International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

Survey on Various Types of Cyber Attacks and its Detection and Prevention

Manav Patel

Fourth Year B.Tech Integrated, NMIMS'S MPSTME

Abstract - *Security is the biggest challenging approach in today's internet accessible technologies like, mobile phones, webmail, instant messaging services, and removable storage media. Internet access has given the ability to easily carry and handle the large amounts of data. With the growing technologies, the usage of internet increases along with the threats/data breaches like view or modify the confidential data by an unauthorized entities. Though the technology increases, there is no guarantee for the overall security. Every web application contains vulnerabilities and it is the most crucial area for the intruders to place cyber attacks on it. These attacks are very harmful for the society. They involve creating financial theft, data threats, blackmailing, resource upholding and many more. This paper provides the approaches to identify, detect and taking preventive measures for the eradication of attacks. For this available tools and scanners can also be used in the present world scenario. SQL injection, DNS attacks and DoS attacks are emphasized towards implementation since the risk encountered is more in such attacks.*

1. INTRODUCTION

Security is the biggest challenging approach in today's internet accessible technologies like, mobile phones, webmail, instant messaging services, and removable storage media. Internet access has given the ability to easily carry and handle the large amounts of data. With the growing technologies, the usage of internet increases along with the threats/data breaches like view or modify the confidential data by an unauthorized entities. Though the technology increases, there is no guarantee for the overall security.

Cyber attacks are increasing from day to day. New variety of cyber attacks are also been heard every day. Rather than their supplementation, their growth is more spreading. The range of their effect starts from a device and spoiling the user credentials with various data thefts. Data loss is the main aim of such attacks that can affect a business, financial organization, enterprise, information portal, web sites etc. Measures must be taken to stop unauthorized users (hackers) from accessing any part of a system. Only then there can be an assurance of a system which guarantees proper authentication and access controls.

2. Types of Cyber Attack

2.1 SQL INJECTION ATTACK

SQL injection attack is an interruption attack, active attack too. It affects the resources and data in computing. Today's most businesses are worked out on internet. Such attack may use malicious SQL code; insert nested queries, queries with different clauses, linking two or three databases for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including private details or other particulars. This attack usually begins at the initial phase of the platform in execution. It stays active on web platforms that employ database services. Likewise users start the experience from logging onto the website and further pages. If considered from login page onwards, the attacker uses logical SQL statements in the username and password fields to get successfully login. The statements like or true 1=1, or true# are used for doing SQL injection. These statements are directly stored on to the database connection which are SQL statements and make these statements vulnerable. This sort of vulnerability occurs in database layers of an application and allows users to login successfully. The attackers thus meet the target and gets access to user credentials.

The so-called SQL injection is to cheat the server to execute malicious SQL commands by inserting SQL commands into the query string of Web form submission or input domain name or page request. For example, many previous video websites leaked VIP membership passwords mostly by submitting query characters via WEB form, which is particularly vulnerable to SQL injection attacks when the application program. SQL injection attacks occur when dynamic SQL statements are constructed using input content to access the database. SQL injection also occurs if the code uses stored procedures, which are passed as strings the website database through the SQL injection attack, and then they can get all the data in the website database. Malicious hackers can tamper with the data in the database through the SQL injection function and even destroy the data in the database. As a web developer, you hate this kind of hacking. It's necessary to understand the principle of SQL injection and learn how to protect your website database by code.

2.1.1 PREVENTITION AND DETECTION OF SQL INJECTION ATTACK

Detection

Checking of Log files is one of the best way to detect the SQL injection attack. It shows whether the SQL injection has occurred or not. A log file is extremely important information provided by the server. The log file records the events and activities during the runtime of a service or an application. The changes that are made in the database from time to time will be recorded in the log file. The admin regularly checks the log files of the database to see what operations are performed in the database and by whom it is made. If the external entity performs any operations on the database, the admin checks it and rollback those operations by estimating that the attacker has done.

Prevention

The reason of SQL injection is that the SQL statements are not written properly and special characters are filtered in the process of program development. As a result, the client can submit some SQL statements through global variables POST and GET to execute normally,

The methods to prevent SQL injection are as follows:

Open the magic_quotes_gpc and magic_quotes_runtime settings in the configuration file, Use add slashes to convert SQL statements when executing SQL statements, Sql statement writing should not omit small quotation marks and single quotation marks as far as possible, filter out some keywords in SQL statements: update, insert, delete, select,.*, Improving the naming skills of database tables and fields, naming some important fields according to the characteristics of the program, which is difficult to guess. Set register_globals to off in the Php configuration file to close global variable registration. Control error information, do not output error information on the browser, write error information to the log file. Filter out some common database operation keywords: select, insert, update, delete, and *, or filter through system function: addslashes (content that needs to be filtered). Register_globals = off in the PHP configuration file; the registered global variable is closed when set to close state//action. For example, the value of a POST form is received using $_POST ['user'], if register_globals = on; the value of a form can be received directly using $user. When writing SQL statements, try not to omit small quotation marks (the one above the tab key) and single quotation marks. Improve database naming skills, for some important fields according to the characteristics of the program naming, not easy to guess. Encapsulate common methods to avoid direct leaking of SQL statements. Open the PHP security mode Safe_mode=on; Open magic_quotes_gpc to prevent SQL from being injected into Magic_quotes_gpc=off; the default is closed, it will automatically convert the query of the SQL statement submitted by the user after opening, which will play an important role in preventing SQL injection. So open: magic_quotes_gpc=on; Control error information Close the error message and write it to the system log. Pretreatment with mysqli or pdo.

2.2 DNS ATTACK

Domain Name Server (DNS) is the main block of the internet. It allows users to access websites and visualize the information.

It converts everything into IP addresses and customizes the users. Attacks on DNS are on the rise from both the outside and the inside an organization. In fact, a recent study found that DNS attacks grew by 600% in 2011 alone. These attacks include holding up resources for long durations, diverting traffic towards malicious links, flooding the system with traffic, masking the IP addresses etc. In case of a web server, this attack diverts the traffic and routes it to other IP address other than the original IP address of webserver. This is done by inserting the wrong IP address and wrong DNS cache in the DNS server.

The objectives of the DNS attack on web are :

- Makes a computing system unavailable
- Overload the web server and sometimes they may even crush or get damaged
- Corrupts users details
- Changes the original IP address of a web server- Changes the IP address of web server and renames DNS server too
- Targets and provides access to users source address, uses victims infrastructure up to any extent.

2.2.1 PREVENTITION AND DETECTION OF DNS ATTACK

Detection

It is very easy to detect the reflected amplification attack because of its noisy nature of volumetric attacks, but it is very difficult to prevent it because the responses come from legitimate sources.

DNS Hardening and avoiding misconfigurations: When DNS servers are installed for the first time, often they left in the default state and exposed to the Internet. Always a misconfigured public recursive resolver is exploited to participate in a DNS amplification attack. The default configuration of DNS server always allow recursion for all clients, this can be exploited by attackers for an amplification attack. The application hardening involves: keep DNS servers up-to-date, hide the DNS version, limiting the recursion to authorized clients, use isolated DNS servers.

Rate Limiting: This is a general category of DDoS mitigation strategy. The rate limit of the UDP fragment packets of the

normal traffic to the DNS server is monitored. When the UDP fragment packet rate is more than this limit, the packets are simply dropped. This approach of Rate limiting at the source is more effective as it is done based on deviation from the access policy. Regular Expression (Regex) Filter: One of the most effective and common defense against amplification attacks is applying traffic signature filters. These attacks have identifiable repetitive structure from which a regular expression can be derived. One of the disadvantages of this type of filter is performance. In this case, DDoS defenses should be kept at every edge of the network and must observe and drop the packet. Every packet should be inspected to provide a defense mechanism using this method.

Threat Intelligence: Attackers continuously scan the internet looking for servers to employ in their DDoS campaigns. The identification of these vulnerable servers is available as a real-time feed from the threat intelligence organization. Knowing these IP addresses and blocking these vulnerable servers is an effective and productive way to mitigate attacks.

Port Blocking: It is always good to block the unwanted ports. There will be some ports that can be shared by both the authorized user and the attacker traffic. DNS is the best example of that because it uses port 53 for both TCP and UDP. Blocking the port no.53 has the same effect as a DoS attack on the surroundings.

Prevention
DNS servers should be kept updated and checked regularly to ensure that their security patches are up-to-date. The network admin should restrict the external users to prevent cache poisoning. The DNS cache should be cleared on both local and shared networks. Installing a robust firewall is one of the best ways to prevent from DNS attack. Apart from firewall protection, it is also best to host the organization's architecture on different servers such that if one server is attacked by DDoS, the other server should immediately take over to survive the attack.

2.3 DOS ATTACK

Denial of service (DoS) is to make sure that a particular is busy and hence unavailable. It is performed to stop the services. This attack is generally performed on a server, Wi-Fi router, Bluetooth host, etc. The attack is done by sending huge amount of useless traffic to the destination server in the form of ICMP echo requests until the destination server gets down. In such a situation, the targeted server cannot process bulk requests at a time. The same attack if made on the Google server, it doesn't go down Google server maintains cloud of servers and the sent traffic shall be distributed amongst them.

The objectives of DoS attack are :

- Slows downs a machine or a network
- Shuts down the network
- Data is inaccessible
- No sharing of resources
- Loss of information or user assets
- Exploit bugs
- Amplifies the traffic
- Denies access to legitimate users

2.3.1 DETECTION ON DOS ATTACK

An anomaly based DoS attack detection system using multivariate correlation analysis approach is proposed in this paper. Network traffic exhibits some statistical correlative properties which can be used in DoS attack detection. Triangle area map technique is used to extract this correlation.

In complete detection process sample-by-sample detection is used.

Following are the three main steps:

Step 1 : Traffic records are formed from the network traffic which enters the internal network where protected servers resides.
Step 2: In this step triangle area map technique is used to draw correlation between the traffic records. This correlation is used by multivariate correlation analysis for detecting any intrusive behavior.
Step 3: This is the detection step. In the training phase, legitimate traffic records are used to form normal profile. In the testing phase test records are used to form test profiles. Test profile for every test record is formed. This test profile is compared with the normal profile of training phase. The dissimilarity between the normal profile and test profile is an indication of some kind of intrusive behaviour. Here a threshold value is used. If the dissimilarity is greater than the threshold value than it is flagged as an attack

The technique can help to detect trivial DoS attacks when conversations between an attacker and the web server deviate from normal user behavior patterns. However, if the attacker is able to mimic properly the browsing behavior of a regular human user, conversations related to this attack might belong to one of the clusters of the normal behavior model and, therefore, remain undetected. In this case, the way how feature vectors are distributed across clusters should be taken into consideration. This vector distribution during an attack can differ markedly from the vector distribution corresponding to legitimate traffic. Thus, we can define whether a computer or network system is under attack during the current time interval, and, moreover, find clients responsible for initiating conversations related to the attack. For this purpose, we group all conversations which

have the same source IP address, destination IP address and destination port together and analyze each such group separately. Such approach is in-line with studies mentioned in.Those studies analyze sequences of conversations (requests) belonging to one HTTP session. In our case, since the session ID cannot be extracted from encrypted payload, we focus on conversations initiated by one client to the destination socket during some short time interval. We can interpret a group of such conversations as a rough approximation of the user session.

3. CYBER ATTACK PREVENTION

High-profile cyber-attacks on companies such as Target and Sears have raised awareness of the growing threat of cybercrime. Recent surveys conducted by the Small Business Authority, Symantec, Kaspersky Lab and the National Cyber security Alliance suggest that many small business owners are still operating under a false sense of cyber security.

The statistics of these studies are grim. The vast majority of U.S. small businesses lack a formal Internet security policy for employees and only about half have even rudimentary cyber security measures in place. Furthermore, only about a quarter of small business owners have had an outside party test their computer systems to ensure they are hacker proof and nearly 40 percent do not have their data backed up in more than one location.

4. DO NOT EQUATE SMALL WITH SAFE

Despite significant cybersecurity exposures, 85 percent of small business owners believe their company is safe from hackers, viruses, malware or a data breach. This disconnect is largely due to the widespread, albeit mistaken, belief that small businesses are unlikely targets for cyber-attacks. In reality, data thieves are simply looking for the path of least resistance. Symantec's study found that 40 percent of attacks are against organizations with fewer than 500 employees.
Outside sources like hackers aren't the only way your company can be attacked. Often smaller companies have a family-like atmosphere and put too much trust in their employees. This can lead to complacency, which is exactly what a disgruntled or recently fired employee needs to execute an attack on the business.

5. ATTACKS COULD DESTROY YOUR BUSINESS

As large companies continue to get serious about data security, small businesses are becoming increasingly attractive targets—and the results are often devastating for small business owners.

According to the Kaspersky Lab, the average annual cost of cyber-attacks to small and medium-sized businesses was over $200,000 in 2014. Most small businesses don't have that kind of money lying around and, as a result, nearly 60 percent of the small businesses victimized by a cyber-attack close permanently within six months of the attack. Many of these businesses put off making necessary improvements to their cyber security protocols until it was too late because they feared the costs would be prohibitive.

6. WAYS TO PREVENT CYBER ATTACK

Even if you don't currently have the resources to bring in an outside expert to test your computer systems and make security recommendations, there are simple, economical steps you can take to reduce your risk of falling victim to a costly cyber-attack:

- Train employees in cyber security principles.
- Install, use and regularly update antivirus and antispyware software on every computer used in your business.
- Use a firewall for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.
- Make backup copies of important business data and information.
- Control physical access to your computers and network components.
- Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace, make sure it is secure and hidden.
- Require individual user accounts for each employee.
- Limit employee access to data and information and limit authority to install software.
- Regularly change passwords.

7. CONCLUSIONS

Internet users face thousands of cyber-attacks every day because of the increasing reliance of users on website communications, emails and numerous 'anytime, anywhere' technology solutions. An intelligence tool that adequately understands cyber-attack mechanisms and users' behaviours in terms of assumptions, decision-making and reactions to cyber threats/risks is still missing**.** The cyber attacks and their hardness are discussed. The way these attacks target the societal issues are been observed. Specifically attacks are elaborated that take place against the websites and their information is illustrated. SQL injection attack, DNS attack, DoS attacks are considered for implementation.

8. REFERENCES

[1] Chen Ping and Wang Jinshuang: Research and Implementation of SQL Injection Prevention Method Based on ISR. In Proceedings of the Computer and Communications (ICCC), 2nd IEEE International Conference,2016.

[2] Li Qian Zhenyuan Zhu and lun Hu, "Research of SQL Injection Attack and Prevention Technology," in Proceedings of Estimation, Detection and Information Fusion(ICEDIF), 2015.
[3] Dr. Fakariah Bt. Hj Mohd Ali, "Detection Model for SQL Injection Attack" in Proceedings of Computer Applications and Industrial Electronics(ISCAIE), IEEE Symposium 2014.
[4] Dr. Amit Chaturvedi and Aijaz Ahmad Rather, "Analysis of SQL Injection Attacks and Prevention Methods in Web Applications", in Proceedings of International Journal of Advanced Research in Computer Science and Software Engineering of Volume 5, Issue 12, December 2015.
[5] Sayyed Mohammad Sadegh Sajjadi and Bahare Tajalli Pour Study of SQL Injection Attacks and Countermeasures," International Journal of Computer and Communication Engineering, Vol. 2, No. 5, September 2013
[6] Symantec, "Internet Security Threat Report," 2016. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr- 21-2016-en.pdf.
[7] InfoSec, "Phishing Tools & Techniques," 2016. [Online]. Available: http://resources.infosecinstitute.com/cateory/enterprise/phishing/phishing-tools techniques/.
[8] McAfee, "McAfee Labs Threats Report," 2015. Available: http://www.mcafee.com/uk/resources/reports/rp-quarterly-threatsaug- 2015.pdf.
[9] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human Behaviour as an aspect of Cyber Security Assurance." Evans, Mark, et al. "Human Behaviour as an aspect of Cyber Security Assurance." arXiv preprint arXiv:1601.03921, 2016.
[10] D. John E, "Data breaches in UK healthcare sector double since 2013, ICO numbers show | Security | Computerworld UK." [Online]. Available: http://www.computerworlduk.com/security/data-breachesin- uk-healthcare-sector-double-since-2013-ico-numbers-show 3589814/.