International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206280

Analysis and Classification of Cryptanalytic attacks in a High-Risk network using Honeypot

Nitha V R
Department of Computer Science, Sree Narayana College, Cherthala, Alapuzha, Kerala, India

ABSTRACT

The online information and system in a high-risk network should be protected from threat, vulnerabilities and other types of cyber attacks. So, we need to identify the threat source, vulnerabilities in our network, category of threat, severity of exploit and many more. There are many categories of cyber criminals of which the one who gain profit from our sensitive data for financial gain are the most dangerous. In this paper, analysis and classification of various cryptanalytic attacks are monitored and classified with the help of honeypot .

Keywords : Cryptanalytic Attack, Exploit, Threat, Honeypot

I. INTRODUCTION

Most of the threats are associated with exploit. There are hackers who use multiple exploits at the same time to access the system. When our system is having any vulnerabilities, we have to identify where the weakness are. Once the weakness is identified, it can be fixed before an attack. This is done by penetration testing by white hat hackers.

II. METHODS AND MATERIAL

HACKING:

A hacker is a skilled programmer who finds and exploits weakness in a system/network. Based on their intent, hackers are classified into different types. White hat hacker, known as ethical hacker never intend to harm a system, rather they try to find out weakness in a system or network as part of vulnerability checking and penetration testing. Black hat hackers, known as crackers gain unauthorized access to a system and harm its operations or steal sensitive information by violating privacy. There are many variants of hackers who do unauthorized activity in a system or network.

CRYPTANALYSIS

It is a technique which involves working of cipher text, ciphers and cryptosystems. It also helps in finding weakness in a system by identifying flawed cryptographic algorithms. Many researchers are trying to find out methods of attack on any encryption algorithm without access to encryption key. More over Cryptanalysis help to identify weakness in the design or implementation of the algorithm.

There are mainly two types of attack in cryptography. Active and Passive attack . In an active attack, the intruder can make some changes to the system, where as in a passive attack, the intruder can only observe the system and network and it can't do any modification. There are mainly three security goals in cryptography. We have to ensure Integrity, Confidentiality and Availability

TYPE OF CYBER ATTACKS

1) DENIAL-OF-SERVICE (DOS) AND DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS

In this type of attack, the attacker makes a server unreachable to its visitors by flooding bogus requests and hence the server won't be able to process valid user requests. Though this attack can't steal website user's information, the attacker can use it for blackmailing the site owners for money in order to stop DDoS attack.

2) MAN IN THE MIDDLE ATTACK: Here the attacker inserts between the communications of a client and server. In a session hijacking attack, he attacker hijacks a session between a trusted client and a network server .IP Spoofing is another type of attack in which the attackers creates IP packets with a modified source address in order to hide sender's identity . In a Replay attack the intruder fetch message from sender and keep on sending to Receiver infinite number of times.

3) Phishing attack : In this attack, the attacker sends emails that appear to be from trusted sources with the goal of gaining personal information by using social engineering technique.

4) Drive by attack : The Drive by Downloads attack spread malware to insecure websites

5) Password attack: A person's password can be obtained by sniffing the network or by using social engineering or by guessing. It can also be done by brute force attack or dictionary attack.

6) SQL Injection Attack: It's a common issue with database driven websites. An attacker can execute SQL queries to the database. A successful SQL injection can read sensitive data from database, or modify database or shutdown database.

7) Eavesdropping attack: This type of attack occurs when the attacker intercepts the network traffic, thereby receiving sensitive information.

8) Birthday attack : These types of attacks are against hash algorithms by finding few random messages that generate same Message Digest when processed by a hash function.

9) Malwares : There are different types of malwares like viruses, Trojans, worms and droppers which adversely affect the system or network.

10)Ransomware is a type of malware that blocks access to victim's data by threatening the victim for ransom. Some ransomwares use a technique called cryptoviral extortion by encrypting victim's file, which can't be recovered without a decryption key. This type of attack is a severe threat to a cryptosystem.

11) SNOOPING: It is a passive attack, wherein the content of message send from the sender to receiver is released, which is a confidentiality threat.

12) TRAFFIC ANALYIS: It's an active attack, where the intruder know from where and to where the message is going and the content of message. This is a confidentiality threat.

13) MODIFICATION: It's an active attack, where the intruder make some modification to the message, thereby compromising integrity

14) MASQUERADE ATTACK: This is an unauthorized active attack, where the integrity is compromised.

15) REPUDIATION ATTACK: Intruder fetch data from sender, he can or can't send message to Receiver.

CRYPTANLYSIS TECHNIQUES AND ATTACK ON CRYPTOGRAPHY

CIPHER TEXT ONLY ATTACK : Here the attacker access to one or more encrypted messages, but doesn't know anything about plain text, the algorithm, and the key

KNOWN PLAIN TEXT ATTACK : Here the analyst access the plain text completely or partly, he is supposed to discover the key used to encrypt and decrypt the message .

CHOSEN PLAINTEXT ATTACK: Here the analyst either knows the algorithm or has access to the device used to do encryption and with the help of algorithm and plain text, he can derive the key.

DIFFERENTIAL CRYPTANALYSIS: It is a type of chosen plain text attack that analyze block ciphers that analyze pairs of plain text, so that the analyst can determine how the targeted algorithm works when it encounters different types of data.

III. RESULTS AND DISCUSSION

IMPLEMENTATION OF A HONEYPOT IN AN ENCRYPTED NETWORK

Cryptanalysis is the process of attempting to recover the plaintext or key from a cipher text. Cryptanalytic attacks depend on the nature and strength of the algorithm. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Honeypot is a security mechanism for trapping hackers or cyber attackers. A high interaction honeypot provide a detailed picture of how an attack or intrusion progresses by showcasing how a malware execute in real time.

Every communication within a high risk network should be protected by an encryption algorithm. In order to protect the network from attackers, we should implement a honeypot along with the same encryption technique next to the firewall. Proper implementation of a strong crypto system within a high interaction honeypot help us to analyze the strength of the algorithm.

Since all the activities of an intruder can be monitored and logged by the honeypot, we can easily identity the type of attack our network or cryptosystem is vulnerable to.

CLASSIFICATION OF CYBER ATTACK

By analyzing the log we will come to know about the type of attacker whether he is a white hat /black hat hacker or not. With this activity monitoring, we can guess the type of attack our crypto system is vulnerable to, thereby protecting the high risk network in advance.

IV.CONCLUSION

With the help of the intruder's depth of interaction with the high interaction honeypot, we can analyze the security risks in our crypto system so that the system or the cryptographic algorithm can be strengthened by the mean time before an actual attack occurs.

V. REFERENCES

[1]. https://www.coursera.org/lecture/classical-cryptosystems/types-of-cryptanalytic-attacks-IXWS1
[2]. https://www.sciencedirect.com/science/article/abs/pii/S0141933117300674
[3]. https://www.researchgate.net/figure/Defense-Scenario-III-with-firewall-IDS-and-honeypot_fig3_328037690

[4]. https://shodhganga.inflibnet.ac.in/bitstream/10603/26543/6/06_chapter1.pdf

Cite this article as :

Nitha V R, "Analysis and Classification of Cryptanalytic attacks in a High-Risk network using Honeypot", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 247-250, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT206280
Journal URL : http://ijsrcseit.com/CSEIT206280