ETHICAL HACKING

Iqbal Singh
Assistant Professor
Computer Science
A.S.B.A.S.J.S.M College Bela, Ropar, India

Abstract: During rise of internet, security has become main issue for internet users. Hacking is big problem faced by internet users, government organizations and companies. Hacking includes steal information, breaking authorization, read others e-mails and damage the network. Ethical hacking can help from hacking. This paper describes ethical hacking, types of hackers, hacking tools and techniques, process of network hacking and website hacking. This paper also focuses on the Vulnerabilities of network and websites which can be removed by ethical hacking.

Keywords: hacking, ethical hacking, hacking tools, hacking the network, hacking websites.

1. INTRODUCTION

Internet is widely used by people due to E-commerce, social networking, communication and transferring information. As rise in growth of internet users, network security issues arise. Because of sensitive and confidential data, security is major issue in the present era. Companies and governments are worried about the illegal access to their sensitive and confidential data. A computer hacker is one who is curious about the working of computers and software. Hackers get access to your bank account and steal money, crack passwords, and try to look into private life of internet users because they can steal private files. So a person is a hacker whether they are bypassing computer's security to files or doing it on someone else's computer without the permission of the owner.

2. ETHICAL HACKING

In terms of computer security, an ethical hacker is penetration tester, someone who tries to find vulnerabilities in a system in order to fix them, rather than to profit from exploiting them.

2.1 TYPES OF HACKERS

2.1.1 White hat hackers

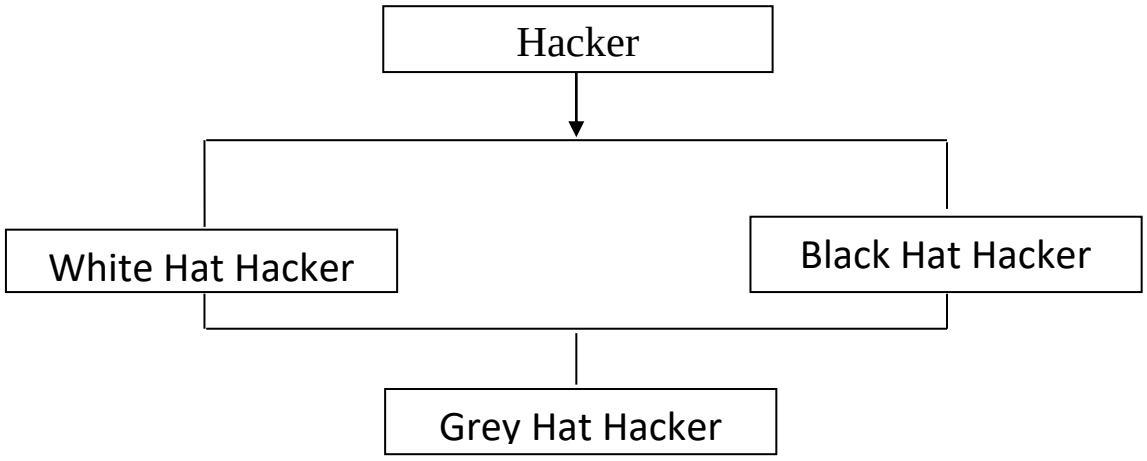
White hat hackers are those who search for exploits and vulnerabilities in order to fix them, and stop others from being able to hack the system. They do not their skills in order to harm others or for illegal activities. They are security experts.

2.1.2 Black hat hackers

Black hat hackers those who hack into systems for malicious reasons, in order to damage and deface websites, steal passwords, or credit cards. They may do so because of profit, or out of pure malice.

2.1.3 Grey hat hackers

These type of hackers are motivated by profit as well as ethical reasons. Grey hat hackers are those who falls in this zone of ambivalent motives. They cannot clearly be placed into the white or black hat categories.



3. NETWORK HACKING

To hack the system there is no need to physical access to it and no information of that system is on hacker's computer. The information is on remote computer in your local network, or on the internet. To hack the remote computer Hackers, need enough all information about the victim. Hacker can begin to research the vulnerabilities in the system and use them to construct an attack. As an ethical hacker, it is important to keep note of the vulnerabilities exploited in each step of way, and patch them.

3.1 PHASES IN NETWORK HACKING

3.1.1 Footprints

It is creation of a profile for the target containing all information about the target's level of security. The target might be on local network or on internet, however in both cases, hacker try to get as much information about the system as hacker can.

Hacker need to find out the IP address or the range of IP addresses which belong to target, the domain names, the subnet, the running on target system. The goal should be to obtain as much information as possible that any malicious hacker would be able to obtain and use for advantages, once hacker have this information, Hacker know how exposed the systems are to harm, and can the system for test its security.

3.1.1.1 For gathering information there are some techniques and tools available

1. Site digger

Site Digger searches Google's cache to look for vulnerabilities, errors, proprietary information, and interesting security nuggets on web sites.

2.Gooscan

It is a tool that automates queries against Google search appliances. These particular queries are designed to find potential vulnerabilities on web pages.

3. Traceroute:

In computing, traceroute and tracert are computer network diagnostic commands for information about the hops on the way to accessing a domain and with this path revealed, hacker could have a better idea of how system connected to a.

4. Search engines

Search engines may help to find about the websites. Few searches can reveal a lot of information which people would rather have kept private. Many services or applications running on the target system might provide remote administration interfaces that might not be secured

3.1.2 Scanning

Gathering information provides us model of network and the routes of network. Scanning is more intrusive and involves actually interacting with the target systems. In this step hacker follow the gathered information and do some actual testing. Now hacker have an idea of the scope of the network that hacker need to infiltrate, hacker start poking and prodding at the computers on the network looking for systems that are vulnerable.

3.1.2.1 Following are the tools for scanning

1.Nmap

Nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine. This tool is a command-line utility that can do everything from a simple ping sweep to a fully comprehensive scan of all open ports on a system.

2. Netcat

Netcat is a networking tool for reading from and writing to network connections using TCP or UDP. The command is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.

3. Superscan

SuperScan is a connect-based port scanning software designed to detect open TCP and UDP ports on a target computer, determine which services are running on those ports.

3.1.3 Enumeration

In first step hacker have minimal interaction with target system, but instead relied on data about the target system available across the internet. In the Scanning stage hacker actually pinged and mapped the exposed the areas of the network. Now hacker actually actively connects to the system, in order to gain information about the services hacker is going to exploit. While hacker is certainly getting more intrusive, hacker have not done any hacking yet. In this step hacker gain the application name, developer and the version number all useful information for hacker. Information such as usernames, machine name, share paths etc are collected in this phase's enumeration provides different services which give information. To secure the system from enumeration, one of the most important rule is to shut down any unnecessary services, so that it become difficult for hacker to gain information about application version number which can be used to find exploit for the system.

3.1.4 Penetration

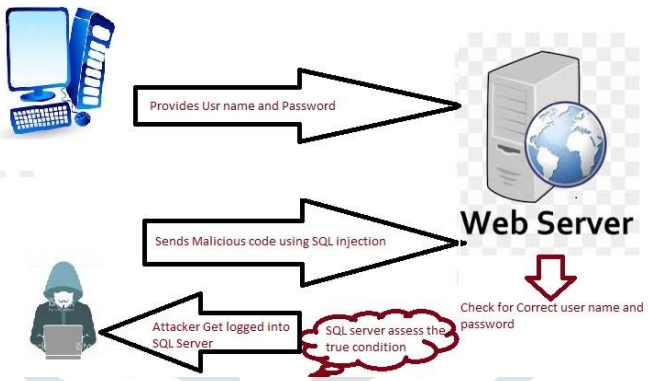
Finally, Hacker reached at actual hacking act. This step involves discovering and exploiting flaws in the applications running on the remote computer. Online database of application exploits is available so that one hacker has information the particular version of remote service, Hacker can simply look up application in online database, and will get a list of exploits for that version of application. A popular example of such a website is www.milwOrm.com which is online searchable database.

4. HACKING THE WEB APPLICATION

In this section we will talk about the vulnerabilities of web applications and how they can be exploited.

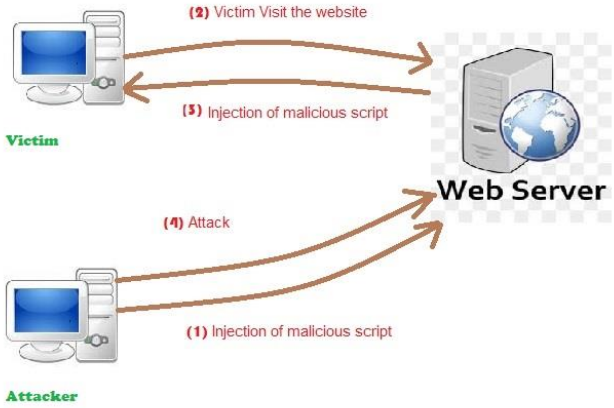
4.1 INJECTION

Injection flaws, such as SQL, OS and LDAP injection, occur when entrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. This means in any application which processes data supplied by user in an interpreter, care must be taken to ensure that an attacker cannot trick the interpreter into running any code they want.



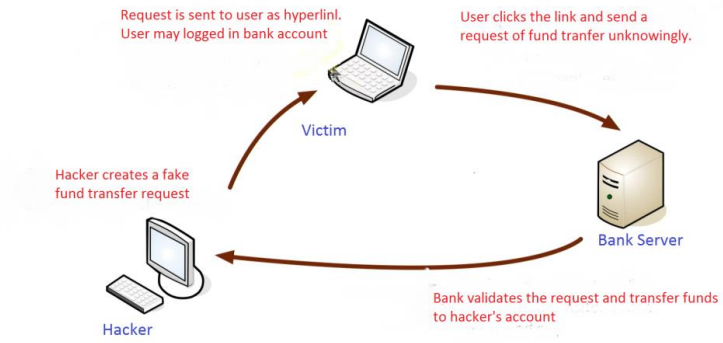
4.2 CROSS SITE SCRIPTING

Cross site scripting flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. XSS flaws occur due to improper sanitization of untrusted data. Untrusted data is any kind of data which does not originate from server. But is provided in the URL and can be modified by end user/attacker. An attacker utilized flaws in the coding of the application in order to inject JavaScript code into web page which can be used for malicious purposes. Any part of an application where any input from URL request is somehow being output in the HTML could be vulnerable to such an attack.



4.3 CROSS SITE REQUEST FORGERY ATTACK

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim. For most web attacks, its authentication is important. The attacker must disguise the attack as if it is an authenticated/ authorized request. The geniuses of the attacks make it difficult to detect and block.



5. CONCLUSION

The web has never been a safe place, but today with the proliferation of new technologies and web development concepts, hackers have an even greater surface to attack. no one can ever be fully secure, there are some very smart hackers out there, and many of them are responsible for discovering these exploits in the first place. Technology is moving at fast pace, and with increased profitability in the industry, it is inevitable that a few bad elements will try to compromise the systems to make money. This is why we need ethical hackers. They are still hackers but they do it to help the systems and networks more secure against attack.

References:

1. https://hackaday.com
2. https://www.hackthissite.org
3. https://news.hitb.org
4. https://www.hacking-tutorial.com
5. https://www.eccouncil.org
6. https://www.greycampus.com/opencampus/ethical-hacking/what-is-ethical-hacking
7. https://www.eccouncil.org/ethical-hacking
8. https://www.udemy.com/topic/ethical-hacking