International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4584–4588

Ethical Hacking Techniques, Tools And Various Attack.

Jai Parmar[1] and Shaikh Mohammad Bilal N[2]
[1]*Department of Computer Science*
K.J. Somaiya College of Science and Commerce
[2] *Assistant Professor Department of Computer Science*
K.J. Somaiya College of Science and Commerce
[1]*jai.parmar@somaiya.edu* , [2] *mohammadbilal@somaiya.edu*

Abstract

Ethical hacking also known as penetration testing, has become a major concern for businesses and governments. Companies are worried about the possibility of being "hacked" and potential customers are worried about maintaining control of personal information. This paper describes ethical hackers: their skills, various tools, various attacks and how they go about helping their customers find and plug up security holes. This is a process with lots of challenges.

Keywords: *– Hacking Techniques, hackers approach, call spoofing attack, brute force attack, Bomber, pen testing, MetaSploit*

1. Introduction

There are different terms for word "hacker" in IT industry today. With the growth of Internet, security is the biggest concern for both business and government bodies. Everyone wants to use Internet for E-commerce, Information distribution and also have access to other luxuries and necessities, but the biggest concern is security about their personal information, bank details, home addresses, and other personal details. [1] This is how the term Ethical Hacking came into existence the organizations and other government bodies, realized the one of the best ways to avoid intruders and other possible threats, Hackers would break into their system, or database, but they would neither damage anything or manipulate their data nor steal them. Instead they would evaluate the target and report back the owner with the vulnerabilities they found and instructions about patching those vulnerabilities. Hence those hackers were termed "Ethical Hackers". Before any Ethical hacker works a written contract is signed by the owner where those Ethical Hackers has approved the permission to get into their systems and find them vulnerabilities. There are mainly three types of hackers

- WHITE HAT
- BLACK HAT
- GREY HAT

White hat hackers are the one who won't use their skills for their benefits, unless and until someone gives them the contract to find the vulnerabilities in their corresponding systems or database.

Black hat hackers are the actual intruders with their malicious intensions, Ethical hackers are hired to provide protection from black hat hackers. The important things they try to hide is their actual identity.

As both black and white color mixes and form grey here it's the same concept Grey hat hackers are the one with malicious intentions but also they will be providing security, but once they are protecting a system they don't try to manipulate it.

2. Techniques

Techniques of ethical hacking:

- Information gathering

ISSN: 2233-7857 IJFGCN

- Vulnerability Scanning
- Exploitation
- Test Analysis

Information gathering:

In this step, the tester collects as much information about the target. The deeper the testers understanding, penetration testing will have more success rate [8]. The tester gathers all the information although it would be useless since no one knows the outcome what information will be needed. This step can be carried out by different public tools such as search engines, using scanners, sending simple HTTP requests or just by using the application.

Vulnerability Analysis:

The testers can conduct testing on configuration management, business logic, authentication, session management, authorization, data validation, denial of service, and web services [8]. Using the knowledge collected from the information gathering step, the testers then scan the vulnerabilities that exist in the application. In this step vulnerabilities, authentication mechanism vulnerabilities, input-based vulnerabilities and function specific vulnerabilities are examined.

Exploitation:

After the vulnerability analysis step, the testers will have a good idea of the areas that will be targeted for exploits. This step is carried out using various tools and methods [10]. Test Analysis Phase:

This phase is the last phase where the results are decided. It's the interface of result and the target. The vulnerabilities found in the system is reported back to the owner or the hirer. Also the patches are to provided form those vulnerabilities

3. APPROACH

Basic approach of the owners is to get the evaluation form the ethical hackers, whether the required security is provided or not that's the major concern. An ethical hacker's evaluation of a system's security seeks answers to three basic questions: What can an intruder see on the target systems? What can an intruder do with that information?

- Does anyone at the target notice the intruder's attempts or successes?

While the first and second of these are clearly important, the third is even more important: If the owners or operators of the target systems do not notice when someone is trying to break in, the intruders can, and will, spend weeks or months trying and will usually eventually succeed. Ethical hacking is a dynamic process Ethical hacking is a dynamic process since running through the penetration test once gives the current set of security issues which subject to change over time therefore penetration testing must be continuous to ensure that system

movements and installation of new applications do not introduce new vulnerabilities in the system.

Areas to be tested:

- Network Securities.
- Firewall and device securities.
- Application servers. Wireless securitise.

Multi layered assessment:

Various areas of security are evaluated using a multi-layered approach.

- Each area of security defines how the target will be assessed.
- Once a vulnerability is protected that particular layer may be protected but the other layers may also have vulnerabilities.

ISSN: 2233-7857 IJFGCN

For example: In an application if the login page is patched that doesn't mean the application is safe. There may be me more vulnerabilities in the application.

Ethical Hackers are hired by companies to hack their own respective company and be able to identify any loopholes where an ill-intentioned hacker could create damage so that the company can buff its security and cover the cracks [9]. They use their skills to make the internet world of a company a fool proof and safe place for both the owners and clients. Ethical Hacking also known as Internet Security is very different from traditional Security. Internet security is more on a proactive basis as compared to traditional security. While traditional security is based on catching the criminals, internet security has Ethical Hackers that try to hack into company/organization before an 'attack' so they are able to find any weak links.

4. VARIOUS ATTACKS AND TOOLS

Automatic tools have changed the world of penetration testing/ethical hacking, IT security researcher has been developed and currently developing different tools to make the test fast, reliable and easier task. Without automatic tools, the hacking process is slow and time consuming

Nmap/Zen map: This tool is mostly used to gather the information of a particular website, a particular ip-address. Nmap is a best tool ever that are used in the second phase of ethical hacking means port scanning, Nmap was originally command line tool that has been developed for only Unix/Linux based operating system but now its windows version is also available and ease to use. It is use for Operating system fingerprinting too. **TOR Browser:** Tor stands for Total onion route, Task done on Google search engine are easily traceable, tor browser is a free and open source software for enabling anonymous communication. Tor enables its users to surf the Internet, chat and send instant messages anonymously, and is used by a wide variety of people for both good and bad purposes.

The usage of Dark web is mainly done on this browser Tor is not meant to completely solve the issue of anonymity on the web. Tor is not designed to completely erase tracks but instead to reduce the likelihood for sites to trace actions and data back to the user. Tor is also used for illegal activities. Here onion is the metaphor as it encrypts the information in a multi layered manner. And provide user anonymity in a network location.

MetaSploit:

An exploit executes a sequence of commands that target a specific vulnerability found in a system or application to provide the attacker with access to the system. Exploits include buffer overflow, code injection, and web application exploits. This is the most used tool by attackers [3]. You've scanned your targets and identified potential vulnerabilities. The next step is to determine whether or not those vulnerabilities present a real risk.

Metasploit contain a database that has a list of available exploit and it is easy to use and best tool for doing penetration testing, Metasploit framework is a sub project and is use to execute exploit code against a machine and get the desire task done.

NETSTUMBLER:

Netstumbler which is also called as network stumbler. It is a windows based tool used for detection of wireless land which is Wi-Fi. The program is commonly used for:

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detecting causes of wireless interference
- Detecting unauthorized access points
- Aiming directional antennas for long-haul WLAN links[2] Call Spoofing Attack: Spoofing is a type of scam in which hackers attempt to obtain someone's personal information by pretending to be a legitimate business, a neighbour, or some other

ISSN: 2233-7857 IJFGCN

innocent party. A call spoofing attack is an attack where the attacker can use any phone number to call anyone. This attack is totally based on VOIP which stands for voice over internet protocol. Tool used for this attack is Zoiper, with proper ip protection layering the attacker is hard to catch. Zoiper is a softphone software. For this attack the attacker crates A-Z sip termination services, this sips are provided by various websites one can either buy it or use it for free for limited time. Website I use is www.compeak.com. [11] Once the sip is created for a particular number then Zoiper is used to make the call and execute the attack. EMAIL/TEXT BOMBER:

In Internet usage, an email/sms bomb is a form of net abuse consisting of sending large volumes of email to an address in an attempt to overflow the mailbox or message box. There are three methods of perpetrating an email bomb: mass mailing, list linking and zip bombing.

- Mass mailing consists of sending numerous duplicate mails to the same email address. These types of mail bombs are simple to design but their extreme simplicity means they can be easily detected by spam filters. Email-bombing using mass mailing is also commonly performed as a DDoS attack
- List linking, also known as "email cluster bomb", means signing a particular email address up to several email list subscriptions. The victim then has to unsubscribe from these unwanted services manually. The attack can be carried out automatically with simple scripts: this is easy, almost impossible to trace back to the perpetrator, and potentially very destructive.
- A ZIP bomb is a variant of mail-bombing. After most commercial mail servers began checking mail with anti-virus software and filtering certain malicious file types, EXE, RAR, Zip, 7-Zip, mail server software was then configured to unpack archives and check their contents as well Some Tools used are Software or websites:

Mail Bomber, https://hackerone.com , BOMBitUP (Mobile apk).

BRUTE FORCE ATTACK:

Brute force attack is attack used to find out the user credentials by trying various possible credentials. Various criteria are

- Guessing the credentials
- Trial and error
- Username list and Password list Tools used: Medusa, John the reaper (Kali Linux), MetaSploit, Air-crack NG.

To execute this attack, it is done in sequential manner Brute Force tool is used to find the username and password, once you have the id password it has to be authenticated whether the credentials are True or False.

To get the list for username and password list a tool name hydra is used in the Terminal of kali Linux. You need to know the webapp is a get or post method.

The command used is:

hydra -l filename.txt –p filename.txt ip address http –get/post

Brute-force attacks can be made less effective by obfuscating the data to be encoded making it more difficult for an attacker to recognize when the code has been cracked or by making the attacker do more work to test each guess. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it. This attack can also be done by using mobile phone application to be used is Termux here the password and username list is required to complete the attack successfully

PENTESTING:

ISSN: 2233-7857 IJFGCN

There are different approaches towards Ethical hackers.

- Remote network: This test simulates an attack across the internet. It can be encountered by border firewall, filtering routes [7].
- Social engineering: This test evaluates the target organization's staff as to whether it would leak information to someone [7]. A typical example of this would be an intruder calling the organization's computer help line and asking for the external telephone numbers of the modem pool. Defending against this kind of attack is the hardest, because people and personalities are involved.
- Remote dialup network: This test simulates an attack against the client's modem. [7]

Reference

1. "Ethical Hacking, January 2015 "
https://www.researchgate.net/publication/271079090_ETHICAL_HACKING_Tools_ Techniques_a nd_Approaches
2. "Tools"http://www.ehacking.net/2011/06/top-6-ethical-hacking-tools.html#sthash.nszGZw4y.dpuf
3. MetaSploit.com
4. "Penetration Testing" http://www.owasp.org/index.php/Web_Application_Penetration_Testing.html
5. http://www.corecom.com/external/livesecurity/pentest.html
6. http://www.networkdefense.com/papers/pentest.html
7. Internet Security Systems, Network and Host-based Vulnerability Assessment
8. http://www.infosecinstitute.com/blog/ethicalhacking_computer_forensics.html
9. http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083715,00.html
10. http://www.owasp.org/index.php/Testing:_Information_Gathering
11. "Call spoofing attack"www.compeek.com

ISSN: 2233-7857 IJFGCN