TECHNICAL REPORT

Introduction:

Today's society is all about Information society. In the last few years, the use of the World Wide Web is into every department of the market and into every part of our lives. The industries and the companies are trying to expand their market by providing additional features to the market demand in-order to sustain their market. In order to add those additional features they depended on most of the new technologies of various software tools. For all those new features that are needed to be added to the existing websites, the companies need to concentrate on the security issues of their website servers. Moreover, the programming languages like Ruby, Dot-net etc. help the attackers to easily attack the websites. The existing World Wide Web servers also added a new set of vulnerabilities which are yet to be addressed in a full fledge manner. Generally vulnerabilities exist in the web servers and often induced into the systems. In order to keep a check to all those vulnerabilities in the websites "Metasploit Framework" came into the picture of security of websites.

What actually is penetrating testing?

If the attackers use the vulnerabilities then obviously they somehow attack the websites of the company and they might all the resources of the company. Penetration testing often called as pen test or ethical hacking. It is the practice of testing a computer system, network or a web application to find the security vulnerabilities that an attacker could exploit. Penetration testing is easily performed with the help of Metasploit which is a collection of tools. With these tools the penetration testing is done at the target system. With the help of these penetration testing the vulnerabilities in the security of the websites or the network or the computer systems is known.

Various phases in penetration testing:

1) **INFORMATION GATHERING**:

The first phase in penetration testing is Information gathering. In this phase we shall gather all information related to server like what is correct domain of web server and how many sub-domains are connected to this domain. Whether there is any firewall is setup for web server or not. In our information gathering phase, we have found that web server's IP - 192.168.43.236. For detection of firewall we will use the tool WAFW00F (Web Application Firewall Detection Tool).

2) **SCANNING**:

In the scanning phase, we identify that what type of services is running on the web server and what is the version of that particular service. We also identify

that at which port this service is running. We identify that all services is running on which Operating system. For doing

this we mainly use NMAP (Network MAPPER) tool and METASPLOIT's AUXILIARY/SCANNER facility.

3) **DISCOVER VULNERABILITY**:

For finding vulnerability in web server or any system pentester mainly use Nikto, Nessus or Metasploit's Auxiliary/scanner facility. This paper mainly discusses about the use of auxiliary's Scanner Facility.

4) **EXPLOITATION**:

After find vulnerability, a pentester's main goal is Breach all type of security and take remote access of server. For doing this we use METASPLOIT. 5) REPORT GENERATION: In this phase we just generate full report of our Penetration testing process.

5) **REPORT GENERATION**:

In this phase we just generate full report of our Penetration testing process.

Various tests performed by the user in Penetration Testing:

1) **INFORMATION GATHERING** :

ATTACKER'S IP: 192.168.43.30 (KALI OS)

VICTIM'S IP: 192.168.43.236

The first work is to login on attacking system. As soon as the information gathering phase has started the immediate task is to collect the address of the victim's IP address, we first gather that what is IP of victim. Now our second work is that we check that, is any firewall enable on this server or not. We shall do this by using WAFW00F tool. After successfully login to attacking system start gathering information.

2) **SCANNING** :

For scanning process we shall use NMAP (network mapper) tool.

3) **DISCOVER VULNERABILITY**:

For discovering the vulnerability in the server we again need to use METASPLOIT

4) **EXPLOITATION**:

Multiple ways to Connect Remote PC using SMB Port

Conclusion:

Penetration testing is a comprehensive method to identify the vulnerabilities in a system. It offers benefits such as prevention of financial loss; compliance to industry regulators, customers and shareholders; preserving corporate image; proactive elimination of identified risks. The testers can choose from black box, white box, and gray box testing depending on the amount of information available to the user. The testers can also choose from internal and external testing, depending on the specific objectives to be achieved. There are three types of penetration testing: network, application and social engineering. This paper discussed a three-phase methodology consisting of test preparation, test, and test analysis phase.

The test phase is done in three steps: information gathering, vulnerability analysis, and vulnerability exploit. This phase can be done manually or using automated tools.