AN OVERVIEW OF BLUE HAT HACKERS FEATURES

Shahbaz[1],Rishabh Rajput[2], Navneet Vishnoi[3]

[1,2]*DEPARTMENT OF CCSIT,TEERTHANKER MAHAVEER UNIVERSITY,MORADABAD UP INDIA*

ASSISTANT PROFESSOR

[1]Shahbazzaidi0980@gmail.com

[2]Rishabh8126@gmail.com

Abstract— **A blue hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch .They look for loop holes that can beex ploited and try to close these gaps .Microsoft also uses the term Blue Hat to represent a series of security briefing events.**

Hacking is the act of gaining unauthorized access to a computer system, and can include view ignore copying data ,or even creating new data .Often hacking is understood to be away of maliciously disrupting a computer system, copying information ,or leaving behind a virus that destroys data.

Keywords— Blue Hat Hacker Review paper

I. INTRODUCTION

Hacking is the act of gaining unauthorized access to a computer system, and can include viewing or copying data, or even creating new data. Often hacking is understood to be a way of maliciously disrupting a computer system, copying information, or leaving behind a virus that destroys data.

II.BLUE HAT HACKERS

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term **BlueHat**to represent a series of security briefing events.

III.ATTACKS

A typical approach in an attack on Internet-connected system is:

1. Network enumeration: Discovering information about the intended target.
2. Vulnerability analysis: Identifying potential ways of attack.
3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

IV.SECURITY EXPLOITS

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, cross-site scripting and cross-site request forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FileTransferProtocol HypertextTransfer Protocol(HTTP), PHP, SSH, Telnet and some Web pages. These are very common in Web site and Web domain hacking.

V.TECHNIQUES

A.Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Firewalls defend computers from intruders by limiting access to ports and machines, but they can still be circumvented.)

B. Finding vulnerabilities

Hackers may also attempt to find vulnerabilities manually. A common approach is to search for possible vulnerabilities in the code of the computer system then test them, sometimes reverse engineering the software if the code is not provided.

C. Brute-force attack

Password guessing. This method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used, because of the time a brute-force search takes.

D.Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. Common approaches include repeatedly trying guesses for the password, trying the most common passwords by hand, and repeatedly trying passwords from a "dictionary", or a text file with many passwords.

E. Packet analyzer

A packet analyzer ("packet sniffer") is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

F. Spoofing attack (phishing)

A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying data and is thereby treated as a trusted system by a user or another program — usually to fool programs, systems or users into revealing confidential information, such as user names and passwords.

G .Rootkit

A rootkit is a program that uses low-level, hard-to-detect methods to subvert control of an operating system from its legitimate operators. Rootkits usually obscure their installation and attempt to prevent their removal through a subversion of standard system security. They may include replacements for system binaries, making it virtually impossible for them to be detected by checking process tables.

VI.SOCIAL ENGINEERING

In the second stage of the targeting process, hackers often use Social engineering tactics to get enough information to access the network. They may contact the system administrator and pose as a user who cannot get access to his or her system. This technique is portrayed in the 1995 film *Hackers*, when protagonist Dade "Zero Cool" Murphy calls a somewhat clueless employee in charge of security at a television network. Posing as an accountant working for the same company, Dade tricks the employee into giving him the phone number of a modem so he can gain access to the company's computer system.

Hackers who use this technique must have cool personalities, and be familiar with their target's security practices, in order to trick the system administrator into giving them information. In some cases, a help-desk employee with limited security experience will answer the phone and be relatively easy to trick. Another approach is for the hacker to pose as an angry supervisor, and when his/her authority is questioned, threaten to fire the help-desk worker. Social engineering is very effective, because users are the most vulnerable part of an organization. No security devices or programs can keep an organization safe if an employee reveals a password to an unauthorized person.

Social engineering can be broken down into four sub-groups:

H.Intimidation :As in the "angry supervisor" technique above, the hacker convinces the person who answers the phone that their job is in danger unless they help them. At this point, many people accept that the hacker is a

supervisor and give them the information they seek.

Helpfulness: The opposite of intimidation, helpfulness exploits many people's natural instinct to help others solve problems. Rather than acting angry, the hacker acts distressed and concerned. The help desk is the most vulnerable to this type of social engineering, as (a.) its general purpose is to help people; and (b.) it usually has the authority to change or reset passwords, which is exactly what the hacker wants.[31]

Name-dropping The hacker uses names of authorized users to convince the person who answers the phone that the hacker is a legitimate user him or herself. Some of these names, such as those of webpage owners or company officers, can easily be obtained online. Hackers have also been known to obtain names by examining discarded documents ("dumpster diving").

Technical- Using technology is also a way to get information. A hacker can send a fax or email to a legitimate user, seeking a response that contains vital information. The hacker may claim that he or she is involved in law enforcement and needs certain data for an investigation, or for record-keeping purposes.

Trojan horses

A Trojan horse is a program that seems to be doing one thing but is actually doing another. It can be used to set up a back door in a computer system, enabling the intruder to gain access later. (The name refers to the horse from the Trojan War, with the conceptually similar function of deceiving defenders into bringing an intruder into a protected area.)

Computer virus

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. By doing this, it behaves similarly to a biological virus, which spreads by inserting itself into living cells. While some viruses are harmless or mere hoaxes, most are considered malicious.

Computer worm

Like a virus, a worm is also a self-replicating program. It differs from a virus in that (a.) it propagates through computer networks without user intervention; and (b.) does not need to attach itself to an existing program. Nonetheless, many people use the terms "virus" and "worm" interchangeably to describe any self-propagating program.

Keystroke logging

A keylogger is a tool designed to record ("log") every keystroke on an affected machine for later retrieval, usually to allow the user of this tool to gain access to confidential information typed on the affected machine. Some keyloggers use virus-, trojan-, and rootkit-like methods to conceal themselves. However, some of them are used for legitimate purposes, even to enhance computer security. For example, a business may maintain a keylogger on a computer used at a point of sale to detect evidence of employee fraud.

Attack patterns

Attack patterns are defined as series of repeatable steps that can be applied to simulate an attack against the security of a system. They can be used for testing purposes or locating potential vulnerabilities. They also provide, either physically or in reference, a common solution pattern for preventing a given attack are defined as series of repeat able steps that can be applied to simulate an attack against the security of a system. They can be used for testing purpose sor locating potential vulnerabilities .They also provide ,either physically or in reference ,a common solution pattern for preventing a given attack.