Security Issues Threats in Hacking -Asurvey

Tarjinder Singh, Saurabh Pandey
Students
IIMT College of Engineering
Gr. Noida

ABSTRACT:
The incidences of computer hacking have increased dramatically over the years. In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers are a global threat that uses their knowledge to get unauthorized access to gain critical information, to harm others, to make profits, or to cripple a system. It's not always that Hackers do something to profit themselves, sometimes they may hack into something just to prove themselves or just for a fun purposes. Supporters argue that despite the inconvenience hackers can cause to the systems of businesses – often targeting the biggest companies in the world, like AT&T and, ironically, Microsoft – highlighting these security gaps ultimately helps to make the internet safer. To counter the security threat from hackers, companies and governments hire the white hat hackers also known as the Ethical Hackers who test for any security threats in the system or network. So the future generations need to go into programming because the world demands people with ability to program. Nearly every field uses computers, and in order to get an edge over other workers one need to fluently work on computer and their languages. Because of this reason computer technology is the future of many jobs. Now only programmers are barrier to the hackers. For normal user the security of their networks can be preserved by knowing the basic tricks of the web and basic hacking techniques as well. It very well defines the phrase "Prevention is better than cure" as the hack is easy to prevent than the cure after security has been breached.

KEYWORDS: HACKERS, SECURITY,THREATS

1. INTRODUCTION:

A**Hacker**is the word those by just looking at it everyone feel scared. Everyone born in this world with attitude wants to be a Hacker. But it is not a job of a new born baby or an old grown lady. A Hacker needs a brilliant mind to hack anything. His skills should be so powerful that no other hacker can hack him. A Hacker doesn't need a software to hack. There are many rules that he should learn to become an Ethical Hacker. These rules include knowledge of HTML, JavaScripts, Computer Tricks, Cracking& Breaking etc. Hackers can work alone or in groups, and in a lot of cases are self-taught. It requires lot of time devotion and very deep understanding of web technologies such as HTML, Javasript, SQLetc, to become a hacker.

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers are global threats that uses their knowledge to get unauthorized access to gain critical information, to harm others, to make profits, or to cripple a system . It's not always that Hackers do something to profit themselves, sometimes they may hack into something just to prove themselves or just for a fun purposes. Hacking is rapidly spreading in the world.

However the term "hacker" is one that is disputed among technology specialists and its meaning has changed over the decades. In the early days of computer science, a hacker was simply a name for a programmer developing technology in an academic environment – the only place where there would be access to computers. "New school" hackers in the 1980s and 1990s with access to their own home computers became a flourishing subculture. The Conscience of the Hacker [1], or The Hacker's Manifestois a small essay written January 8, 1986 by a computer security hacker who went by the handle (or pseudonym) of The Mentor (born Loyd Blankenship), still inspires bedroom hackers today. who belonged to the 2nd generation of Legion of Doom(a hacker group active from the 1980s to the late 1990s and early 2000). It was written after the author's arrest, and first published in the underground hacker ezinePhrack and can be found on many websites, as well as on T-shirts and in films.Considered a cornerstone of hacker culture,The Manifesto acts as a guideline to hackers across the globe, especially those new to the field.

The **hacker culture** is a subculture of individuals who enjoy the intellectual challenge of creatively overcoming and circumventing limitations of systems to achieve novel and clever outcomes . The act of engaging in activities (such as programming or other media) in a spirit of playfulness and exploration is termed "hacking". However, the defining characteristic of a hacker is not the activities performed themselves (e.g. programming), but the manner in which it is done - hacking entails some form of excellence, for example exploring the limits of what is possible, thereby doing something exciting and meaningful.

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 whom they do not agree. Eric S. Raymond, author of The New Hacker's Dictionary[2], advocates that members of the computer underground should be called crackers. Yet, those people see themselves ashackers and even try to include the views of Raymond in what they see as a wider hacker culture, a view that Raymond has harshly rejected. Instead of a hacker/cracker dichotomy, they emphasize a spectrum of different categories, such as white hat, grey hat, black hat and script kiddie. In contrast to Raymond, they usually reserve the term crackerfor more malicious activity.

2. CATEGORIZATION:

The hackers are categorized into following terms depending on their intentions and skills.

2.1 WHITE HAT:

A white hat hacker breaks security for non-malicious reasons, either to test their own security system, perform penetration tests or vulnerability assessments for a client - or while working for a security company which makes security software. The term is generally synonymous with ethical hacker, and theEC-Council, among others, have developed certifications, courseware, classes, and online training covering the diverse arena of ethical hacking.

2.2 BLACK HAT:

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). The term was coined by Richard Stallman, to contrast the maliciousness of a criminal hacker versus the spirit of playfulness and exploration of hacker culture, or the ethos of the white hat hacker who performs hacking duties to identify places to repair.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".

2.3 GREY HAT:

A grey hat hacker lies between 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 a security defect, for example. They may then offer to correct the defect for a fee. Grey hat hackers sometimes find the defect of a system and publish the facts to the world instead of a group of people. Even though grey hat hackers may not necessarily perform hacking for their personal gain, unauthorized access to a system can be considered illegal and unethical.

2.4 ELITE HACKER:

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

2.5 SCRIPT KIDDIE:

A script kiddie (also known as a skid or skiddie) is an unskilled hacker who breaks into computer systems by using automated tools written by others (usually by other black hat hackers), 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), usually with little understanding of the underlying concept.

2.6 NEOPHYTE:

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

2.7 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.

2.8 HACKTIVIST:

A hacktivist is a hacker who utilizes technology to publicize a social, ideological, religious or political message.

Hacktivism can be divided into two main groups:

- Cyberterrorism — Activities involving website defacement or denial-of-service attacks; and,
- Freedom of information — Making information that is not public, or is public in non-machine-readable formats, accessible to the public.

2.9 NATION STATE:

Intelligence agencies and cyberwarfare operatives of nation states

2.10 ORGANIZED CRIMINAL GANGS:

Groups of hackers that carry out organized criminal activities for profit

3. INCIDENTS OF HACKING:

Hacking came to mainstream attention with the 1983 movie [6] War Games, the story of a high school student played by Matthew Broderick, who nearly starts World War III from his bedroom. In the 1990s, the romanticized idea of the hacker as a loveable rogue was the inspiration for movies including The Matrix, Sneakers and Hackers, and for conspiracy theorist group The Four Horsemen in the TV series The X Files.

Mary L Radnofsky, author of Corporate and Government Computers Hacked by Juveniles, a 2006 [3] research paper with the ominous sub-title Your Government Computer Is Being Targeted for a Hack Right Now. The Hackers Are Teenagers. They'll Never Be Caught, and They Know It, wrote: "Many such crimes are committed by students—not because they really want state secrets, but just to prove they can do it. Many more do it for the millions of dollars they can generate through extortion."

In 1988, hacker Robert Morris devised the "internet worm", a self-replicating virus that spread so quickly through computers it shut down the entire network for two days. Even back in 1998, hacking groups claimed that should they so wish, they could shut down the entire internet in half an hour. Viruses can spread across the world in hours, causing billions of dollars of damage through lost data and productivity. In the 21st century, hacking became political in nature; in 2001, Chinese hackers infiltrated American government computers in a co-ordinated attack in retaliation for the death of a Chinese pilot in a spyplane collision. With this politicization of hacking, it is increasingly regarded as a weapon in the arsenal of "cyber terrorists".

One of the most high profile cases of hacking is that of Gary MacKinnon, who managed to break into NASA and Pentagon computers in 2002. US authorities accused him of stealing hundreds of passwords, deleting files and shutting their whole system down for 24 hours. McKinnon, diagnosed with Asperger's syndrome, did it all from his bedroom in London, England – having taught himself to hack, inspired as a child by War Games. Where McKinnon described himself as a "bumbling computer nerd", the United States government considered his actions "the biggest military hack of all time". He faced 60 years in prison.[4]

Supporters argue that despite the inconvenience hackers can cause to the systems of businesses – often targeting the biggest companies in the world, like AT&T and, ironically, Microsoft – highlighting these security gaps ultimately helps to make the internet safer. This has also been Gary McKinnon's defense for his hacking of the Pentagon computers: "I was amazed at the lack of security," he said. "The reason I left not just one note, but multiple notes on multiple desktops was to say, ‘look, this is ridiculous'." Businesses are increasingly employing "ethical hackers" to test their online security systems and keep ahead of threats.

The 2011 PlayStation Network outage was the result of an "external intrusion" on Sony's PlayStation Network and Qriocity services, in which personal details from approximately 77 million accounts were compromised and prevented users of PlayStation 3 and PlayStation Portable consoles from playing online through the service.The attack occurred between April 17 and April 19, 2011, forcing Sony to turn off the PlayStation Network on April 20. On May 4 Sony confirmed that personally identifiable information from each of the 77 million accounts may have been exposed. The outage lasted 23 days.[5]

At the time of the outage, with a count of 77 million registered PlayStation Network accounts,it was one of the largest data security breaches in history. It surpassed the 2007 TJX hack which affected 45 million customers. Government officials in various countries voiced concern over the theft and Sony's one-week delay before warning its users.Sony stated on April 26 that it was attempting to get online services running "within a week." On May 14, Sony released PlayStation 3 firmware version 3.61 as a security patch.

Ryan Collins, 36, of Pennsylvania , USA was accused of gaining access to more than 100 Google and Apple accounts, many belonging to famous women . Collins engaged in the phishing scheme between November 2012 and September 2014, when the photos were finally released. He sent emails asking victims for their usernames and passwords — supposedly for official purposes — and then used this information to seize control of their emails. He also utilized a “brute force” software program called iBrute to illegally download the contents of their iCloud backups, by guessing passwords repeatedly until it got them right.There were many private pictures and videos of many popular celebrities that were sold for Bitcoins . The accused was caught after 19 months of the hack. Due this Apple has now decided to double down on its beliefs about user privacy, by working on a new encryption method that will mean it can no longer decode user information stored in iCloud [6].

Just before Christmas of 2015, that theoretical threat become all too real for more than 225,000 Ukrainians who were plunged into darkness by a sophisticated attack on one of the nation's power companies. The attackers struck late in the afternoon on 23 December and used the remote access they had gained to computers in the control centre of power firm Prykarpattyaoblenergo to flip circuit breakers and shut down substations. About 30 substations were turned off, including those that served one of the control rooms for Prykarpattyaoblenergo, so staff struggling to get the lights back on were forced to find a fix in the dark.Even now, months after the attack, computer systems at the Ukrainian energy company are not quite fixed because the "Killdisk" malware used in the attack deleted key files.[7]

4. CONCLUSION:

Hackers have been around the globe for long and will be there till life exists on the earth . To counter the security threat from hackers companies and governments hire the white hat hackers also known as the Ethical Hackers who test for any security threats in the system or network. So the future generations need to go into programming because the world demands people with ability to program. Nearly every field uses computers, and in order to get an edge over other workers one need to fluently work on computer and their languages. Because of this reason computer technology is the future of many jobs. Now only programmers are barrier to the hackers .For normal user the security of their networks can be preserved by knowing the basic tricks of the web and basic hacking techniques as well. It very well defines the phrase “Prevention is better than cure” as the hack is easy to prevent than the cure after security has been breached.

REFERENCES:

1. The Conscience of the Hacker aka The Hacker's Manifestohttp://phrack.org/issues/7/3.html
2. Blomquist, Brian (May 29, 1999). "FBI's Web Site Socked as Hackers Target Feds".New York Post
3. Mary L Radnofsky, author of Corporate and Government Computers Hacked by Juveniles, a 2006
4. The Briton facing 60 years in US prison after hacking into Pentagon http://www.theguardian.com/world/2008/jul/27/internationalcrime.hacking
5. PlayStation network breach https://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony
6. http://www.cultofmac.com/417931/icloud-hacker-behind-the-fappening-faces-five-years-in-prison/
7. Could hackers turn the lights out(23 December 2015)http://www.bbc.co.uk/news/technology-35204921