DSC CYBER SECURITY DIVISION

Cyber Security Awareness.

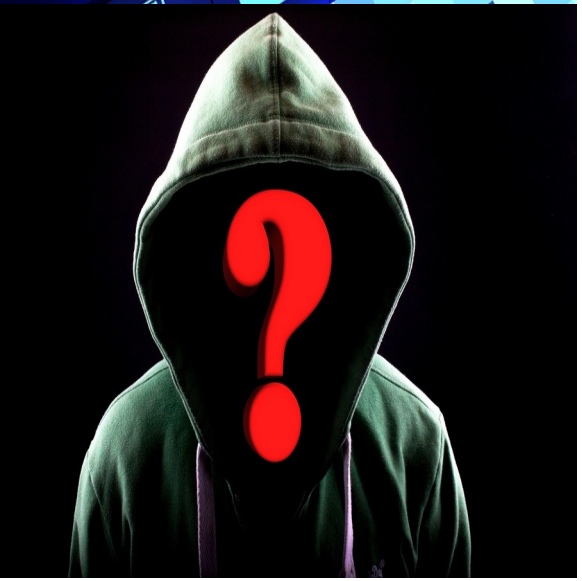
HOW TO GET HACKED!!

HOW TO GET HACKED!!

It’s October!!! You know what October is for?

Take a lucky guess!

Come on, Give it a try!



Prerequisites

0001

echo “whoami”

D_captainkenya.

0010

Intro to Hacking

What is hacking?
Types of hackers.
Cybersecurity vs Information security.
Threats to cybersecurity.

0011

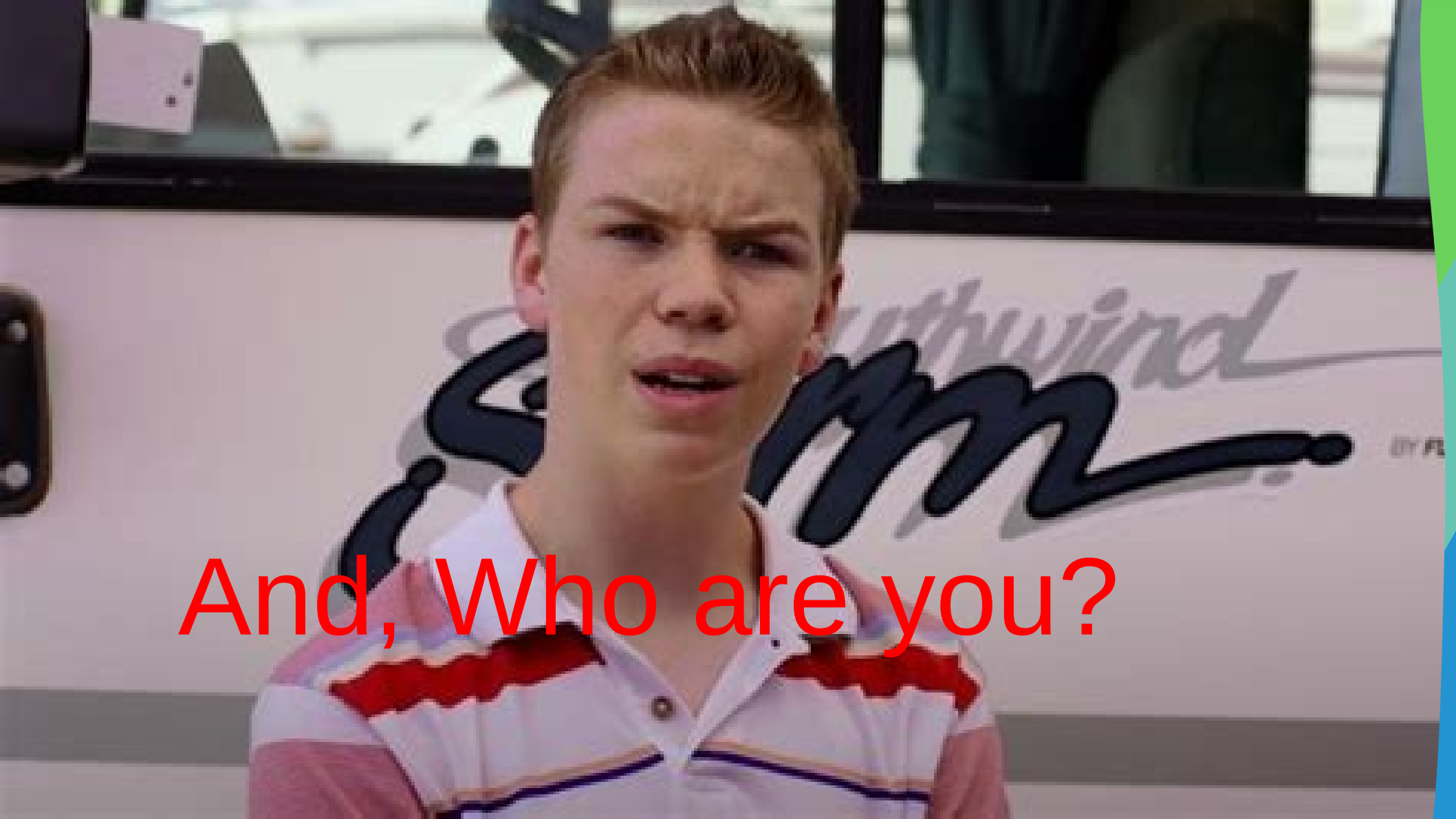
How to ‘NOT’ get hacked

How hackers get to you.
How to avoid/escape them.

0100

AoB

Everything else.


And, Who are you?

D_captainkenya

> Cybersecurity enthusiast
  (web apps, Networks, cryptography)
> Software Developer(Django)
> Technical writer
> CTF player @Fr334aks-Mini
> Bug bounty hunter @TheShield
> Interests:
  Shotokan, Bikes, Philosophy, Space science
> Climate change advocate(Earth, a dying planet?)

https://D-captainkenya.github.io

D_captainkenya

What I’m not!

Facebook

WhatsApp

Instagram

Mobile Phone

HACKING!!!!

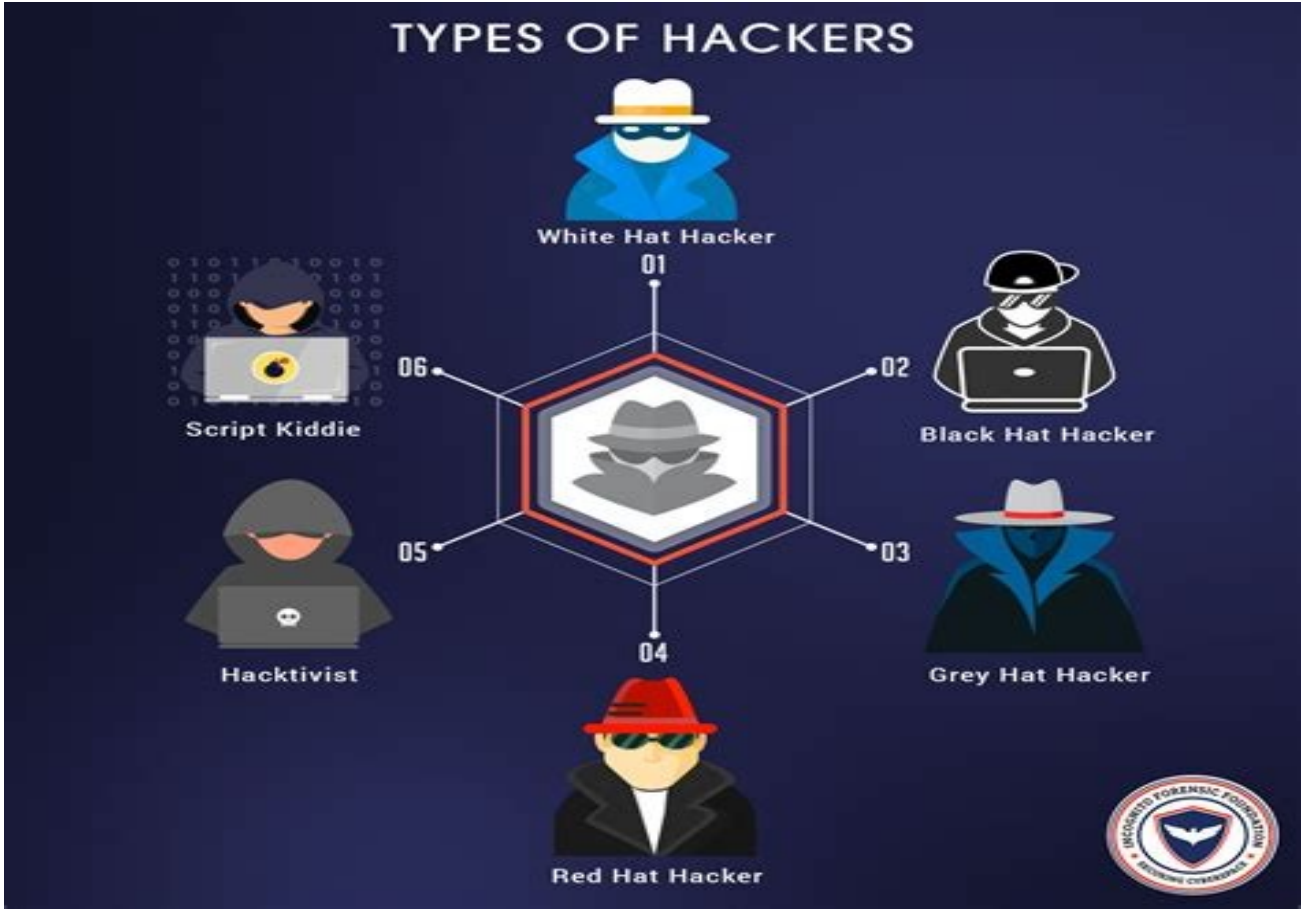
> Hacking is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data. Hacking is not always a malicious activity, but the term has mostly negative connotations due to its association with cyber crime. (Kaspersky)

Why do people hack?

a. Money - Ransomware
b. Corporate espionage - stealing trade secrets from competitor companies.
c. Political espionage - Nation states
d. Revenge - anger
e. Hack-tivism - promoting a particular political agenda or social movement.
f. Notoriety - boast about their activities.
g. Security improvements - whites

Hacker types

- Black hat
- White hat
- Grey hat
- Script kiddie
- State sponsored
- Hacktivists
- Blue hat
- Green hat
- Red hat



1) Black Hat Hacker

Black hat hackers are the evil guys who want to use their technical skills to defraud and blackmail others. They usually have the expertise and knowledge to break into computer networks without the owners' permission, exploit security vulnerabilities, and bypass security protocols.
Companies protect only 3% of their folders, which makes it easy to access their information. A famous breach of privacy was when 500 million Yahoo accounts were compromised in 2014. The activities of Black Hat Hackers are illegal.

2) White Hat Hacker

Also known as ethical hackers, they use their technical skills to protect the world from bad hackers.
Companies and government agencies hire white hats as information security analysts, cybersecurity researchers, security specialists, penetration testers, etc. They work as independent consultants or freelancers as well. White hat hackers employ the same hacking techniques as black hat hackers, but they do it with the system owner’s permission and their intentions are noble.

2) White Hat Hacker

White hat hackers hack to:

>> Find and fix vulnerabilities in the system before black hat hackers exploit them.
>> Develop tools that can detect cyberattacks and mitigate or block them.
>> Strengthen the overall security posture of the software and hardware components.
>> Build security software like antivirus, anti-malware, anti-spyware, honeypots, firewalls, etc.

3) Grey Hat Hacker

Fall somewhere between white hat and black hat hackers. They may penetrate your website, application, or IT systems to look for vulnerabilities without your consent. But they typically don’t try to cause any harm.

Grey hat hackers draw the owner’s attention to the existing vulnerabilities. They often launch the same type of cyber-attacks as white hats on a company/government servers and websites. These attacks expose the security loopholes but don’t cause any damage.

Grey hat hackers sometimes charge a fee to:

- Fix bugs or vulnerabilities,
- Strengthen the organization’s security defenses, or
- Provide recommendations, solutions, or tools to patch vulnerabilities.

4. Script Kiddies

Script Kiddies are amateur hackers that don’t want to improve but look for tools made by others to carry out their malicious intents.
Script kiddies will use these programs/tools without even knowing how they work or what they do.
It is generally assumed that most script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own
They often buy and download malware and scripts. Due to their lack of vision and education, they don’t have an understanding of the consequences which can be dangerous.
Their actions are usually illegal.

4. State Sponsored Hackers

State/Nation Sponsored Hackers are hackers who carry out the interests of the state/nation that sponsors them.
They gain information on other countries, which gives an advantage to their government.
That way, they can be prepared for attacks and have the upper hand in political games. Their actions are illegal in the targeted country.
Over 50% of state/nation sponsored hacks are related to Russian hackers.

4. State Sponsored Hackers

They are employed by their state or nation’s government to snoop in and penetrate through full security to gain confidential information from other governments to stay at the top online.

They have an endless budget and extremely advanced tools at their disposal to target individuals, companies or rival nations.
State-sponsored hacker groups are generally referred to as advanced persistent threats (APTs) by security researchers.

World's most dangerous APTs

1. Cozy Bear (APT29) - Russia
2. Lazarus Group (APT38) – North Korea
3. Double Dragon (APT41) - China
4. Fancy Bear (APT28) - Russia
5. Helix Kitten (APT34) - Iran

4. Hacktivists

If you've ever come across social activists propagandizing a social, political, or religious agenda, then you might as well meet hacktivists, the online version of an activist.

Hacktivists are hackers or a group of anonymous hackers who think they can bring about social changes and often hack governments and organizations to gain attention or share their displeasure over opposing their line of thought.

- Chaos Computer Club (CCC)
- Anonymous
- Worms against nuclear killers(WANK)
- The level seven
- Xbox underground

Rest

Blue Hat

Are another form of novice hackers much like script kiddies whose main agenda is to take revenge on anyone who makes them angry. They have no desire for learning.

Green Hat

Are amateurs in the online world of hacking. Consider them script kiddies but with a difference. These newbies have a desire to become full-blown hackers and are very curious to learn. You may find them engrossed in the hacking communities bombarding their fellow hackers with questions.

Red Hat

Have an agenda similar to white hat hackers which in simple words is halting the acts of Black hat hackers. However, there is a major difference in the way they operate. They are ruthless when it comes to dealing with black hat hackers.

Instead of reporting a malicious attack, they believe in taking down the black hat hacker completely.

Whistle blowers

Someone who works within an organization and has the intent to exploit information and security system holes for personal gain or revenge. They use the same spectrum of techniques as all other hackers and their activities are illegal.

Cybersecurity vs Information Security

Information security refers to the safety of information in all its forms, whether it's stored on a computer system or not.
>> the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability(CIA).

Cybersecurity involves the safety of computer systems and everything contained within them, which includes digital data.
>> protecting data that is found in electronic form (such as computers, servers, networks, mobile devices, etc.) from being compromised.

Cybersecurity Threats

Cybersecurity refers to the process of protecting all of cyberspace from unauthorized access.
Encompasses the protection of servers, online accounts, computer networks and individual computers, mobile phones.

Cybersecurity extends to smart gadgets/Internet of Things (IoT).
Ranging from smart TVs - home surveillance systems - smart window shades - internet-enabled fish tanks.

Hackers can gain unauthorized access to connected devices and then use that access as a stepping stone to gain entry to networks with sensitive data.

Cybersecurity Threats of All Time

[ ] Malware attack

[ ] Social engineering attacks

[ ] Software supply chain attacks

[ ] Advanced persistent threats (APT)

[ ] Distributed denial of service (DDoS)

[ ] Man-in-the-middle attack (MiTM)

[ ] Password attacks

Cybersecurity Threats of All Time

1. Malware(Malicious Software) attack

Attacks use many methods to get malware into a user's device, most often social engineering. Users may be asked to take an action, such as clicking a link or opening an attachment. In other cases, malware uses vulnerabilities in browsers or operating systems to install themselves without the user's knowledge or consent.

Once malware is installed, it can monitor user activities, send confidential data to the attacker, assist the attacker in penetrating other targets within the network, and even cause the user's device to participate in a botnet leveraged by the attacker for malicious intent.

Cybersecurity Threats of All Time

Malware attacks include:

Trojan virus — tricks a user into thinking it is a harmless file. A Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.

Ransomware — prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid. Learn more in our guide to ransomware prevention.

Wiper malware — intends to destroy data or systems, by overwriting targeted files or destroying an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.

Cybersecurity Threats of All Time

Worms — this malware is designed to exploit backdoors and vulnerabilities to gain unauthorized access to operating systems. After installation, the worm can perform various attacks, including Distributed Denial of Service (DDoS).

Spyware — this malware enables malicious actors to gain unauthorized access to data, including sensitive information like payment details and credentials. Spyware can affect mobile phones, desktop applications, and desktop browsers.

Cybersecurity Threats of All Time

Fileless malware — this type of malware does not require installing software on the operating system. It makes native files such as PowerShell and WMI editable to enable malicious functions, making them recognized as legitimate and difficult to detect.

Application or website manipulation — OWASP outlines the top 10 application security risks, ranging from broken access controls and security misconfiguration through injection attacks and cryptographic failures. Once the vector is established through service account acquisition, more malware, credential, or APT attacks are launched.

Cybersecurity Threats of All Time

2. Social engineering attacks

This is psychologically manipulating users into performing actions desirable to an attacker, or divulging sensitive information.

It is often called “Hacking the human brain”

Cybersecurity Threats of All Time

Social engineering attacks include:

Phishing — attackers send fraudulent correspondence that seems to come from legitimate sources, usually via email. The email may urge the user to perform an important action or click on a link to a malicious website, leading them to hand over sensitive information to the attacker, or expose themselves to malicious downloads. Phishing emails may include an email attachment infected with malware.

Spear phishing — a variant of phishing in which attackers specifically target individuals with security privileges or influence, such as system administrators or senior executives.

Cybersecurity Threats of All Time

Malvertising — online advertising controlled by hackers, which contains malicious code that infects a user's computer when they click, or even just view the ad.

Drive-by downloads — attackers can hack websites and insert malicious scripts into PHP or HTTP code on a page. When users visit the page, malware is directly installed on their computer; or, the attacker's script redirects users to a malicious site, which performs the download. Drive-by downloads rely on vulnerabilities in browsers or operating systems.

Vishing — voice phishing (vishing) attacks use social engineering techniques to get targets to divulge financial or personal information over the phone.

Cybersecurity Threats of All Time

Scareware security software — pretends to scan for malware and then regularly shows the user fake warnings and detections. Attackers may ask the user to pay to remove the fake threats from their computer or to register the software. Users who comply transfer their financial details to an attacker.

Baiting — occurs when a threat actor tricks a target into using a malicious device, placing a malware-infected physical device, like a USB, where the target can find it. Once the target inserts the device into their computer, they unintentionally install the malware.

Whaling — this phishing attack targets high-profile employees (whales), such as the chief executive officer (CEO) or chief financial officer (CFO). The threat actor attempts to trick the target into disclosing confidential information.

Cybersecurity Threats of All Time

Pretexting — occurs when a threat actor lies to the target to gain access to privileged data. A pretexting scam may involve a threat actor pretending to confirm the target's identity by asking for financial or personal data.

Scareware — a threat actor tricks the victim into thinking they inadvertently downloaded illegal content or that their computer is infected with malware. Next, the threat actor offers the victim a solution to fix the fake problem, tricking the victim into downloading and installing malware.

Diversion theft — threat actors use social engineers to trick a courier or delivery company into going to a wrong drop-off or pickup location, intercepting the transaction.

Cybersecurity Threats of All Time

Honey trap — a social engineer assumes a fake identity as an attractive person to interact with a target online. The social engineer fakes an online relationship and gathers sensitive information through this relationship.

Tailgating or piggybacking — occurs when a threat actor enters a secured building by following authorized personnel. Typically, the staff with legitimate access assumes the person behind is allowed entrance, holding the door open for them.

Pharming — an online fraud scheme during which a cybercriminal installs malicious code on a server or computer. The code automatically directs users to a fake website, where users are tricked into providing personal data.

Cybersecurity Threats of All Time

3. Software supply chain attacks

A software supply chain attack is a cyber attack against an organization that targets weak links in its trusted software update and supply chain.
A supply chain is the network of all individuals, organizations, resources, activities, and technologies involved in the creation and sale of a product.
A software supply chain attack exploits the trust that organizations have in their third-party vendors, particularly in updates and patching.

Cybersecurity Threats of All Time

Types of software supply chain attacks:

- **Compromise of software build tools or dev/test infrastructure**
- **Compromise of devices or accounts owned by privileged third-party vendors**
- **Malicious apps signed with stolen code signing certificates or developer IDs**
- **Malicious code deployed on hardware or firmware components**
- **Malware pre-installed on devices such as cameras, USBs, and mobile phones**

Cybersecurity Threats of All Time

4. Advanced persistent threats (APT)

When an individual or group gains unauthorized access to a network and remains undiscovered for an extended period of time, attackers may exfiltrate sensitive data, deliberately avoiding detection by the organization’s security staff.

APTs require sophisticated attackers and involve major efforts, so they are typically launched against nation states, large corporations, or other highly valuable targets.

Cybersecurity Threats of All Time

Common indicators of an APT presence include:

New account creation
Abnormal activity —stale account suddenly being active.
Backdoor/trojan horse malware
Odd database activity — sudden increase in database operations with massive amounts of data.
Unusual data files — the presence of these files can indicate data has been bundled into files to assist in an exfiltration process.

Cybersecurity Threats of All Time

5. Distributed denial of service (DDoS)

The objective of a denial of service (DoS) attack is to overwhelm the resources of a target system and cause it to stop functioning, denying access to its users.

Distributed denial of service (DDoS) is a variant of DoS in which attackers compromise a large number of computers or other devices, and use them in a coordinated attack against the target system.

Cybersecurity Threats of All Time

Methods of DDoS attacks include:

Botnets — systems under hacker control that have been infected with malware. Attackers use these bots to carry out DDoS attacks. Large botnets can include millions of devices and can launch attacks at devastating scale.

Smurf attack — sends Internet Control Message Protocol (ICMP) echo requests to the victim's IP address. The ICMP requests are generated from 'spoofed' IP addresses. Attackers automate this process and perform it at scale to overwhelm a target system.

TCP SYN flood attack — attacks flood the target system with connection requests. When the target system attempts to complete the connection, the attacker's device does not respond, forcing the target system to time out. This quickly fills the connection queue, preventing legitimate users from connecting.

Cybersecurity Threats of All Time

6. Man-in-the-middle attack (MitM)

When users or devices access a remote system over the internet, they assume they are communicating directly with the server of the target system. In a MitM attack, attackers break this assumption, placing themselves in between the user and the target server.

Once the attacker has intercepted communications, they may be able to compromise a user’s credentials, steal sensitive data, and return different responses to the user.

Cybersecurity Threats of All Time

MitM attacks include:

Session hijacking — an attacker hijacks a session between a network server and a client.

Replay attack — a cybercriminal eavesdrops on network communication and replays messages at a later time, pretending to be the user.

IP spoofing — The attacker forges its packet with the IP source address of a trusted host, rather than its own IP address.

Eavesdropping attack — attackers leverage insecure network communication to access information transmitted between the client and server.

Bluetooth attacks — Because Bluetooth is often open in promiscuous mode, there are many attacks, particularly against phones, that drop contact cards and other malware through open and receiving Bluetooth connections. Usually this compromise of an endpoint is a means to an end, from harvesting credentials to personal information.

Cybersecurity Threats of All Time

7. Password attacks

A hacker can gain access to the password information of an individual by ‘sniffing’ the connection to the network, using social engineering, guessing, or gaining access to a password database.

An attacker can ‘guess’ a password in a random or systematic way.

Cybersecurity Threats of All Time

Password attacks include:

Brute-force password guessing — an attacker uses software to try many different passwords.

Dictionary attack — a dictionary of common passwords is used to gain access to the computer and network of the victim. One method is to copy an encrypted file that has the passwords, apply the same encryption to a dictionary of regularly used passwords, and contrast the findings.

Pass-the-hash attack — an attacker exploits the authentication protocol in a session and captures a password hash (as opposed to the password characters directly) and then passes it through for authentication and lateral access to other networked systems.

Golden ticket attack — a golden ticket attack starts in the same way as a pass-the-hash attack, where on a Kerberos (Windows AD) system the attacker uses the stolen password hash to access the key distribution center to forge a ticket-granting-ticket (TGT) hash. Mimikatz attacks frequently use this attack vector.

How to ‘NOT’ get hacked

Common Myths in Cybersecurity

1. I have nothing to hide. Why should I protect myself? cyber crimes only happen to businesses and influential people.
2. I use antivirus software, so I don’t need to worry.
3. I know my device and would notice if it got hacked.
4. I'm safe because I only use my smartphone.
5. A strong password is all I need.

How to ‘NOT’ get hacked

Let’s face it: the future is now. We are already living in a cyber society, so we need to stop ignoring it or pretending that is not affecting us.
Cyber Security attacks are on the increase, Let us all demystify ways to identify, respond and prevent cyber attacks on our digital lifestyles, devices and organizations.

Let’s get a few things straight

1. Your SIM can be swapped by a stranger
2. Your files deserve to be backed up
3. If attacked by a ransomware it can affect you emotionally
4. Over sharing your private data online is risky
5. Cyber criminals are on steroids to attack

How to ‘NOT’ get hacked

How Hackers get you

They use the various nefarious cyber security threats we saw earlier on:

Malware: Viruses, Trojans, worms, MitM

These are delivered to victims in a couple of ways and means:

Emails, SMS, Websites, Mobile phone calls(Zero-click attacks) insecure networks, social engineering(Enticing links, grandma), watering hole....

How to ‘NOT’ get hacked

How to avoid/escape them.

1. Use strong passwords
2. Use multi-factor authentication (MFA)
3. Be vigilant against phishing
   - Starts with phishing emails or texts.
   - Includes a link or attachment.
   - Don’t open messages from unknown senders
   - Never click on a link or open attachments in an email you’re not sure about,
   - Delete messages you suspect to be spam.

How to ‘NOT’ get hacked

How to avoid/escape them.

Think twice before clicking that link.

What may possibly happen if you click on a malicious link?

1. Redirection to a phishing website
2. Installation of Malware
3. Third-party applications can be granted extreme permissions on your device/ applications.

How to ‘NOT’ get hacked

How to avoid/escape them.

What to do when you receive a suspicious link.

To expand shortened links or to get a snapshot of the landing page, use the following websites:

Expand URL. - https://www.expandurl.net/
CheckshortURL. - http://checkshorturl.com/
URL2PNG — a screenshot as a service.
- https://www.url2png.com/

Check the link on Virustotal - https://www.virustotal.com/gui/home/upload

How to ‘NOT’ get hacked

How to avoid/escape them.

4. Manage your digital footprint

A digital footprint is the data you leave behind when using the internet. It’s a good idea to proactively manage your digital footprint:

> Deleting old accounts and apps you no longer use
> Reviewing your privacy settings on social media and ensuring these are set to a level you feel comfortable with
> Being careful about what you post and avoiding disclosing personal or financial details about yourself in public
> Checking your browser for cookies and regularly deleting unwanted cookies
> Using privacy tools such as anonymous browsers, private search engines or anti-tracking tools

How to ‘NOT’ get hacked

5. Keep your devices and software up to date
6. Keep devices secure
7. Avoid questionable websites(http>https) and software
8. Turn off features you don’t need(GPS, BT, WIFI...)
9. Don’t access personal or financial data with public Wi-Fi
10. Use good quality antivirus

Thank you!

Q &A

@D_captainkenya

Now let’s go take some photos
Out there!!

or you get hacked