SWISS KNIFE

A PROJECT REPORT ON
SWISS KNIFE

Submitted by

UPWAN, UMANG, VAISHALI, SAHIJ, RAJIV

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

ELECTRONICS ENGINEERING

Chandigarh University

MAY 2022

CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

CERTIFICATE

Certified that this project report **“SWISS KNIFE”** is the bonafide work of “UPWAN, UMANG, VAISHALI, SAHIJ, RAJIV” who carried out the project work under my/our supervision.

SIGNATURE	**SIGNATURE**
HEAD OF THE DEPARTMENT	**SUPERVISOR**
INTERNAL EXAMINER	**EXTERNAL EXAMINER**

TABLE OF CONTENTS

ABSTRACT

Hacking is basically expertise in any field. Hackers are classified as per working and as per knowledge. The ethical hackers come under white hat hackers. Ethical hackers use hacking techniques in order to provide security. They are legally authorized hackers. Various tools are used in order to carry out hacking. The most common hacking technique used is phishing. Since, there is a rapid growth in the number of attack, there is a need for people to learn ethical hacking concepts to secure themselves.

Abbreviations and Symbols

IN THIS PROJECT THERE ARE NO ABBREVIATION AND SYMBOL NEEDES

CHAPTER-1

INTRODUCTION

Hacking has been a part of computing for 40 years. Some of the first hackers were members of the Massachusetts Institute of Technology (MIT) Tech Model Railroading Club (TMRC) in 1950s. Security is the condition of being protected against danger or loss. In general sense, security is a concept similar to safety. In the case of networks the security is also called the information security. Information security means protecting information and information system from unauthorized access, use, disclosure, disruption, modification, or destruction. The intent of hacking is to discover vulnerabilities so system can be better secured. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment or to evaluate those weaknesses to assist in removing them. Basic purpose of hacker is to know the system internally without any bad intension.cyber security is a field that is evolving every day, as technology keep’s on evolving the more the digital crimes keep on get more popular and growing. As systems keep on getting more sophisticated the more the cyber criminals keep on finding various ways to get to the sensitive information. The motive of each hacker varies from one hacker to another some are motivated by the money they get paid to hack a system, others are just motivated because of the ego and others are motivated by the act of protecting the wellbeing of the people.

Cyber security is the process of protecting organization’s assets from unauthorized access but also from potential damages which might be caused by potential security breaches.In cyber security there are terminologies that need to be understood by various individual’s in-terms of careers in this field.

(a) Penetration testing – is the process of looking for weakness in the systems before theyare being exploited by hackers

(b) Ethical hacking – is the process of trying to exploit a network by covering all hacking methodologies with other similar hacking techniques as a black hat hacker would do according to EC-COUNCIL.

(c) Cyber security – is the process of defending an organization’s network from various threats. The cyber security is divided into two teams.

CYBER SECURITY

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

· Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

· Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

· Information security protects the integrity and privacy of data, both in storage and in transit.

- Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and

various other important lessons is vital for the security of any organization

TYPES OF CYBER THREATS

The threats countered by cyber-security are three-fold:
1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.
2. Cyber-attack often involves politically motivated information gathering.
3. Cyber terrorism is intended to undermine electronic systems to cause panic or fear.
So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:
Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks. There are a number of different types of malware, including:

· Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

· Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

· Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

· Ransom ware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

· Adware: Advertising software which can be used to spread malware.

·   Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user’s permission

WHAT IS A HACKER

A hacker is an individual who uses computer, networking or other skills to overcome a technical problem. The term also may refer to anyone who uses their abilities to gain unauthorized access to systems or networks in order to commit crimes. A hacker may, for example, steal information to hurt people via identity theft or bring down a system and, often, hold it hostage in order to collect a ransom.

The term *hacker* has historically been a divisive one, sometimes being used as a term of admiration for individuals who exhibit a high degree of skill and creativity in their approach to technical problems. However, the term is also commonly applied to individuals who use this skill for illegal or unethical purposes.

Hacker was first used in the 1960s to describe a programmer or an individual who, in an era of highly constrained computer capabilities, could increase the efficiency of computer code in a way that removed, or *hacked*, excess machine code instructions from a program. It has evolved over the years to refer to someone with an advanced understanding of computers, networking, programming or hardware

WHAT ARE TYPES OF HACKERS

In the past, the security community informally used references to hat color as a way to identify different types of hackers, usually divided into five main types. A few of these terms have been replaced to reflect cultural changes.

- Ethical hackers or authorized hackers -- previously known as *white hat hackers* -- strive to operate in the public's best interest rather than to create turmoil. Many ethical hackers who work doing pen testing were hired to attempt to break into the company's networks to find and report on security vulnerabilities. The security firms then help their customers mitigate security issues before criminal hackers can exploit them.
- Threat actors or unauthorized hackers -- previously known as *black hat hackers* -- intentionally gain unauthorized access to networks and systems with malicious intent. This includes stealing data,

spreading malware or profiting from ransomware, vandalizing or otherwise damaging systems, often in an attempt to gain notoriety. Threat actors are criminals by definition because they violate laws against accessing systems without authorization, but they may also engage in other illegal activity, including corporate espionage, identity theft and distributed denial-of-service (DDoS) attacks.

- Gray hat hackers fall somewhere between ethical hackers and threat actors. While their motives may be similar to those two groups, gray hats are more likely than ethical hackers to access systems without authorization; at the same time, they are more likely than threat actors to avoid doing unnecessary damage to the systems they hack. Although they aren't typically -- or only -- motivated by money, gray hat hackers may offer to fix vulnerabilities they have discovered through their own unauthorized activities rather than using their knowledge to exploit vulnerabilities for illegal profit.
- Red hat hackers, also called *eagle-eyed* or *vigilante*

hackers, are similar to ethical hackers. Red hat hackers intend to stop unethical attacks by threat actors. While red hat hackers may have a similar intent to ethical hackers, they differ in methodology, as red hat hackers may use illegal or extreme courses of action. Often, red hat hackers will deploy cyber attacks toward the systems of threat actors.

- Blue hat hackers, also known as *vengeful hackers*, use hacking as a social weapon. Frequently, it is used as a means for revenge against a person, employer or other organization. Hackers who post personal and confidential data online to ruin reputations or attempt to gain unauthorized access to email and social media accounts are classified as blue hats.
- Script kiddies are amateur, inexperienced hackers who attempt to use pre-written scripts in their hacking efforts. Often, these are fledgling hacking enthusiasts who cause little damage.
- Hacktivists are organisations of hackers that use cyber attacks to affect politically motivated change. The purpose is to bring public attention to something

the hacktivist believes might be a violation of ethics or human rights. Hacktivism attacks may attempt to reveal evidence of wrongdoing by publicizing private communications, images or information.

Identification of Problem

While your computer is connected to the Internet, the malware a hacker has installed on your PC quietly transmits your personal and financial information without your knowledge or consent. Or, a computer predator may pounce on the private information you unwittingly revealed. In either case, they will be able to:

- Hijack your usernames and passwords
- Steal your money and open credit card and bank accounts in your name
- Ruin your credit
- Request new account Personal Identification Numbers (PINs) or additional credit cards
- Make purchases
- Add themselves or an alias that they control as an authorized user so it's easier to use your credit
- Obtain cash advances
- Use and abuse your Social Security number
- Sell your information to other parties who will use it for illicit or illegal purposes

Predators who stalk people while online can pose a serious physical threat. Using extreme caution when agreeing to meet an online "friend" or acquaintance in person is always the best way to keep safe

Identification of the task

When you arm yourself with information and resources, you're wiser about computer security threats and less vulnerable to threat tactics. Hackers and predators pose equally serious and but very different threats

- **Protect yourself while online**
- **Practice safe email and virus/malware protocols**

TIMELINE

- PROJECT SCOPE, PLANNING ON DATE 04-OCT-22
- LITERATURE REVIEW AND PROBLEM IDENTIFICATION ON 09-OCT-22
- PRELIMINARY DESIGN ON 23-OCT-22
- DETAILED SYSTEM AND DESIGN ON 19-NOV-22
- OUTCOME AND WORK ETHICS ON 26-NOV-22

Organization of the Report

In each of the chapter we will explain all the asks and the necessary doubts and the questions
through out the reports

CHAPTER 2

Time line of the reported problem

Hacking has been around pretty much since the development of the first electronic computers. Here are some of the key events in the last four decades of hacking.

1960s: The Dawn of Hacking
The first computer hackers emerge at MIT. They borrow their name from a term to describe members of a model train group at the school who "hack" the electric trains, tracks, and switches to make them perform faster and differently. A few of the members transfer their curiosity and rigging skills to the new mainframe computing systems being studied and developed on campus.
1970s: Phone Phreaks and Cap'n Crunch
Phone hackers (phreaks) break into regional and international phone networks to make free calls. One phreak, John Draper (aka "Cap'n Crunch"), learns that a toy whistle given away inside Cap'n Crunch cereal

generates a 2600-hertz signal, the same high-pitched tone that accesses AT&T's long-distance switching system.

Draper builds a "blue box" that, when used in conjunction with the whistle and sounded into a phone receiver, allows phreaks to make free calls.

Shortly thereafter, Esquire magazine publishes "Secrets of the Little Blue Box" with instructions for making a blue box, and wire fraud in the United States escalates. Among the perpetrators: college kids Steve Wozniak and Steve Jobs, future founders of Apple Computer, who launch a home industry making and selling blue boxes.

1980: Hacker Message Boards and Groups

Phone phreaks begin to move into the realm of computer hacking, and the first electronic bulletin board systems (BBSs) spring up.

The precursor to Usenet newsgroups and e-mail, the boards -- with names such as "Sherwood Forest" and "Catch-22" -- become the venue of choice for phreaks and hackers to gossip, trade tips, and share stolen computer passwords and credit card numbers.

Hacking groups begin to form. Among the first are Legion of Doom in the United States, and Chaos Computer Club in Germany.

1983: Kids' Games

The movie "War Games" introduces the public to hacking, and the legend of hackers as cyberheroes (and anti-heroes) is born. The film's main character, played by Matthew Broderick, attempts to crack into a video game manufacturer's computer to play a game, but instead breaks into the military's nuclear combat simulator computer.

The computer (codenamed WOPR, a pun on the military's real system called BURGR) misinterprets the hacker's request to play Global Thermonuclear War as an enemy missile launch. The break-in throws the military into high alert, or Def Con 1 (Defense Condition 1).

The same year, authorities arrest six teenagers known as the 414 gang (after the area code to which they are traced). During a nine-day spree, the gang breaks into some 60 computers, among them computers at the Los Alamos National Laboratory, which helps develop nuclear weapons.

1984: Hacker 'Zines

The hacker magazine 2600 begins regular publication, followed a year later by the online 'zine Phrack. The editor of 2600, "Emmanuel Goldstein" (whose real name is Eric Corley), takes his handle from the main character in George Orwell's "1984." Both publications provide tips for would-be hackers and phone phreaks, as well as commentary on the hacker issues of the day. Today, copies of 2600 are sold at most large retail bookstores.

1986: Use a Computer, Go to Jail

In the wake of an increasing number of break-ins to government and corporate computers, Congress passes the Computer Fraud and Abuse Act, which makes it a crime to break into computer systems. The law, however, does not cover juveniles.

1988: The Morris Worm

Robert T. Morris, Jr., a graduate student at Cornell University and son of a chief scientist at a division of the National Security Agency, launches a self-replicating worm on the government's ARPAnet (precursor to the Internet) to test its effect on UNIX systems.

The worm gets out of hand and spreads to some 6,000 networked computers, clogging government and university systems. Morris is dismissed from Cornell, sentenced to three years' probation and fined $10,000.

1989: The Germans and the KGB

In the first cyberespionage case to make international headlines, hackers in West Germany (loosely affiliated with the Chaos Computer Club) are arrested for breaking into U.S. government and corporate computers and selling operating-system source code to the Soviet KGB.

Three of them are turned in by two fellow hacker spies, and a fourth suspected hacker commits suicide when his possible role in the plan is publicized. Because the information stolen is not classified, the hackers are fined and sentenced to probation.

In a separate incident, a hacker is arrested who calls himself "The Mentor." He publishes a now-famous treatise that comes to be known as the Hacker's Manifesto. The piece, a defense of hacker antics, begins, "My crime is that of curiosity ... I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all."

1990: Operation Sundevil

After a prolonged sting investigation, Secret Service agents swoop down on hackers in 14 U.S. cities, conducting early-morning raids and arrests.

The arrests involve organizers and prominent members of BBSs and are aimed at cracking down on credit-card theft and telephone and wire fraud. The result is a breakdown in the hacking community, with members informing on each other in exchange for immunity.

1993: Why Buy a Car When You Can Hack One?

During radio station call-in contests, hacker-fugitive Kevin Poulsen and two friends rig the stations' phone systems to let only their calls through, and "win" two Porsches, vacation trips and $20,000.

Poulsen, already wanted for breaking into phone-company systems, serves five years in prison for computer and wire fraud. (Since his release in 1996, he has worked as a freelance journalist covering computer crime.)

The first Def Con hacking conference takes place in Las Vegas. The conference is meant to be a one-time party to say good-bye to BBSs (now replaced by the Web), but the gathering is so popular it becomes an annual event.

1994: Hacking Tools R Us

The Internet begins to take off as a new browser, Netscape Navigator, makes information on the Web more accessible. Hackers take to the new venue quickly, moving all their how-to information and hacking programs from the old BBSs to new hacker Web sites.

As information and easy-to-use tools become available to anyone with Net access, the face of hacking begins to change.

1995: The Mitnick Takedown

Serial cybertrespasser Kevin Mitnick is captured by federal agents and charged with stealing 20,000 credit card numbers. He's kept in prison for four years without a trial and becomes a celebrity in the hacking underground.

After pleading guilty to seven charges at his trial in March 1999, he's eventually sentenced to little more than time he had already served while he wait for a trial.

Russian crackers siphon $10 million from Citibank and transfer the money to bank accounts around the world. Vladimir Levin, the 30-year-old ringleader, uses his work laptop after hours to transfer the funds to accounts in Finland and Israel.

Levin stands trial in the United States and is sentenced to three years in prison. Authorities recover all but $400,000 of the stolen money.

1997: Hacking AOL

AOHell is released, a freeware application that allows a burgeoning community of unskilled hackers -- or script kiddies -- to wreak havoc on America Online (AOL). For days, hundreds of thousands of AOL users find their mailboxes flooded with multi-megabyte mail bombs and their chat rooms disrupted with spam messages. (AOL Time Warner is the parent company of CNN.com.)

1998: The Cult of Hacking and the Israeli Connection

The hacking group Cult of the Dead Cow releases its Trojan horse program, Back Orifice -- a powerful hacking tool -- at Def Con. Once a hacker installs the Trojan horse on a machine running Windows 95 or Windows 98, the program allows unauthorized remote access of the machine.

During heightened tensions in the Persian Gulf, hackers touch off a string of break-ins to unclassified Pentagon computers and steal software programs. Then-U.S. Deputy Defense Secretary John Hamre calls it "the most organized and systematic attack" on U.S. military systems to date.

An investigation points to two American teens. A 19-year-old Israeli hacker who calls himself "The Analyzer" (aka Ehud Tenebaum) is eventually identified as their ringleader and arrested. Today Tenebaum is chief technology officer of a computer consulting firm.

1999: Software Security Goes Mainstream

In the wake of Microsoft's Windows 98 release, 1999 becomes a banner year for security (and hacking). Hundreds of advisories and patches are released in response to newfound (and widely publicized) bugs in Windows and other commercial software products. A host of security software vendors release anti-hacking products for use on home computers.

2000: Service Denied

In one of the biggest denial-of-service attacks to date, hackers launch attacks against eBay, Yahoo!, CNN.com., Amazon and others.

Activists in Pakistan and the Middle East deface Web sites belonging to the Indian and Israeli governments to protest oppression in Kashmir and Palestine.

Hackers break into Microsoft's corporate network and access source code for the latest versions of Windows and Office.

2001: DNS Attack

Microsoft becomes the prominent victim of a new type of hack that attacks the domain name server. In these denial-of-service attacks, the DNS paths that take users to Microsoft's Web sites are corrupted. The hack is detected within a few hours, but prevents millions of users from reaching Microsoft Web pages for two days.

Proposed solution

Cybersecurity is critical for businesses of all sizes. These 18 tips can help you secure your computers and mobile devices from malicious actors.

- Hackers are criminals who gain unauthorized access to a network and devices, usually with the intent to steal sensitive data, such as financial information or company secrets.
- You can protect your computers by using firewalls and antivirus software and by following best practices for computer use.
- You can protect your mobile devices by turning off Bluetooth when it's not in use, being mindful of the Wi-Fi networks you connect to and using security applications to improve monitoring and protection.

The growth of the World Wide Web in the 1990s introduced new possibilities and spawned new industries, but it also brought about new downsides of connectivity. Tons of spam started to infiltrate email accounts, and computer viruses wreaked havoc on business networks. A new threat known as computer hacking extended the definition of thievery to include infiltrating your computer, stealing personal information, tricking you into revealing private data, and using that data to steal and extort personal information, such as business secrets, bank account credentials and even people’s identities.

GOALS

There are many types of hacking these days some of them are

- Phishing – ...
- Virus – ...
- UI redress – ...
- Cookie theft – ...
- Distributed Denial-of-service(DDoS) –
- DNS spoofing – ...
- Social Engineering – ...
- Missing Security Patches –

And many more our goals is to secure everyone who is unaware of these types of risk over the internet

Problem Defination

Can you imagine a stranger—or even worse, a thief—sitting in front of your computer, going through your files and doing whatever they want? That’s what happens once a hacker has used Sub7 to take control of your computer.

It’s as if they’re sitting in your cozy computer chair, using your computer and seeing all of your data and files on your computer monitor. And you have no idea that this is going on.

The hacker could be across the street or across the country. No matter where they are, they can copy photos from your computer onto theirs, or delete your tax records. They can steal your personal data or delete the programs you have on your computer. Worse yet, they can download more viruses.

A sophisticated hacker might be able to find out all kinds of personal information about you. How much? That will be depend on how well you protect yourself by making smart decisions online. For example:

- Do you keep your passwords secret, or write them down and store them on your computer?
- Do you have a habit of keeping browser windows open on websites, windows that reveal your bank account or credit

card numbers?

- Do you make digital images of bank or credit card statements and store them in an easy-to-get-to folder on your computer?

Skilled hackers could gain access to the following:

- Your credit card numbers
- Your bank account
- Your Social Security number

PYTHON

Python is a dynamic, interpreted (bytecode-compiled) language. There are no type declarations of variables, parameters, functions, or methods in source code. This makes the code short and flexible, and you lose the compile-time type checking of the source code. Python tracks the types of all values at runtime and flags code that does not make sense as it runs.

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically-typed and garbage-collected. It supports multiple programming paradigms, including structured, object-oriented and functional programming

Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development, as well as for use as a scripting or glue language to connect existing components together. Python's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. Python supports modules and packages, which encourages program modularity and code reuse. The Python interpreter and the extensive standard library are available in source or binary form without charge for all major platforms, and can be freely distributed

Often, programmers fall in love with Python because of the increased productivity it provides. Since there is no compilation step, the edit-test-debug cycle is incredibly fast. Debugging Python programs is easy: a bug or bad input will never cause a segmentation fault. Instead, when the interpreter discovers an error, it raises an exception. When the program doesn't catch the exception, the interpreter prints a stack trace. A source level debugger allows inspection of local and global variables, evaluation of arbitrary expressions, setting breakpoints, stepping through the code a line at a time, and so on. The debugger is written in Python itself, testifying to Python's introspective power. On the other hand, often the quickest way to debug a program is to add a few print statements to the source: the fast edit-test-debug cycle makes this simple approach very effective.

HISTORY OF HACKING

Nowadays, different people have different views on the hacking scene. Often times people of similar skill level have similar opinions. There is no official definition of a hacker, rather a vague idea amongst the masses. In addition, the media loves to add false information to draw audiences' attention across the nation, for the pure sake of money.

It all began in the 1960s at MIT, origin of the term "hacker", where extremely skilled individuals practiced hardcore programming in FORTRAN and other older languages. Some may ignorantly dub them "nerds" or "geeks" but these individuals were, by far, the most intelligent, individual, and intellectually advanced people who happen to be the pioneers and forefathers of the talented individuals that are today the true hackers. The true hackers amongst our societies have an unquenchable thirst for knowledge. Boredom is never an object of challenge for hackers. They have an almost anomalous ability to absorb, retain, and exert vast amounts of knowledge with regard to intricate details. In 1969, Bell Labs employee Ken Thompson invented UNIX and permanently changed the future of the computer industry. Then in the very early 1970s, Dennis Ritchie invented the computer programming language “C” which was specifically invented to be used with UNIX. Programmers ceased to use assembler, while developing an appreciation for the portability of “C.”

Hackers used to be viewed as people who sat locked in a room all day programming nonstop, hours on end. No one seemed to mind hackers back in the 1960s when this was the most widely excepted reputation. In fact, most people had no idea what hacking was. The term hacker was accepted as a positive label slapped onto computer gurus who could push computer systems beyond the defined limits. Hackers emerged out of the artificial intelligence labs at MIT in the 1960s. A network known as ARPANET was founded by the Department of Defense as a means to link government offices. In time, ARPANET evolved into what is today known as the Internet.

In the 1970s, “Captain Crunch” devised a way to make free long distance calls and groups of phone hackers, later dubbed “phreakers” emerged. Throughout the 1970s and halfway into the 1980s, XEROX’s Palo Alto Research Center (PARC) spit out fresh new innovations such as the laser printer and LANs.

During the early 1980s, the term “cyberspace” is coined from a novel called “Neuromancer.” A group called the “414s” is one of the earliest hacker groups to ever get raided by the FBI and they get charged with 60 computer intrusions. Usenets began to pop up around the nation at this time and hackers exchanged thoughts using their UNIX based machines. While all of this was going on, the Secret Service was granted jurisdiction over credit card and computer fraud. During the 1980s, hacking was not known amongst the masses as it is presently. To be a hacker was to be a part of a very exclusive and secluded group. The infamous hacker groups the “Legion of Doom,” based in the USA and the “Chaos Computer Club,” based in Germany, were founded and are still two of the most widely recognized and respected hacker groups ever founded. Another significant foundation is that of “2600: The Hacker Quarterly,” an old school hacker magazine or “zine.” 2600 Magazine still continues to play a role in today’s hacker community. As the end of the decade approached, Kevin Mitnick was arrested and sentenced to a year in prison on convictions of stealing software and damaging computers. In addition, federal officials raided Atlanta, where some members of the Legion of Doom were residing, at the time. The LOD, CCC, and 2600 Magazine have become known as old school hackers and are still widely respected and recognized.

During the 1990s, Kevin Mitnick is arrested after being tracked down by Tsutomu Shimomura. The trials of Kevin Mitnick were of the most publicized hacker trials in hacker history.

As hackers and time progressed, hackers found ways to exploit holes in operating systems of local and remote machines.

Hackers have developed methods to exploit security holes in various computer systems. As protocols become updated, hackers probe them on a neverending mission to make computing more secure. In fact, due to the tendency hackers have of exploiting society, there have been spinoff categories such as “cracking” which deals with cracking software, “phreaking” which deals with exploiting phone systems, and “social engineering” which is the practice of exploiting human resources. When hacking first originated, the urge to hack into computer systems was based purely on curiosity. Curiosity of what the system did, how the system could be used, HOW the system did what did, and WHY it did what it did.

Some modern day hackers archive exploit upon exploit on their machines, but archiving and using exploits is definitely not what modern hackers do. All too often, media figures and the general public mistake those who deface webpages, steal credit card numbers and/or money, and otherwise constantly wreak havoc upon the masses as hackers. You must be thinking, “Well, isn’t that what hackers DO? They gain unauthorized access to computers,” and technically you would be correct. HOWEVER, that’s not all they do. Hackers find and release the vulnerabilities in computer systems which, if not found, could remain secret and one day lead to the downfall of our increasingly computer dependant civilization. In a way, hackers are the regulators of electronic communication. Hackers come up with useful new computer systems and solutions to make life easier for all of humanity. Whether you know it or not, I know from personal experience that ANYBODY you know could very well lead an unexposed life as a hacker. Hackers live amongst us all. They work in all of our major corporations, as well as in many small companies. Some choose to use their skills and help our government, others choose to use their skills in a more malicious and negative way. If you look around you, ANY INDIVIDUAL you see is a potential hacker. Often, it’s the people who you would suspect the least that are the hackers in our society.

People in our modern day society tend to stereotype hackers as well. All hackers aren’t 31337lbs, 5’5, wearing glasses and suspenders, scrawny, pale skinned, with a comical Steve Urkel resemblance and no social life. If you think this, you are WRONG. Hackers are black, white, asian, european, tall, short, socially active (and not), cool, nerdy, and a bunch of other miscellaneous categories. Just like you can’t make an assumption that if someone is from “Clique X” than they must be really [whatever], you can’t apply a stereotype to genres of hackers. Although there are people running around saying, “Look, I defaced a website, I did it, and therefore I’m a hacker,” doesn’t mean that they’re a hacker. Nevertheless, nor does it mean that ALL people claiming to be hackers are fakes and wannabes. It’s the same in the digital underground as it is with any other realm of society.

Currently, we see the commercialization of hacking. If you were to take a trip to a respectable bookstore with a good selection of books, you would find books with flat out hacking techniques. Whether these techniques can truly be classified as hacking by the classic definition of hacking is debatable. They claim to teach you hacking methods, how to become a hacker, and supposedly reveal hacker tricks to the common man.

Another common misconception is that people who distribute and deal with illegal software, which is commonly known as “warez” are hackers. “Warez kings,” as they are commonly known, are not necessarily hackers, however that doesn’t mean that they are NOT hackers. You cannot determine the intellectual content of people by what they say or have. Moreover, hackers are not people who go around using programs in Windows such as “WinNuke” and various ICMP bombers and other miscellaneous Denial of Service programs designed to crash remote party’s machines. Hackers don’t distribute remote administration tools and use them as trojan horse viruses to wreak havoc on the general public and make other people’s lives miserable. Real hackers want to know as much as they can and are more helpful than wreckless. While it is true that there ARE hackers that DO commit malicious acts against users, they are not to be used as a model of the norm of hackers.