JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cybersecurity: Various methods and techniques of Cybercrime

Prabhakar Pal[1], Vinit Mehta[2]

[1]*BE Electronics and Telecommunication Engineering Student, Atharva College of Engineering, Mumbai, India, Mumbai University*

[2]*BE Electronics and Telecommunication Engineering Student, Atharva College of Engineering, Mumbai, India, Mumbai University*

Abstract:

In the modern times with an exponential increase in digitization, the world is reaching new heights in computerization and networking as each and every being is interconnected to each other via some network to increase efficiency and advancements. The digital era has many merits which supports the new technological demands of the world, but with merits there are also obstacles which might hinder the usual workflow of the environment. Many intruders, hackers or unethical users of this digital platform can exploit to harm the system or network of another person. These intruders generally hack the system for a ransom in return. So, we must analyze all the different types of attacking methods, tools, techniques and study them thoroughly to protect our digital data, platform and devices.

Keywords: *Security, Intruder, Hacker.*

I. Introduction:

Cybersecurity is currently the need of the hour. Cybersecurity is needed when we're trying to fight against the various Cybercrimes. If we define both these terms then Cybercrime can be termed as "It is crime done in cyberspace using digital devices or computers as an Instrument" and Cybersecurity means securing or protecting information, equipment devices, computers and its resources against unauthorized access, modification, disruption, disclosure or destruction. Criminals use many methods and tools to locate the vulnerabilities of their target. Further, we will look into various methods and tools used.

II. Planning of an Attack:

The attacker generally follows a three step process which are: 1. Reconnaissance 2. Scanning and Scrutinizing 3. Launching an attack.

1. Reconnaissance is an act of exploring to find someone or something. Reconnaissance phase begins with Footprinting. Footprinting involves gathering information about the target's environment to penetrate it. It provides an overview of system vulnerabilities. The objective of this phase (reconnaissance) is to understand the system, its networking ports and services, and any other related data.

2. Scanning involves intelligent examination of gathered information about the target. The objectives of scanning are: Port scanning, Network scanning, Vulnerability scanning

Scrutinizing is also called enumeration. 90% of the time in hacking is spent in reconnaissance, scanning and scrutinizing information. The objectives are: Find valid user accounts or groups, Find network resources or shared resources, OS and different applications running on the target

3. Launching an attack:

An attack follows the below steps: Crack the password, Exploit the privileges, Execute malicious software (backdoor), Hide or destroy files (if required), Cover the tracks.

III. Various Methods:

Here we discuss about various methods which are used by hackers or attackers to accomplish their attack:

1. Social Engineering:

Engebretson defines social engineering as one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherent to every organization. In essence, social engineering refers to the design and application of deceitful techniques to deliberately manipulate human targets. In a cyber security context, it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information. The basis of a social engineering attack is to avoid cyber security systems through deceit, exploiting the weakest link, the people involved. Throughout the interaction, victims are unaware of the destructive nature of their actions. The social engineers exploit innocent instincts, not criminals. Explicit methods such as threats or bribery do not fall within the scope of social engineering. A talented practitioner of this discipline understands and perceives social interaction patterns to manipulate the psychological aspects of the human mind. With this resolution, the attacker is capable of executing an efficient and cheap security compromise, without the need to invest in breaking technical security measures. Nevertheless, an educated social engineer on computer science may also complement technological means to the attack in order to accomplish malicious intentions.

1.1 Categories

A social engineering attack can be classified by one of two possible categories, hunting and Farming.

1.1.1 Hunting

This approach seeks to execute the social engineering attack through minimal interaction with the target. Once the specified objective is achieved and the security breach is established, communication is likely to be terminated. This is the most frequently used methodology to support cyber attacks and as a rule, the modus operandi involves a single encounter.

1.1.2 Farming

Social engineering farming is not often practiced, nevertheless this technique may be used for situational purposes. The attacker aims to establish a relationship with the victim in order to extract information for a longer period of time. Throughout the process, the interaction can change, the target may learn the truth and the social engineer may attempt to bribe or blackmail the target, thus resorting to traditional criminal behavior.

1.2 Phases:

In order to achieve a specified objective, social engineering attacks can range from a single encounter to a series of operations, possibly involving several threat actors, intended to gather fragments of related information from different sources. Attacks of this nature, even if dependent on a sole interaction typically consist of four distinct phases: research, hook, play and exit.

1.2.1 Research:

Regularly, the operation initiates with the phase of reconnaissance, studying and gathering as much information as possible about the people and business model associated with the target. A well known sentence from Sun Tzu in The Art of War is: "Know your enemy", knowledge is power and in the context of cyber security, the investment on this stage can be invaluable to unveil possible vulnerabilities. Nevertheless, rather than executing a targeted attack, an experienced social engineer is capable of exploiting chance encounters, and thus opening further opportunities with no research prior to that point.

1.2.2 Hook

In this phase, the threat actor initiates the communication with the potential victim. He engages
the target, spins the story, builds a level of intimacy and takes control of the interaction.

1.2.3 Play

The play aims to accomplish the purpose of the attack, which can be to extract information or to manipulate the target in order to compromise the system.

1.2.4 Exit

Lastly, the social engineering finalizes the interaction with the victim, preferably without arousing any suspicions. After this last phase, the attacker is typically very difficult to track down.

2. Phishing:

Phishing is the act of attempting to pay off information such as username, password and credit card details as a trustworthy entity in an electronic communication. Communication purporting to be from popular social websites, auction sites, online payments process or IT administrator is commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is an example of Social Engineering. Phishing is mainly used in email hacking, in email phishing the hacker sends a link via mail to the user of let's say some bank details or any personal information, so now the user goes to that link and fills all the details in that link and then the hacker gets all the information of the user. This is how phishing is done.

Phishing is explained step-by-step:

1. Attacker sends an email to the victim.
2. Victim clicks on the email and goes to a phishing website.
3. Attacker collects victim's credentials.
4. Attackers use the victim's credentials to access a website.

Phishing starts with an email or other communication type that is designed to help in attacking the victim. The message is made as if that message is coming from a trusted sender. If it fools the victim, the victim is providing the personal information to a spam website. Sometimes malware is also downloaded onto the target's computer. Further we discuss some types of Phishing.

Types of Phishing:

2.1 Deceptive Phishing: This is a most common type of phishing, in this type the attackers impersonate a legitimate company and try to steal people's personal information or their login passwords. And then they blackmail the users to do as the hacker wants.

2.2 Spear Phishing

Wireless based Intrusion Detection Prevention System analyzes the traffic of wireless networks by analyzing wireless protocol activities and taking appropriate actions. It detects unauthorized wireless local area networks in use. It cannot identify suspicious activity in the application layer, transport
layer and protocol activities. It is deployed in a particular range where the organization can monitor the wireless network.

2.3 Clone Phishing

Clone phishing is one of phishing attacks where a legal or a previously gained email contains the attachment and link shared, recipients address (es) taken and used to create the same identical or cloned email. That attachment or link within the mail is replaced with some external malicious version and then sent to the victim from an email address spoofed to appear to come from the original sender. This technique can be used to pivot (indirectly) from the infected machine and take all the information or can gain a foothold on another machine.

3. Malware Attack:

Malicious software is any program that causes harm to a user, system, computer, or network, such as Trojan horses, Worms, Viruses, Rootkits,... and Scareware (Honig 2012). These malwares are not exclusive types.. However, as long as the computer system is constantly evolving with increasing use in all areas of modern life, it has become fundamental to the success of the political, economic, military, and personal objectives. Therefore, it is necessary to protect the computer system from security threats.

3.1 Virus:

Malicious code usually hides within another seemingly innocuous executable program and that autonomously produces copies of itself, which might even modify copies and inserts them into other executable programs or on a victim machine once introduced to the system. Viruses cannot transmit themselves to a new machine autonomously, they require human intervention. It is transported via storage devices, peer to peer clients or the internet.

3.2 Worms:

A malware program that replicates itself in order to spread across the entire network of computers without user intervention or authorization and it is stand-alone. Deceive novice users through the use of the attractive title Email. Worms spread via communication media such as Email, exploit the computers and network vulnerability by using network or computer resources and worms spread via storage devices.

3.3 Trojan Horse:

Trojans mask themselves by appearing to be something legitimate. They hide silently on the infected computer machines, while the computer's users continue with their usual activities. If a program just bypasses remote access, it is considered a backdoor. But, if the malware authors work to gild these backdoor capabilities as some other legal program, then it considers Trojan horse. Trojan horse spreads through user interaction by tricking the victim into downloading or opening an e-mail attachment and installing it, then attacks, often providing a rootkit and the attacker runs the Trojan from the internet. Note it is not self-replicated.

3.4 Botnet:

Remotely controlled autonomous software that permits the remotely access to the computer system by an attacker. However, all machines that are infected with the particular botnet are controlled by a single command-and control server. Botnet infrastructures consist of hundreds, thousands, or even millions of computer hosts that are all under one control of attackers. Botnets are usually delivered via infected internet web pages, or download links to malicious websites.

3.5 Scareware:

Malware designed to scare victims by showing fake security warnings on their computers, and urges users to buy useless, commercial versions of their software to rid bogus. It generally has a user interface that could be looked at as a legitimate antivirus AV or other security software. It warns computer users that there is malware on their computers without scanning the victims' file systems. It differs from crude AV in that it doesn't detect malicious software, while crude AV detection quality is not good enough to apply it in practice. It can be installed by the user when downloading bogus security software, opening spam attachments, by visiting a malicious website or even from famous download sites that are sometimes exploited.

4. DoS and DDoS:

4.1 DoS

In this attack, the attacker keeps on sending or makes the network or bandwidth overflow.By emails or spam mail, but depriving the victim to access services. It is a continuous effort of attackers to make victims unable to see any Internet service or resources. Target for website or services which include financial side, banks site or credit card give systems. The targeted network which are root for DOS or mobile phone network or credit card Gateway network. Buffer overflow.Technique is used to make denial service attack.What attacker does is it takes packets or is divided into small chunks. The attacker checks for the IP address of a particular network in that packet and floods the victim's network with repeated requests as the IP is fake from the attacker's machine. It consumes bandwidth which lets other services fail or unavailable for another user. Now we discuss two types of DoS attack:

4.1.1 Flood Attack:

That keeps on flooding or overloading victims' systems with numbers of ping packets which results in two huge traffic which the victim itself cannot handle. It is very simple to launch but difficult to handle.

4.1.2 Ping of Death Attack:

Sending huge ICMP packet.These packets are used in the IP layer or network layer for indicating error messages. The attacker sends these huge oversize packets to the victim system which causes the victim system to crash or freeze resulting in DOS.

4.1.3 ICMP Flood:

Ping Flood, also known as ICMP Flood, is a common denial of service attack in which an attacker takes down a victim's computer by overpowering it with an ICMP echo request, also known as pinks. Involves flooding the victims network with request packets, knowing that the network will react with an equal number of reply packets. Additional methods for bringing down our target with ICMP request includes this use of conventional tools or code such as hping and scappy. This strains both the incoming and outgoing channels of the network, consuming considerable bandwidth and resulting in a denial of service.

4.1.4 UDP Flood:

A UDP flood attack is a denial of service attack using the User Datagram Protocol, a connectionless computer networking protocol. Using UDP for denial of service attacks is not as easy as the transmission control protocol. However, a UDP flood attack can be initiated by sending a huge number of UDP packets to random ports on a remote host. As a result, the distant host will verify for the application listening at the port; see that no application is listening at the port; reply with an ICMP destination unreachable packet. Thus, for a large number of UDP packets, the ill-treated system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients. The attackers may also spoof the IP address of the UDP packets, ensuring that the unnecessary ICMP return package does not reach them and anonymizing their network locations. Most operating systems ease this part of attack by limiting the rate at which ICMP responses are sent.

4.2 DDoS:

A distributed denial of service attack is an attack in which multiple compromised computer systems attack targets such as server, website or other network resource and cause a denial of service for users of the targeted resource. The flood of incoming message connection requires or malformed packets to the target system.Use it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

5. SQL Injection:

In this era, websites have become the most essential part of our lives. Among the top most security threats SQL Injection attack ranks top based on OWASP Top 10 security vulnerability report. Through these websites we insert a number of personal data which gets stored in the database. We can access it from anywhere using a network. This opened the gate for the attackers to grab those data from vulnerable web pages. To find those vulnerable web pages the attackers can find many efficient tools like botnets which generate the list of vulnerable web pages. Once the webpage is detected the attacker starts to steal the data using SQL Injection attack. Webpage detection is mainly done to intrude inside the database. So they target the webpage which is connected with the back end database. It is a source code injection technique in which malicious SQL statements are inserted into the entry field of a database to dump database content. Attacker targets the database organization where confidential data is stored. Its main focus is to get information from the database stored in the database table by sending malicious queries since the database can be accessible by query.When a legitimate user enters an additional database via web form, the attacker sets its own command through the same web form field. The attackers before proceeding always checks whether the organization's database has any loop. Is it vulnerable or not?

IV. Conclusion

Overall in this paper, we have discussed various methods of attacks, how the attacker plans the attack and some other aspects. But, the cybercrime doesn't end here, a well trained, professional team of cybersecurity experts are important to handle these incidents and crimes. Here, the Ethical Hacker’s come into play. With vast knowledge about the field, they can help the common people to deal with these criminals. Also, as a society we all should start addressing the need of cyber knowledge and how crime takes place. We have only discussed the crimes and not the prevention techniques, which is also needed.

V. References:

1. Breda, Filipe, Hugo Barbosa, and Telmo Morais. "Social engineering and cyber security." *International Technology, Education and Development Conference*. Vol. 3. No. 3. 2017.

2. Bhavsar, Vaishnavi, Aditya Kadlak, and Shabnam Sharma. "Study on phishing attacks." *Int. J. Comput. Appl* 182 (2018): 27-29.

3. Bhaya, Wesam S., and Mustafa A. Ali. "Review on Malware and Malware Detection Using Data Mining Techniques." *Journal of University of Babylon for Pure and Applied Sciences* 25.5 (2017): 1585-1601.

4. Z. Chao-yang, "DOS Attack Analysis and Study of New Measures to Prevent," 2011 International Conference on Intelligence Science and Information Engineering, 2011, pp. 426-429

5. Halfond, William G., Jeremy Viegas, and Alessandro Orso. "A classification of SQL-injection attacks and countermeasures." *Proceedings of the IEEE international symposium on secure software engineering*. Vol. 1. IEEE, 2006.