Hacking

Devila Bakrania

Computer Science, Stevens Institute of Technology
Instructor : Dr. Edward Amoroso

Abstract- The act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.
It refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.

Index Terms- Ethical Hacking, Cyber Security, Hacking, Hackers, Security

I. Introduction

Hacking in another way is simply the use of technology or related knowledge to successfully bypass a challenge.

II. Techniques used in hacking

Phishing, DNS spoofing, Cookie theft, Cross-site scripting, SQL injection

III. Hacking Phases

Phase 1. Reconnaissance

Reconnaissance, also known as the preparatory phase, is where the hacker gathers information about a target before launching an attack and is completed in phases prior to exploiting system vulnerabilities.

It is also called as Footprinting and information gathering Phase, and during this phase hacker finds valuable information such as old passwords, name of important employees.

Footprinting is a method of collecting data from target system.
These data include important areas:
- Finding out specific IP addresses
- TCP and UDP services
- Identifies vulnerabilities

Footprinting Types: **Active** and **Passive**

Phase 2.. Scanning

Hackers are probably seeking any information that can help them penetrate attack such as computer names, IP addresses, and user accounts. In fact, hacker identifies a quick way to gain access to the network and look for information.

Four types of scans are used:
Pre-attack
Port scanning/sniffing
Vulnerability Scanning
Information extraction

Phase 3. Gaining Access

At this point, Hacker has the information she/he needs. So first she designs the network map and then decides how to carry out the attack.
Examples:
- Phishing attack
- Man in the middle attack
- Brute Force attack
- Spoofing attack
- Dos attack
- Buffer overflow attack
- Session hijacking
- BEC attack

After entering into a system, hacker has to increase the privilege to administrator level to install an application to modify or hide data.

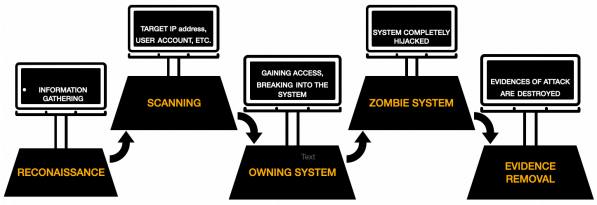
Phase 4. Zombie System

It is also known as Maintaining access. Attacker tries to retain his or her ownership of the system. Attackers prevent the system from being accessed or owned by other attackers by securing exclusive access with backdoors, root kits, malware, Trojans etc. Attackers can have access to upload, download, or make changes in data or applications. Attackers now make the system in their control for future attacks.

Phase 5. Evidence Removal

Attacker first track their activities to hide and remove their traces from victim's machine. Attacker does this by:
- Clearing the cache and cookies
- Modifying registry values
- Modifying or Corrupting or Deleting values of Logs
- Clearing out sent emails
- Closing all open ports
- Uninstalling all applications that attacker has used

Hacking Phases are explained in below Fig.(Zoom in)



IV. CLASSIFICATION OF HACKERS

1. White Hat Hackers


White-hat Hacker

They are experts in cybersecurity and are authorized or certified to hack the systems. They work for governments or organizations by getting into the system. They hack the system from the loopholes in the cybersecurity of the organization. This hacking is done to test the level of cybersecurity in their organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. They work as per the rules and regulations set by the government. Also known as ethical hackers.

2. Black Hat Hackers


Black-hat Hacker

These are knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry. On gaining entry they might steal the data or destroy the system. The hacking practices used by these types of hackers depend on the individual's hacking capacity and knowledge. As the intentions of the hacker make the hacker a criminal. The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking.

3. Gray Hat Hackers


Grey-hat Hacker

The intention behind the hacking is considered while categorizing the hacker. The Gray hat hacker falls in between the black hat hackers and white hat hackers. They are not certified, hackers. These types of hackers work with either good or bad intentions. The hacking might be for their gain. The intention behind hacking decides the type of hacker. If the intention is for personal gain then the hacker is considered to be a gray hat hacker.

4. Script Kiddies

They are amateurs hackers in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites. The intention behind the hacking is just to get attention from their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.

5. Green Hat Hackers

They are learning the ropes of hacking and are slightly different from the Script Kiddies due to their intention. The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.

6. Blue Hat Hackers

They are similar to Script Kiddies. The intent to learn is missing. They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries. Blue Hat Hackers are dangerous due to the intent behind the hacking rather than their knowledge.

7. Red Hat Hackers

These are synonymous with Eagle-Eyed Hackers. They are similar to white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red and white hat hackers is in the process of hacking through intention remains the same. Red ones are quite ruthless while dealing with black ones or counteracting with malware. The red hat hackers continue to attack and may end up having to replace the entire system set up.

8. State/Nation Sponsored Hackers

Government appoints hackers to gain information about other countries. They are known as State/Nation sponsored hackers. They use their knowledge to gain confidential information from other countries to be well prepared for any upcoming danger to their country. The sensitive information aids to be on top of every situation but also to avoid upcoming danger. They report only to their governments.

9. Hacktivist

Intend to hack government websites. They pose themselves as activists, so known as a hacktivist. Hacktivist can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks. The data gained from government files accessed are used for personal political or social gain.

10. Malicious insider or Whistleblower

Individuals working in an organization who can expose confidential information. The intent behind the exposure might be a personal grudge with the organization or the individual might have come across the illegal activities within the organization. The reason for expose defines the intent behind the exposure. These individuals are known as whistleblowers.

V. ADVANTAGES OF ETHICAL HACKING

- Prevention against cyber theft
- Protection against cyber terrorism, data breaches
- Role of government bodies increases
- Helps in understating importance of security
- Increases knowledge
- Helps in experimenting things
- Protection to services and marketing

VI. Disadvantages of Ethical Hacking

- Data Breach
- Cyber Contrabend
- System Failure and Error
- Malicious Activities
- Lacking Reliability
- Expensive
- Hectic
- Data Privacy unsurity

VII. Conclusion

The work done in the referenced paper is remarkable, providing great hacking insights. Author talked about open source but have not mentioned anything that many companies avoid third party tool in order to protect their data. This referenced paper has presented a new and improved technique of hacking ethically while in some case have ignored about how to prevent the same.

References

1. https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/
2. https://www.itperfection.com/network-security/five-phases-of-ethical-hacking-clearing-tracks-reconnaissance-scanning-hacker-security-cybersecurity/
3. GeeksforGeeks.org
4. https://www.avg.com/en/signal/what-is-hacking
5. IIOABJ_9.2_61-77TOWARDSTHEIMPACTOFHACKINGONCYBERSECURITY.pdf