International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Network Security and Business Protection through Ethical Hacking

Sayli Raut

Student of Department of MCA, Late Bhausaheb Hiray Samiti Trust, Hiray Group of Institutes
Mentor: Prof. Vikram Patalbansi

Abstract: ***The rise of network security and ethical hackers is due to technology advances and the growing number of threats in the computer world. This paper defines what is ethical hacking, Network Security and Business Protection through Ethical Hacking. This paper deliberate the different types of hacking with its stages.***

Keywords: Ethical Hacking

1. Introduction

1.1 What is Hacking?

Hacking is a term that refers to someone gaining access to digital files or systems without permission, usually with a vicious intent in mind like stealing information or installing malware. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer. Hacking is typically technical in nature (like creating malvertising that deposits malware in a drive-by attack requiring no user interaction). But hackers can also use psychology to trick the user into clicking on a malicious attachment or providing personal data. It catch-all term for any type of misuse of a computer to break the security of another computing system to steal data, corrupt systems or files, commandeer the environment or disrupt data-related activities in any way.

1.2 What is Ethical Hacking?

Ethical Hacking is also known as penetration testing involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal. Independent computer security professional breaking into the computer system. Neither damage the target system nor steal information, evaluation target system security and report back to owner about the bugs found. To protect data, every small or large organization adopts this as the front layer of security. Understanding the general public's true intensions in these days is quite a difficult task, & it even more difficult to appreciate the motives of each ethical hacker entering vulnerable networks or systems. Ethical hacking becoming a powerful policy in fighting online threats with the rise of cybercrime. Using a firewall and regularly updating passwords are just the first steps to enhancing security – but they won't keep hackers from penetrating business systems. Unfortunately, even complicated passwords can be cracked and are often subject to poor security practices, like storing them on a company server or computer that is also susceptible to being hacked. Hackers are also getting more sophisticated, using emerging technology, holding data for ransom and causing catastrophic damage to small businesses and corporations alike.

2. Types of Hacking/Hackers are follows:

2.1 White Hat Hackers

White hats are good guys, who use their hacking skill for defensive purposes. This means that the white hackers use their knowledge for the good of others. White hats are those who hack with permission from data owner. White hat hackers are those individuals professing hacker skills and using them for defensive purposes.White and black hats, in general, do the same thing: they look for weaknesses in a system. While the latter takes advantage of the loopholes for monetary or other illegal advantages, the ethical hacker alerts the system's owner to the problem. Corporations frequently engage white hat hackers to examine their systems and identify security flaws before a black hat hacker can exploit them.

2.2 Black Hat Hackers

Black hat hackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities. Black hats are the bad guys the malicious hackers who use their skills for illegal or malicious purposes for their own personal gains probably by hurting others. Black hats are generally associated with malware, data breaches, intrusions, or destroying victim computers, devices, or networks. Their attacks can range from simple Malware spreading to complex vulnerability exploitation and data theft.

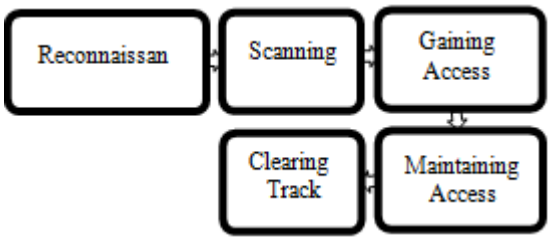
2.3 Grey Hat Hackers

These are individuals who work both offensively and defensively at various times. We cannot predict their behavior. Sometimes they use their skills for the common good while in some other times he uses them for their personal gains. These hackers may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hack. Then they may offer to repair their systems for a small fee. Somewhere between white hat hackers and black hat hackers lie grey hat

hackers. These hackers often think that they're doing a service to companies by hacking their systems and exposing their security risks, but generally speaking business owners don't appreciate unauthorised access to their system infrastructure.

3. Hacking Phases

Hacking can be performed by following these five 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. One of the first phases of Reconnaissance is dumpster diving. It is during this phase that the hacker finds valuable information such as old passwords, names of important employees (such as the head of the network department), and performs an active reconnaissance to know how the organization functions. As a next step, the hacker completes a process called foot printing to collect data on the security posture, reduces the focus area such as finding out specific IP addresses, identifies vulnerabilities within the target system, and finally draws a network map to know exactly how the network infrastructure works to break into it easily. Footprinting provides important information such as the domain name, TCP and UDP services, system names, and passwords. There are also other ways to do footprinting, including impersonating a website by mirroring it, using search engines to find information about the organization, and even using the information of current employees for impersonation.

Phase 2: Scanning: Three types of scanning are involved: Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host. Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools. Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

Phase 3: Gaining Access: This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

Phase 4: Maintaining Access: Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

Phase 5: Clearing Track: No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

4. Network Security and Business Protection through Ethical Hacking

Many Businesses that hire ethical hackers do so after a security breach has been experienced. Instead of allowing your systems to get penetrated and having your data get stolen, you can employ an ethical hacker.They use the same tricks and techniques as an actual hacker would to circumvent security. The business can use the findings of the security holes found by the ethical hacker to prevent these from occurring and hence reduce the business risk significantly. This way, you'd be able to discover present susceptibilities in your system that can threaten your security. Thus, a system attack would become more difficult for hackers, and your business wouldn't have to lose money or reputation. Ethical hackers perform serve to identify and eliminate vulnerabilities before they result in full-scale breaches scenarios. Similarly, ethical hacking efforts can show if security controls like firewalls or data loss protection protocols are operating effectively and whether new protocols need to be implemented. This can also serve as an excellent tool during software development to secure new applications before they are implemented across a business. The main objective of ethical hacking is to promise safety in wireless infrastructure which constitutes most of the current business companies' aims. Ethical hacking has the privilege of gathering access to a company's network and information system. This automatically provides security to intellectual attacks and threats like viruses. Ethical hacking, as a result, ends up also testing the security levels of the programs and software.

5. Conclusion

Ethical hacking came around as a solution to the continuous cyber-attacks performed by hackers. Since the early 2000s, when the internet became highly adopted, businesses have been at increased risk of getting hacked. Data transfer to the cloud has also made company data more vulnerable. Businesses need ethical hackers because they understand hackers and prevent the high costs of mitigating the effects of hacks. Ethical hacking is a growing industry. Several black hat hackers have also started converting because of the growing professional service and valuation. Ensuring the protection of businesses, including the government, will always be essential. Hence, the future of ethical hacking would be upward. The industry offers tremendous growth opportunities. Businesses are using ethical hackers to identify weak points in their cyber defenses, provide valuable insights

into the actions of their less ethical counterparts and create better, stronger and more resilient networks.

References

[1] Gurpreet K. Juneja,"Ethical hanking :A technique to enhance information security" international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013
[2] A. Boudreau, L. J. Van't Veer, and M. J. Bissell, "An 'elite hacker': Beast tumors exploit thenormal micro environment program to instruct their progression and biological diversity," Cell Adhesion and Migration. 2012, doi: 10.4161/cam.20880.
[3] K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393
[4] Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2013)
[5] "Innovation in Engineering, Technology and Education for Competitiveness and Prosperity" August 14 - 16, 2013 Cancun, Mexico. "Faculty Attitudes toward Teaching Ethical Hacking to Computer and Information Systems "Undergraduates Students Aury M. Curbelo, Ph.D, Alfredo Cruz, Ph.D.
[6] Kumar Utkarsh" SYSTEM SECURITY AND ETHICAL HACKING
[7] S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, "Ethical hacking: The need for cyber security," in IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017, 2018, doi: 10.1109/ICPCSI.2017.8391982.
[8] S. Tulasi Prasad, "Ethical Hacking and Types of Hackers," Int. J. Emerg. Technol. Comput. Sci.Electron., 2014.
[9] S.-P. Oriyano, "Introduction to Ethical Hacking," in CEHTMv9, 2017.