An Approach on 'Hacking' with White Heart

Pathan Feroz Khan
II MCA
SITAMS, Chittoor, A.P, India

Dr. M. Kalpana Devi
Sr. Asst. Professor, MCA Department
SITAMS, Chittoor, A.P, India

ABSTRACT

With the increasing use of digital technology in the areas of business and society, and growing connectivity comes in greater challenges on the level of security. Cyber security is the number one problem of humankind in the digital world. This is because of "Hackers". The term Hacking sounds something with negative shade. Hacking is not what we think; it is an art of exploring the threats in the system. Programmers who are good at programming can protect the weak points from being hacked. It is true that the impact of hackers will be felt most in the developments to do with the Internet in the short term. A hacker is someone who pushes the bounds of technology. This study is to highlight the intensions of most of the hackers who explores how the system works and how the system can fail. The idea is that there exists a new breed of ethical-minded hackers, who can penetrate systems to aide companies and their systems administrators in securing the information and technology that keeps their businesses running.

Keywords- Digital Technology, Cyber security, Hacking.

I. INTRODUCTION

With the explosion of the Internet, the client/server model, and the distributed computing, information is everywhere, is non-stop and proves to be extremely critical to safe guard. Every individual and organization has issues of security related to their confidential and sensitive data where internet is used. This is because of **Hackers.** Hacker is a programmer who enjoys the challenge of breaking into other computers, but does no harm. **Hacking** can be defined as a process of ascertaining and the subsequent exploitation of various shortfalls and weakness of a computer system in networking environment.

A. History Of Hacking

1960's:

The issue of security in internet is not just problem of 21st century. it began from 1960s, during 1960's a group of computer students used the word "HACKING". Essentially the hack meant a shortcut that doesn't necessarily solve a problem in a good way. The first hacking action from phone phreaking, by blowing a high-pitch whistle tone into the phone, 2600-hertz, AT&T's long-distance switching system could be accessed. Later hackers were engineering special boxes with a whistle that came free in cereal boxes to make free calls, it became so popular.

The 1980's hacking hub:

There was an increase in sales of home personal computers that were able to talk to one another via the phone network during 1980's and were considered as the "Golden Age" of hacking [1]. Often Kids were breaking into any computer system, just to be able to say they did and to explore. And also small crimes were committed, like printing out lots of paper at a business.

By the late 80's, Congress passed a Computer Fraud and Abuse Act, making breaking into computer systems a crime, the FBI was really catching on to hackers. This didn't stop anything. In 1989 Employees were even destroying company systems as revenge for being fired. German hackers were found hacking into the Pentagon, who worked for Russia's KGB.

As the Internet evolved and systems became more sophisticated, hackers no longer are curious and playing games, they are out for blood and extremely dangerous. Many companies have had security breaches such as social security numbers and e-mail addresses of millions and exposing credit card information, this information is sold to the highest bidder on the black market. To diffuse their enemies' nuclear programs, US government used computer viruses. In 2008, Russia used hackers to coordinate their attack on Georgia. As we go more and more digital every day one has to wonder what the future holds.

II. HACKING TERMINOLOGY

A. Vulnerability:

Vulnerability means weakness, in hacking terminology vulnerability refers to a flaws in a system that are open to cyber attacks. Hackers may use Vulnerability Scanners to find insecure configuration of a system by using databases containing thousands of signatures.

B. Exploit:

Vulnerability of a system definitely leads to exploitation. Exploitation is to gain access over a device due to its security loopholes. It may help in further attacks either on compromised machines or machines on local network.

C. Bruteforce:

Brute forcing is an exhaustive search method in which all the possibilities are tried to reach the solution of a problem. It is a method used to decode the encrypted data and passwords through trial and error methods.

D. Doxing:

Discovering and then publishing the identity of an internet user by following their details online.

III. SECURITY FOCUSED OPERATING SYSTEM

There are operating systems based on Linux kernel which are built in favor of hackers which are packed with bunch of hacking tools [2]. These operating systems help the hacker to discover the vulnerability of a computer and its network and let us explore.

A. Kali Linux:

Kali Linux is the most suitable operating system for ethical hackers developed by OFFENSIVE SECURITY. It is debian based operating system comes with more than 500+ pre-installed pen testing tools and application which makes it as rich hacking tool. Offensive securities also provides great support for its users by releasing frequent updates based ARM and VMware platforms. Kali Linux become a unique Linux operating system with its wide range of features live boot, reverse engineering, forensic jobs etc.

B. Parrot security OS:

Parrot OS is a debian based OS developed by frozen box Team. Comparing with other operating systems it is a lightweight cloud friendly OS with efficient working capabilities. Parrot OS is a mixture of Kali Linux and Frozen box OS with a strong support from its community.

C. Backbox:

Backbox is Ubuntu based Linux operating system used for penetration testing and security assessment. Backbox is fast and efficient working OS having a wide range of security analyzing tools, that can be used for web applications and networking. Backbox has applications which updates are regularly provided for stable performance.

D. Pentoo Linux:

Pentoo is a Gentoo based operating system mostly focused on pen testing. it has a different types of tools belongs to exploit, scanning, cracking, database etc...

E. DEFT Linux:

DEFT stands for Digital Evidence and Forensic Toolkit. DEFT is a Ubuntu based and built around DART (Digital Advanced Response Toolkit) software. Many forensic tools and documents are inbuilt with OS used by hackers.

F. Network Security Toolkit (NST):

A NST can easily convert the x86 system into a hacking machine with its hacking tools. Network security toolkit is fedora based Linux which runs x32 and x86 systems.

IV. DIFFERENT HACKING TECHNIQUES

Exploiting unauthorized information is unethical activity. A hacker uses simple tools and techniques to exploit other personal and sensitive data. these tools and techniques creates a great opportunity to hackers to gain personal data like emails, passwords, personal files, bank card details, etc...
Here are some techniques which hackers may use [3].

A. Bait and switch:

With this technique an attacker can buy ad spaces on websites for advertising, whenever the user clicks on those ads the user is redirected to webpage consisting of malware, further malware may be installed into device through malicious webpage to take control over.

B. Cookie theft:

A Browser holds our data like personal login credentials, browsing history in the form of cookies. Once hacker get access cookies, he can even authenticate himself as you on a browser. It is also known as session hijacking. it is a popular method which allows users packet to pass through hackers' machine.

C. Clickjacking Attacks:

It is also known as UI REDRESS. In this attack, the hacker hides actual UI of a website where user may click. Whenever the user clicks malware sites open, he may be hacked. This is very common in app download and streaming. Hackers mostly employ this technique to earn and steal personal data.

D. Virus, Trojans...:

Virus or Trojans are harmful software programs which get installed into victim's computer and these Trojans keep sending users personal information to the hacker. Sometimes it may lock user files on hackers' instructions like **RANSOMEWARE** did.

E. Phishing:

Phishing is a hacking technique which a hacker creates a clone of a most accessed websites and ambush the victim by a spoof link. it is most dangerous vector attack over internet with a combination of social engineering. Once the user access clone website and enters his credentials those were send to the hacker using Trojan running on a cloned website.

F. Eavesdropping:

Eavesdropping is a passive attack. Hacker just monitors the computer and its network to get some unwanted data. This technique is used to get some information without being identified. These kind of attacks mostly done on emails, phone calls and other communications.

G. Fake WAP:

Fake WAP is creating fake wireless access point using software. Once people connect they may become victim for a hacker. Then hacker can access their personal information. It is one of the easiest way of hacking with a simple wireless network and a software.

H. Denial of Service:

Denial of service is an attacking technique which is used to slow down a server or a website by generating lot of fake requests to it that the server fails to process request and finally crashes due to heavy requests.

I. Key logger:

Key logger is a common and famous simple technique to obtain user data. The key logger may be in the form of software or hardware, it records the key strokes of a victim. It might contain emails, login credentials, bank accounts, passwords. This is the reason why most of commercial websites and banking websites suggests using virtual keyboard.

A Hacker may use any of the above technique to enter into the user's system violating its security to gather personal information or to crash the computers. An ethical hacker always will be there to protect from these malicious things.

V. IS HACKING BAD OR GOOD....?

Most of the people whenever they hear the word hacking they just remain of exploring illegal things. Exploring illegal things is not just thing which can done with hacking skills there is something more than this. A hacker can provide security apart from destroying systems. In the past five years there is a rapid increase in cyber-attacks. These were strongly controlled by security providers.

A. Type of Hackers:

According to Falk et. all. (2014) hackers are divided into two categories: "white hat" and "black hat". White hats use their skills against to criminal activities, while black hats use their abilities for malicious and illegal purposes [4]. They introduce a third category: the "gray hat" hacker who gains unauthorized access to computing resources for the purpose of helping organizations to identify and resolve security issues. This type of hacker is not specifically malevolent, they operate in an ethical gray area and do gain unauthorized access to the computing resources they feign to exploit.

The white hats goal is to attempt to infiltrate systems in an effort to help identify weaknesses, so that they can be patched in time before the black hats find and exploit these same vulnerabilities. In 2015, CNN reported that Cyber security consultant Chris Roberts was detailed after allegedly hacking into the control systems of more than 20 United Airlines commercial flights (Perez 2015). However, the negative consequences that might arise if a malevolent "black hat" hacker attempted the same things is truly shocking, though he claimed that his actions were intended solely to raise awareness of aircraft's software critical security issues.

Media coverage has given the term 'hacker' a negative connotation. However, the original usage was complimentary, indicating someone with a high level of technical sophistication, or someone who enjoyed the intellectual challenge of overcoming or circumventing limitations.

B. White Hat hackers are the Best:

In reality White hat hackers are more powerful than black hat hackers. But because of many criminal articles and movies are about black hats. Most of us heard about stories of bad guys rather than good guys in hacking era. Therefore, all these led us to believe as black hat hacker are powerful. White hat hackers are actually good programmers. They breach security like a black hat hacker and fix it.

a.From the Company's perspective:

A company should provide security to its customers for the sake of its name and profits as every customer expect a secured service. Some white hat hackers are hired by a company to see their systems secured. Finding weakness of a system is easy to those who tries to exploit or find weakness than who creates systems. Every company must strongly believe that, if a white hat hacker is hired to hack their own system a security weakness may be pointed out before a black hat hacker find it. Sometimes a white hat hacker may use same technique as black hat hacker used to hack system and find vulnerabilities, which can be patched by company administrators.

b.Non-Profit Groups:

There are many non-profit hacking communities which work for the welfare of the society. They protect public from harmful viruses like ransome wares. A Major group "Anonymous" stands as a best example for this. During Paris blasts Anonymous group members stayed on the side of humanity and united from all over the world to hack down ISIS terrorist group.

2015 Cyber War On ISIS Terrorist Group: In Paris during November 2015[5], the ISIS group organized attacks by gun men, suicide bombers left 100 people dead and 100 wounded with more than hundred in critical condition. In response, Anonymous announced a major, sustained operation against ISIS, declaring, "Anonymous from all over the world will hunt you down. You should know that we will find you and we will not let you go". ISIS responded on Telegram by calling them "idiots", and asking "What they gonna to hack?" By the next day, however, Anonymous claimed to have taken down 3,824 pro-ISIS Twitter accounts, and by the third day, more than 5,000 recruiters were doxed.

As increase in use of computer with internet the count of cyber-crimes increases. The white hat hacker always tries to control it from either side of a corporate company or from himself as a public interest.

Looking at the top hackers, it should be clearly evident that many are strongly affiliated with the open source movement. A main example of a prominent hacker having strong open source leanings is how Tim Berners-Lee made his idea about the World Wide Web available freely. While not directly contributing code to an open source project, he laid the foundations to become one of the great revolutions in computing. John Carmack, a very prominent video game designer and hacker is probably the most vocal advocate of open source [6].

VI. CONCLUSION

Most people think hacking is illegal activity as the media and social sites highlights only about negativity of hacking. The two sides of positive and negative depends upon individual mindsets and their behaviors. There are many situations which reflects positivity of ethical hacking. There are many former black hat hackers who are now employed in the computer security industry, since they are being compensated and legitimized by these companies no doubt it reflects a ethical change in the intended outcome of their actions.

REFERENCES

[1] https://prooncall.com/the-history-of-computer-hacking-and-how-it-has-evolved-over-the-years/

[2] https://resources.infosecinstitute.com/top-10-linux-distro-ethical-hacking-penetration-testing/

[3] https://fossbytes.com/hacking-techniques/

[4] http://digitalcommons.pace.edu/honorscollege_theses/14

[5] https://en.wikipedia.org/wiki/Anonymous(group)

[6] https://courses.cs.washington.edu/courses/csep590a/06au/projects/hacking.pdf