International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 02 | Feb -2020 ISSN: 2582-3930

Ethical Hacking And Security Process

Roshan Roy D Souza, Namratha K H, Divya Jyothi
Dept. of Computer Science
St. Philomena's college Mysore

Security

The word itself defines that some data is under threat or in danger it needs to be protected from the theft or Some danger Security, in IT (Information Technology) , is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services,it is the state of being free from danger or threat.

What is Hacking

Hacking has been a hot topic since the 1960s. It is the process we find the loop holes in the system and get into the system and find the data required or to stay in the system .The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" originated. 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. A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Types of Hacking

- Ethical Hacking
- Unethical Hacking

Ethical Hacking

When the hacker helps organizations or individuals with finding loopholes and fixing them with their permission is referred to as ethical hacking.

Unethical Hacking

When a hacker uses his knowledge to steal from or cause damage to other people , it's known as an unethical hacker.

Let me give an example considering you and your family planned for a trip. And you locked the house and went for the trip you locked the door and went now the house is empty a thief comes to your house checks your house surrounding tries to figure out in which way to enter into the house. This process is called vulnerability checking. Similarly, hackers also try to enter into your system. The thief finds a glass window which is not protected he enters into to the house after he enter to the house he checks for the valuable item he finds the safe which was easy to guess and opens the safe by trying all possible common passwords and he takes the valuable item and escapes from the same path he entered latter you and your family comes back to home and find out that your house has been under theft then you call up security experts these are also called as ethical hackers with your permission they use the same tricks used by the hacker and find out the vulnerabilities. And give you a detailed report how to secure your system

Here the vulnerability were

- The Glass Window did not have protection.
- Safe was easy to find.
- Password for the locker was easy to guess.

Ethical hackers also do the same process to safeguard your system. It can be web application , app, network passwords and so on with the permission of the organisation they find all the loopholes in the system and helps the organisation to safeguard the system.

Types of hackers

- White hat hackers(ethical hackers)
- Black hat hackers (unethical hackers)
- Gray hat hackers : they are the combination of both white hat hacking and black hat hacking

Steps followed by Black hat hacker

1. Collect information : here he collects information about the target and the system .
2. Finds weak spot to get into the system
3. Ties to stay inside the system as long as possible
4. Clear tracks :here he clears all the tracks about the hacker

Steps followed by Ethical Hacker

1. Legal Documentation : they sign a document such that organisation accepts them to hack into the system ie: MOU ,NDA…
2. Scope Assessment : all the possibilities and scope of system is calculated
3. Information Assessment
4. Vulnerability Assessment
5. Penetration Testing : process where security expert tries all the possible ways to get into the system
6. Gaining Access
7. Privilege Escalation
8. Report Generation: process where all the vulnerability will be listed and security measures will be given
9. Patch Assistance : it is the process where security experts helps the organisation to fix the vulnerability
10. Revalidations : it is the process where the security experts check the system by repeating the hacking process to find out whether the patches are fixed properly in the system.

Methods of hacking

Reconnaissance:Information Gathering and getting to know the target systems is the first process in ethical hacking (footprinting, Scanning ,Enumeration) are the techniques used to gather the information about the system.

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

Sniffing: It is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and getting to know about the conversation. It is also called wiretapping applied to computer networks. There are also online sniffing tools. Email traffic

- Email traffic
- FTP passwords
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

Are the places where the sniffing is done to know the crucial data of the system. To gain access to the system.

ARP Spoofing: Address Resolution Protocol (ARP) Spoofing is the process where the attacker uses man in middle attack where he has access to all the packets between two connections.

Exploitation: Exploitation is a piece of software or script which can allow hackers to take control over a system, exploiting its vulnerabilities. Hackers normally use vulnerability scanners like Nessus, Nexpose, OpenVAS, etc. to find these vulnerabilities.
The exploitation tools are Metasploit ,Exploit Database,Common Vulnerabilities and Exposures,National Vulnerability Database
Torjens: torgens are the simple program which is replicant of actual programs using tokens we can create backdoors in the system to gain access to the system and steal the crucial data of the system.

TCP/IP and Email Hijacking : In tcp/ip hijacking the the hacker uses the tools to find the ip and gains access to the data.
In Email hijacking the hacker uses phishing tools where he uses social engineering where he sends the emails offering discounts and payment

to get the crucial information and perform payments to hacker account using phishing technique tools : Shijack,Hunt…

Password Hacking : Password hacking is what most commonly done by the hackers and most of us are interested in the different ways to hack a password is by Dictionary attack, Bruteforce attack , sniper attack fairytale attack,rainbow attack.

Cross-site scripting (XSS): it is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser. The attacker does not directly target his victim. Instead, he exploits a vulnerability in a website that the victim visits, in order to get the website to deliver the malicious JavaScript for him. To the victim's browser, the malicious JavaScript appears to be a legitimate part of the website, and the website has thus acted as an unintentional accomplice to the attacker. These attacks can be carried out using HTML, JavaScript, VBScript, ActiveX, Flash, but the most used XSS is malicious JavaScript.

Sql injection : it is where the application is tested with a set of sql command where it makes the application work differently from the actual what it had to perform.

Security Processes

1. Keep the system up to date updated
2. Do Not note down password anywhere
3. Frequently change passwords
4. Use vpn to secure your original ip from displaying
5. Never open spam emails as it may contain trojan.
6. Use security experts suggestions to secure your system.
7. Never tell your ip to random people or over the internet.
8. Behavior of the phishing mails.
9. Update the tools used in websites.
10. Use genuine fire walls over the network.

Conclusion

As the information technologies (IT) is advancing even the threat to the data is also getting more so we need to ensure that the data to be safer therefor we have to take the suggestion of the security experts to ensure our data to be safe thus by knowing some of the methods hackers use we can at least be free from the some of the methods that hackers use like phishing SMiShing .. thus the awareness of the hacking helps us to safeguard our data at least to some extent by following the security processes head in the journal.

Reference

https://internshala.com/

https://www.udemy.com/

www.tutorialspoint.com/ethical_hacking

https://www.wikipedia.org/