Scrutinizing Security

Ms. Urmila, Tridev Nath Tripath, Rajeev Singh

Btech Computer Science

Manav Rachna University, Sector-43,SurajKund Road, Faridabad, Harayana, India

Abstract: *Securing the cyber world has become the greatest challenge of all time. Cyber crimes are increasing uniformly all around the world. The undesirable acts are been 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.*

Keywords*:* ***Cyber Security, Armitage, Metaspolit Framework, VAPT, Information Gathering.***

Introduction: 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 cyber crimes. As in today's world every task is performed through computer system. There are various steps taken by the organizations to protect their systems. The offenders gain the access of 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 safer world.

Background/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 : Rest of 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.

1. **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.
2. **Metasploit 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.
3. **Armitage:** It is a GUI form of the Nmap and Metasploit Framework.

Project: Horus

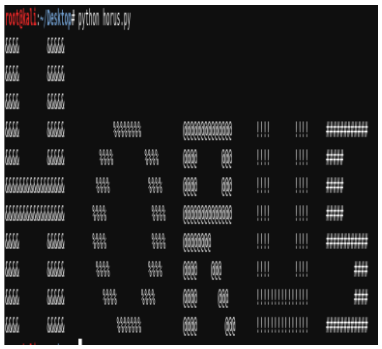

Fig. i

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

1. Pinging Network: Firstly, it scans the whole network and get the IP's that are alive and a list is formed
2. Scanning IP's: Second step involves the scanning and enumerating of the alive IP's also known as 'Information Gathering'.
3. Attack IP's: Based upon the information available it tries to exploit each and every combination that is possible.

Fig.ii

4. Report: 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.
5.

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 foremost 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.

References:

[1]. www.wikipedia.org

[2]. http://www.manchester.ac.uk/research/d.armitage/publications

[3]. https://nmap.org/bennieston-tutorial/

[4]. https://www.metasploit.com/