ISSN: 0976-3104
ISSUE: COMPUTER SCIENCE

ARTICLE

IMPLEMENTATION OF SCRUTINIZING SECURITY

Tridev Nath Tripathy*, Rajeev Singh

Department of CSE, Manav Rachna International Institute of Research & Studies, Faridabad, INDIA

ABSTRACT

Securing the cyber world has become the greatest challenge of all time. Cybercrimes are increasing uniformly all around the world. The undesirable acts are being done to gain the vital information of the well-known companies and individuals. My tool is a step towards the safer cyber world. It just scans the system and tell about the vulnerabilities of the system that can be used to exploit it and generating the alerts of the vulnerabilities of the system may be used to gain the access of the system.

KEY WORDS
Cyber Security, Armitage, Meta spolit Framework, VAPT, Information Gathering.

Received: 28 Mar 2019
Accepted: 21 May 2019
Published: 11 June 2019

***Corresponding Author**
Email:
tridev098@gmail.com

INTRODUCTION

At Security of the cyber world is required to enhance the privacy of an individual. On the daily basis, there are various companies that are affected by the cybercrimes. There are various steps taken by the organizations to protect their systems. The offenders gain the access to the system through two ways.

Hardware hacking

In the hardware hacking mostly there is an involvement of the pen drives or key loggers. These hardware's are enough to provide the important information of the system.

Software hacking

In the software hacking the felon enters into the system remotely by exploiting the services that are running on the victim's computer.

We have done the work to generate the report of vulnerabilities in the system by scanning and testing the exploits on it remotely. It is an automated tool for stepping forward in the direction of the world safer.

LITERATURE REVIEW

After studying and going through various research papers we found that it is almost impossible to provide 100 percent security to the system. But we can defend our systems among the known attacks around the world, which makes very difficult for the attacker to enter into the system. The basic way to protect the systems are firewalls, then there are VAPT (Vulnerability Assessment and Penetration Testing) tests that are performed by the computer experts, but if the experts have to do the VAPT for a company then it requires a lot of experts if there is no automated system. All the experts have to do the VAPT of each and every computer one by one. So, by this project we try to solve this problem and automate the VAPT of the network.

ORGANIZATION OF THE PAPER

The paper is organized in the four divisions. In the first division we discuss about the previous related tools. In the second section we describe our project. In the third section, we discuss the difference. In the fourth section we give the conclusion and proposed work and in the fifth section we have given the references.

EXISTING SOFTWARE'S

There are various software's that are used for the VAPT of the systems for example:- Nmap, Metasploit Framework, Armitage.

Nmap

It is used to scan the remote system, which helps us to gather information about the system like which ports are open and what service is running on them. It is also used to enumerate various types of services like smb service etc.

ISSN: 0976-3104

Metaslpoit framework

It is a framework used to exploit the various platforms. There are various exploits that are uploaded to its database and are used to gain excess of the system.

Armitage

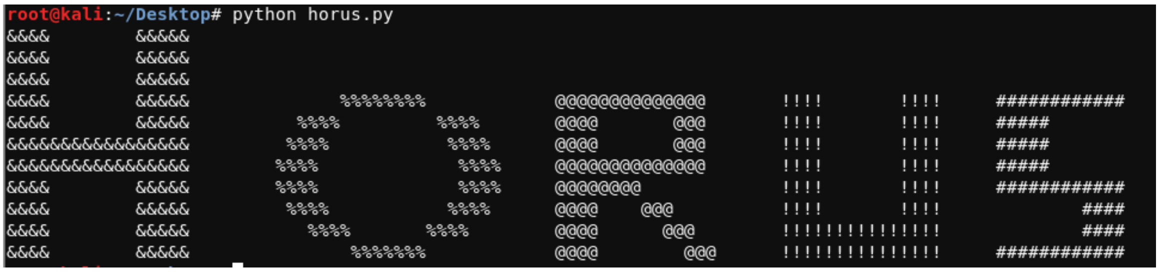
It is a GUI form of the Nmap and Metasploit Framework.

PROJECT HORUS

One It is automated tool and can be used to do VAPT of the whole network. It has a four tier operation:

Pinging Network

Firstly, it scans the whole network and get the IP's that are alive and a list is formed [Fig-1].



```
root@kali:~/Desktop# python horus.py
&&&&        &&&&&
&&&&        &&&&&
&&&&        &&&&&
&&&&        &&&&&              %%%%%%%%           @@@@@@@@@@@@@@       !!!!       !!!!     ############
&&&&        &&&&&          %%%%         %%%%      @@@@       @@@       !!!!       !!!!     #####
&&&&&&&&&&&&&&&&&         %%%%           %%%%     @@@@       @@@       !!!!       !!!!     #####
&&&&&&&&&&&&&&&&&        %%%%             %%%%    @@@@@@@@@@@@@@       !!!!       !!!!     #####
&&&&        &&&&&        %%%%             %%%%    @@@@@@@@             !!!!       !!!!     ############
&&&&        &&&&&         %%%%           %%%%     @@@@    @@@          !!!!       !!!!             ####
&&&&        &&&&&           %%%%       %%%%       @@@@      @@@        !!!!!!!!!!!!!!!             ####
&&&&        &&&&&               %%%%%%%           @@@@        @@@      !!!!!!!!!!!!!!!     ############
```

Fig. 1: HORUS Welcome Message Network Security Threats

Scanning IP's

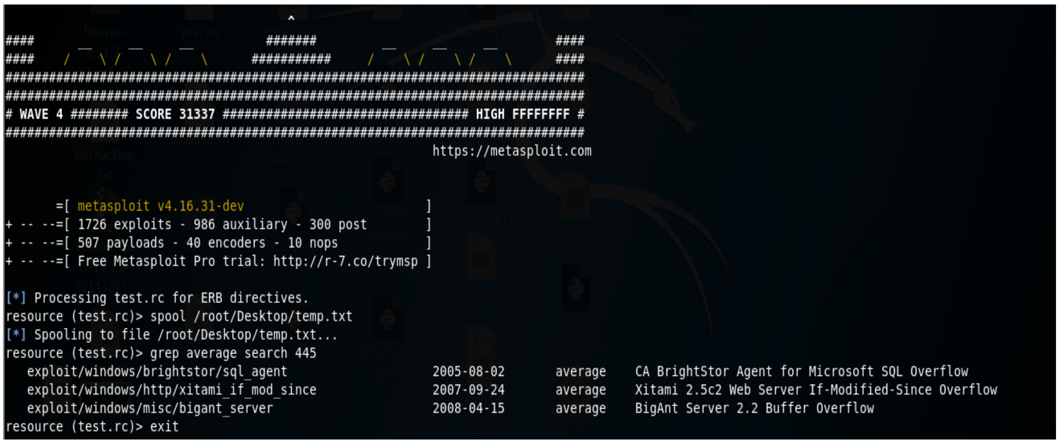
The second step involves the scanning and enumerating of the alive IP's also known as 'Information Gathering'.

Attack IP's

Based upon the information available it tries to exploit each and every combination that is possible.

Report

Based upon the information available it tries to exploit each and every combination that is possible. After attacking the IP's a report is generated which shows the vulnerabilities of the respective IP and if the IP exploitation is successful it generates high alert for that IP [Fig-1].



```
                                        ^
####      __     __     __           #######         __     __     __        ####
####    /     \ /    \ /    \      ###########     /    \ /    \ /     \     ####
#################################################################################
#################################################################################
# WAVE 4 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
#################################################################################
                                                            https://metasploit.com

       =[ metasploit v4.16.31-dev                         ]
+ -- --=[ 1726 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing test.rc for ERB directives.
resource (test.rc)> spool /root/Desktop/temp.txt
[*] Spooling to file /root/Desktop/temp.txt...
resource (test.rc)> grep average search 445
   exploit/windows/brightstor/sql_agent                 2005-08-02       average    CA BrightStor Agent for Microsoft SQL Overflow
   exploit/windows/http/xitami_if_mod_since             2007-09-24       average    Xitami 2.5c2 Web Server If-Modified-Since Overflow
   exploit/windows/misc/bigant_server                   2008-04-15       average    BigAnt Server 2.2 Buffer Overflow
resource (test.rc)> exit
```

Fig. 2: Implementation of Scrutinizing Security

COMPARATIVE STUDY

After going through many research papers and tool reports, we concluded that there is a large difference between Horus and other tools. First and fore most difference is that there is no tool which is able to perform the automated VAPT. Secondly, it is a able to provide better results in the network also. Thirdly, if we consider the scanning part Horus first version is weaker as compared to the other scanning tools.

CONCLUSIONS AND FUTURE WORK

In the first version of the tool we are able to perform simple scanning of networks and IP's and tries to exploit the systems by the familiar exploits. In the future we are trying to scan the IP's by various other methods and will add the feature of scanning the services that are running on the system.

CONFLICT OF INTEREST

None

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to Accendere Knowledge Management Services., for providing us a platform and opportunity to pursue the research.

FINANCIAL DISCLOSURE

None

REFERENCES

[1] www.wikipedia.org
[2] http://www.manchester.ac.uk/research/d.armitage/publications.
[3] https://nmap.org/bennieston-tutorial/.