PANIMALAR INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ANNA UNIVERSITY

ZEROTH REVIEW – BATCH NUMBER: B4

Prevention of IP Spoofing in Vulnerable Networks

PROJECT MEMBERS :

ASHWIN KUMAR A (211518104013)

DHUGESH WARAN P (211518104029)

GIRIDARAN S (211518104038)

Under the guidance of

Mr. T. A. Mohanaprakash

Associate Professor - Department of Computer Science

BASE PAPER

TITLE :

“IDENTIFYING NETWORKS VULNERABLE TO IP SPOOFING”

AUTHOR :

OSVALDO FONSECA, ´ITALO CUNHA, ELVERTON FAZZION, WAGNER MEIRA JR., BRIVALDO JUNIOR, RONALDO A. FERREIRA, ETHAN KATZ-BASSETT

ABSTRACT

- This aids in refining any organization’s security policy due to identification of vulnerabilities, and guarantees that the security measures taken actually gives the protection that the organization expects and requires.
- Administrator needs to perform vulnerability which helps them to uncover shortcomings of network security that can lead to device or information being compromised or destroyed by exploits.
- These outputs are typically heterogeneous which makes the further analysis a challenging task. Normal user network may give the way to unauthorized people to access as a authorized agents.
- Whenever, users step into online networks, without knowing them third party or any other harmful person monitoring their behavior.
- Before obtaining the malicious activity, admin or authorized person want to check the user networks such as IP address checking.
- However, user enter into the admin page, should be provided code word, to access the main service page.

EXISTING SYSTEM

CONCEPT :

NETWORK CAN USE TO SYSTEMATICALLY VARY BGP ANNOUNCEMENT CONFIGURATIONS TO INDUCE CHANGES TO INTERNET ROUTES AND TO THE SET OF SOURCES ROUTED TO EACH PEERING LINK.

TECHNIQUE :

BGP BEST-PATH SELECTION ALGORITHM

DISADVANTAGE :

THIS SCHEME CANNOT BE USED TO DETECT LOOPS

PROPOSED SYSTEM

CONCEPT :

WHENEVER STEP TO THE APPLICATION, THEIR IP ADDRESS TO BE OBTAINED BY THE AUTHORITY PERSON WITH VALID REQUEST FROM THE CONCERN PERSONS.

TECHNIQUE :

AES ALGORITHM

ADVANTAGE :

RELIABLE AND EFFECTIVE METHOD OF SAFEGUARDING SENSITIVE INFORMATION.

MINIMUM SYSTEM REQUIUREMENTS

HARDWARE REQUIREMENTS

PROCESSOR	:	DUAL CORE 2 DUOS
RAM	:	2 GB DD RAM
HARD DISK	:	250 GB

SOFTWARE REQUIREMENTS

FRONT END	:	J2EE (JSP, SERVLET)
BACK END	:	MY SQL 5.5
OPERATING SYSTEM	:	WINDOWS 7
IDE	:	ECLIPSE

REFERENCE PAPERS

[1] ETHAN KATZ-BASSETT, COLIN SCOTT, DAVID R. CHOFFNES, ÍTALO CUNHA, VYTAUTAS VALANCIUS, NICK FEAMSTER, HARSHA V. MADHYASTHA, THOMAS ANDERSON, ARVIND KRISHNAMURTHY, “LIFEGUARD: PRACTICAL REPAIR OF PERSISTENT ROUTE FAILURES”

[2] TASNUVA MAHJABIN, YANG XIAO, GUANG SUN, WANGDONG JIANG, “A SURVEY OF DISTRIBUTED DENIAL-OF-SERVICE ATTACK, PREVENTION, AND MITIGATION TECHNIQUES”

[3] ARTŪRS LAVRENOVS, “TOWARDS MEASURING GLOBAL DDOS ATTACK CAPACITY”

[4] THEERASAK THAPNGAM, SHUI YU, WANLEI ZHOU, GLEB BELIAKOV, “DISCRIMINATING DDOS ATTACK TRAFFIC FROM FLASH CROWD THROUGH PACKET ARRIVAL PATTERNS”