International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Digital Forensics: How to Counterattack Hackers Motive

Rohit Vijaykumar Menon

Department of MCA, YMT College of Management, Kharghar, Navi Mumbai, Maharashtra, India

ABSTRACT

As we all know security over internet is a big issue due to various loopholes in the system. The system hackers usually checks for these loopholes and once they are aware of it exploiting it brutally would be a child's play for any smart advanced hacker. The only way to avoid these is to understand the hacker's real motive and plans so that counterattacking can be carried out to safeguard the system. This paper would talk about various digital forensic strategies to counterattack the hackers if any suspicious activities are found out.

KEYWORDS: *Hacking, Digital Platform, Countermove, Neutralization, Retribution, Threatening, Damage, Deface*

How to cite this paper: Rohit Vijaykumar Menon "Digital Forensics: How to Counterattack Hackers Motive" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.590-591, URL: www.ijtsrd.com/papers/ijtsrd33415.pdf

IJTSRD33415

INTRODUCTION

Hacking is a sharp witted technique of exploiting the vulnerabilities in the system or network and using it for selfish motives. Every business organizations have to use laptops or pc's to carry out their daily tasks which are usually connected to a system network. Hacking such types of system may be able to bring about confidential data to the hacker's sleeve and they can use these data for making money by sending it to their competitors or even blackmailing them.

Digital forensics is the art of detecting the crime which takes place over the digital medium. It can be very similar to the original forensic techniques which are used to find out the evidences in a crime location. It is a structured investigation process through which evidences are collected reconstructed and presented in court. Digital forensics also defines tools and techniques which can be used against any hacker who are trying to enter the system without authentication.

Counterattacking can be termed as the art of giving reply to an unplanned attack or fighting against secret criminals to safeguard the information or property from getting stolen. Counterattack is basically a type of warfare which has been used from time memorial. The same principal is used in the digital platform and it is condensed in a more sophisticated way.

Motives can be defined as the behavioural pattern of any person or entity regarding a particular action. They can be for good or bad reason depending on the person in general. A good motive may include going by the systematic laws of the system and following the regulations and protocols which are predefined. A bad motive may include disobeying the laws of the system and making individual rules which may not coincide with the general rule system. When it comes to hackers they may be of both category. The good motive hacker may try to protect the system by hacking a hacker's system and a bad motive hacker may try to damage the system or steal information from them ignoring the later consequences of it.

LITERATURE REVIEW:

The virtual hacker underground is a world few people in society are intimately familiar with and it is difficult for them to understand the impact of certain types of illegal hacking activities. (Sarr, S. How to Minimize Hacking: Understanding the Motives of Hackers to Plan a Counter Attack and Prevention Techniques. *Concord McNair Scholars Research Journal*, 221.)

The psychology behind hacker getting involved in hacking can be investigated through a challenge-skill balance factor in the flow state of a hacker should be investigated experimentally by establishing diverse situations: high skill-high challenge, high skill, low challenge and low skill-low challenge. (Hyung -Jin Woo The Hackers Mentality: Exploring The Relationship between Psychological Variables And Hacking Activities Under The Direction Of Joseph. R. Dominick)

With attacker information available, companies find themselves in a dilemma-counter attack for immediate self-defense, retaliate for future deterrence, inform the

appropriate law enforcement authorities, or do nothing. We examine justification for the hack back self-defense and deterrence arguments in the context of current technology and legal framework. (Jayaswal, V., Yurcik, W., & Doss, D. (2002, June). Internet hack back: Counter attacks as self-defense or vigilantism?. In *IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293)* (pp. 380-386). IEEE.)

RESEARCH METHODOLOGY:

Discovery of Invasion

Discovery of any invasion occurs when an unauthorized user tries to invade the system and something or the other immediately detects it as soon as some unreliable behavior takes place in the system network .Digital forensic defines some useful techniques for the network administrators to actually build invasion uncovering systems to actually notice the movement of hackers. This usually gets executed when there is hell amount of traffic in the network region and the network administrator is soon alerted to be careful. They usually act as first gem of investigators which are identical to the police officers or the people involved in the fire brigade system. The invasion uncovering systems act as soon as something unusual activity is discovered and they try to analyze the cause of it. The attacks which may occur might be performed by a single black hat hacker or a group of hackers which have been deployed and backed by some government agencies to uncover crucial information. This is usually carried out with the administrators blocking a particular user from logging in or stopping the traffic which is coming from a particular network region. Though it may act successful in most scenarios still it's not a permanent solution because of the talent and experience of some hackers to actually prevent any clues of their personal identity.

COUNTERATTACKING THE HACKER BRUTALLY WITH BOOBY-STRAP

Digital forensics also defines the latest technique which is termed as booby-trap which is also sometimes called the hackers worst enemy .When any experienced hacker tries to invade the system they suffer from damage themselves. Booby-strap has its own disadvantages since it may attack and damage the system of some innocent victim analyzing them as some kind of hacker. Usually counterattacking is also an illegal activity and it should be only executed with the permission of government officials. Booby-strap is a tool which can be used by only top end systems who have secret recorded information about the government and country affairs. If someone is victimized by any cybercriminal it will better to report to the high authorities and take permission for the usage of this tool.

CONCLUSION:

If you try to analyze all the activities and the reports which are generated from the last few years regarding the attacks of hackers you will immediately understand how important it is to safeguard your system since no system is 100% free from loopholes .A single loophole may be enough for the experienced hacker to enter your system and achieve what they really desire. So it becomes a necessary factor to use the tools invented by the science of digital forensics to protect your system and safeguard the crucial information it contains. Also studying the hacker's psychology becomes a necessary factor since all entities are driven by emotions and have a similar structured pattern of mind.

No matter how aware you are as far as system security is concerned a smart hacker still find their way to detect the small loophole in your system and take that vulnerability factor in to their personal advantage. So the only way possible to be ahead of hacker is to learn hacking and their inbuilt techniques so that when you are securing the system you will consider all the necessary factors that is responsible to keep away the hacker from hacking your system.

FUTURE ENHANCEMENTS:

Artificial intelligence is the future weapon of counter attackers though a lot of development is still going on in this field and it's not yet properly structured and defined. They can be used to find the patterns to identify any deviation from it.

ACTIVE DEFENCE MEASURES (ADM) are developing more crystallized counterattacking weapons to fight against hacker's motive. A lot of these techniques would me made available to the normal public and business organizations in the nearby future.

QUANTUM COMPUTING are high speed computers with a tremendous computing power which can be used by the government agencies to protect their information. They can protect the current encryption technologies and can even cause a lot of havoc for the criminal hacker.

REFERENCES:

[1] "The Art of Memory Forensics" authors Andrew Case and Jamie Levy [2014]

[2] "Mobile Forensic Investigations" author Lee Reiber [2019]

[3] "Digital Forensic Diaries" author Mike Sheward [2017]

[4] "Practical Forensic Imaging" author Bruce Nikkel [2016]

[5] "Python Digital Forensics Cookbook" authors Preston Miller and Chapin Bryce [2017]

[6] "Digital and Document Examination" author Max. M. Houck [2018]

[7] "System Forensics, Investigation and Response" author Chuck Easttom [2017]

[8] "Big Data Forensics" author Joe Sremack [2015]

[9] "Network Forensics" authors Sherri Davidoff and Jonathan Ham [2012]

[10] "Cyber Forensics" authors Albert. J. Marcella Jr and Frederic Guillossou [2012]