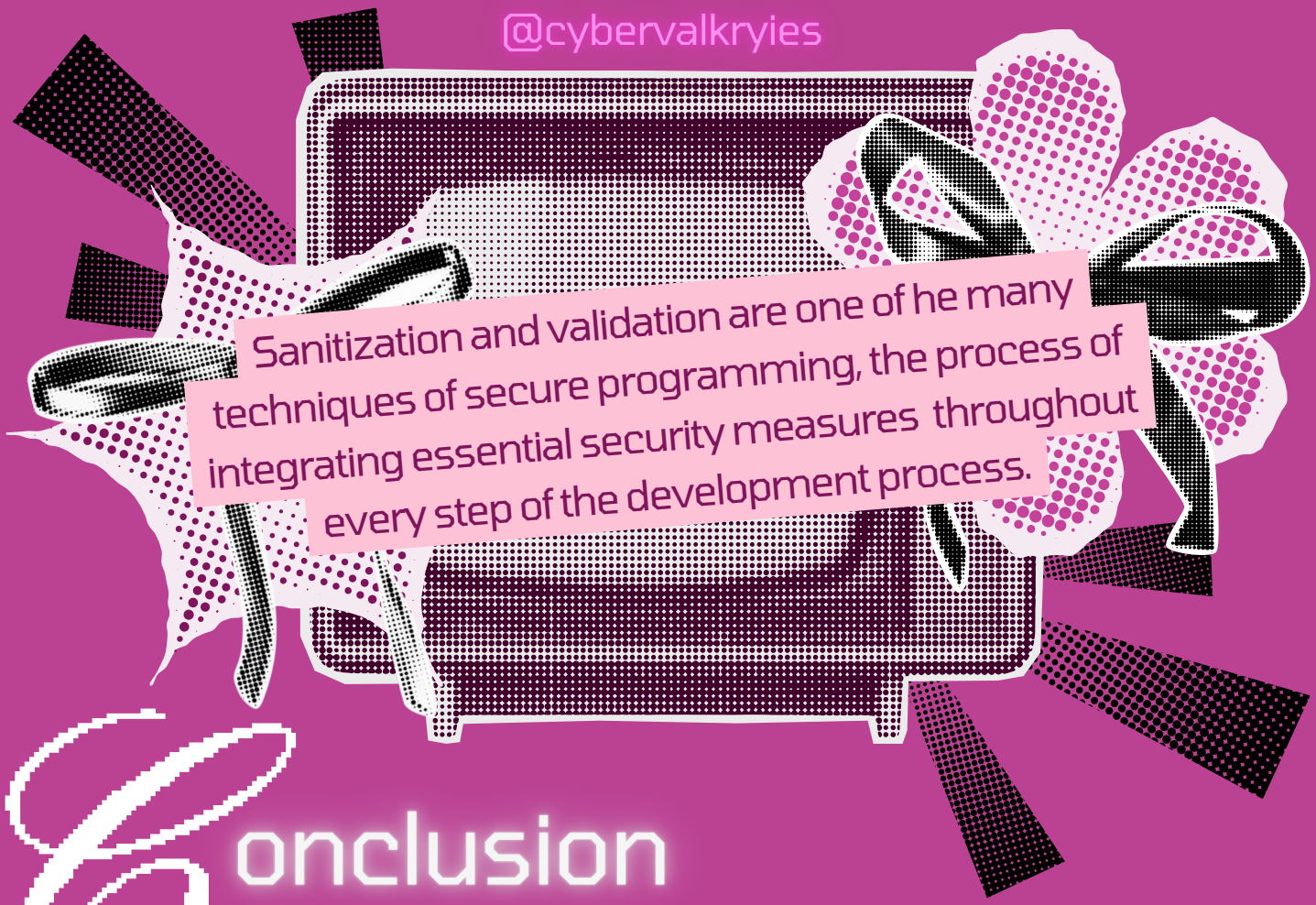
2

SQL injections: SQL (Structured Query Language) is the standard programming language used to search and manipulate databases through the use of queries. Code in the SQL syntax is injected to modify a system's databases or view sensitive data (i.e, if passwords or critical user information is stored in databases).

3

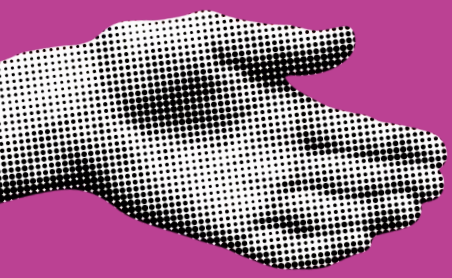
*LDAP injections: Lightweight directory access protocol (LDAP) is the industry standard that allows applications to query user information through queries that use metacharacters (like *, |, &, etc). An attacker may inject inputs that misuse these characters to prompt the server to grant unauthorized access or directing it to execute malicious commands.*

@cybervalkryies



Conclusion

If you're interested in offensive security, learning these attack types and who is behind them can help you think creatively about where and what to target in a system and how. If you're interested in defensive security, it'll help you effectively and efficiently respond to incidents, determine severity of attacks, and build the necessary countermeasures to prevent them from happening.



ORRR

If you're just a regular user, awareness is your greatest power when traversing the web or interacting with any type of system. Learning and sharing what you learn with friends and family, especially those who aren't familiar with technology is ALWAYS the first step in protecting yourself and those you love.

As you progress in your cybersecurity journey, you'll learn much more about these ever-evolving attacks (and other ones!), from how to mimic them and find vulnerabilities or how to acknowledge and prevent them outright. Stay tuned and keep learning!