ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A COMPREHENSIVE STUDY ON ETHICAL HACKING

Suriya Begum*, Sujeeth Kumar, Ashhar
* Professor,Department of Computer Science and Engineering, New Horizon College of Engineering,Bangalore, India
Student, Department of Computer Science and Engineering, New Horizon College of Engineering,Bangalore, India
Student, Department of Computer Science and Engineering, Bangalore, India

DOI: 10.5281/zenodo.59534

ABSTRACT

Explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: criminal hackers. An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. There are many techniques used to hack the information. This paper explores the ethics behind techniques of ethical hacking and whether there are problems that lie with this new field of work. In this paper we have discussed in detail history and types of hackers , different techniques used to hack the users, Operating System used in hacking , its pros and cons and a detail case study of J.P.Morgan.

KEYWORDS: Computer Ethics, Ehical Hacking , Malware Ethics, Research Ethics; Malicious Hacker; Pornography.

INTRODUCTION

In today's busy world we are always required to be connected to each other, and this is achieved through internet. But care needs to be taken about what information we reveal to others on the net because those who intend on causing harm to you will use this information against you [3]. So it is important to protect oneself online from variety of threats online [3].

Hacking refers to gaining access to a computer to obtain information stored on it by means of password cracker software or any other technique to get data . This is done to either point out the loop holes in the security or to cause intentional sabotage of the computer [3].

They are the computer programmers who have knowledge of computer programming and have enough information on the systems they are about to hack [3]. Thus , a hacker whether he wants to sabotage the system or check its security will have to have exceptional knowledge of computers..

CONCEPT OF HACKING

Hacking refers to gaining access to a computer to obtain information stored on it by means of password cracker software or any other technique to get data . This is done to either point out the loop holes in the security or to cause intentional sabotage of the computer [3].

HISTORY OF HACKING

1939: The "bombe" became the world's first ethical hacking machine. It was used by the British to decipher encrypted German messages during WWII [8].
1960: The Computer Penetration was first discussed by leading experts with the mention of deliberate tests by professionals.
1971 : The first "Tiger-Team" was formed. USAF contracted James Anderson to test time-sharing systems.
1974: The US Air Force conducts one of the first ethical hacks to test the security of the Multics OS [8].
1986: The US Computer Fraud and Abuse Act makes black and grey hat hacking a criminal offense.
1995: Dan Farmer & Wietse Venema released SATAN, an automated vulnerability scanner, which becomes a popular hacking tool.
1999: Software security goes mainstream with the release of Microsoft Window's 98.
2003: OWASP releases the first OWASP testing guide to teach best practices in penetration testing [8].
2009: PTES is founded leading to an increase in ethical hacking jobs. They offer business and security service providers a common language and scope for performing penetration testing.
2014: Worldwide security spending reaches $71.1 billion. Security executives begin to use on demand penetration testing services for cost effective ethical hacking [8].

TRUTH ABOUT HACKERS

They are the computer programmers who have knowledge of computer programming and have enough information on the systems they are about to hack [3]. Thus , a hacker whether he wants to sabotage the system or check its security will have to have exceptional knowledge of computers.

CLASSIFICATION OF HACKERS

Hackers are mainly classified into 3 types:

a) White hat hackers: They are the also called Ethical Hackers who hack computers of corporate companies to check for any loop holes in their security [3]. They are paid for this job known as Penetrating Testing.
b) Black hat hackers: They are the opposite of white hat hackers who don't take hacking jobs from companies but do it to cause harm to them. They sabotage the systems so as to obtain information about their target which includes bank information, personal details, phone numbers , etc [3].
c) Grey hat hackers: They are the hybrid of white hat and grey hat hackers [3].
Other types of Hackers are :
d) Crackers: They are the college students who hack systems for personal use.
e) Script-kiddie: They are the non technical people who know how to use professional hacking tools.

VARIOUS OPERATING SYSTEM (OS) USED IN HACKING

1. Backtrack Linux: It is one of the first OS used for hacking purposes. It has been designed for hacking by Offensive Security Organization of Israel Hackers [3].
2. Kali Linux: It is the most widely used OS across the world for hacking currently. This OS is the reborn version of Backtrack Linux as it contains much more advanced tools than Backtrack Linux [3].

DIFFERENT TECHNIQUES USED FOR HACKING

There are many techniques which are used for Ethical Hacking .Here , elaboration of about 4 commonly used Hacking techniques has been discussed [5].

Phishing Hack :

In this technique the attacker will want to obtain information about the people or a particular person who has sensitive information like credit card number, account password ,etc[4].

There are different types of Phishing:

i. Clone phishing
ii. Spear phishing
iii. Phone phishing

iv. DNS-Based Phishing(Pharming)
v. Man-in-the-middle attack

There are different techniques of a Phishing Hack:

1) Email spoofing
2) Web spoofing
3) DNS Cache Poisoning
4) Malware

FTP Brute Force Hack:

In this technique , a hacker will use the Brute Force algorithm to find out a person's account password on the FTP Client. The Brute Force algorithm is designed in such a way that it will try every combination of the password, until the correct password has been obtained. We usually can use FileZilla software to achieve this [1] .

Denial of Service (DoS) :

In this type of attack , a hacker attacks a target machine and makes sure that the system is unavailable for intended users for a short time or a particular period of time[7]. A Distributed Denial of Service (DDoS) is an advanced type of DoS in which the hacker attack a group of system used in business, shops, corporate ,etc.

Symptoms of Denial of Service:

a) An attempt on flooding network traffic to prevent legitimate network traffic.
b) To disturb connections between 2 systems, thereby stopping access to a particular service being provided.
c) Preventing a client or may be an employee of the company from accessing a particular service or system.
d) To stop a service from being given to a particular person (like an employee) [7] .

Types of DoS:

1. SYN flood attack
2. TCP Reset attack
3. ICMP attack
4. UDP storm attack
5. DNS request attack
6. CGI request attack
7. Mail bomb attack
8. ARP storm attack
9. Algorithmic complexity attack
10. Spam attack

Malware :

It refers to all the virus, trojans, bombs , etc., created by hackers to ensure that they can damage the target systems and collect required data and ensure that the target system will always have vulnerabilities in them[2].

Types of Malware:

a) Smartphone malware
b) Worms, viruses
c) Spyware, keystroke loggers, information theft malware
d) Botnet attacks and detection/tracking and defense
e) Rootkit and virtualization technique

PHASES OF PENETRATION TESTING

1. Reconnaissance: It refers to collecting of information about the target system, either by the attacker or by the white hats. This is done by a few techniques like Foot printing, WHOIS, Google hacking [3].

2. Exploitation: It is the usage of loopholes in the target system to gain access to the system. This is done using a few techniques like network hacking here Ftp Anonymous issues is most prevalent so we can use Ftp Brute Force; Web Exploitation [3].
3. Maintaining Access: This phase refers to having a remote connection established with the target system. This can be done using Backdoors, Rootkits. [8]
4. Post Exploitation: This phase is different for white hats and attackers. For white hats , they have to they have to give a penetration test report with 3 parts: a) *Executive summary* b) *Detailed Report* c) *Raw output*. But for attackers they have to cover their tracks and make sure that there is no knowledge of their attack on the target [8].

CASE STUDY

J.P.Morgan's Data Breach :

In this case study ,we will give some insights of how the Mega Bank J.P.Morgan got hacked :

This event has happened in June 2014, when an employee of the company had his login credentials stolen as his system was infected with malware [6]. The employee tried to login to the corporate network through a VPN, and the hacker was able to obtain access to the internal network of the company. The hacker was able to get pass all the security measures present and gain full control of the network , as he obtained administrator privilege level and soon took over more than 90 servers of the company[6]. To avoid detection by the company the information was extracted slowly for several months without being noticed. The breach would have gone unnoticed had they not hacked one of the company's charity sites. The Hold Security, Inc. had discovered billions of usernames and passwords stolen, so they checked their company's corporate network and found that they too had been breached. Since , Hold Security, Inc. had discovered the hack in time so that the damage done could be minimized [6] .But the hackers had already stolen usernames, passwords, contact information 76 million individuals and 7 million small businesses. With the amount of data that had been stolen from J.P.Morgan could face future breaches as their vulnerabilities are very large[6] .

PROS OF ETHICAL HACKING

i. It help us to think like a criminal(black hat, grey hat).
ii. Helps us to create secure systems less vulnerable to external attacks.
iii. It gives us a chance of knowing the weak spots in the security of the systems [1,8] .

CONS OF ETHICAL HACKING

i. It only gives us a brief overview of what is happening.
ii. Loss of sensitive information.
iii. A thought of feeling secured without realizing an external attack already happening [1,8].

CONCLUSION

From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures, produced without a requirement for security. As long as there is support for ad hoc and security pack-ages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, proper security will not be a reality. Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of an organization's security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, embarrassment, loss of revenue or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place. In the future , more and more techniques will be discussed with its advantages and disadvantages.

REFERENCES

[1] Sonal Beniwal , Sneha , "Hacking FTP Server Using Brute Force Algorithm " , International Journal of Computer Engineering and Applications, Volume 9, Issue 6, Part 1, June 2015 , ISSN 2321-3469
[2] Umer Asgher , Fahad Moazzam Dar , Ali Hamza , Abdul Moeed Paracha ,"Analysis of Increasing Malwares and Cyber Crimes Using Economic Approach " , The International Journal of Soft Computing and Software

Engineering ,Vol. 3, No. 3, Special Issue: The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13], San Francisco State University, CA, U.S.A., March 2013

[3] Parag Pravin Shimpi , Prof Mrs Sangeeta Nagpure , " Penetration Testing: An Ethical Way of Hacking " , Global Journal For Research Analysis, Volume-4, Issue-4, April-2015 , ISSN No 2277 – 8160

[4] Dr. M. Nazreen Banu S. Munawara Banu , "A Comprehensive Study of Phishing Attacks", International Journal of Computer Science and Information Technologies, Vol. 4 (6) , 2013, 783-786

[5] Minakshi Bhardwaj and G.P. Singh, "Types of Hacking Attack and their Counter Measure ", International Journal of Educational Planning & Administration. Volume 1, Number 1 ,2011, pp. 43-53 © Research India Publications

[6] Allen Jeng , "Minimizing Damage From J.P. Morgan's Data Breach",GIAC (GSEC) Gold Certification ,Author: Allen Jeng, ajeng@adobe.com ,Advisor: Tim Proffitt ,Accepted: March 15th, 2015 ,Copyright SANS Institute

[7] Shenam Chugh, Dr. Kamal Dhanda , "Denial of Service Attacks ", International Journal of Advanced Research in Computer Science and Software Engineering. Volume 5, Issue 8, August 2015

[8] http://www.slideshare.net/installCore/install-core-history-of-ethical-hacking-and-penetration-testing

[9] Gurpreet K. Juneja ," ETHICAL HACKING: A TECHNIQUE TO ENHANCE INFORMATION SECURITY ", International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 12, December 2013

[10] Sonal Beniwal, 2 Sneha, "Ethical Hacking: A Security Technique ", International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 5, Issue 4, 2015 ISSN: 2277

[11] Murugavel, "Survey on Ethical Hacking Process in Network Security ",International Journal of Engineering Sciences & Research Technology [836-839, [July, 2014] ISSN: 2277-9655

OTHER PUBLICATIONS

1. Suriya Begum , Dr. Prashanth C.S.R , "Review of Load Balancing in cloud Computing", International Journal of Computer Science Issues, ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814 , Vol. 10, Issue 1 , No. 2 , January-2013 , pg. 343 – 352 .
2. Suriya Begum , Dr. Prashanth C.S.R , "Investigational Study of 7 Effective Schemes of Load Balancing in cloud Computing" ,International Journal of Computer Science Issues , ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 , Vol. 10, Issue 6 , No. 1 , November-2013, pg. 276 – 287.
3. Suriya Begum , Dr. Prashanth C.S.R , "Mathematical Modeling of Joint Routing & Scheduling for an Effective Load Balancing in cloud", International Journal of Computer Application, (0975 – 8887) , Volume 104 – No.4, October-2014 , pg. 32 – 38 .
4. Suriya Begum , Dr. Prashanth C.S.R , "Stochastic Based Load Balancing Mechanism for Non-Iterative Optimization of Traffic in Cloud ", IEEE International Conference , SSN Colg of Engg, Chennai, 23-25 March-2016, WiSPNET 2016.
5. Suriya Begum , Vasanthi , Dr. Prashanth C.S.R , "Ensuring Data Security in Cloud Computing From Single To Multi Cloud For Multi Share Users" ,National Level Technical Paper Presentation, MVJ CE , Bangalore, 4th-5th October ,FVCT-2012.
6. Suriya Begum , Archana , Dr. Prashanth C.S.R , "Performance Analysis of Cloud Computing Centres using M=G=m=m+r Queuing Systems", National Level Technical Paper Presentation, NHCE , Bangalore, 28th March,NCICT-2013.
7. Suriya Begum , Ayub Inamdar , "Priority Based Pre-Emptive Scheduling of Real Time Services Request with Task Migration for Cloud Computing", National Level Technical Paper Presentation , Akshaya IT Tumkur, 29th April Technika-2014
8. Suriya Begum , Asha C , Dr. Prashanth C.S.R , "A Novel Load Balancing Strategy for Effective Utilisation of Virtual Machines in Cloud", International Journal of Computer Science & Mobile Computing, ISSN : 2320-088X, Vol 4, Issue 6, June-2015, pg. 862-870.
9. Suriya Begum , Ananth Raju , Dr. Prashanth C.S.R , "Resource Management By Virtual Machines Migration In Cloud Computing", International Journal of Computer Science & Mobile Computing, ISSN : 2320-088X, Vol 4, Issue 12, December-2015, pg. 307-312.

10. Suriya Begum , Sachin , Ram Charan, Nikhit, Sai Prathap, "Analysis of Various Load Balancing Techniques in Cloud Environment" ,International Journal of Computer Science & Mobile Computing, ISSN : 2320-088X, Vol 5, Issue 2, Feb-2016 , pg . 248 -254.
11. Suriya Begum , Venugopal , "Comparison Of Various Techniques In IoT For Healthcare System" ,International Journal of Computer Science & Mobile Computing, ISSN : 2320-088X, Vol 5, Issue 3, March-2016, pg. 59 – 66 .
12. Suriya Begum , Kavya , "Analysis of Various Big Data Techniques For Security" ,International Journal of Computer Science & Mobile Computing, ISSN : 2320-088X, Vol 5, Issue 3, March-2016, pg. 54 – 58 .
13. Suriya Begum , Venugopal, " Analysis of Load Balancing Algorithms in Cloud Environment", International Journal of Emerging Technology & Advanced Engineering, ISSN : 2250-2459, Vol 6, Issue 4, April-2016, pg. 151 – 154 .
14. Suriya Begum , Kavya , " A Study on Load Balancing techniques in Cloud Computing Environment", International Journal of Emerging Technology & Advanced Engineering, ISSN : 2250-2459, Vol 6, Issue 5, May-2016, pg. 72 – 74 .
15. Suriya Begum , Kavya , Venugopal , "A Study on Load Balancing techniques in Cloud Computing Environment", 3rd International Conference On Convergent Innovative Technologies, ,Cambridge IT, Bangalore . ISSN(Online) : 2319-6890, 20th May-2016,ICCIT-2016 .
16. Suriya Begum , Kavya , Venugopal , "A Study on Load Balancing techniques in Cloud Computing Environment", International Journal of Engineering Research, ISSN(Online) : 2319-6890, ISSN(Print) : 2347-5013, Vol 5, Issue Special 4, May-2016, pg.904-909 .
17. Suriya Begum , Rohit Mulay , Ashhar ,"Near Field Communication: A Survey", International Journal of Emerging Technology & Advanced Engineering, ISSN : 2250-2459, Vol 6, Issue 6, June-2016, pg. 92 –9 7