# Ethical Hacking

***N.Vinodh Kumar, J.Arun Kumar***

**ABSTRACT**

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks. Types of hacking; Website Hacking, Network Hacking, Email Hacking, Ethical Hacking Password Hacking, Computer Hacking. Hackers type; White hat hackers, Black hat hackers, Grey hat hackers, miscellaneous hackers, Red hat hacker.

**Keywords-** Ethical hacking, Website hacking, Network hacking

## ETHICAL HACKING

Ethical hacking is one of the certified any hacking to the computer to important files to hacking. Hacking refers to an array of activities which are done to intrude some one else's personal information space so as to use it for malicious, unwanted purposes.Hacking is a term used to refer to activities aimed at exploiting security flaws to obtain critical information for gaining access to secured networks.

## WEBSITE HACKING

Hacking a website means taking control from the website owner to a person who hackers the website. The hackers will get user name and password and the hackers will use that website for any purpose which may sometimes to destroy some valuable information or even reputation.

## NETWORK HACKING

Network hacking is a generally means gathering information about domain by using tools like Telnet, Ns look UP, Ping, Tracert, Netstat, etc., over the network.

## HISTORY

One of the first examples of ethical hackers at work was in the 1970s, when the United States government used groups of experts called *red teams* to hack its own computer systems. According to Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global Integrity consulting practice, ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technology sectors where it began. Many large companies, such as IBM, maintain employee teams of ethical hackers.

***N.Vinodh Kumar,*** *I MBA*
*Department of Management Studies*
*Er.PerumalManimekalai College of Engineering*
*Hosur*
***J.Arun Kumar,*** *I MBA*
*Department of Management Studies*
*Er.PerumalManimekalai College of Engineering*
*Hosur*

## FAMOUS HACKERS IN HISTORY

- IAN MURPHY
- KEVIN MITNICK
- JOHAN HELSINGUIS
- LINUS TORVALDS
- MARK ABENE
- ROBERT MORRIES

## TYPES OF HACKERS

- WHITE HAT HACKERS
- GRAY HAT HACKERS
- BLACK HAT HACKERS

## WHITE HAT HACKERS

Positive people or the good person / ethical hacker. They hack with having the data owner know about it. The main aim is to look for vulnerabilities and have them fixed.

## GREY HAT HACKERS

Mixed, depending on situation can be good or bad at times. You never know how they work and when they may act differently. They can also be initial black hat person who work as white hat.

## BLACK HAT HACKERS

Negative people or the bad person / malicious hacker. They will hack without the knowledge of the owner with the intent to cause financial or some other loss like destroying information.

## HACKING PROCESS

- FOOT PRINTING
- SCANNING
- GAINIG ACCESS
- MAINTAING ACCESS

## FOOT PRINTING

Foot printing (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get the information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

## SCANNING

Making use of the first phase information to further get more detail information about the network. The hacker may use some tools to scan or ping sweep the network and collect information. Using these they try and collect information about the Operating system, IP address or user account etc.

## GAINING ACCESS

This builds on the earlier phase and it is this phase where more skills of hacking take place. The flaws, weakness of vulnerabilities found from the previous stages are now to be exploited and need to take access of the target system. Techniques like buffer overflow, DoS (Denial of Service), Session hijacking etc are used.

## MAINTAINING ACCESS

Once you are into a target system with all the effort of previous stages or phases, the hacker would like to maintain access to the system rather than trying to figure out ways to compromise the target system every time. They would like to get into the target system on a future date or time and so have something like a backdoor, Trojan etc left on the target system so it can be accesses easily later.

## REFERENCE

1. CEH Certified Ethical Hacker All-in-One Exam Guide by Matt Walker
2. CEH Certified Ethical Hacker Study Guide by Kimberly Graves
3. Certified Ethical Hacker Exam Prep by Michael Gregg
4. Hacking: The Art of Exploitation, 2nd Edition by Jon Erickson
5. Metasploit: The Penetration Tester's Guide by Devon Kearns& Mati Aharoni
6. Official Certified Ethical Hacker Review Guide by Steven DeFino
7. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series) 1st Edition by Patrick Engebrets