IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12415

Ethical Hacking

Suwarna Nimkarde[1], Shobhana Gaikwad[2]

Lecturer, Computer Technology, BVIT, Navi Mumbai, Maharashtra[1]

Lecturer, Computer Technology, BVIT, Navi Mumbai, Maharashtra [2]

Abstract: Hacking is an identifying and exploiting weakness in computer systems or computer networks. Hacking is a process of gaining unauthorized access into a computer system in order to steal, change or destroy information.

Keywords: Impersonation, Phishing scams, hacker, cracker, Netsparker.

I. INTRODUCTION

Traditionally, the one who like to play with software or electronic systems are termed as hackers. They find excitement and happiness in exploring and learning how computer system operates. Recently, a hacker has been termed as one who maliciously breaks into systems for personal gain. Technically, they are criminal hackers also known as crackers. Crackers break into systems with malicious intent and they do this for revenge, fame, profit or for personnel gain. They modify, delete, and steal critical information as well as take entire networks offline.

Hackers (or external attackers) try to compromise your computers, access sensitive information, and even entire networks usually from the outside as unauthorized users. Malicious users (or internal attackers) try to compromise your computers and access sensitive information from the inside as ‘’authorized’’ and “trusted” users. Malicious user is a rogue employee, contractor, intern, or other user who abuses his or her trusted privileges. Malicious users’ accesses sensitive information, e-mail confidential client information to competitor, deletes sensitive files from servers. Ethical hackers (or good guys) hack systems to discover vulnerabilities to protect against unauthorized access, abuse, and misuse. Information security researchers, consultants, and internal staff fall into this category.

II. CLASSIFICATION OF HACKERS ACCORDING TO THEIR INTENT

White hat hackers use their skill and knowledge to identify and fix weaknesses in the system. They may also perform penetration Testing and vulnerability assessments.

Black hat hacker (Cracker or Unethical hacker): They use their skill and knowledge for illegal purpose. They are nothing but criminals or crackers
A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, spread malware, earn profit, etc.

Grey hat hacker: A hacker who is in between white hat hackers and black hat hackers. Hackers do not have any malicious intension and hack computer systems for fun. Grey hat hacker identify weaknesses in system and tell them to the system owner but without owner’s permission .Grey hat hacker does not perform hacking for any personnel gain or for third party benefit.

Script kiddies: Hackers with limited skills are sometimes called script kiddies. They use hacking tools and documentation available on the internet to gains access to computer systems.

Hacktivist: A hacker who use hacking to send social, religious, and political messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

III. DIFFERENCE BETWEEN HACKERS AND CRACKERS

There are many articles describing the difference between hackers and crackers-just for correcting the misconceptions of the public. The real word is cracker, but media has named it hacker. The public thinks that the hacker is someone who breaks into computer systems, which is a actually false.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12415

Definition of a hacker: The person who is interested in the workings of any computer operating system is called hacker. The hackers are good programmers. Hackers have advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

Definition of a cracker: The people who break into others system with malicious intentions are called crackers. Crackers causes problems to victims by an unauthorized access, destroying important data, stopping services provided by server, etc. Crackers can easily be identified because their actions are malicious. Hackers try to do constructive work while crackers just destroy system. Hackers are professionals, while crackers are criminals.

IV. WHAT IS ETHICAL HACKING

Ethical hacking is a penetration testing, white hat hacking, and vulnerability testing — involves the same tools, tricks, and techniques that criminal hackers use, but with one major difference: Ethical hacking is performed with the owner's permission. The intend of ethical hacking is to discover vulnerabilities from hackers point of view to better secure systems. Ethical Hacking is identifying weakness in computer systems or computer networks and coming with countermeasures (an action taken to counteract a danger or threat). That protects the weaknesses. Ethical hacking is part of an overall information risk management program that allows for ongoing security improvements.

Ethical hackers must obey following rules:
Get written permission from the owner of the computer system and/or computer network before hacking. Protect the privacy of the organization been hacked. Transparently report all the identified weaknesses in the computer system to the organization. Inform hardware and software vendors of the identified weaknesses.

V. POLICY CONSIDERATIONS

If you choose to make ethical hacking an important part of your business's information risk management program, you really need to have a documented security testing policy. Security testing policy outlines: Who is doing the security testing? The general type of testing that is performed.

How often the testing takes place? Specific procedures for carrying out your security tests. Security testing tools that are used and specific people performing the testing. You might also list standard testing dates, such as once per quarter for external systems and biannual tests for internal systems.

VI. UNDERSTANDING THE NEED TO HACK YOUR OWN SYSTEMS

To catch a thief, you must think like a thief. That's the basis for ethical hacking. In the current world, as we all know, both vulnerabilities and hacking activities have increased. So, the time will come when all computer systems and applications will be hacked in some way. It is important to protect your system from bad guys. If you know hacker tricks, you will be able to find out weaknesses in your systems.

To make your system more secure, it's important to hack your own system to identify weaknesses in your systems. As hackers expand their knowledge, you also need to expand your knowledge. You must think like them and work like them to protect your systems from them. Your overall goals as ethical hacker are as follows: Hack your systems in a non-destructive fashion. Identify vulnerabilities and, if necessary, prove to management that vulnerabilities exist and can be exploited.

VII. UNDERSTANDING DANGEROUS YOUR SYSTEM FACE

Systems are generally under fire from hackers around the world and malicious users around the office; it's important to understand the specific attacks against your systems that are possible.

For example, a default Windows OS configuration, a weak SQL Server administrator password, or a server hosted on a wireless network might not be major security concerns by themselves — but someone exploiting all three of these vulnerabilities at the same time could lead to serious issue. Some well-known attacks are as follows:

A. Nontechnical Attacks
B. Network-infrastructure attack
C. Operating system attacks
D. Application and other specialized

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12415

Nontechnical Attacks:

Attacks based on non-technical approach are performed through human deception (untrue falsehood, or is the act of lying); Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes. Social engineering is the art of manipulating people so they give up confidential information. Some of the methods of doing social engineering are stated below:

Impersonation (an act of pretending to be another person for the purpose of entertainment or fraud) over the phone: is the easiest way to manipulate a person over the phone. Phishing scams will use email, spam, and fake websites constructed to look identical to a real site in order to steal sensitive information like bank account passwords and credit card numbers. Other common and effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or steal computers, servers, and other valuable equipment. Physical attacks can also include dumpster diving — Dumpster diving is the process of searching trash to obtain useful information about a person/business that can later be used for the hacking purpose.

Network-infrastructure attack:

Attacks against network infrastructures can be easy to accomplish because many networks can be reached from anywhere in the world via the Internet.
Some examples of network infrastructure attacks are-
Connecting to a network through an unsecured wireless access point attached behind a firewall.
Exploiting weaknesses in network protocols, such as TCP/IP and Secure Sockets Layer (SSL)
Flooding a network with too many requests, creating a denial of service (DoS) for legitimate requests.
Installing a network analyzer on a network segment and capturing every packet that travels across it.

Operating system attacks:

Hacking an operating system (OS) is a preferred method of the bad guys.
OS attacks make up a large portion of attacks simply because every computer has an operating system.
some operating systems are more secure such as the Novell NetWare, OpenBSD, and IBM Series i are attacked But hackers prefer attacking Windows, Linux, and, more recently, Mac OS X, because they're more widely used.
Some examples of attacks on operating systems:
1. Exploiting missing patches:
2. Attacking built-in authentication systems
3. Breaking files system security
4. Cracking passwords and weak encryption implementations

Application and other specialized attacks:

Applications take a lot of hits by hackers. Programs (such as e-mail server software and web applications) are often beaten down. For example: Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these services over the Internet. Mobile apps face increasing attacks given their importance in business settings. Unsecured files containing sensitive information are scattered across workstation and server shares. Database systems also contain numerous vulnerabilities that malicious users can exploit

VIII. UNDERSTANDING THE ETHICAL HACKING PROCESS

Like practically any IT or security project, you need to plan your security testing. It's been said that action without planning is at the root of every failure. Formulating your plan: Getting approval for security testing is essential. Obtain authorization to perform security testing from your manager, executive or from your client. A well-defined scope include following information: Specific systems to be tested: When selecting systems to test, start with the most critical systems. Risks that are involved: When the tests will be performed and your overall timeline: Whether or not your intend to be detected: One of your goals might be to perform the tests without being detected.

Knowledge of the systems you have before you start testing: Actions you will take when a major vulnerability is discovered: Don't stop after you find one or two security holes. Keep going to see what else you can discover. The specific deliverables: This includes report the important vulnerabilities to address, along with recommendations and countermeasures to implement. Selecting tools: As with any project, it is difficult to perform the task if you don't have the right tools for your ethical hacking. Many tools focus on specific tests, and no single tool that can test for everything. Whichever tools you use, familiarize yourself with them before you start using them.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12415

While selecting tools, Make sure you're using the right tool for the task: To crack passwords, you need cracking tools, such as Ophcrack and Proactive Password Auditor. For an in-depth analysis of a web application, a web vulnerability scanner (such as Netsparker or AppSpider) is more appropriate than a network analyzer(such as Wireshark or OmniPeek). Executing the plan: Good security testing takes persistence. Time and patience are important. Also, be careful when you're performing your ethical hacking tests.

It's important that you keep everything as quiet and private as possible. Start with a broad view and narrow your focus: Search the Internet for your organization's name, your computer and network system names, and your IP addresses. Narrow your scope, targeting the specific systems you're testing. Further narrow your focus with a more critical eye. Perform actual scans and other detailed tests to uncover vulnerabilities on your systems. Perform the attacks and exploit any vulnerability you find if that's what you choose to do. Evaluating the results: Assess your results to see what you've uncovered. Your skill at evaluating the results and correlating the specific vulnerabilities discovered will get better with practice. Submit a formal report to management or to your client, outlining your results and any recommendations you need to share. Moving on: When you finish your security tests, you (or your client) still need to implement your recommendations to make sure the systems are secure. Otherwise, all the time, money, and effort spent on ethical hacking goes to waste.

IX. CONCLUSION

Hacking is an identifying and exploiting weakness in computer systems or computer networks. Hacking is a process of gaining unauthorized access into a computer system in order to steal, change or destroy information. Ethical hackers (or good guys) hack systems to discover vulnerabilities to protect against unauthorized access, abuse, and misuse. Information security researchers, consultants, and internal staff fall into this category.

REFERENCES

[1]. https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078)
[2]. Hacking For Dummies, 5th Edition By Kevin Beaver
[3]. http://cdn.ttgtmedia.com/searchNetworking/downloads/hacking_for_dummies
[4]. http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking
[5]. https://www.guru99.com/what-is-hacking-an-introduction.html#2