SENG 31222

Assignment 01

J M Sandun Rangana Jayasekara

SE-2018-020

What is security hacking and types of hackers

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose

The people who engage in hacking are commonly referred to as hackers. First used in a 1980 magazine article, this term was popularized a few years later by the movies “Tron” and “WarGames”. Over the years, hackers have become a staple of popular culture. However, the usual portrayal of hackers as selftaught, thrill-seeking programming geniuses is not only stereotypical but also greatly exaggerated.

Although usually technical in nature, hacking doesn’t necessarily require excellent computational skills. Hackers can also break into computers and systems using social engineering, a set of psychological tactics designed to trick an unsuspecting target into giving hackers access to their data. What’s more, while hacking does require at least some grasp of computer technology, anyone can go to the dark web to purchase the tools they need to carry out an attack or hire a professional hacker to do it for them.

In addition to fun and thrill, hackers can be motivated by numerous other factors. These include financial gain, theft of personal data, access to confidential information, the desire to take down websites, as well as idealism and political activism. While some forms of hacking are completely legal, most of them are not and are considered criminal offenses. Depending on the severity of their attack, hackers in the United States can serve anywhere from a few weeks to 15 years in prison for computer tampering.

Types Of Hackers

White Hat Hackers

The good person who uses his or her capabilities to damage your organization. but only hypothetically. Instead, the real purpose is to uncover security failings in your system. In order to help you safeguard your business from the dangerous hackers.

Companies hire White Hats to stress test their information systems. They run deep scans of networks for malware, attempt to hack information systems using methods Black Hats would use, and even try to fool staff into clicking on links that lead to malware infestations.

They are one of the reasons large organizations typically have less downtime and experience fewer issues with their websites. Most hackers know it will be harder to get into systems managed by large companies than those operated by small businesses that probably don't have the resources to examine every possible security leak.

For that reason, it's very important for any online business to make sure it takes strong preventative measures by installing quality anti-malware security, spyware removal tools, and firewall software defense. Customers need to feel secure that online service providers are protecting their data, or they will take their business elsewhere.

Black Hat Hackers

Black Hat hackers are criminals who have maliciously hacked into computer networks. This can also unleash malware that destroys files, refuses computers, steals passwords, credit card numbers, and other personal data. However, hacking has become a major tool for government intelligence gathering. Black Hat operates more often for easy money alone or with organized criminal organizations.

Hacking is not illegal because all hacking is not for criminal activity. Anyhow black hat hacking is illegal, and the results of black hat hacking are considered as cyber-crimes that make black hat hacking a criminal activity. Black hat hacking is illegal because it breaks policies and TOS, it hurts fair play and a free market, etc. The most common cybercrime is accessing a system or network without permission and stealing the data from the system, which is also black hat hacking. The cybercrimes range from class B misdemeanors carrying a penalty of six months in prison and a thousand dollars fine to class B felonies carrying a penalty of twenty years in prison and a fifteen thousand dollars fine in the United States.

The hacker Albert Gonzalez had stolen one hundred and seventy million credit cards and any time money numbers, and he was sentenced to twenty years in prison. This is one of the serious cybercrimes in the history of the United States. Albert Gonzalez and his co-workers were made to pay back hundreds of millions of dollars. All such types of black hat hackers are being arrested and charged not only in the United States but all over the world.

Grey Hat Hackers

A gray hat hacker is someone who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers. Gray hat hackers may engage in practices that seem less than completely above board but are often operating for the common good. Gray hat hackers represent the middle ground between white hat hackers, who operate on behalf of those maintaining secure systems, and black hat hackers who act maliciously to exploit vulnerabilities in systems. Many people see the world of IT security as a black-and-white world.

However, gray hat hacking does play a role in the security environment. One of the most common examples given of a gray hat hacker is someone who exploits a security vulnerability in order to spread public awareness that the vulnerability exists. In this case, experts might say that the difference between a white hat hacker and a gray hat hacker is that the gray hat hacker exploits the vulnerability publicly, which allows other black hat hackers to take advantage of it. By contrast, a white hat hacker may do it privately in order to alert the company, without making the results public.

Hacking Titles

- **Vulnerability Brokers**

  Vulnerability brokers typically refers to grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.

- **Cypher Criminals**

Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data and generating profit.

Cybercriminals are known to access the cybercriminal underground markets found in the deep web to trade malicious goods and services, such as hacking tools and stolen data. Cybercriminal underground markets are known to specialize in certain products or services.

Laws related to cybercrime continue to evolve across various countries worldwide. Law enforcement agencies are also continually challenged when it comes to finding, arresting, charging, and proving cybercrimes.

- **State Sponsored Hackers**

They are armed and trained by the government. State-sponsored hackers construct sophisticated and personalized attack code, frequently utilizing just-discovered software flaws, Steal, collect intelligence, destroy networks, and learn about government secrets systems. Corporations, terrorist organizations, and foreign governments are their main targets. The majority of nations worldwide take part in state sponsored hacking. For the development of the most cutting-edge and stealthy.

- **Script Kiddies**

Script kiddie is a derogative term that computer hackers coined to refer to immature, but often just as dangerous, exploiters of internet security weaknesses. Not all novice hackers are script kiddies. Some inexperienced attackers do try to learn about and understand the tools they use. Script kiddies aren't interested in learning and understanding the exploits they use, instead using what is easy to find and available.

The typical script kiddie uses existing, well-known techniques, programs, and scripts to find and exploit weaknesses in internet-connected computers. Their attacks are random and with little understanding of the tools they are using, how they work and the harm they cause.

What Is User Authentication And Process

User authentication is the fundamental building block and the primary line of defense. It is the basis for most types of access control and for user accountability

Authentication helps ensure only authorized users can gain access to a system by preventing unauthorized users from gaining access and potentially damaging systems, stealing information, or causing other problems. Almost all human-to-computer interactions other than guest and automatically logged-in accounts perform user authentication. It authorizes access on both wired and wireless networks to enable access to network and internet-connected systems and resources.

1. Identification step

Presenting an identifier to the security system. Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.

2. Verification Step

Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

Means Of Authentication

i. Something The Individual Knows
ii. Something The individual Possesses
iii. Something The Individual Is
iv. Something The Individual Does

All these methods, properly implemented and used, can provide secure user authentication. However, each method has problems. An adversary may be able to guess or steal a password. Similarly, an adversary may be able to forge or steal a token. A user may forget a password or lose a token. Further, there is a significant administrative overhead for managing password and token information on systems and securing such information on systems. With respect to biometric authenticators, there are a variety of problems, including dealing with false positives and false negatives, user acceptance, cost, and convenience.

Password Based Authentication And Vulnerabilities Of Passwords

A widely used line of defense against intruders is the password system. Virtually all multiuser systems, network-based servers, Web-based ecommerce sites, and other similar services require that a user provide not only a name or identifier (ID) but also a password. The system compares the password to a previously stored password for that user ID, maintained in a system password file. The password serves to authenticate the ID of the individual logging on to the system. In turn, the ID provides security in the following ways.

The ID determines whether the user is authorized to gain access to a system. In some systems, only those who already have an ID filed on the system are allowed to gain access. The ID determines the privileges accorded to the user. A few users may have supervisory or “superuser” status that enables them to read files and perform functions that are specially protected by the operating system. Some systems have guest or anonymous accounts, and users of these accounts have more limited privileges than others. The ID is used in what is referred to as discretionary access control. For example, by listing the IDs of the other users, a user may grant permission to them to read files owned by that user.

Vulnerabilities Of Passwords

- **Offline Dictionary Attack**

Typically, strong access controls are used to protect the system’s password file. However, experience shows that determined hackers can frequently bypass such controls and gain access to the file. The attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by that ID/password combination.

Countermeasures include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords should the password file be compromised.

- **Specific Account Attack**

The attacker targets a specific account and submits password guesses until the correct password is discovered. The standard countermeasure is an account lockout mechanism, which locks out access to the account after a few failed login attempts. Typical practice is no more than five access attempts.

- **Popular Password Attack**

A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess. Countermeasures include policies to inhibit the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns.

- **Workstation Hijacking**

The attacker waits until a logged-in workstation is unattended. The standard countermeasure is automatically logging the workstation out after a period of inactivity. Intrusion detection schemes can be used to detect changes in user behavior.

Multifactor Authentication

- Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint).
- Your credentials must come from two different categories to enhance security - so entering two different passwords would not be considered multi-factor. So, look at a simple scenario: logging in to your bank account. If you've turned on MFA or your bank turned it on for you, things will go a little differently. First and most typically, you'll type in your username and password. Then, as a second factor,
- you'll use an authenticator app, which will generate a one-time code that you enter on the next screen. Then you're logged in. In most cases it's even easier than that. Most MFA approaches will remember a device. So, if you come back using the same phone or computer, the site remembers your device as the second factor.

- Between device recognition and analytics, the bank is likely performing such as whether you’re logging in 20 minutes later from halfway around the world most of the time the only ones that must do any extra work are those trying to break into your account.