
//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*//////

BASICS OF HACKING- (BY ANOOP KAUSHAL)

Hacker means someone who finds weaknesses in a computer or computer network, though the term can also refer to someone with an advanced understanding of computers and computer networks.Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground but it is now an open community. While other uses of the word hacker exist that are not related to computer security, they are rarely used in mainstream context.

Classifications:-

Several subgroups of the computer underground with different attitudes use different terms to demarcate themselves from each other, or try to exclude some specific group with which they do not agree. Eric S. Raymond (author of The New Hacker's Dictionary) advocates that members of the computer underground should be called crackers. Yet, those people see themselves as hackers and even try to include the views of Raymond in what they see as one wider hacker culture, a view harshly rejected by Raymond himself. Instead of a hacker/cracker dichotomy, they give more emphasis to a spectrum of different categories, such as white hat, grey hat, black hat and script kiddie.

White hat:-

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council , also known as the International Council of Electronic Commerce Consultants has developed certifications, course ware, classes, and online training covering the diverse arena of Ethical Hacking.

Black hat:-

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

Part 1: Targeting

The hacker determines what network to break into during this phase. The target may be of particular interest to the hacker, either politically or personally, or it may be picked at random. Next, they will port scan a network to determine if it is vulnerable to attacks, which is just testing all ports on a host machine for a response. Open ports—those that do respond—will allow a hacker to access the system.

Part 2: Research and Information Gathering

It is in this stage that the hacker will visit or contact the target in some way in hopes of finding out vital information that will help them access the system. The main way that hackers get desired results from this stage is from "social engineering", which will be explained below. Aside from social engineering, hackers can also use a technique called "dumpster diving". Dumpster diving is when a hacker will literally search through users' garbage in hopes of finding documents that have been thrown away, which may contain information a hacker can use directly or indirectly, to help them gain access to a network.

Part 3: Finishing The Attack

This is the stage when the hacker will invade the preliminary target that he/she was planning to attack or steal. Many "hackers" will be caught after this point, lured in or grabbed by any data also known as a honeypot (a trap set up by computer security personnel).

Grey hat:-

A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.

Elite hacker:-

A social status among hackers, elite is used to describe the most skilled. Newly discovered exploits will circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

Script kiddi:-

A script kiddie (or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature).

Neophyt:-

A neophyte, "n00b", or "newbie" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.

Blue hat:-

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 exploits so they can be closed. Microsoft also uses the term BlueHat to represent a series of security briefing events.

Hacktivis:-

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks. Nation state Intelligence agencies and cyberwarfare operatives of nation states.

Attack:-

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.

Security exploit:-

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 FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in website/domain hacking.
Techniques

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. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)
Password cracking:-

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer:-

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

A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.
Rootkit:-

A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.
Social engineering:-

When a Hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers who use this technique, is to contact the system administrator and play the role of a user who cannot get access to his or her system.
Trojan horses:-

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

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. While some are harmless or mere hoaxes most computer viruses are considered malicious.
Worm:-

Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people conflate the terms "virus" and "worm", using them both to describe any self-propagating program.

Key loggers:-

A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some key loggers uses virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security. As an example, a business might have a key logger on a computer used at a point of sale and data collected by the key logger could be used for catching employee fraud.