WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

How Can Ethical Hacking Can Protect Organization from Greater Threat

Madhukara S.[1], Pradeep J.[2]

[1]Assistant Professor, [2]Student, Dept. of ECE, SJCIT, Chikkaballapur, India,

ABSTRACT

Hackers have been broken into websites of credit card companies, online retailers and even government and military sites holding most crucial and confidential information with them. To recall, an examination of 250,000 diplomatic cables exposed by WikiLeaks by the U.S. newspaper proved that high-standard Chinese civilians and military officials assisted fruitful hacking attacks aimed at gaining a broad range of U.S. government and military information. In a sign, cyber security must be aided with quality advancements. In a row, two more U.S. companies, McDonalds Corp. and Walgreen Co., revealed that they had been compromised along with U.S. media company, Gawker. Much of this hacked information was supposed to be provided by end customers when they used to sign up for online subscriptions. The main objective of this paper is to cover core elements of information security, security challenges, effects of breaching and lastly emphasis on why ethical hacking is needed, what qualities must an ethical hacker posses even with its scope and limitations

INTRODUCTION

Universities and other higher education institutions represent a tempting target for hackers and are under an increasing risk of hacking attacks. Educational institutions maintain databases of personal information about faculty, staff, and students. Such databases represent a tempting target for cybercriminals who sell stolen personal information on the black market to other criminals for profit (Burrell, n.d.). Cybercriminals may be looking to steal university research. Ethical hacking is an important information security risk management strategy higher education institutions and businesses use against the growing threat of hacking attacks.Most information security management books on ethical hacking focused on its technical application in information security risk assessment practices. The broader societal context of ethical hacking implementation was less considered. Non-technical challenges involved in the implementation of ethical hacking within higher education organizations intersect several perspectives. The study focused on effective ethical hacking implementation in an higher education organization understood within the broader societal/industry context—within the ethical, social/sociocultural, and technical/technological context.This is the technique which is being used by number of professionals to do hacking but that is not illegal it is rather ethical.

BLOCKDIAGRAM

Fig: Ethical hacking process

Reconnaissance: It refers to gather as more information as we can about target in prior to perform an attack. It can be further classified into Active and Passive. Former involves information gathering with direct interaction like social engineering and the later without any direct interaction by searching news release or public records.

Scanning: It refers to scan for all the open as well as closed ports and even for the known vulnerabilities on the target machine.

Gaining Control: It can be gained at OS level, system level or even network level. From normal access hacker can even proceed with privilege escalation. It often includes password cracking, buffer overflows, DoS attack etc.

Maintaining Access: It is where hacker strives to retain its control over target with backdoors, root kits or Trojans. Compromised machines can even be used as Bots and Zombies for further attacks.

Log clearing: It is also known as Daisy Chaining. To avoid being exposed or caught, a good hacker will leave no impressions of his presence. So he attempts to overwrite the system and application logs.

WHAT DOES AN ETHICAL HACKER DO

An ethical hacker is a person doing ethical hacking that is he is a security personal who tries to penetrate in to a network to find if there is some vulnerability in the system. An ethical hacker will always have the permission to enter into the target network. An ethical hacker will first think with a mindset of a hacker who tries to get in to the system.

REQUIRED SKILLS OF AN ETHICAL HACKER

- Microsoft: skills in operation, configuration and management.
- Microsoft: skills in operation, configuration and management.
- Firewalls: configurations, and operation of intrusion detection systems.

SECURITY HURDELS

Once when we start building notions about providing security to a standalone system or an organization, security risk factor must be taken in account. The main challenges come in way of security:

- Will it be according to government rules and regulations? By applying any of the planned strategy, no rule violation must be happened.
- What will be the consequence of security violation on an organization base as well as its market value?
- It is damn difficult to provide centralized security in an distributed environment.
- How will it be possible to secure the hugely overspread network applications?

IMPACT OF ETHICAL HACKING

World is at an threatened edge built up by cyber crimes or deeds by script kiddies [4]. Hacking consequences are much more horrible than ever thought of. It can damage company goodwill and most importantly its trust from customers. The major impacts that are actually a negative impact are

- Damage to confidentiality, availability and integrity of the data.
- Attackers may leverage a compromised machine as ‘bots’ and ‘zombies’.
- Hackers can leave a backdoor open in targeted machines to exploit them whenever desired.
- Theft of e-mail ID for spamming.

WHO THE HACKER IS

Several definitions for hackers are given below:

- Hackers are capable individuals with extreme computer knowledge about software as well as hardware.
- For some notorious individuals, hacking is just an hobby to test their ability by themselves.
- Some do it with well planned strategy to complete their wrong intentions.

To better understand them, they are further classified into four categories. They are:

- Black Hat Hacker: Their deeds results into destructive activities. They are also known as crackers.
- White Hat Hacker: They are professional hackers. They use their skill for defensive purpose in purely an ethical way.
- Suicide Hacker: They are such notorious individuals who aim to bring down critical structure and even do not care about facing punishment.
- Gray Hat Hacker: They are the hackers who are mixture of both white hat and black hat hackers i.e. works both offensively and defensively [5].

WHY ETHICAL HACKING IS NEEDED

So now what is the need of an ethical hacking? Well, if we start thinking like a thief, we can better know about the weak locks and how to break them. Means, until and unless we do not know about the vulnerability or flaws in our system or an organization, how will we find better and yet effective patches for them. Hackers just have in their mind “Hack Value” that refers to what they have gained during their practice.

- There are convincing reasons I have found out for the mere need of ethical hacking.
- To pre-discover the loopholes or flaws in a system before the hackers do.
- As one cannot rely just only on vulnerability testing and security audits.
- Implementing a Defense in Depth notion by performing extreme penetration testing.

ADVANTAGES

- Provides security to banking and financial establishments
- Prevents website defacements
- An evolving technique
- Fighting against terrorism and national security breaches
- Having a computer system that prevents malicious hackers from gaining access

APPLICATIONS

- A Hacking application that is open-source and free.
- LiveAction automates the gathering of network data required to assess security alarms quickly
- Multiple big companies use this globally - recognized ethical hacking application.
- Real-time threat detection and alert systems.
- Scans systems for new vulnerabilities in real-time.
- Network enumeration and mapping.
- It gives organizations control over scans by delivering pertinent information and data visualization in real-time

SCOPE AND LIMITATION

Even with wide range of applications and its necessity, an ethical hacking has its own scope as well as limitation. Ethical hacking can be emerged as primary component for risk assessment, security audit, better practices and governance. It can be leveraged more to determine risks and also dropping a spotlight on their respective remedial actions. However, less knowledge of this task in businesses why should they hire an outside vendor to look after their security? An ethical hacker can only guide the organization to understand its security strategy but it is solely up to an organization to place the right guards on web.

FUTURE SCOPE

The Ethical Hacking course deals with subjects such as cyber ethics hacking, information gathering, google hacking databases, penetrations testing, software technology, countermeasures, etc. This course is mainly pursued by the candidates who are interested in cybersecurity and have an interest towards computer systems and networks.

CONCLUSION

To conclude all the aspects of hacking as well as an ethical hacking, it is now must for all to hire methodology of an ethical hacking to avoid hacking consequences. In prior, to expose all loopholes in a system to broad network, it becomes crucial.

REFERNCES

1. Puspendra Kumar and RK Pateriya. A survey on sql injection attacks, detection and prevention techniques. In Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on, pages 1–5. IEEE, 2012.
2. Dimitris Mitropoulos and DiomidisSpinellis. Fatal injection: a survey of modern code injection attack countermeasures. PeerJ Computer Science, 3:e136, 2017.
3. Saman TaghaviZargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. IEEE communications surveys & tutorials, 15(4):2046–2069, 2013.
4. Bhupendra Singh Thakur and Sapna Chaudhary. Content sniffing attack detection in client and server side: A survey. International Journal of Advanced Computer Research, 3(2):7, 2013.
5. Michael Kassner. Ethical hackers' top motivation isn't money, according to hackerone - techrepublic. https://www.techrepublic.com/article/ethical-hackers-top-motivation-isnt-money-according-to-hackerone/, February 2018.
6. Aaron Yi Ding, Gianluca Limon De Jesus, and Marijn Janssen. Ethical hacking for boosting iot vulnerability management: a first look into bug bounty programs and responsible disclosure. In Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing, pages 49–55. ACM, 2019.
7. Steve Mansfield-Devine. Hacktivism: assessing the damage. Network Security, 2011(8):5–13, 2011. 36 A PREPRINT - MARCH 30, 2021 .
8. Martin Libicki. The coming of cyber espionage norms. In 2017 9th International Conference on Cyber Conflict (CyCon), pages 1–17. IEEE, 2017.
9. Emma Chanlett-Avery, John W Rollins, Liana W Rosen, and Catherine A Theohary. North Korean Cyber Capabilities: In Brief. Congressional Research Service, 2017.
10. Malcolm Nance and Christopher Sampson. Hacking ISIS: how to destroy the cyber jihad. Simon and Schuster, 2017. 37 A PREPRINT - MARCH 30, 2021
11. Sonali Patil, Ankur Jangra, Mandar Bhale, Akshay Raina, and Pratik Kulkarni. Ethical hacking: The need for cyber security. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pages 1602–1606. IEEE, 2017.
12. David H McElreath, Daniel Adrian Doss, Leisa McElreath, Ashley Lindsley, Glenna Lusk, Joseph Skinner, and Ashley Wellman. The communicating and marketing of radicalism: A case study of isis and cyber recruitment. International Journal of Cyber Warfare and Terrorism (IJCWT), 8(3):26–45, 2018.