International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Hacking Vs Ethical Hacking

[1]Kanusu Srinivasa Rao and [2]Ratna Kumari Challa

Asst Professor, Dept of Computer App., Yogi Vemana University, Kadapa, A.P, India

Asst Professor, Dept of Computer Science, JNTUK, Kakinada, A.P, India

***Abstract*— The complexity of security requirements is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities in many ways. A computer adept someone who enjoys working with computers and testing the limits of systems and also suggests someone who breaks into computer network and steals or vandalizes information. A hacker or cracker is someone who accesses a computer system by evading its security system. Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources. It involves modifying system or application features to achieve a goal outside of the creator's original purpose. Ethical Hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security. It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the system security. Most people do not understand the difference between hacking and ethical hacking. These two terms can be differentiated on the basis of the intentions of the people who are performing hacking activity. However, understanding the true intentions of hackers can be quite difficult.**

A hacker is a person who illegally breaks into a system or network without any authorization to destroy, steal sensitive data or perform malicious attacks. Hackers may be motivated by a multitude of reasons: 1) Intelligent individuals with excellent computer skills with the ability to create and explore the computer's software's and hardware. 2) For some hackers, hacking is hobby to see how many computes or networks they can compromise. 3) The intention can either be to gain knowledge or to poke around doing illegal things. 4)Some hacks with malicious intent, such as stealing business data, credit card information, social security numbers, email passwords etc.

In this paper we present how important it is for an organization to keep their information resources secure and safe against various security threats and attacks. We introduce the concept of hacking with different phases and classification of hackers i.e. Black hats, white hats, Gray hats, Suicide hackers, Script kiddies, spy hackers, cyber terrorists, state sponsored hackers. Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities to ensure system security. Ethical hackers help organizations to better understand their security systems and identify the risks, highlight the remedial actions, and also reduce ICT costs by resolving those vulnerabilities. An Ethical hacker possesses platform knowledge, network knowledge, computer expert, security knowledge, and technical knowledge skills. Ethical hacking is a crucial component of a risk assessment, auditing, counter fraud, best practices, and good governance.

Key words: Hacking, Ethical Hacking, cracker, Black hats, white hats, Gray hats, Suicide hackers, Script kiddies, spy hackers, cyber terrorists, state sponsored hackers, Information security.

I. INTRODUCTION

Hacking is the practice of modifying the features of a system, in order to accomplish goal outside of the creator's original purpose. Computer hacking is the practice of modifying computer hardware and Software to accomplish a goal outside of the creator's outside purpose. It is most common among teenagers and young adults.

According to the Symantec 2012 state of information survey, information costs business worldwide $1.1 trillion annually. Every business must provide strong security for its customers; otherwise the business may put its reputation at stake and may even face lawsuits. Attackers use hacking techniques to steal, pilfer, and redistribute intellectual property of business and in turn to make even its reputation.

Once an attacker gains control over the user's system, he or she can access all the files that are stored on the computer, including personal or corporate financial information, credit card numbers, and client or customer data stored on that system. If any such information falls into the wrong hands, it may create chaos in the normal functioning of an organization. Organizations must provide a strong security to its critical information sources containing customer data and its upcoming releases or ideas. If the data is altered or stolen, a company may lose credibility and the trust of its customers. In addition to the potential financial loss that may occur, the loss of information may cause a business to lose a crucial competitive advantage over its rivals. Sometimes attackers use botnets to launch various types of Dos and other web-based attacks. This cause the target business services to go down, which in turn may lead to loss of revenues.

There are many things that businesses can do to protect themselves and their assets. Knowledge is a key component in addressing this issue. Assessment of the risk prevalent in a business and how attacks could potentially affect that business is paramount from a security point of view. One does not have to be a security expert to recognize the damage that can occur when company is victimized by an attacker. By understanding the problem and empowering employees to facilitate protection against attacks, the company would be able to deal with any security issues as they arise.

II. WHO IS HACKERS

A hacker is a person who illegally Brecks into a system or network without any authorization to destroy, steal sensitive data, or perform malicious attacks. Hacker may be motivated by a multitude of reasons. Some of the reasons are intelligent individuals with excellent computer skills, with the ability to create and explore the computer's software and hardware. For some hackers, hacking is a hobby to see how many computers or networks they can compromise. Their intention can either be to gain knowledge or to poke around doing illegal things. Some hack with malicious intent, such as stealing business data, credit card information, social security numbers, email, passwords etc.

III. HACKER CLASSES

Hackers are mainly divided into eight classes. These are Black hats, White hats, Gray Hats, Suicide hackers, Script kiddies, Cyber Terrorists, State Sponsored hackers

Black Hats: These hats are individuals with extraordinary commuting skills, resorting malicious or destructive activities and are also known as crackers. These individuals mostly use their skills for only destructive activities, causing huge losses for companies as well as individuals. They use their skills in finding vulnerabilities in the various networks including defence and government websites, banking and finance, etc. Some do it to cause damage, steal information, destroy data, or earn money easily by hacking IDs of bank customers.

White Hats: These Hats are individuals who possess hacking skills and use them for defensive purposes, they are also known as security analysts. These days, almost every company has security analysts to defind their systems against the malicious attacks. Whitehats help companies secure their networks from outside intruders.

Gray Hats: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats fall between white and black hats. Gray hat might help hackers by finding various vulnerabilities of a system or network and the same time help vendors to improve products(software and hardware) by checking limitations and making them more secure, etc.

Suicide hackers: Suicide hackers are individuals who aim to bring down critical infrastructure for a cause and are not worried about facing 30 years in jail for their actions. Suicide hackers are closely related to suicide bombers, who sacrifice their life for the attack and are not concerned with the consequences of their actions. There has been a rise in cyber terrorism in recent years.

Script kiddies: Script kiddies are the unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They utilize small, easy-to-use programs or scripts as well as distinguished techniques to find and exploit the vulnerabilities of a machine. Script kiddies usually focus on the quantity of attacks rather than the quality of the attacks that they initiate.

Cyber Terrorists: Cyber terrorists could be people, organized groups formed by terrorist's organizations, That have a wide range of skills, motivated by religious or political beliefs, to create fear by large-scale disruption of computer networks. This type of hacker is more dangerious as they can hack not only a website but whole internet zones.

State Sponsored hackers: State Sponsored hackers are individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments.

IV. HACKING PHASE

Hacking cannot be accomplished in a single action. It needs to be done in phases. The information gathered or the privileges gained in one phase can be used in the next phase for advancing the process of hacking. The various phases involved in hacking are

Reconnaissance

Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack. Also in this phase, the attacker draws on competitive intelligence to learn more about the target. This phase may also involve network scanning, either external or internal, without authorization. Could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale. Reconnaissance target range may include the target organization's clients, employees, operations, network, and systems. There are two types first one is active and passive. In Passive reconnaissance involves acquiring information without directly interacting with the target , for example For example, searching public records or news releases. In Active reconnaissance involves interacting with the target directly by any means, for example, telephone calls to the help desk or technical department.

Scanning

Scanning is what an attacker does prior to attacking the network. In scanning, the attacker uses the details gathered during reconnaissance to identify specific vulnerabilities. Scanning can be considered a logical extension (and overlap) of the active reconnaissance. Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance. Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, etc. Attackers extract information such as live machines, port, port status, OS details, device type, system uptime, etc. to launch attack.

Gaining Access

Gaining access is the most important phase of an attack in terms of potential damage. Gaining access refers to the point

where the attacker obtains access to the operating system or applications on the computer or network. The attacker can gain access at the operating system level, application level, or network level. Factors that influence the chances of an attacker gaining access into a target system include the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. The attacker initially tries to gain minimal access to the target system or network. Once he or she gains the access, he or she tries to escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised. Examples include password cracking, buffer overflows, denial of services, session hijacking, etc.

Maintaining Access

Once an attacker gains access to the target system, the attacker can choose to use both the system and its resources and further use the system as a launch pad to scan and exploit other systems, or to keep a low profile and continue exploiting the system. Both these actions can damage the organization. For instance, the attacker can implement a sniffer to capture all network traffic, including telnet and ftp sessions with other systems. Attackers may prevent the system from being owned by other attackers by securing their exclusive access with backdoors, rootkits, or Trojans . Attackers can upload, download, or manipulate data, applications, and configurations on the owned system. Attackers use the compromised system to launch further attacks.

Clearing Tracks

An attacker would like to destroy evidence of his or her presence and activities for various reasons such as maintaining access and evading punitive action. Trojans such as spent cat come in handy for any attacker who wants to destroy the evidence from the log files or replace the system binaries with the same. Once the Trojans are in place, the attacker can be assumed to have gained total control of the system. Rootkits are automated tools that are designed to hide the presence o f the attacker. By executing the script, variety o critical files are replaced with trepanned versions, hiding the attacker in seconds. Covering tracks refers to the activities carried out by an attacker to hide malicious acts. The attacker`s intentions include: continuing access to the victims system, remaining unnoticed and uncaught, deleting evidence that might lead o his prosecution. The attacker overwrites the system, and application logs to avoid suspicion.

V. TYPES OF ATTACKS

There are several ways an attacker can gain access to a system. The attacker must be able to exploit a weakness or vulnerability in a system. Some types of attacks are

Operating system attacks: Attackers search for os vulnerabilities and exploit them to gain access to a network system.

Attacks performed at the os level include:

Exploiting specific network protocol implementations
Attacking built in authentication systems
Breaking file system security
Cracking passwords and encryption mechanisms

Application-level attacks: Software applications come with myriad functionalities and features. There is a dearth of time to perform complete testing before releasing products. Those applications have various vulnerabilities and become a source of attack.

The applications are vulnerable to attack because of the following reasons:

Software developers have tight schedules to deliver products on time.

Software applications come with a multitude of features and functionalities there is a dearth of time to perform complete testing before releasing products

Security is often an afterthought, and frequently delivered as an “add-on” component poor or nonexistent error checking in applications leads to

Buffer overflow attacks
Active content
Cross-site scripting
Denial of service and SYN attacks
SQL injection attacks
Malicious bots

Other application-level attacks include:

Phishing
Session hijacking
Man-in the middle attacks
Parameter/from tampering
Directory traversal attacks

Example of Application-Level attacks:

Session Hijacking : Attackers may exploit session information in the vulnerable code to perform session hijacking when you enable cookies authentication in your application. When the target tries to browsw through a URL, the session or authentication token appears in the request URL instead of the secure cookie, to give access to the URL requested by the target. Here, an attacker using his or her skills and monitoring tools can hijack the targets session and steal all sensitive information.

Vulnerable Code :Attackers may exploit session information in the vulnerable close to perform session hijacking

```
<configuration>
<system.web>
        <authentication mode=”Forms”>
        <forms cookiesless=”UseUri”>
< /System.web>
 </Configuration>
```

Secure Code : The code can be secured by using Use Cookies instead of UserUri

```
<configuration>
<system.web>
        <authentication mode="Forms">
        <forms cookiesless="UseCookies>
< /System.web>
 </Configuration>
```

Denial-of-Service : The code that follows is vulnerable to a Denial-of-Service attack, as it fails to release a connection resource.

Vulnerable Code:

```
Statement stmnt=conn.createstatement();
Resultset rsltset=stmnt.executequery();
stmnt.close();
```

Secure Code: The code can be secured by releasing the resources in a finally block.

```
Statement stmnt=conn.createstatement();
Resultset rsltset=stmnt.executequery();
stmnt.close();


statement stmnt;
    try {
          stmnt=conn.createStatement();
          statement.executequery();
       }
    finally
    {
          if(stmnt != null)
          {
              try{
                    stmnt.close();
                  }
              catch(SqlException sqlexp)   {          }
          } catch (SqlException sqlexp)     {          }
    } catch (SqlException sqlexp)           {          }
```

Misconfigurationattacks: Most administrators don't have the necessary skills to maintain or fix issues, which may lead to configuration errors. such configuration errors may become the sources for an attacker to enter into the target's network or system.

Shrink wrap code attacks: Operating system applications come with numerous sample scripts to make the job of administrator easy, but the same scripts have various vulnerabilities, which can lead to shrink wrap code attacks.

VI. Limitations of the Ethical Hacking

Unless businesses first know what it is they are looking for and why they are hiring an outside vendor to hack systems in the first place, chance are that there will not be much to gain from the experience. A Ethical Hacking therefore can help the organization only be better understand their security system, but it is up to the organization to implement the right safeguards on the network.

VII. 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.

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

VIII. 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.

IX. References

[1] Global Information Assurance Certification Paper
[2] Internet Crime Complaint Centre link: www.ic3.gov
[3] 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.
[4] Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI: 10.1147/sj.403.0769,Page(s): 769-780
[5] Bradley, Rubin "Computer Security Education andResearch: Handle with care" IEEE Conference Publication, DOI: 10.1109/MSP.2006.146, Page(s): 56-59