Need of Ethical Hacking in Online World

Monika Pangaria[1], Vivek Shrivastava[2]

[1]M. Tech (I.T.) Student, I.T.M. College, Bhilwara, Rajasthan, India
[2]Assistant Professor (I.T.), I.T.M. College, Bhilwara, Rajasthan, India

monika.pangaria@gmail.com
viveks2001@gmail.com

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.***

Keywords: Hacking, Hacker, Ethical Hacking, Information Security, Hack value, Daisy Chaining.

1. Survey on Cyber Security

Cyber Security, the most talked about topic and the most concerned area in today's online world [3]. The numerous numbers of complaints were received about hacking acts. People around there, using internet medium for most of their sort of stuff including business, communication, fun have a fear of being observed or hacked by malicious users. Here, I got a report from government website that is actually "Internet Crime Current Report". The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

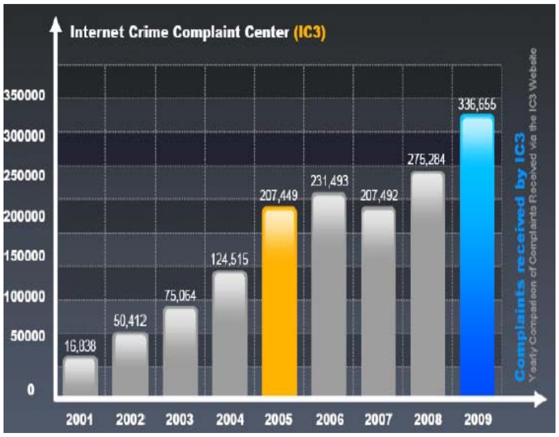

Figure 1: IC3 Report [1]

It is but obvious that year by year, numbers of complaints received are increasing at an exponential rate. Along with complaints magnitude, I have collected a data that signifies purpose of hacking [2]. Like hacking is done for stealing login credentials, brute force attacks, SQL Injection attacks, back dooring, foot printing, fingerprinting, cross side scripting, call sms forging, phishing attacks. All these stuff are used to gain hack values.

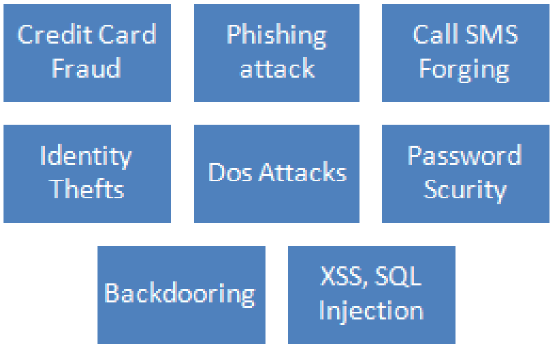

Figure 2: Ways to gain Hack Values

Further proceeding with the market survey, I tried to find out what type of data is generally stolen. And result was payment card information stealth was at the top. To complete the queue, non-payment card information, intellectual information and sensitive information are after payment card information.

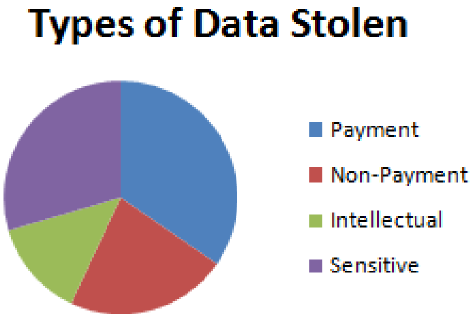

Figure 3: Types of data stolen

2. Core of Data Security

Information Security lays in a principle of "CIA" that confidentiality, Integrity and Availability.

- Confidentiality: It ensures information will be accessible to only authorized user.

- Integrity: It ensures from start to an end means from source to destination, no further changes has occurred in data in middle of transmission. Means data has retained its integrity throughout the route.
- Availability: It ensures the presence of systems given charge of handling certain tasks like delivery, storage and processing.

3. Security Hurdles

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?

4. Impact of 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.
- Theft of passwords for accessing others bank accounts or even lead to illegal fund transfer.
- Loss to social security.

5. 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].

Hacking can be divided into many phases:

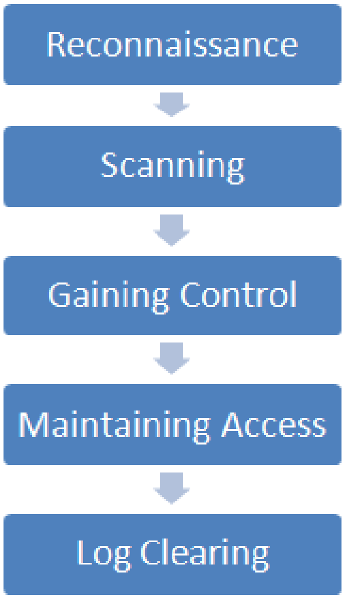

Figure 4: Hacking Process

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.

6. Why Ethical Hacking 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.
- To counter the attacks by anticipating techniques.

7. 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.

8. Future Scope and 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 a broad network, it becomes crucial.

Keeping in mind the security challenges, one must strive for a strategy that can be proven fruitful in all cases whether it is related to distributed environment, considering risk factors of implementing this method as well as a condition where one patch for present system can cause vulnerability in future changes.

References

[1] Internet Crime Complaint Centre link: www.ic3.gov

[2] Liu, Bingchang; Shi, Liang; Cai, Zhuhua; Li, Min; "Software vulnerability Discovery Techniques: A Survey" IEEE Conference Publication, DOI: 10.1109/MINES.2012.202, Page(s) 152-156, 2012

[3] Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI: 10.1147/sj.403.0769, Page(s): 769-780

[4] Bradley, Rubin "Computer Security Education and Research: Handle with care" IEEE Conference Publication, DOI: 10.1109/MSP.2006.146, Page(s): 56-59

[5] Wilbanks "When Black Hats are really white" IEEE Conference Publication, DOI: 10.1109/MITP.2008.146, Page(s): 64