1. What is Ethical Hacking?
Hacking often refers to the unauthorized intrusion into a network or computer, normally carried out by one or more “hackers.” However, a hacker can be anyone and their activities do not have to be malicious or unauthorized to count as hacking. Hacking can mean using skills to achieve a goal in a clever way. They can be an individual like you or me. They can work solo or be employed by an organization for good or for ill. Often, they look to alter security systems to achieve their goal.

There are many organizations that hire hackers as a part of their staff. These hackers use their skills to find vulnerabilities in the organization’s security. This is done to find and fix the weaknesses and prevent malicious hackers from breaking into the security system.

2. Types of Hackers
White, black, and grey refer to the relationship between the hacker and the systems they are attacking.

2.1 Black Hat Hackers
The term “black hat” originated from Western movies, where the bad guys wore black hats and the good guys wore white hats. A black-hat hacker is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons. The black-hat hacker does not have any permission or authority to compromise their targets. They try to inflict damage by compromising security systems, altering functions of websites and networks, or shutting down systems. They often do so to steal or gain access to passwords, financial information, and other personal data.

2.2 White Hat Hackers
White-hat hackers, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system. A white hat has permission to engage the targets and to compromise them within the prescribed rules of engagement. White-hat hackers are often referred to as ethical hackers. This individual specializes in ethical hacking tools, techniques, and methodologies to secure an organization’s information systems. Unlike black-hat hackers, ethical hackers exploit security networks and look for backdoors when they are legally permitted to do so. White-hat hackers always disclose every vulnerability they find in the company’s security system so that it can be fixed before they are being exploited by malicious actors. Fortune 50 companies like Facebook, Microsoft, and Google also use white-hat hackers.

2.3 ‘Grey Hat’ Hackers
Grey hats exploit networks and computer systems in the way that black hats do, but do so without any malicious intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies. Usually, grey-hat hackers surf the net and hack into computer systems to notify the administrator or the owner that their system/network contains one or more vulnerabilities that must be fixed immediately. Grey hats may also extort the hacked, offering to correct the defect for a nominal fee.
3. Most Popular Hacking Technique - Social Engineering

Social engineering is a common term cybersecurity professionals use to talk about the many ways we are all vulnerable to data theft. The term social engineering usually means the process of taking advantage of the human instinct to help someone in need to serve the purpose of the criminal.

The problem of social engineering has been evolving for many years but today it is the main source of cyber attacks and cyber terrorism. Malware installed via a technical flaw accounts for only 3% of instances whereas social engineered attacks amount to a massive 97%. The hacking pattern has changed from targeting of software or hardware to more focused on human vulnerabilities.

Different Types of Social Engineering Attacks Phishing

91% of data breaches come in the form of phishing, making it the most exploited form of social engineering. Phishing is a type of cybercrime in which emails are sent to the target in order to lure individuals to provide personal information, banking and credit card details, email or social media account passwords, or other confidential information.

Phishing scams often demonstrate the following characteristics:

- Trying to obtain personal information, passwords, or other bank related details.
- Sending shortened links that will redirect to compromised websites that can track your details.
- Incorporating a sense of urgency, threat, or fear to manipulate the victim to react before thinking.

A perfect example of this type of a social engineered attack is the phishing scam that occurred a month after Tax Day in 2018 in the US when criminals sent misleading emails asking for tax return details. This was done to obtain access to accounts and use the information to file fraudulent tax returns.

3.1.2 Impersonation

Cybercriminals often look for the weakest link to compromise a system, and that weakest link is often the humans. Impersonation requires a lot of effort to understand the target and plan the attack, hence, this is the least common form of social engineering.

Some common roles that an impersonator might take on to implement the attack are an IT executive, a manager, an auditor, or a fellow employee. Usually, impersonation attacks focus on roles with authority because when people receive a request asking to share information from authoritative persons, they will act immediately without verifying the true identity of the sender.

Even though impersonation is not as commonly performed when compared to other social engineering forms of attacks, the attacks have risen by nearly 400% in 2017.

Vishing

Voice phishing, or vishing, is growing rapidly as a form of social engineering. Vishing attacks are where an attacker will call into the target organization and attempt to gain information and credentials
over the phone. Another vishing scam is where the attacker attempts to get the person on the other end of the phone to perform some action on their PC. These actions include running desktop scripts and viewing infected websites. These attacks are difficult to monitor and trace and unfortunately, employees working in HR departments, customer service, sales, and marketing, etc. are highly vulnerable to these attacks.

From 2012 to 2016, a group of cyber criminals ran a massive IRS vishing scam. During these four years, more than 15,000 victims in the United States lost “hundreds of millions” of dollars to this sophisticated scam, and more than 50,000 individuals had their personal information compromised.

**Smishing**

Smishing is a portmanteau of “SMS phishing” which is similar to phishing but is performed through text messages. Smishing criminals normally send messages to contact numbers that they obtain through various black-hat techniques like web-crawling, data breaches, or random number generators. The messages sent by scammers use different techniques to get you to share the information they are after. They may promise coupons or discounts on desirable products or they may pose as your bank looking to verify your account details. You may also receive texts from suspicious numbers like “5000” or other numbers linked to email-to-text services which could be automated.

As reported by NBC Nightly News, a smishing scam was attempted by asking victims to activate their new credit card by entering private information over the phone. In another smishing scam, users were informed that their online accounts were expiring and that they were required to renew their account by entering their passwords on a fake website.

4. **Common Hacking Tools**

To accomplish a perfect hack, hackers implement a wide variety of techniques such as:

**Rootkits**

A rootkit is a program or set of software tools that allow threat actors to gain remote access to control a computer system that interacts or connects with the internet. Originally, a rootkit was developed to open a backdoor in a system to fix specific software issues. Unfortunately, this program is now used by hackers to destabilize the control of an operating system from its legitimate operator or user.

There are different ways to install rootkits in a victim’s system, the most famous of them being social engineering and phishing attacks. Once rootkits are installed in the system, it secretly allows the hacker to access and control the system, giving them the opportunity to bring the system down or steal crucial data.

**Keyloggers**

This is a specially designed tool that logs or records every key pressed on a system. Keyloggers record every keystroke by clinging to the API (application programming interface) when typed through the computer keyboard. The recorded file then gets saved, which includes data like usernames, website visit details, screenshots, opened applications, etc.
Keyloggers can capture credit card numbers, personal messages, mobile numbers, passwords, and other details as long as they are typed. Normally, keyloggers arrive as malware that allows cybercriminals to steal sensitive data.

Vulnerability Scanners

A vulnerability scanner classifies and detects various system weaknesses in networks, computers, communication systems, etc. This is one of the most common practices used by ethical hackers to find potential loopholes and fix them on an immediate basis. On the other hand, vulnerability scanners can also be used by black-hat hackers to check the system for potential weak spots in order to exploit the system.

5. Popular Software Used By Hackers and Criminals

Apart from using different attack techniques to crack and steal passwords from users and organizations, cybercriminals tend to use password hacking and decrypting software. Here are some popular ones:

**John The Ripper (JTR)**

This software is designed to crack open some of the most complicated passwords, as it can crack passwords ‘offline.’ JTR takes different text string samples, commonly referred to as ‘wordlists,’ that contain complex and popular words found in the dictionary or real passwords which were cracked before. This tool uses both the key and encryption algorithm and compares the output to the encrypted string. JTR can also be used to perform a variety of alterations towards dictionary attacks.

**5.2 Aircrack-ng**

This tool/software is used to crack wireless passwords; the tool is very effective when used by a trained user. Aircrack-ng is an 802.11 WPA-PSK and WEP keys cracking software which can recover passwords when sufficient data packets are captured in monitor mode. Professionals who are experienced in penetration testing and auditing wireless networks can get the best results from this software.

**Cain and Abel**

This extremely popular tool is often referred to as just ‘Cain.’ At its core, the Cain and Abel Password Hacking Tool is used to recover passwords for Microsoft Windows but can also be used as a password cracking tool by hackers and criminals worldwide.

**THC Hydra**

This tool is similar to JTR, except for the fact that THC Hydra works online. This hacking tool supports a variety of network protocols such as LDAP, SSH, VNC, Mail (IMAP, POP3, etc.), SMB, and databases. THC Hydra is an essential hacking tool to log into a stable network, using a dictionary and brute-force attacks to crack open complicated tough passwords present in the login page.
6. Common Password Hacking Techniques

SQL Injection Attack

Structured Query Language (SQL) is designed to exploit the data in a database. SQL Injection is a type of cyber-attack that targets databases through SQL statements to trick systems. This kind of attack is executed via a website interface that attempts to issue SQL commands through a database to hack usernames, passwords, and other database information.

Web applications and websites that are poorly coded are prone to SQL injection attacks because these web-based applications contain user-input fields (such as search and login pages, product and support request forms, comments section, etc.) that are vulnerable and can be easily hacked by manipulating the codes.

Distributed Denial-of-Service (DDoS)

DDoS is a type of malicious attack that distorts normal traffic to enter a server, flooding the network traffic (resulting in a denial of service). It acts like a traffic jam that clogs the road and prevents regular traffic from arriving at their destination. Devices that easily connect to the network (such as computers, IoT devices, mobile phones, etc.) are prone to DDoS attacks.

The Guessing Game

As the name suggests, this technique relies completely on guessing the password of a user. Passwords like ‘password’, ‘qwerty’, ‘admin’, ‘default’, your name, or even your birthday are commonly used to set default passwords. If the user has not changed the default password or if the user is careless while setting a new password, then they can be hacked easily.

Brute Force Attack

A brute force attack is one of the most common techniques used by hackers and cybercriminals against web applications. The main focus of such an attack is to gain access to user accounts using a trial-and-error technique to guess a user’s password or personal identification number (PIN). A brute force attack methodically tries one password after another until the attacker successfully logs in to the target account. For example, the attacker will use automated tools to try Password, then Password1, Password2, Password3, etc. and iterate through every possible option within a defined keyspace (a-z, A-Z, 0-1, etc.) By using bots to test random combinations of lower and upper case alphabets and numbers to generate the right password to your account in a couple of seconds, the attacker can gain access to your account!

There is a similar attack technique known as reverse brute force attack where instead of hacking a specific user, the hacker attempts to hack multiple accounts using a single commonly-used password.

Dictionary Attack

A dictionary attack uses a pre-defined wordlist in a systematic process against individual usernames or usernames of an entire organization to gain access to the system. The possibility of a hacker
gaining access using this method is high as many users often use basic words that can be found in the dictionary as passwords. Wordlists are available for nearly every language (real and fictional) and are even separated into genres or themes. For example, if your server is named Gandalf, then a Middle Earth dictionary file that contains words and languages from the Lord of the Rings books and movies might be effective. The best way to deter a dictionary attack is to use a multiple-word (random combination of lowercase, uppercase characters with numerals) password.

Sources:

3. https://blog.eccouncil.org/your-password-has-been-hacked-do-you-know-how-it-happened/