IP ADDRESS SHUFFLING USING MOVING TARGET DEFENSE (MTD)

Abhishekh Patil[1], Sunil Naklekar[2], Bhagwat Rodge[3], Akshaykumar Nimbalkar[4], Devyani Bonde[5]

[1234]*Student, Department of Computer, MMIT, Maharashtra, India*
[5]*Professor, Department of Computer, MMIT, Maharashtra, India*

Abstract

Enormous people are getting attracted to growing network technologies. Today, almost the whole world wants to get connected to information technology. Likewise, attackers are also getting smarter to trap victims. Due to this, victims are facing tremendous problems in terms of different network attacks such as DDOS, botnet, IP prefix hijacking, etc. The major reason behind these attacks is static and deterministic network configuration. So, Moving Target Defense (MTD) is a method that will overcome the static IP configuration. MTD introduces two patterns for randomly shuffling network configuration in the form of DYNAT and NASR. In this project, we present a brief introduction to the research achievements of network address shuffling according to two shuffling patterns which are identified and defined by us. We then summarize and analyze the supporting techniques 2 and related features for each network address shuffling technique mentioned in this project. What's more, the key issues to implement an effective network address shuffling mechanisms are implemented, with the expectation of invigorating subsequent research.

Keywords:*1. Computer Communication and Network: A.1 Data Communication*

i) A.1.1 Security and Protection

2. DDoS Attack Prevention

i. B.1 MTD

ii. B.2 DYNAT and NASR

----------***----------

1. INTRODUCTION

It is very unpredictable to say that every organization have secured themselves in terms of their data or in terms of hosts. Today, every single thing is vulnerable. This vulnerability is created by malicious attackers. Attackers are those entities who keep watch on confidential data. But users are not aware of this. So, they are always vulnerable to these attackers. Some mechanisms like NTS prediction, MOTAG were introduced to predict these attacks. But they were having limitations in terms of network traffic. Later, MTD was introduced overcome these limitations. Moving target focuses on system security by means of algorithms like DYNAT and NASR. We see this mechanism as a spring board to improve network traffic. Network address space randomization is effective against various hit list worms.

1.1 Software Requirement

1.1.1 Back End: Python

Python is a widely used high-level, general-purpose, interpreted, dynamic programming language. Its design philosophy emphasizes code readability, and its syntax allows programmers to express concepts in fewer lines of code than possible in languages such as C++ or Java The language provides constructs intended to enable writing clear programs on both a small and large scale.

1.1.2 Shell Script

A shell script is a computer program designed to be run by the Unix shell, a command-line interpreter. The various dialects of shell scripts are considered to be scripting languages. Typical operations performed by shell scripts include file manipulation, program execution, and printing text. A script which sets up the environment, runs the program, and does any necessary cleanup, logging, &c is called a wrapper.

1.1.3 Front End:-JAVA JDK 1.8, Eclipse

For developing this system we will required and Eclipse IDE and implementation language will be Java. For backend we are going to use Python or shell script.

Above mention software are easily available on internet. So that we can get them easily.

1.2 Hardware Requirement

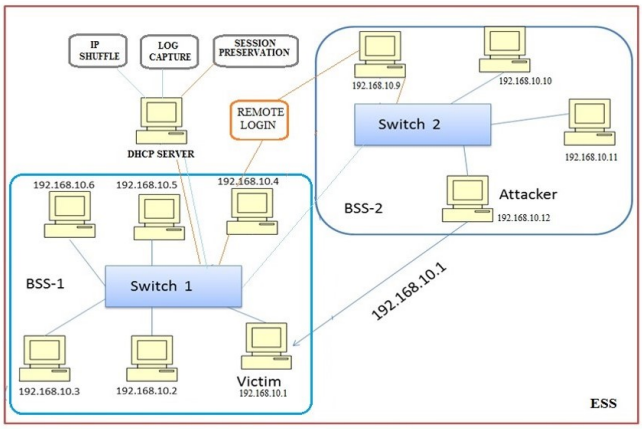
1) RAM : 512 MB
2) Processor Speed : 500-800 MHZ
3) Processor : Intel P-IV system
4) Hard Disk : 20 GB

For the implementation we need a linux system having minimum Random Access Memory of 512 MB upto the latest RAM memory. Its processor speed required is minimum of 500-800 MHZ. And the Intel processor should be having processor IV system or the latest processor.

1.3 Problem Statement

Dynamic IP allocation using DHCP is intended to achieve secure communication between hosts through defense algorithms like DYNAT and NASR. This system should also be able to monitor the network by fetching logs and persist on session preservation by keeping static IP addresses when hosts are interested to communicate with each other remotely. Insider attack prevention is the key aspect of moving target defense(MTD).

2. SYSTEM ARCHITECTURE



Initially there are number of systems connected to each other with the help of switch.

One of the systems acts like DHCP server. So, DHCP server is configured on that system. Responsibility of DHCP server is to assign IP addresses to the systems connected to the network. NASR Algorithm is implemented along with the DHCP server to shuffle and reassign the new IP addresses after some fixed time interval. A threshold time interval is set by the DHCP server. NASR has full access of IP address pool present at the server. After certain time interval DHCP server shuffles the IP address.

Because of this an attacker cannot target a system for so long. Hence, attacker fails to perform successful attack (specially DDoS). phone usage, schedule internet hours, etc.

3. MATHEMATICAL MODEL

- **S**={S_{dhcp}, S_x, $\mathbf{S_p}$,A, $\mathbf{S_{lp}}$, P, DD, NDD, success, failure}
- **S_{dhcp} (DHCP configuration function):**

  Let S_{dhcp}be the DHCP configuration function(dhcp3-server).

  S_{dhcp}={R,h,G} where,

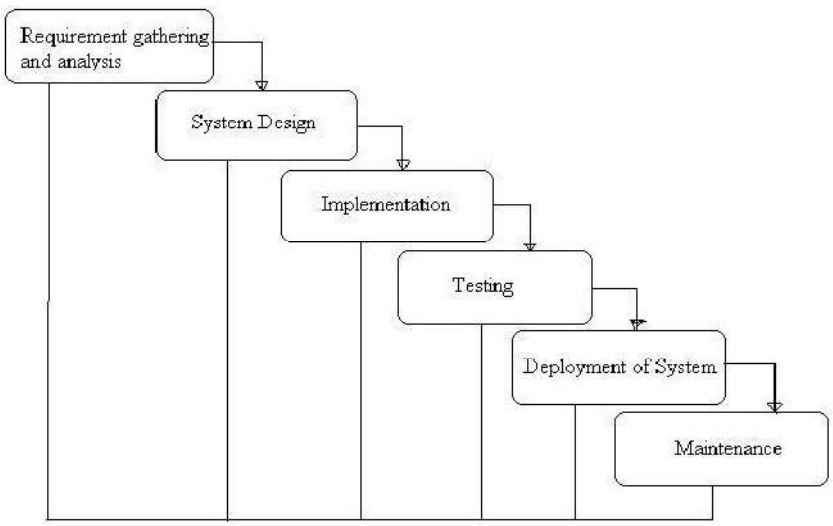
  R={1,2,3,…,n} is a set of IP addresses
  h={h_1,h_2,…,h_n} is a set of hosts.
  G=Default Gateway

- **S_x(Shuffling Function):-**
  S_x€S_{dhcp}

  $S_x$is responsible for changing the IP address after certain time interval.

  A maps all hosts $h_k$to addresses A(h_k)=r € R.
  Let P be the probability of getting infected.
  P=(m/n) where,
  m is the mean time for successful DDOS attack.
  n is the average shuffling period.
- **S_p(Session Preservation function):-**
  K=S_p€ h_k. Where,
  K listens to port ofh_k
  port entry is made under /etc/system.
  if(ssh=1) receive request otherwise

4. WATERFALL MODEL



The Waterfall Model was first Process Model to be introduced. It is also referred to as a linear-sequential life cycle model. It is very simple to understand and use.

In a waterfall model, each phase must be completed fully before the next phase can begin. This type of model is basically used for the for the project which is small and there are no uncertain requirements. At the end of each phase, a review takes place to determine if the project is on the right path and whether or not to continue or discard the project. In this model the testing starts only after the development is complete. In waterfall model phases do not overlap.

5. ALGORITHM TO BE USED

Network Address Space Randomization (NASR): A threshold time limit is set. At each threshold time interval IP address of each system in the network shuffled.

- Consider an abstract system model with address space, R={1,2,…,m}, Where R is the pool of IP addresses.
- Consider set of hosts, H={h_1,h_2,…,h_n}, where m>=n.
- Mapping of ip addresses to the hosts, i. e.R € h_k Where Each IP address is assigned to each host.
- Let t_a be the initial time and t_x be the time of attack
- Change the ip address at time t_b, where $t_a<t_b<t_x$

6. ADVANTAGES

1. Strong security against malicious attacks.
2. Dynamic configuration of network helps to confuse attacker in order to focus target.
3. Mitigation of DDoS is achieved using NASR method.
4. This method is comparatively cheaper than other mitigation techniques.

7. DISADVANTAGE

1. This method requires skilled administration.

8. CONCLUSION

We propose a system that will prevent attacks by analyzing network logs and shuffling the ip address dynamically. This system also implements some algorithms like DYNAT and NASR

ACKNOWLEDGEMENT

We express our sincere thanks to Head of Department of Computer Engineering for her kind co-operation. We express our sincere thanks to Prof. Devyani Bonde.