A STUDY OF RED TEAM WITHIN INFORMATION SECURITY USING COVERT CHANNEL

Miss. Nishita H. Dave [1], Dr.Ravi K Sheth [2]
[1]*Student, School of Information Technology and Cyber Security, Raksha Shakti University, Lavad , Gandhinagar, Gujarat, India.*
[2]*Assistant Professor , School of Information Technology and Cyber Security, Raksha Shakti University, Lavad , Gandhinagar, Gujarat, India.*

***Abstract*- Information security isn't tied in with making sure about things from an online premise and unauthorized access. Information security teaches us how to prevent from unauthorized users. How to describe ourselves with strangers. We have to secure ourselves in both world physical world as well as cyber world.. So prevent our system physically as well as virtually from the attacker. We have to prevent our details, our profile on social media, our data on the mobile. Thus, Information security is valuable in numerous zones with its new methods like Cryptography, Digital Crime scene investigation, Online Web-based social networking, and so on.. Information security have 2 teams: primary and secondary teams, which working to approach CIA triad and maintain security of the organization. A study of red team functionality using covert channel attack analysis. So, the analysis of this attack are vital point to know.**

***Index Terms*- Information security, CIA triad, Red Team, Attacker ,Covert channel.**

I.INTRODUCTION

Information security plays an important role in any organization nowadays. With the help of e-security, we can find if any unauthorized activities had happened within the group. Mainly security program are built around 3 pillars: Confidentiality, Integrity and Availability. These terms are commonly known as **CIA triad**

CIA triad.

Mainly, the information security principles are Confidentiality, Integrity, Availability.

• **Confidentiality:** It is perhaps the element of the triad that most immediately comes to mind when you think of information security. Data is confidential when only those people that are authorized to access it can do so; to make sure confidentiality, you would like to be ready to identify who is trying to access data and block attempts by those without authorization. Passwords, encryption, authentication, and defense against penetration attacks are all techniques designed to make sure confidentiality.

• **Integrity**: It means maintaining data in its correct state and preventing it from being improperly modified, either by accident or maliciously. Many of the techniques that ensure confidentiality will also protect data integrity—after all, a hacker can't change data they can't access—but other tools help provide a defense of integrity in-depth checksums can assist you verify data integrity, as an example , and version control software and frequent backups can assist you restore data to an accurate state if need be. Integrity also covers the concept of non-repudiation you must be able to prove that you've maintained the integrity of your data, especially in legal contexts.

• **Availability**: It is the mirror image of confidentiality: while you need to make sure that your data can't be accessed by unauthorized users, you also need to ensure that it can be accessed by those who have the proper permissions. Ensuring data availability means matching network and computing resources to the number of data access you expect and implementing an honest backup policy for disaster recovery purposes.

In real world, the data should always be kept confidential, in its correct state, and available; in practice, of course, you often need to make choices about which information security principles to emphasize, and that requires assessing your data.**[Citation].**

In this study, a network covert channel has been developed. Gaining a better understanding and developing improved methods of network covert channel analysis are vital to the information security effort in an organization.

II. TEAMS WITHIN INFORMATION SECURITY

To approach CIA triad strategy, information security are mainly classified into two teams:

1.Primary Team:

Yellow Team, Blue Team, Red Team

2.Secondary Team:

Green Team, Purple Team, Orange Team

B. Secondary Team:

Its provide support to the primary team for enhance efficiency function of security.

Green Team:

The yellow team changes security policies based on blue team accomplishment.

Purple Team:

The blue team changes defense methods method based on red team expertise.

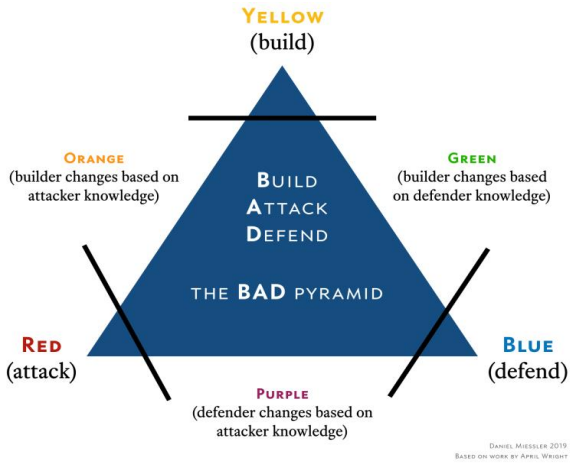


Figure: BAD Pyramid

Orange Team:

The yellow team changes security mechanism method based on red team expertise.

III. OVERVIEW OF RED TEAM

As red team act as attacker. It will show vulnerabilities and risk concerning:

Technology- Network, applications, gadgets

Individuals-Workforce, Business partner, Department, Contractors

Physical- Offices, Data centers, Warehouses, Substation

They perform attack scenarios to disclose prospective physical, technology and individuals vulnerabilities.

The goal of red team have had experience supporting system and not just trying to break them. They hold this experience to void in on vulnerabilities which were exploit and provide actionable remediation guidance to make system more secure.

IV. LITERATURE REVIEW

Title	Author	Year	Theory Used
PSCAN: A Port Scanning Network Covert Channel[1]	emad eldin mohamed and adel ben mnaouer	2016	A port scanning method is used, that scans the data transfer between sender and receiver
An Enlarging-the-Capacity Packet Sorting Covert Channel[2]	lejun zhang, tianwen huang, waqas rasheed	2019	The-capacity packet sorting covert channel model is used and derive the functional relationship between number of ports.
A Protocol Independent Approach in Network Covert Channel Detection[3]	Md. Ahsan Ayub,Steven Smith,Ambareen Siraj	2019	They have Proposed generic detection model, they have used different protocols for that.
ATwo-WayVoLTECovertChannelWithFeedback Adaptive to Mobile Network Environment[4]	xiaosong zhang, linhong guo,yuan xue	2019	It creates a two-way communication channel between ports to get the data. By checking the real time data it analyze the robustness and other performance of mobilenet environment.

V.COVERT CHANNEL

In computer security, a **covert channel** is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. .**[Citation].**

Covert :"not openly acknowledged or display"

Channel: "Network of communication"

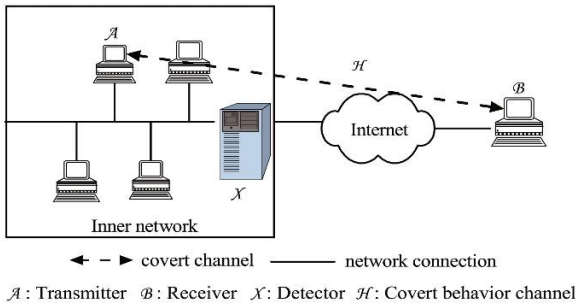


Figure: Covert Channel

A.CLASSIFICATION OF COVERT CHANNEL:

There are two kinds of covert channel:

1.Storage Channel: Communicate by modifying a "storage location", such as a hard drive, memory, network protocol headers, network payload.

2.Timing Channel: Perform operations that affect the "real response time observed" by the receiver, such as a disk accesses, memory accesses, network packet arrivals.

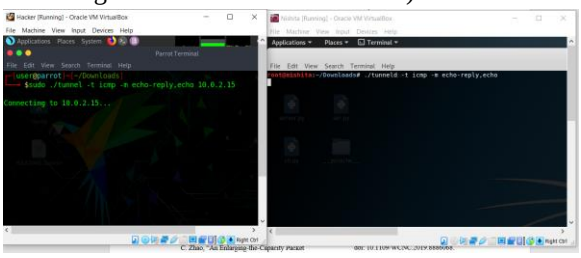
Both types of channels depends on the communication approach to exchange information with otherwise unauthorized subjects.

VI. IMPLEMENTATION

Establish channel using ICMP ,TCP/UDP:

1.First attacker allow only after achieve privileged escalation after that they using this communication channel. (network).

2.Create hidden tunnel using port service ICMP,HTTP and DNS between attacker and victim machine over virtual environment.(Through this attacker get access over victim device)



3.Analysis through **netstat command,** that can be used to list out all the network(socket)connection on the system. It lists out all the tcp, udp socket connection.

4. Attacker want to communicate to transfer data secret through hidden tunnel which were not detected by netstat command.

VII. CONCLUSION

In this work, analysis covert channel using tcp/udp connection on virtual environment which were not detective by network command. So, It is concluded that red team take possible attack that can thump an organization and they perform all possible attack that attacker would use. By take for granted/surmise the role of an attacker ,they show organizations what could be backdoor or unsuspecting vulnerabilities that cause a threat to their security. The goal of red team is not to break the security of organization but escalate the awareness about how to protect your information from the attacker.

So, information security is vital because it enclosed everything that concern to protecting our sensitive information and industry information system from theft and damage attempted by attacker.

REFERENCES

[1] E. E. Mohamed, A. Ben Mnaouer, and E. Barka, "PSCAN: A Port Scanning Network Covert Channel," *Proc. - Conf. Local Comput. Networks, LCN*, pp. 631–634, 2016, doi: 10.1109/LCN.2016.109.

[2] L. Zhang, T. Huang, W. Rasheed, X. Hu, and C. Zhao, "An Enlarging-the-Capacity Packet Sorting Covert Channel," *IEEE Access*, vol. 7, pp. 145634–145640, 2019, doi: 10.1109/ACCESS.2019.2945320.

[3] M. A. Ayub, S. Smith, and A. Siraj, "A protocol independent approach in network covert channel detection," *Proc. - 22nd IEEE Int. Conf. Comput. Sci. Eng. 17th IEEE Int. Conf. Embed. Ubiquitous Comput. CSE/EUC 2019*, pp. 165–170, 2019, doi: 10.1109/CSE/EUC.2019.00040.

[4] W. Xie, "SPECIAL SECTION ON SECURITY AND PRIVACY IN EMERGING DECENTRALIZED Physical Layer Security Performance Analysis of the FD-Based NOMA-VC System," *IEEE Access*,

vol. 7, pp. 115568–115573, 2019, doi: 10.1109/ACCESS.2019.2936036.

[5] B. B. Yilmaz, N. Sehatbakhsh, A. Zajic, and M. Prvulovic, "Communication Model and Capacity Limits of Covert Channels Created by Software Activities," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1891–1904, 2020, doi: 10.1109/TIFS.2019.2952265.

[6] M. Tahmasbi, A. Savard, and M. R. Bloch, "Covert Capacity of Non-Coherent Rayleigh-Fading Channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 1979–2005, 2020, doi: 10.1109/TIT.2019.2956489.

[7] J. W. Ho, "Covert Channel Establishment through the Dynamic Adaptation of the Sequential Probability Ratio Test to Sensor Data in IoT," *IEEE Access*, vol. 7, pp. 146093–146107, 2019, doi: 10.1109/ACCESS.2019.2945974.

[8] K. S. K. Arumugam and M. R. Bloch, "Covert Communication over a K-User Multiple-Access Channel," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 7020–7044, 2019, doi: 10.1109/TIT.2019.2930484.

[9] H. Q. Ta and S. W. Kim, "Covert Communication under Channel Uncertainty and Noise Uncertainty," *IEEE Int. Conf. Commun.*, vol. 2019-May, pp. 19–24, 2019, doi: 10.1109/ICC.2019.8761935.

[10] A. Sheikholeslami, M. Ghaderi, and D. Goeckel, "Covert Communications in Packet Collision Channels," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2019-April, 2019, doi: 10.1109/WCNC.2019.8886068.