International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.104.23

Insight Of Hacking In Cyber Crime

Dr. Vidyashankar M.H[1]
[1]*Chairman, Dept. Of Computerscience, Sahyadri Science College, Shivamogga*

Abstract- "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones is called as Cyber crime.. Cyber security means protection of computer system from theft and damage. In this paper I am discussing about how to use ethical hacking in securing our digital information and to secure from crime.
Aim- Exposure to avoid cyber crime using ethical hacking.
Objective- To observe the current problems of cyber crime
To determine the effectiveness of ethical hacking to secure our digital information.

I. PROBLEM STATEMENT:

Now a days we can here daily a cyber crime activity being reported, as Cyber-crimes have gone beyond conventional crimes security is big challenge. The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks (DOS), malware (malicious code). The illegal act may be facilitated by computer network or devices with target independent of the computer network or device". However, ethical hacking has been used by various telecommunication companies to cover the loophole and this study is providing an overview on the issues and the solutions.
Definition: Hacking is an attempt to exploit a computer system or a private network inside a computer for some illicit purpose.
Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services.
Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. Also, due to malpractice by operators.
Cyber crime, or computer related crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)" Cybercrime may threaten a person or a nation's security and financial health.
An ethical hacker is a computer and network expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security loop holes through which hackers can attack.
The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerability to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures.

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. It carries out the crypto viral extortion attack from crypto virology that blocks access to data until a ransom is paid

II. TYPES OF HACKERS:

White hat: professionals hack to check their own security systems to make it more hack-proof.
Black hat: These types of hackers will hack system for the personal benefit, they will steal data or hide it and sometimes they will change pass words so that authorized persons cannot open it.
Gray hat: People who have enough computer skills to enable them to hack a system to locate potential loopholes in the network security system. These hackers will bring notice to admin about loophole.

Ethical hackers use the same methods and techniques to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any susceptibility found, they document them and provide actionable advice to improve its overall security (Laura, 1995).. One of the first examples of ethical hacking occurred in the 1970s, when the United States government used groups of experts called "red teams" to hack its own computer systems (Laura, 1995). It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.

The first recorded cyber murder was committed in the United States seven in 1995 (Indian Express, January 2002), an underworld don in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient. Now a day we can find at least one death per day due to cyber crime.

III. TYPES OF CYBER CRIME

3.1 Hacking:

Hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendancy such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator's intent, others just want to cause destruction.

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

3.2 Virus dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean selfreplicating "malware" (MALicious softWARE). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate

3.3 Logic bombs

A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

3.4 Identity Theft and Credit Card Fraud

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands.

Revenge pornography, or revenge porn (informal), is the sexually explicit portrayal of one or more people that is distributed without their consent via any medium. The sexually explicit images or video may be made by a partner of an intimate relationship with the knowledge and consent of the subject, or it may be made without his or her knowledge. The possession of the material may be used by the perpetrators to blackmail the subjects into performing other sex acts, to coerce them into continuing the relationship, or to punish them for ending the relationship.

3.5 Suggestions

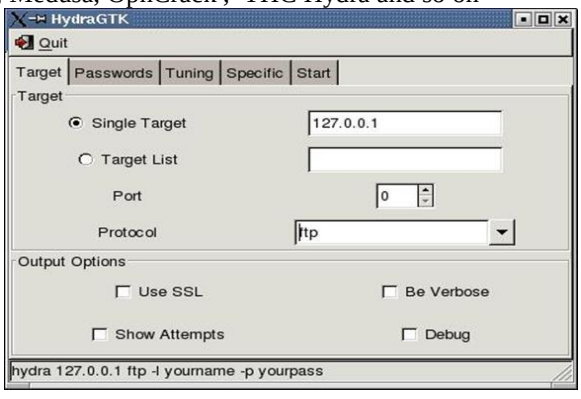
1. Social media should be used very carefully,
2. We should not upload personal photo to media in public sector
3. If we respond to the Nigerian mail by giving details they can hack our account.
4. If we gave our devices to hacker for few minutes on humanity ground then everything will collapse as they will insert virus within few seconds.
5. Don't use public network for any important activity
6. Every time see the address bar whether it is secured or not
7. Don't respond to mails which is suspicious,
8. Don't share IP address
9. Update antivirus time to time
10. Aware of malware, trozen horse and virus etc

3.6 Algorithms can be used:

FPGA (Field Programmable Gate Arrays) are programmable pieces of hardware specifically designed for encryption/decryption. ASIC (Application Specific Integrated Circuits) are also specialized hardware that can test 200 million keys per second. We have certification course about hacking its better to have a basic knowledge of hacking else it will be quiet difficult to save our data. Certified Ethical Hacker (CEH) is a qualification obtained by assessing the security of computer systems, using penetration testing techniques. The code for the CEH exam is 312-50, and the certification is in Version 9 as of 2016.

3.7 Password cracking tools

Brutus, RainbowCrack, Wfuzz, Medusa, OphCrack , THC Hydra and so on



As key lengths increase, the number of combinations that must be tried for a brute force attack increase exponentially. For example a 128-bit key would have 2^128 (3.402823669209e+38) total possible combinations. For example, to theoretically crack the 128-bit IDEA key using brute force one would have to: develop a CPU that can test 1 billion IDEA keys per second

- build a parallel machine that consists of one million of these processors
- mass produce them to an extent that everyone can own one hundred of these machines
- network them all together and start working through the 128 bit key space

3.8 Causes of Cyber Crime

Untruthfulness of Human is the main cause, to become rich in short span without wasting physical energy leads to cyber crime.

IV. CONCLUSION

Publics should get information about hacking, by improving security algorithms we can avoid several attacks. cyber crime involves technology as weapon but user of that weapon is human being only. We have to be very careful and we should have knowledge of cyber crime and hacking. It is better to learn cyber security and ethical hacking, and then only we can avoid cyber crimes. Second thing is our law should be strict and should be track against criminals.

****

V. REFFERENCES:

[1] https://www.tutorialspoint.com/ethical_hacking/
[2] https://en.wikipedia.org/wiki/Hacker_ethic
[3] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
[4] Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
[5] "Distributed Denial of Service Attack". csa.gov.sg. Retrieved 12 November 2014.
[6] "What is Spoofing? – Definition from Techopedia".
[7] Adebusuyi, A. (2008): The Internet and Emergence of Yahooboys sub-Culture in Nigeria, International Journal Of Cyber-Criminology, 0794-2891, Vol.2(2) 368-381, July-December
[8] Odinma, Augustine C. MIEEE (2010): Cybercrime & Cert: Issues & Probable Policies for Nigeria, DBI Presentation, Laura, A. (1995):
[9] Cyber Crime and National Security: The Role of the Penal and Procedural. Law",Research Fellow, Nigerian Institute of Advanced Legal Studies.
[10] Cybercrime In Nigeria, Business Intelligence Journal, Retrieved
[11] Financial Weapons of War". Minnesota Law Review. 2016. SSRN 2765010 .