University of Sindh Journal of Information and Communication Technology (USJICT)
Volume 4, Issue 1, January 2020
ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/

The World of Hacking: A Survey

Imran Memon[1], Riaz Ahmed Shaikh[2], Hadiqua Fazal[1], Muhammad Hanif Tunio[2], Qasim Ali Arain[3]

[1] Department of Computer Science, Bahria University, Karachi campus, Sindh, Pakistan
[2]Department of Computer Science, Shah Abdul Latif University, Khairpur, Sindh, Pakistan
[3]Department of Software Engineering, Mehran University of Engineering & Technology, Jamshoro
imranmemon.bukc@bahria.edu.pk, riaz.shaikh@salu.edu.pk, hadiqua.bukc@bahria.edu.pk, hanif.tunio@salu.edu.pk, qasim.arain@faculty.muet.edu.pk

Abstract: Hacking is the most genius field of computing science which is getting bigger with the passage of time. This research paper has the methods and techniques of hacking, types of hacking, types of hackers, types of hacking attacks, common tools of hacking, the geography of hackers, phases of hacking, protection processes, past reports, instruments of hacking and at last the future discussion on this field. This paper is enough to get to know some beginning information of hacking.

Keywords:., Security; Hacking , Access

I. INTRODUCTION

The world computing science is advancing towards the more advanced and hybrid computing. The future of computing science is getting bigger with the passage of time. This advancement indicates that the future of computing takes this world or coming generations towards the new world of science which may be harmful or moneyed for humanity and for the technology of computing or systems. This enhancement brings success and relief for humanity along with the security issues. The field of hacking is also getting bigger with the time which is going towards future. The field of hacking includes legal hacking or illegal hacking. Both the hackings have their own sub fields. The advancement in illegal hacking is not good for the future because this advancement should increase the security issues to a great extent. But good thing is that with security issues may be the security systems increase their capability and their flexibility [1].

II. HACKING

Hacking is not a basic or regular activity. Hacking consists of two paths. The first path is towards the legal and permissioned work while the other path is towards the illegal and unapproved work. The permissioned hacking is also known as approved engineering or valid engineering. And the illegal hacking is also called reverse engineering. The valid engineering and reverse engineering is totally depend to each other. The enhancement in reverse engineering makes compulsory to make advancement in the security systems or in valid engineering [2-8].

A. Vulnerability

The weakness in the system or any computing source which allow the unauthorized access in the system is called vulnerability.

B. Threats

A threat is a possible danger which is available for the system or any computing source. This is thing which is totally acceptable for the organization.

C. Risk

Risk is the damage which is caused by the hackers or attackers. In other words, we can say the damage done by the threats in the system is called risk.

D. Hackers

Hacker is a type of programmer or coder or software engineer. Hacker is not a particular or simply profession. This profession is divided into many sub parts such as blue hat hacker, grey hat hacker, black hat hacker and white hat hacker etc. Each hacker performs different job. Each specific task is design for the specific hacker [2].

E. Profiling The Hacker

It is very difficult to describe a profile of a hacker especially the profile of back door hackers. According to the report of FBI in 1999:

- The hacker is mostly a nerd, punky, wild and teenager.

- The hacker is seen as the unacceptable under achiever.
- The average age of a hacker is 16 to 19.
- The hacker spends an average time of 57 hours a week on their system [9].

F. Qualities Of Hacker

One should have the following qualities to become a typical hacker:

- Experienced in C, C++ and PERL programming languages.
- Must has knowledge of networking protocols of the internet.
- Should be the heavy user of internet
- Must familiar with at least two operating systems, one of which is surely the UNIX. UNIX is a computer operating system designed for multi-tasking and multi-users.
- Must be the collector of outdated hardware and software [9].

G. Crackers

Crackers have the same interest that is show by the hackers. But there is a minor difference between the hackers and crackers. Crackers are also known as script kiddies. We can also say that the crackers are the unprofessional or unskilled type of hackers. This hacker used the others hacking tools for hacking which is not so true hacking. Crackers can be easily identified because their malicious work is not so confidential. Crackers are mostly involved in the minor hackings such as hacking of social media ID's, controlling others computer screen etc [3].

H. Phreak

A phreak is a person who break or damage the networks of telephone or other secured communication networks only [9].

I. Cyberpunk

A cyberpunk is the recent modification in the field. Cyberpunk can be considered as a combination of hackers, crackers and phreak. Cyberpunk contains the characteristics of all three [9].

III. PROTECTION FROM HACKERS

We can perform few exercises to protect the system from the hackers:

A. Security Infrastructure

The basic principle of information security is the firewall. Firewall block the access of unapproved and malicious approach. Firewall creates a barrier between a trusted internal network and untrusted external network such as internet. When attacker makes any network attack then firewall only allow the trusted system to access to the system and block the malicious users.

EXAMPLES:
Next-Gen firewalls
Application level gateways

B. Intrusion Detection System

An intrusion detection system is a device or a software application. It is used to observe or monitors the network malicious or malware activity. When any malicious activity is occur then it reported to an administrator or security information and event management.

C. Network Intrusion Detection System

A system that monitors the main and important operating system files is an example of network intrusion system.

D. Host-Based Intrusion Detection System:

A system that resolve the incoming network traffic is an example of host based intrusion detection system.

E. Code Review

Code review is a software quality checking activity. In this activity, the authors of the code and the quality testers get together to review the code. During this activity, the security vulnerabilities of the program or software is observe by the testers and authors which is essential before handed the software to the user.

IV. SECURITY PATCHES::

A patch is a supporting data of computer program which is designed to update, fix and improve it. This includes removing security vulnerabilities and other defects, such type of patches is known as bug fixes. These patches are also known as security patches.
Security patches improve the usability and performance of the computer program.

A. Types Of Security Patches

There are three main type of patches, Binary patches, Source code patches and Large patches [7].

B. Protection From Crackers

We can easily protect the systems from the script kiddies or crackers by following some guidance:

1) Do not post any personal information on the social media.
2) Use professional passwords, which cannot be broken by guessing or brute force.
3) Use 2 factor authentication, when available.
4) Do not share any social media content password on any request email.
5) Verify source of contact.
6) Be careful from unknown links, investigate it before clicking.
7) Always scan a removable devices after connecting.
8) You must ensure that antivirus is installed in the system.
9) Must set root password for installation. [6]

V. GEOGRAPHY OF HACKERS

Table 1 Geography of hacking various country and global attack percentage [14]

POSITION	COUNTRY	GLOBAL TRAFFIC ATTACK
1ST	CHINA	41%
2ND	UNITED STATES	10%
3RD	TURKEY	4.7%
4TH	RUSSIA	4.3%
5TH	TAIWAN	3.7%
6TH	BRAZIL	3.3%
7TH	ROMANIA	3.3%
8TH	INDIA	2.3%
9TH	ITALY	1.6%
10TH	HUNGARY	1.4%

There are countless skillful hackers are present in the different countries but some countries are the leading the position in the field of hacking. And the global traffic attacks of these countries are also leading the chart. Let's consider a chart which was observed in the quarter of 2012 shown in Table 1 [4].

VI. TYPES OF HACKERS

A. Black Hat Hackers

Black hat hackers are viewed as terrible and horrible humans. They utilize their abilities and skills for malicious and illegal purposes. Black hat is the one who unofficially enter into the other systems or network for some malicious and damaging purposes. The black-hat hacker does not have any permission or authority to access to their targets. Black hat have such a great skills that theirs conference are often attended by security professionals and academics [2].

B. Grey Hat Hackers

Grey hat hackers are also utilize their skills for their entrance in the other system just like black hat but there aim and target don't have malicious purposes. Grey hat is usually hire for the checking of security systems. Grey hats may also break the hacked [2].

C. White Hat Hackers Or Ethical Hackers

White hat hacker is viewed as a good guys in the field of hacking. White hat is working with the full permission of the organization for which hacker is working for. White hat is mainly make organization save from the malicious attacks or unapproved approach [2].

D. Blue Hat Hackers

Blue hat hackers are the security professionals who can check the dangers and the errors in the software before the company launched it. Blue hat hackers are the security professional who not the member of organization. [2, 5].

E. Elite Hackers

Elite hacker have a social status among the hackers. Elite hacker is considered to be the most skill full hacker, because the new discovered exploit is circulate among the elite hackers[2,5].

F. Hacktivist

Hacktivist is the hacker who uses the technology to communicate a social, ideological, religious or political message. Hacktivist can be divided into two types. First is Cyberterrorism and the other is Freedom of information [2,5].

G. Neophyte

A neophyte is a term which is used for beginner hackers. Neophyte has almost no knowledge or experience about the field [2, 5].

H. Cyber Terrorists

Group of hackers that perform the malicious activities for the profit [2, 5].

I. Ethical Hacker

An ethical hacker is also known as white hat hacker. Ethical hacker is an information security expert who solve the defects of computer system, network, application or other computing

content. With the permission, ethical hacker also find the vulnerabilities that malicious user can enter in the source. The main purpose of ethical hacker is to check the security of the source and identify the vulnerabilities in the source such as networks or system infrastructure. Ethical hackers use their skills and techniques to test and maintain the organizations.

VII. PHASES OF HACKING

Hacking usually is divided into 5 main phases as illustrated in figure 1.

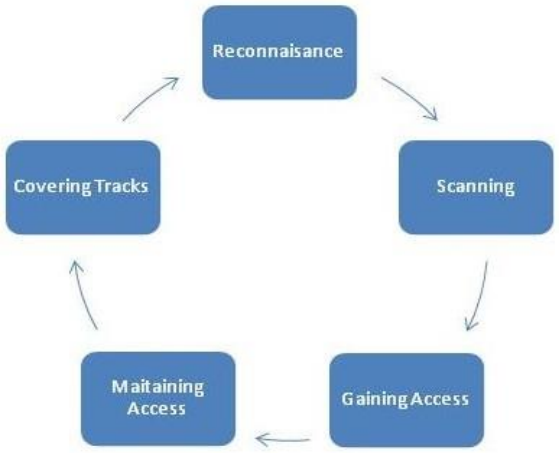

Figure 1: Phase of hacking [6]

A. *Reconnaisance*

This is the first phase of hacking. This phase is also known as investigation step. In this phase, the hacker tries to collect the information of the target shown in figure.1. This phase may include identifying the Target, finding out the target's IP Address Range, Network or domain name system [6].

B. *Scanning*

This is the second phase of hacking. This phase may include usage of hacking tools such as dialers, sweepers and vulnerability scanner etc. to scan data. The investigation step gives the basic information of the target to the hacker. Now, hackers decide the couple of methods and couple of tools which is required for the access or attack [6].

C. *Gaining Access*

In this phase, hacker design or develop the blueprint or sketch of the network of the target with the help of phase 1 and phase 2. The hacker has finished the listing and scanning the network and, now hacker have some options to gain access to the targeted system [6].

D. *Maintaining Access*

This is the most phase of hacking. Because, once a hacker gained the access or achieve the access to the targeted system then the most important is that to keep that access for future malicious attacks. When the hacker gained the access to the system then hacker can also use this system as a base for future malicious attacks [6].

E. *Covering Tracks*

The last phase of hacking is covering tracks or clearing tracks. Clearing tracks means on one can reach them. The attacker should change their MAC address and run their attacking machine or attacking tool through VPN to cover or hide their identity. This phase is essential because the direct attack is noisy and clearly identified by the target [6].

VIII. INSTRUMENTS OF HACKING:

There are few regular hacking instruments are available which are used by hackers:

A. *Trojan Horse*

Trojan horse is a malicious computer program which is used to mislead the official user of the system. Trojan horse must require the interaction with the hacker or attacker. It cannot enter into the system by its own. Trojan horse act as a back door of your system. It gives malicious user or hacker access to your system and allow the hacker to find all the personal information of the user.

EXAMPLES:
- Magic-Lantern
- Net-Bus
- Sub7
- Zeus
- Back-Orifice

B. *Worm*

Worm is an independent computer malware program. Worm is also called self-duplicating program. Worm make duplicates of it-self and spread via computer networks without any help.

EXAMPLES:
- E-mail worms
- Instant messaging worms
- IRC worms
- Internet worms
- Bacteria and rabbits

C. *Virus*

Virus is also a computer malware program. Virus is also called duplicating program. The purpose of virus is same as the computer worm. Virus make duplicates of it-self and spread via computer networks, but it require the interaction with the attacker.

EXAMPLES:
- Resident virus

Browser hijacker
Overwrite virus
Macro virus
Network virus
Space filler virus

D. Vulnerability Scanner

A vulnerability scanner is a computer program which is used to know the weakness of systems, networks and applications. Vulnerability scanner is used in the 2nd phase of hacking (scanning). This scanner discover the weakness in systems, networks or applications and show the report to the attacker then attacker design there attack according to the given report.

EXAMPLES:
OpenVAS
Air-Crack
MBSA
Wire-Shark

E. Sniffer

Sniffer is a malicious tool used for network attack. This tool allow the malicious user to enter in the require network and catches the information that is travel in the network among the connected systems.

EXAMPLES:
Packet analyzer
Auto LYCUS

F. Exploit

Exploit is an anti-hacking software which is used to find and remove the defects present in the network, system or application. This software is mainly used by ethical hackers to check the security and to remove the vulnerabilities.

EXAMPLES:
SQL injection
Cross site scripting
Cross site request forgery
Zero day exploit [2]

IX. TYPES OF ATTACKS:

A. Non-Technical Strike:

Strike that is made on the individual or on someone's system is called non-technical strike. This strike is obtained due to the misuse of trust. This strike is mostly make through the social web sites. In this strike, the hacker makes a room between the original connection that lies between the user and the web application or websites.

B. Network Foundation Strike

This strike is made on a network or on a place where number of networks can be come through internet. This strike may affect the all systems that are connected with the network. This strike may allow the malicious user to get access to all the information and data of the connected systems and also allow the attacker to control the whole network.

C. Operating Frame-Work Strike

Hacking of operating system is one of the most supportive technique of the hacker. The operating system of each computer must have one or huge numbers of vulnerabilities. These vulnerabilities are used by the attacker to strike that system. The operating systems that are much secure remains safe from this strike such as Novell, NetWare and the kinds of UNIX. The main target of the hackers remain towards few operating systems and that are LINUX and Windows which are better known for their vulnerabilities.

D. Application Strike

Applications regularly deal with the great number of strikes. The main target of the hackers remain towards the web applications and email server software. Following are the strikes which are made on these projects:

Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) are regularly strike by the hackers and their security firewall is unable to break that malicious approach.

Malicious software like Trojan horse, worms and virus threats etc. obstruct the network and bring the system down.

SPAM (garbage emails) crash the understandability and storage room. Ethical hackers always keep the system free from the SPAM to avoid the strikes [2,8].

X. TYPES OF HACKING

A. Inside Job

Most security breaks begin from inside the network that is affected. This hacking is mostly probably perform by the member of that network. The member have the enough information to hack the network or the systems of the network. It's not a difficult task for a member of the network to strike that network because the attacker is well aware with the vulnerabilities and content (password and activities etc.) of the group. This attack contains the characteristics of both non-technical attack and network foundation attack.

B. Rogue Access Points:

Roger access point is an unsecure wireless network access (WAN). The attackers prompt this network and make unaware users to join this network. This access point or network have all the insensible and innocent users that make the desirable

atmosphere in the network but the appearance of hacker in the network destroy the user's system present in that network.

C. Back Doors

When hacker can make an unapproved approach to any network by using a sound easy routes then this hacking is known as back door hacking. Hackers find the any shortcoming in any network with the help of a computerized searchers. This hacking contain the characteristics of all strikes.

D. Denial Of Service

This service make hacker capable of cut down or break any network without getting access in the network. Denial of service (DOS) mainly target the email or transmission control protocol. This hacking have the characteristics of network foundation strike and operating system strike.

E. Distributed Doss

Distributed Doss make the DOS strike make efficient with number of sources. It is very hard to get rid of distributed doss because it changes the IP address of the targeted systems. This hacking have the characteristics of network foundation strike and operating system strike.

F. Anarchists Hacking

This hacking is performed by crackers or script kiddies. This is not a professional type of hacking because it cannot deal with any unapproved access. This hacking also cannot deal with the networks or systems. This hacking makes strike only on an application or on any web content such as Facebook, Instagram and twitter. This hacking have the characteristics of application strike and nontechnical strike [2].

XI. TOOLS OF HACKING

A. NMAP

Network mapper is a free and open source network vulnerabilities scanner. This tool detects the vulnerabilities of the network and presented the report to the user.

B. Wireshark

Wireshark is a free and open source network scanner. This tool detects the vulnerabilities of the network and also used for the development of the network.

C. Metasploit

The metasploit project provides you the vulnerabilities information of the targeted system. This tool enables the attacker to hack any system or computer or any computing source.

D. Aircrack-Ng

Aircrack-Ng is a network software which is used as cracker. It is used to analysis and crack WEP and WPA/WPA2-PSK.

E. Nessus

Nessus is also a vulnerabilities scanner. It gives access to the remote hacker to the data and information of the target system. It also used to misconfigure the targeted system and it is also used for DOS strike.

F. Thc Hydra:

Hydra is the password cracking tool. It is used to crack the passwords of the web content such as Facebook, Instagram and twitter etc. It also used to break the passwords of the computing sources. Hydra is the most popular password cracking tool of this decade [2].

XII. FUTURE DISCUSSION

Both the hacking and ethical hacking is advancing towards the future success. But at present the ethical hacking overheads the reverse engineering or hacking. The development of asset and different penetration tests make ethical hacking more efficient. The security measures of IT engineers and ethical hackers such extra firewalls, strong authentications, anti-virus programs and different cryptography methods close the success door of the reverse engineering in Table 2.

Table 2 cyber-attacks in various time period

YEAR	CYBER ATTACKS
2016	82,000
2017	350,000
2018	550,000
2019	100,000

The year of 2016 and 2017 was in the favor of hacking but the report of cyber-attacks shows that the number of cyber-attacks in 2018 become 64% of number of attacks in 2017. This decline shows the success of ethical hacking [10].

XIII. CONCLUSION

This paper deals with complete intro of hacking. This field is the essential part of computing science but in good means such as to protect the valuable data or for securities purpose. Both the hacking and ethical hacking is the part of the computing science, but we should prefer ethical or legal hacking because it gives you big success according to the latest report. Hackers and IT engineers both are the programmer but one uses their skills to harm others and other use it to protect the victims.

REFERENCES

[1] Shim, Jung P., et al. "Past, present, and future of decision support technology." Decision support systems 33.2 (2002): 111-126.

[2] Kumar, Sunil, and Dilip Agarwal. "Hacking Attacks, Methods, Techniques and Their Protection Measures." International Journal of Advance Research in Computer Science and Management, 4 (4) (2018).

[3] Baird, Bruce J., Lindsay L. Baird Jr, and Ronald P. Ranauro. "The moral cracker?" Computers & Security 6.6 (1987): 471-478.

[4] Cyware News (2020), "TOP 10 COUNTRIES WITH MOST HACKERS IN THE WORLD" , CYWARE Social, Retireved on December, 2019, URL: https://bit.ly/2s46ILS.

[5] Wikipedia, (2020), "Security hacker" From Wikipedia, the free encyclopedia , Retrieved on January, 2020, URL https://en.wikipedia.org/wiki/Security_hacker

[6] Aditya Chatterjee, (2020) "5 Phases of Hacking", Geeks For Geeks, Retrieved on (December, 2019, URL: https://www.geeksforgeeks.org/5-phases-hacking/

[7] Ebersohn, Gerrie. "Catching hackers." Juta's Bus. L. 12 (2004): 14.

[8] Murotake, David K., and Antonio Martin. "Achieving high assurance connectivity on computing devices and defeating blended hacking attacks." U.S. Patent No. 7,490,350. 10 Feb. 2009.

[9] Chirillo, John. Hack attacks revealed: A complete reference with custom security hacking toolkit. John Wiley & Sons, 2002.

[10] Pam Baker, (2011), "The Nightmare Future of Hacking" eSecurity Planet, Retrieved on December 2020, URL: https://bit.ly/2Jjdua2.