IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

A Review Paper on Ethical Hacking

Aniket Kalbende, Bharat Zile, Bhairav Shende, Jayesh Gharad, Pranav Kherde
Department of Master of Computer Application
Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, India

Abstract: *An ethical hacker is the network specialist & computer who pounce some security systems on the behalf of its possessor seeking amenability that could be exploited by a malicious hacker. The Internet's explosive growth has conduct many virtuous things: e- commerce, e-mail, collaborative computing & new fields for advertisement and information distribution. Ethical hacking has become a main anxiety for businesses & governments, also known as the intrusion testing or penetration testing or red teaming. Organizations are concerned about the probability of being "hacked" & potential clients are concerned about keeping personal information under control. Hackers are classified according to their work and knowledge. The white hat hackers are the ethical hackers. Ethical hackers use hacking approaches to ensure safety. Ethical hacking is needed to protect the system from the hacker's damage. The major reason behind the ethical hacking study is to assess the security and report back to the owner of the target system.*

Keywords: Cybercrimes, Clearing Tracks, Computer Security, Ethical Hacking

I. INTRODUCTION

Ethical hacking technology spreads to diverse areas of life and in particular to every walks of the computer industry. The required to protect dominant data of the common should be communicate with the correct technology. Because of the smartness of hackers, ethical hacking arose as the latest and innovative computer technology [1]. To protect their data, every small or large organization adopts this as the front layer of security. Understanding the general public's true intentions 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.

Generally speaking, ethical hackers that are allowed to shatter into ostensibly 'secure' computer system without malevolent intent, but with the goal of finding susceptibility in sequence to conduct about better preservation. Sometimes the local IT security officers or managers in a company are told that such an assault is to take place usually called a 'penetration test' and may even look over the shoulder of the hacker but frequently they are not, & knowledge of the attack is limited to the senior staff, sometimes just 2 or 3 members of the board. Many ethical hackers works for consultants & others are wage earning workers who regularly perform a scheduled hacks program.

II. ETHICAL HACKING

2.1 Ethical Hacker

Ethical hacking is the practice of performing security assessments using the same techniques that hackers use, but with proper approvals and authorization from the organization you're hacking into. The goal is to use cybercriminals' tactics, techniques, and strategies to locate potential weaknesses and reinforce an organization's protection from data and security breaches. Cybersecurity Ventures predicts that cybercrime will globally cost an estimated $10.5 trillion every year in damages by 2025 [1]. They also predict that ransomware alone will cost victims $265 billion every year by 2031. The present threat of cybercrime combined with the shortage of experienced information security professionals has created a crisis for businesses, organizations, and governmental entities, according to Forbes. It also presents a unique opportunity for a career path. We've rounded up some key points to consider if you're thinking of going into ethical hacking. of first generation was below par capacity, reckless handoff, inferior accent associations, and with no safety measures, since audio calls were accumulated and played in radio towers due to which weakness of these calls from not so needed connections.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

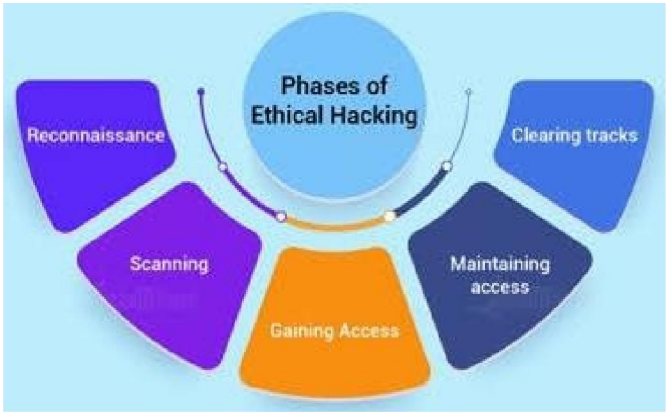

Fig: 1.Ethical Hacker Steps

2.2 Reconnaissance

It is the set of procedures & technique used to gather information's about the target systems secretly. In this, the ethical hacker seeks to gather as more information as possible about the target systems, following the 7 steps mentioned below

- Identification of active machines
- Preliminary information collection
- Identification of every ports services
- Network mapping
- Identification of open ports & access points & OS fingerprinting.

2.3 Scanning

The 2nd step of the penetration testing & ethical hacking is the enumeration and scanning. Scanning is the common technique that pen tester uses to find the open door. Scanning is worn to determine the weaknesses of the service that operate on the port. They need to figure out the operating systems included, live host, firewalls, services, intrusion detection, perimeter equipment, routing & general networks topology (physical network layout) that are parts of the targets organization during this phase.

2.4 Gaining Access

Once the observation is finished & every weakness are tested, the hackers then attempts with the helps of some tools & techniques to gain access. This essentially focuses on the retrieval of the password. Either bypass techniques (like using konboot) or password cracking the techniques that can be used for this by hacker

2.5 Maintaining Access

Once the intruder has got access to the targeted systems, he can take advantage of both the systems & its resources & use the systems as a catapult pad for testing & harming other system, or can retain the low profile & continue to exploit the systems without the genuine user knowing every acts. Those 2 acts will demolish the organization that leads to a calamity. Rootkits gain entrance at the operating systems level, while the Trojan horses gain entrance at the program levels. Attackers that can use the Trojan horses to migrate on the system user passwords, names & credit card information's. Organizations that can use tools for honeypots or intrusion detection to detect the intruders.

2.6 Clearing Tracks:

For several purposes such as avoiding detection & further penalizing for intrusion, an offender will destroy confirmation of his activities and existence. Eliminating evidence that is often referred to the ' clearing tracks ' is the requirement for every intruder who needs to remain anonymous and prevent detect back. Usually this steps begins by delete the adulterate logins or all other possible errors messages generated from the attack process on the victim

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

system. For e.g., a buffer overflow attack usually leaves a message that needs to be cleared in the systems logs. Next attention is focused on making changes in order not to log in to potential logins. The 1st thing a systems administrator does to trace the system's uncommon activity is to review all the systems log file, it is necessary for trespasser to use the tool to change the system logs so that the administrator cannot track them. Making the system look like it did before they obtain access & set up backdoor for their own use is important for attackers.

III. TOOLS USED IN ETHICAL HACKING

3.1 Invicti

Invicti is a web application security scanner hacking tool to find SQL Injection, XSS, and vulnerabilities in web applications or services automatically. It is usually available on SAAS solution

Features:

- It detects Dead accurate vulnerability with the help of unique Proof-Based Scanning Technology.
- It requires minimal configuration with a scalable solution.
- It automatically detects URL rewrite rules as well as custom 404 error pages.
- There is a REST API for seamless integration with the SDLC and bug tracking systems.
- It scans up to 1,000 plus web applications within just 24 hours.
- Price: It will cost from $4,500 to $26,600 with Invicti Security features.

3.2 Fortify WebInspect

Fortify WebInspect is a hacking tool with comprehensive dynamic analysis security in automated mode for complex web applications and services.

- It is used to identify security vulnerabilities by allowing it to test the dynamic behavior of running web applications.
- It can keep the scanning in control by getting relevant information and statistics.
- It provides Centralized Program Management, vulnerability trending, compliance management, and risk oversight with the help of simultaneous crawl professional-level testing to novice security testers.
- Price: It will cost around $29,494.00 provided by HP company with Tran security and virus protection

3.3. Cain & Abel

Cain & Abel is an Operating System password recovery tool provided by Microsoft.

- It is used to recover the MS Access passwords
- It can be used in Sniffing networks
- The password field can be uncovered.
- It Cracks encrypted passwords with the help of dictionary attacks, brute-force, and cryptanalysis attacks.
- Price: It is free. One can download it from open source.

3.4. Nmap (Network Mapper)

Used in port scanning, one of the phases in ethical hacking, is the finest hacking software ever. Primarily a command-line tool, it was then developed for operating systems based on Linux or Unix, and the windows version of Nmap is now available.

Nmap is basically a network security mapper capable of discovering services and hosts on a network, thereby creating a network map. This software offers several features that help in probing computer networks, host discovery as well as detection of operating systems. Being script extensible it provides advanced vulnerability detection and can also adapt to network conditions such as congestion and latency while scanning. These are the some tools and their features of ethical hacking.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

IV.TYPES OF CYBER HACKER

4.1 White Hat Hackers

White hat hackers are types of hackers who're professionals with expertise in cybersecurity. They are authorized or certified to hack the systems. These White Hat Hackers 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 the organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. White hat hackers work per the rules and regulations the government sets. White hat hackers are also known as ethical hackers.

Motives & Aims: The goals of these types of hackers are helping businesses and an appetite for detecting gaps in networks' security. They aim to protect and assist companies in the ongoing battle against cyber threats. A White Hat hacker is any individual who will help protect the company from raising cyber crimes. They help enterprises create defences, detect vulnerabilities, and solve them before other cybercriminals can find them.

4.2 Black Hat Hackers

Black hat hackers are also 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 these types of hackers use 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

Motives & Aims: To hack into organizations' networks and steal bank data, funds or sensitive information. Normally, they use the stolen resources to profit themselves, sell them on the black market or harass their target company

4.3 Script Kiddies

It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateurs types of 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 the attention of their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.

Motives & Aims: One standard Kiddie Script attack is a DoS (Denial of Service) or DDoS attack (Distributed Denial of Service). This simply means that an IP address is flooded with too much excessive traffic that it collapses. Consider several Black Friday shopping websites, for instance. It creates confusion and prevents someone else uses the service.

4.4. Green Hat Hackers

Green hat hackers are types of hackers who learn the ropes of hacking. They 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.

4.5. Red Hat Hackers

Red Hat Hackers are synonymous with Eagle-Eyed Hackers. They are the types of hackers who're similar to white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is that the process of hacking through intention remains the same. Red hat hackers are quite ruthless when dealing with black hat hackers or counteracting malware. The red hat hackers continue to attack and may end up having to replace the entire system setup. Above are 5 types of hackers broadly referred to in the cybersecurity world.

V. CONCLUSION

The security problems will endure as long as constructor remain committed to present systems architectures, generated without some security requirements. Proper security will not be a fact as long as there is funding for ad-hoc & security solutions for these insufficient designs & as long as the delusory results of intrusion team are recognized as evidence of computer systems security. Regular monitoring, attentive detection of intrusion, good systems management practice &

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

awareness of computer security that all essential components of the security effort of an organization. In any of these places, a single failure could well expose a company to cyber vandalism, loss of revenue, humiliation or even worse. Each new technology has its advantages & risks.

REFERENCES

[1] G. R. Lucas, "Cyber warfare," in The Ashgate Research Companion to Military Ethics, 2016.
[2] P. Engebretson, "Reconnaissance," in The Basics of Hacking and Penetration Testing, 2011.
[3] Ehacking, "Scanning and Enumeration- Second Step of Ethical Hacking," ehacking, 2011.
[4] R. Baloch, Ethical Hacking and Penetration Testing Guide. 2017.