A Study on Cyber Crime and Digital Forensics in Network Security

Vaishali Salvi[1], Sejal D'mello[2], Reena Somani[3], Pranoti Nage[4],Pragyamani Sharma[5]

[1](Department of Information Technology, University of Mumbai, India)
[2](Department of Information Technology, University of Mumbai, India)
[3](Department of Information Technology, University of Mumbai, India)
[4](Department of Information Technology, University of Mumbai, India)
[5](Department of Information Technology, University of Mumbai, India)

Abstract: *The progress of technology has made man dependent on Internet for all his needs. Internet has given man easy access to everything while sitting at one place. With increasing internet penetration, Cybercrime have also increased in the last few years. A Cyber Crime is a crime in which main objective of the crime is computer or it can be used as a tool to make an offence like cyber terrorism, credit card fraud. Cyber forensics is an electronic discovery technique used to determine and reveal technical criminal evidence. It often involves electronic data storage extraction for legal purposes. In this paper we overview about cyber forensics and network forensics.*

Keywords*-Cyber Crime, Cyber Forensics, Network Forensics, Network Security.*

I. Introduction

The development of the internet has also resulted into development of the concept of cybercrimes. Cybercrimes are committed in different forms. Cybercrimes can be defined as the unlawful acts in which the computers are used either as a tool for crime or a target or both. This generally includes financial crimes like credit card frauds, scams,sale of illegal articles; email spoofing,cyber terrorism, creation and/or distribution of viruses, Spam and so on. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

Cyber forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. Digital forensics is defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

II. Need For Digital Forensics

To be able to thoroughly investigate today's digital crime; computer forensics is needed to access the type of digitally encrypted and hidden information that is stored in computer hard drives and other types of digital storage. In a world of professional hackers and ingenious hacking techniques, it would be impossible to uncover needed evidence for digital and other types of crimes, without this form of forensic science.

Evidence uncovered through computer forensics is subject to the same legal guidelines as all other criminal evidence. It must be legally obtained to be admissible in court. Each country also has its own set of unique guidelines for use of computer forensic evidence, and this science has been utilized in some major criminal court cases since the mid 1980's. Examples of such cases are the BTK Killer, Dennis Rader, the case of the Corcoran Group, and in the criminal trial of Dr. Conrad Murray who was accused of negligence in the death of pop superstar, Michael Jackson.

In the digital times we live in today, it would be practically impossible to retrieve the kinds of evidence required to solve many of the cases brought forth to the court system in a digital era. Computer forensics science is an extremely reliable and helpful resource needed to try such cases in court.

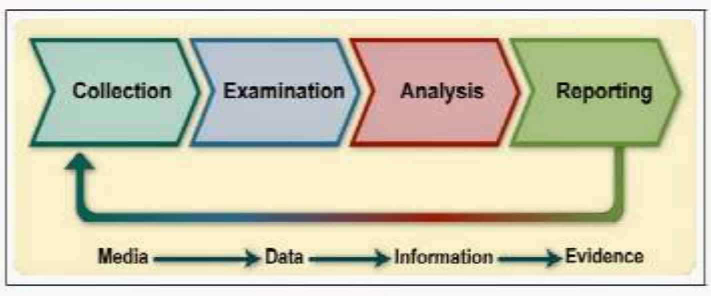
Computer forensic investigations require specialist skills which involves not just the preservation and identification of digital evidence but the correct interpretation of that evidence. When confronted with a forensic `investigation, organizations initially tend to focus on the costs involved. Yes there is an up- front cost and depending on the complexity of the investigation and the number of computers involved, it can appear to be expensive. However consider the following: Evidence that can only be obtained by a forensic examination can often prove vital to the successful outcome of the investigation.

III. DIGITAL FORENSICS INVESTIGATION PROCESSES

Digital forensics includes the process which applies computer science and technology to collect and analyze evidences that are crucial and admissible to cyber investigations. Network forensics is used to find out attackers' behaviors and trace them by collecting and analyzing log and status information. A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in the Cyberspace or digital world. The investigation process is as follows (as per National Institute of Standards and Technology) [1].

Figure 1 shows the complete phases of Digital Forensic investigation processes.

2.1 Collection phase: The first step in the forensic process is to identify potential sources of data and acquire forensic data from them. Major sources of data are desktops, storage media, Routers, Cell Phones, Digital Camera etc. A plan is developed to acquire data according to their importance, volatility and amount of effort to collect [2].



Fig[1]. Digital Forensic Investigation Process

2.2 Examination: Once data has been collected, the next phase is to examine it, which involves assessing and extracting the relevant pieces of information from the collected data [2].

2.3 Analysis:This is perhaps the most important part of the investigation process which involves careful examination and analysis of the data using forensic tools. In this Extracted and relevant data is analysed to draw conclusions. If additional data is sought for detail investigation will call for in depth data collection.

2.4 Reporting: The Reporting phase is when the evidence and your conclusion are presented to the person or group requesting the investigation.

IV. TYPES OF CYBER ATTACKS

There are literally a dozen ways in which a cybercrime can be perpetrated, and you need to know what they are. In order to protect yourself you need to know about the different ways in which your computer can be compromised and your privacy infringed. In this section, we discuss a few common tools and techniques employed by the cyber criminals. This isn't an exhaustive list by any means, but will give you a comprehensive idea of the loopholes in networks and security systems, which can be exploited by attackers, and also their possible motives for doing so.

Cybercrimes also share a number of common characteristics:

- ➢ Cybercriminals usually are located internationally, which makes finding and extraditing them difficult.
- ➢ Cybercrimes often are directed and targeted toward a specific person(s) or entity.
- ➢ Cyberattacks are multifaceted in terms of their tools, vectors and type, and at times, can lead to a cybercrime that is actually a combination of crimes.

If you've ever studied famous battles in history, you'll know that no two are exactly alike. Still, there are similar strategies and tactics often used in battle because they are time-proven to be effective.

Similarly, when a criminal is trying to hack an organization, they don't reinvent the wheel unless they absolutely have to. They'll draw upon a common arsenal of attacks that are known to be highly effective, such as malware, phishing, or cross-site scripting (XSS). Whether you're trying to make sense of the latest data breach headline in the news or analyzing an incident in your own organization, it helps to understand the different ways an attacker might try to cause harm. Here's an overview of some of the most common types of attacks seen today.

Malware

If you've ever seen an antivirus alert pop up on your screen, or if you've mistakenly clicked a malicious email attachment, then you've had a close call with malware. Attackers love to use malware to gain a foothold in users' computers—and, consequently, the offices they work in—because it can be so effective.

"Malware" refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base.

Attackers will use a variety of methods to get malware into your computer, but at some stage it often requires the user to take an action to install the malware. This can include clicking a link to download a file, or opening an attachment that may look harmless (like a Word document or PDF attachment), but actually has a malware installer hidden within.

SQL Injection Attack

SQL (pronounced "sequel") stands for structured query language; it's a programming language used to communicate with databases. Many of the servers that store critical data for websites and services use SQL to manage the data in their databases. A SQL injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn't. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information, which are tempting and lucrative targets for an attacker.An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.

Cross-Site Scripting (XSS)

In an SQL injection attack, an attacker goes after a vulnerable website to target its stored data, such as user credentials or sensitive financial data. But if the attacker would rather directly target a website's users, they may opt for a cross-site scripting attack. Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.

One of the most common ways an attacker can deploy a cross-site scripting attack is by injecting malicious code into a comment or a script that could automatically run. For example, they could embed a link to a malicious JavaScript in a comment on a blog.

Cross-site scripting attacks can significantly damage a website's reputation by placing the users' information at risk without any indication that anything malicious even occurred. Any sensitive information a user sends to the site—such as their credentials, credit card information, or other private data—can be hijacked via cross-site scripting without the website owners realizing there was even a problem in the first place.

Denial-of-Service (DoS)

Imagine you're sitting in traffic on a one-lane country road, with cars backed up as far as the eye can see. Normally this road never sees more than a car or two, but a county fair and a major sporting event have ended around the same time, and this road is the only way for visitors to leave town. The road can't handle the massive amount of traffic, and as a result it gets so backed up that pretty much no one can leave.

That's essentially what happens to a website during a denial-of-service (DoS) attack. If you flood a website with more traffic than it was built to handle, you'll overload the website's server and it'll be nigh-impossible for the website to serve up its content to visitors who are trying to access it.

This can happen for innocuous reasons of course, say if a massive news story breaks and a newspaper's website gets overloaded with traffic from people trying to find out more. But often, this kind of traffic overload is malicious, as an attacker floods a website with an overwhelming amount of traffic to essentially shut it down for all users.

In some instances, these DoS attacks are performed by many computers at the same time. This scenario of attack is known as a Distributed Denial-of-Service Attack (DDoS). This type of attack can be even more difficult to overcome due to the attacker appearing from many different IP addresses around the world simultaneously, making determining the source of the attack even more difficult for network administrators.

Session Hijacking and Man-in-the-Middle Attacks When you're on the internet, your computer has a lot of small back-and-forth transactions with servers around the world letting them know who you are and requesting specific websites or services. In return, if everything goes as it should, the web servers should respond to your request by giving you the information you're accessing. This process, or session, happens whether you are simply browsing or when you are logging into a website with your username and password.

The session between your computer and the remote web server is given a unique session ID, which should stay private between the two parties; however, an attacker can hijack the session by capturing the session ID and posing as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server. There are a number of methods an attacker can use to steal the session ID, such as a cross-site scripting attack used to hijack session IDs.

An attacker can also opt to hijack the session to insert themselves between the requesting computer and the remote server, pretending to be the other party in the session. This allows them to intercept information in both directions and is commonly called a man-in-the-middle attack.

Credential Reuse

Users today have so many logins and passwords to remember that it's tempting to reuse credentials here or there to make life a little easier. Even though security best practices universally recommend that you have unique passwords for all your applications and websites, many people still reuse their passwords—a fact attackers rely on.

Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in. No matter how tempting it may be to reuse credentials for your email, bank account, and your favorite sports forum, it's possible that one day the forum will get hacked, giving an attacker easy access to your email and bank account. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to managing the various credentials you use.

This is just a selection of common attack types and techniques (follow this link to learn more about web application vulnerabilities specifically). It is not intended to be exhaustive, and attackers do evolve and develop new methods as needed; however, being aware of, and mitigating these types of attacks will significantly improve your security posture.

V. CYBER THREATS

Hackers are constantly finding new targets and refining the tools they use to break through cyberdefenses. The following are some significant threats to look out for year 2018.More huge data breaches The cyberattack on the Equifax credit reporting agency in 2017, which led to the theft of Social Security numbers, birth dates, and other data on almost half the U.S. population, was a stark reminder that hackers are thinking big when it comes to targets. Other companies that hold lots of sensitive information will be in their sights in 2018. Marc Goodman, a security expert and the author of Future Crimes, thinks data brokers who hold information about things such as people's personal Web browsing habits will be especially popular targets. "These companies are unregulated, and when one leaks, all hell will break loose," he says.

Ransomwarein the cloud :The past 12 months have seen a plague of ransomware attacks, with targets including Britain's National Health Service, San Francisco's light-rail network, and big companies such as FedEx. Ransomware is a relatively simple form of malware that breaches defenses and locks down computer files using strong encryption. Hackers then demand money in exchange for digital keys to unlock the data. Victims will often pay, especially if the material encrypted hasn't been backed up.

That's made ransomware popular with criminal hackers, who often demand payment in hard-to-trace cryptocurrencies. Some particularly vicious strains, such as WannaCry, have compromised hundreds of thousands of computers (see "The WannaCry Ransomware Attack Could've Been a Lot Worse"). One big target in 2018 will be cloud computing businesses, which house mountains of data for companies. Some also run consumer services such as e-mail and photo libraries. The biggest cloud operators, like Google, Amazon, and IBM, have hired some of the brightest minds in digital security, so they won't be easy to crack. But smaller companies are likely to be more vulnerable, and even a modest breach could lead to a big payday for the hackers involved.

Theweaponization of AI

This year will see the emergence of an AI-driven arms race. Security firms and researchers have been using machine-learning models, neural networks, and other AI technologies for a while to better anticipate attacks, and to spot ones already under way. It's highly likely that hackers are adopting the same technology to strike back. "AI unfortunately gives attackers the tools to get a much greater return on their investment," explains Steve Grobman, chief technology officer at McAfee.

An example is spear phishing, which uses carefully targeted digital messages to trick people into installing malware or sharing sensitive data. Machine-learning models can now match humans at the art of crafting convincing fake messages, and they can churn out far more of them without tiring. Hackers will take advantage of this to drive more phishing attacks. They're also likely to use AI to help design malware that's even better at fooling "sandboxes," or security programs that try to spot rogue code before it is deployed in companies' systems.

Cyber-physical attacks

More hacks targeting electrical grids, transportation systems, and other parts of countries' critical infrastructure are going to take place in 2018. Some will be designed to cause immediate disruption (see "A Hack Used to Plunge Ukraine into Darkness Could Still Do Far More Damage"), while others will involve ransomware that hijacks vital systems and threatens to wreak havoc unless owners pay swiftly to regain control of them. During the year, researchers—and hackers—are likely to uncover more chinks in the defenses of older planes, trains, ships, and other modes of transport that could leave them vulnerable.

Mining cryptocurrencies

Hackers, including some allegedly from North Korea, have been targeting holders of Bitcoin and other digital currencies. But the theft of cryptocurrency isn't the biggest threat to worry about in 2018; instead, it's the theft of computer processing power.

Mining cryptocurrencies requires vast amounts of computing capacity to solve complex mathematical problems. As my colleague Mike Orcutt has noted, that's encouraging hackers to compromise millions of computers in order to use them for such work (see "Hijacking Computers to Mine Cryptocurrency Is All the Rage"). Recent cases have ranged from the hacking of public Wi-Fi in a Starbucks in Argentina to a significant attack on computers at a Russian oil pipeline company. As currency mining grows, so will hackers' temptation to breach many more computer networks. If they target hospital chains, airports, and other sensitive locations, the potential for collateral damage is deeply worrying.

Hacking elections

Fake news isn't the only threat facing any country running an election. There's also the risk of cyberattacks on the voting process itself. It's now clear that Russian hackers targeted voting systems in numerous American states ahead of the 2016 presidential election . With midterm elections looming in the U.S. in November, officials have been working hard to plug vulnerabilities. But determined attackers still have plenty of potential targets, from electronic voter rolls to voting machines and the software that's used to collate and audit results.

VI. Conclusion

Digital forensics is an important field in current days. This paper gives detailed study of cybercrime and digital forensics.We have described need and steps followed in digital forensics investigation process. In this paper lists various cyberattacks. Further we have discussed about various cyber threats. As the number of Internet users are increasing rapidly frequencies of cybercrimes have increased. Development of efficient tools to detect these attacks is required. The knowledge of digital forensics will help users of computer and Internet in various aspects like court cases and investigation process.

References

[1] K. Kent, S. Chevaller, T. Grance and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST SP800-86 Notes, 2006.

[2] S. K. Brannon and T. Song, Computer Forensics: Digital Forensic Analysis Methodology,Computer Forensics Journal, Vol. 56, No. 1, 2008, 1-8.

[3] Stephenson, P. . Cyber Investigation. In S. Bosworth, M. Kabay, & E. Whyne, Computer Security Handbook, (Hoboken: John Wiley & Sons, Inc., 2009) 55.1 - 55.27.

[4] D. Birk and C. Wegener, Technical issues of forensic investigations in cloud computing environments, Proceedings of the Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2011.

[5] Casey, E. Digital Evidence and Computer Crime. Academic Press. 2001

[6] Casey, E. Handbook of Computer Crime Investigation: Forensic Tools and Technology. Academic Press 2002.

[7] Kruse, W.G. III, &Heiser, J.G, Computer Forensics : Incident Response Essentials. Addison-Wesley 2002.

[8] Mandia, K., Prosise, C., & Pepe, M, . Incident Response: Investigating Computer Crime. Osborne, 2002.

[9] Muhammad Shamraiz Bashir and M. N. A. Khan, Triage in Live Digital Forensic Analysis, The International Journal of Forensics Computer Science, 2013.

[10] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and F. Daryabar, Digital Forensic Trends &Future,International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 2, no. 2, 48–76, 2013.