Penetration Testing

RushikeshRavindraShete
Computer Engineering Department,
Fr. C. Rodrigues Institute of Technology,University of Mumbai,
Navi Mumbai, India

Aaditya Panikath
Computer Engineering Department,
Fr. C. Rodrigues Institute of Technology, University of Mumbai,
Navi Mumbai, India

Aayush Vats
Computer Engineering Department,
Fr. C. Rodrigues Institute of Technology, University of Mumbai,
Navi Mumbai, India

Mrs. Shweta Tripathi
Computer Engineering Department,
Fr. C. Rodrigues Institute of Technology, University of Mumbai,
Navi Mumbai, India

***Abstract*—Computers are widely used at our home, industry, banks, defence, administration, medical sciences, etc. A Hacker is a person who exploits the weakness in the system. Cyber-crimes have been increasing exponentially. Cyber laws have been broken to a very large extent. Confidential information gets leaked which causes a loss to the individual and may even harm the entire country. Cyber-crimes can be reduced by taking preventive measures by finding and fixing the flaws in the system. Penetration Testing helps to identify the vulnerabilities present in the system. Our aim is to understand the need of it, steps, frameworks related to Penetration testing.**

Keywords*—System Security, Penetration Tesing, Vulnerability, Exploit, Payload, Nmap, Wireshark, Metasploit.

INTRODUCTION

System Security is defined as the protection of the system from the unauthorized access. It covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction.The basic security goals namely Confidentiality, Integrity and Availability are tried to be met by the system.

Penetration Testing means attacking a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.The process involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal. A penetration test target may be a white box (where all background and system information is provided) or black box (where only basic or no information is provided except the company name). A penetration test will advise if a system is vulnerable to attack, if the defenses were sufficient and which defenses (if any) were defeated in the penetration test.

LITERATURE SURVEY

Penetration testing is one of the most important methods to reduce the cyber-crimes. It is valuable for several reasons:

1. Determining the feasibility of a particular set of attack vectors.
2. Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence.
3. Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software.
4. Assessing the magnitude of potential business and operational impacts of successful attacks
5. Testing the ability of network defenders to successfully detect and respond to the attacks
6. Providing evidence to support increased investments in security personnel and technology.

A Vulnerability is a security hole in a piece of software, hardware or Operating systems that provides a potential angle to attack the system. A vulnerability can be as simple as weak passwords or as complex as buffer overflows or SQL injection vulnerabilities.To test if you have any vulnerabilities in your systems, you typically use a Penetration Testing solution.

To take advantage of a vulnerability, we often need an Exploit, a small and highly specialized computer program whose only reason of being is to take advantage of a specific vulnerability and to provide access to a computer system. Exploits often deliver a payload to the target system to grant the attacker access to the system.

A Payload is the piece of software that lets you control a computer system after it's been exploited. The payload is typically attached to and delivered by the exploit. We can imagine an exploit that carries the payload in its backpack

when it breaks into the system and then leaves the backpack there.

Steps in Penetration Testing

The various steps in Penetration Testing are as follows:
1. Data collection.
2. Vulnerability Assessment.
3.Actual Exploit.
4. Result analysis and report preparation

1. Data Collection:
Various methods including Google search are used to get target system data. One can also use web page source code analysis technique to get more info about the system, software and plugin versions. There are many free tools and services available in the market which can give you information like database or table names, DB versions, software versions, hardware used and various third party plugins used in the target system.

2. Vulnerability Assessment:
Based on the data collected in first step one can find the security weakness in the target system. This helps penetration testers to launch attacks using identified entry points in the system.

3. Actual Exploit:
This is crucial step. It requires special skills and techniques to launch attack on target system. Experienced penetration testers can use their skills to launch attack on the system.

4. Result Analysis and Report Preparation:
After completion of penetration tests detailed reports are prepared for taking corrective actions. All identified vulnerabilities and recommended corrective methods are listed in these reports. The vulnerability report format (HTML, XML, MS Word or PDF) can be customized as per your organization needs.[1]

Frameworks for Penetration Testing

The various frameworks available for performing Penetration Testing are as follows:
1.Nmap.
2.Wireshark.
3.Metasploit.

1.Nmap:
Nmap (*Network Mapper*) is a security scanner used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

The software provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection,vulnerability detection, and other features. Nmap is also capable of adapting to network conditions including latency and congestion during a scan. Nmap is under development and refinement by its user community[2].

E.g.:

a. Operating system and version detection
To find the operating system of the target we will use -O option.
Usage: nmap -O 192.168.217.131

Fig. 1: Operating system detection using nmap

b. To find the version detection:
Using Nmap we can find versions of the services running on the ports. We wiluse -sV option to do this.
Usage: nmap -sV 192.168.217.131

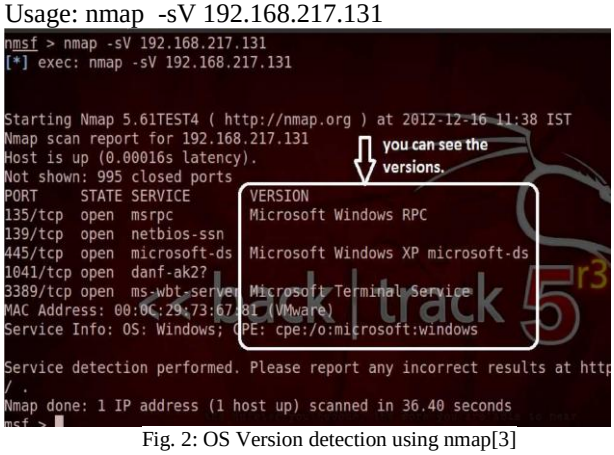


Fig. 2: OS Version detection using nmap[3]

2.Wireshark:
Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.Wireshark "understands" the structure of different networking protocols, so you are able to view the fields of each one of the headers and layers of the packets being monitored, providing a wide range of options to network administrators when performing certain traffic analysis tasks.

Similarly to Tcpdump, Wireshark includes a command line version, called Tshark, although this document focuses on its graphical-front end version. It is also important to mention that the functions detailed in this document represent only a small proportion of what Wireshark can do

and is meant as a guide for any administrator who needs to detect, analyse and resolve network anomalies[4].

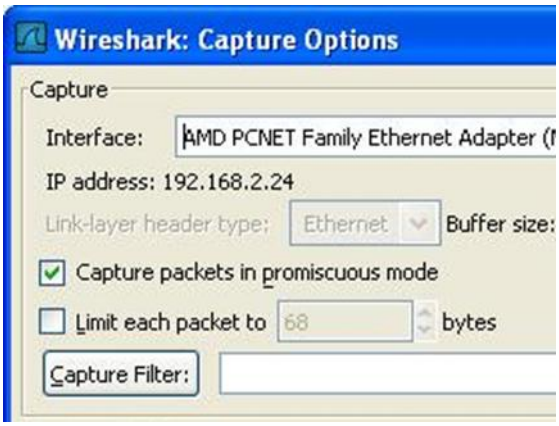
2.1 Working of Wireshark :

Step 1

Starting a Capture in Promiscuous Mode

1. Click Start, All Programs,Wireshark, Wireshark.
2. From the Wireshark menu bar, click Capture, Interfaces. Find the Interface with an IP address starting with 192.168.1. That's the interface that connects to the Internet in room. Click the Options button in that interface's line.
3. In the Wireshark Capture Optionsbox, verify that the Capture packets in promiscuous modebox is checked.

   Click the Startbutton.



Step 2

Entering a Password in the CCSF WebMail Client

1. Now, open a browser and go to hills.ccsf.edu/mail
2. In the Namebox, enter joeuser
3. In the Password box, enter topsecretpassword.
4. Click the LOGINbutton. If you see a message asking whether to remember the password, click "Not Now". After a few seconds, a message appears saying Username/PasswordFailure.
5. In the Wireshark: Capturebox, click Stop.

Step 3

Viewing the Password Captured From Your Own Computer

1. Wireshark shows the captured packets. To find the packet containing the password, click Edit, "FindPacket". In the Byline, click the Stringbutton. Enter a string of passand click the Findbutton.
2. Examine the data shown in the bottom pane, on the right-hand side. This is the text contained in the packet. In that data, you should find login_usernameand secretkeyfields, revealing the username and password you typed in, as shown below :

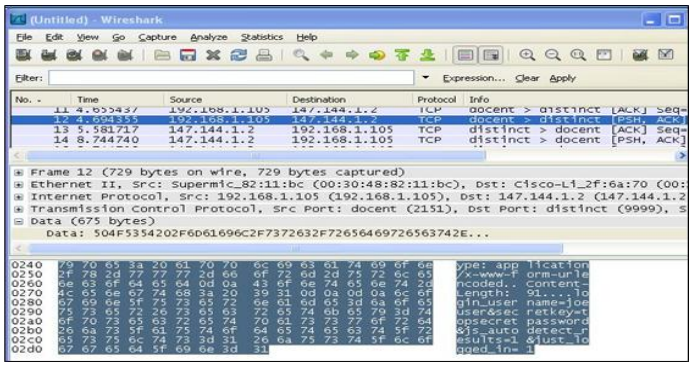


Fig 3 : Screenshot of Packet Sniffed in Wireshark [5]

3. Metasploit:

MetaSploit is an open source exploit development framework, allowing exploit plugins and reuse of payloads interchangeably, in a plug-and play fashion. It also comes with stock piles of ready-to-use exploits. Metasploit came about primarily to provide a framework for penetration testers to developexploits.

Metasploit offers more than one interface to its underlying functionality.

1.MSFconsole.
2. MSFcli
3. Armitage.

3.1. MSFconsole:

It is most popular part of Metasploit framework. It's like a one-stop shop for all of your exploitation dreams.Msfconsole is by far the most popular part of the Metasploit Framework, and for good reason. It is one of the most flexible, feature-rich, and well supported tools within the Framework. Msfconsole provides a handy all-in-one

interface to almost every option and setting available in the Framework; it's like a one-stop shop for all of your exploitation dreams. You can use msfconsole to do everything, including launching an exploit, loading auxiliary modules, performing enumeration, creating listeners, or running mass exploitation against an entire network. Although the Metasploit Framework is constantly changing, subsets of commands remain relatively constant. By mastering the basics of msfconsole, you will be able to keep up with any changes.

3.2. MSFcli:

Msfcli and msfconsole take very different approaches to providing access to the Framework. Unlike MSFconsole, MSFcli totally relies upon scripting or typed commands.Wheremsfconsole provides an interactive way to access all features in a user-friendly manner, msfcli puts the priority on scripting and interpretability with other console-based tools. Instead of providing a unique interpreter to the Framework, msfcli runs directly from the command line, which allows you to redirect output from other tools into msfcli and direct msfcli output to other command-line tools. Msfcli also supports the launching of exploits and auxiliary modules, and it can be convenient when testing modules or developing new exploits for the Framework.

3.3.Armitage:

It is a fully interactive GUI created by Raphael Mudge.This interface is highly impressive, feature rich and available for free. We won't be covering armitage in depth, but it is definitely worth mentioning as something to explore. Our goal is to teach the ins and outs of Metasploit, and the GUI is awesome once you understand how the Framework actually operates. To launch armitage, run the command armitage. During startup, select Start MSF, this will allow armitage to connect to your Metasploitinstance[6].

3.4.Working of Metasploit:

EXPLOIT : Microsoft Server Service Relative Path Stack Corruption

We study how to exploit a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts

Step 1**:**We search any SMB exploit such as 'netapi'.
Command:search netapi

We get a list of exploits under 'netapi' main module of exploit**.**

Fig. 4:Search exploitnetapi in Metasploit

Step 2: We use any one of the exploits that we get from step 1 and then we see all the possible module options under it.

Commands:use exploit/windows/smb/ms08_067_netapi.
Show options

Fig. 5: Use exploit and show options in Metasploit

Step 3: We find all the connected hosts to find our target system.
Command : hosts

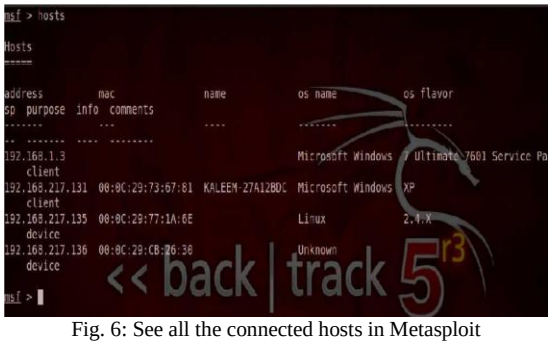


Fig. 6: See all the connected hosts in Metasploit

Step 4**:** Select one host among all hosts that we get in step 3.We then give the command to specify out remote host(target system).
Command:set RHOST 192.168.217.131

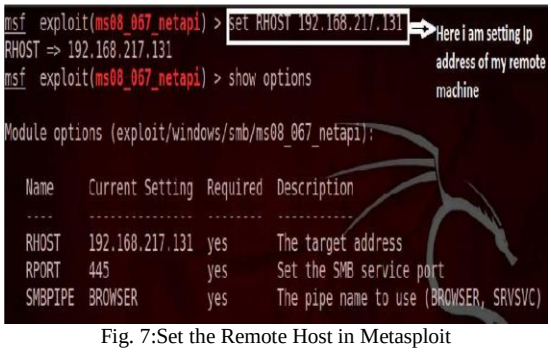


Fig. 7:Set the Remote Host in Metasploit

Step 5:We then select a payload for our exploit.
Command: show payloads

Fig. 8: View the payloads in Metasploit

Step 6:We seea huge payload list.Now we will use a payload bind shell.It directly binds with the target port 445
Command:set Payload windows/shell/bind_tcp

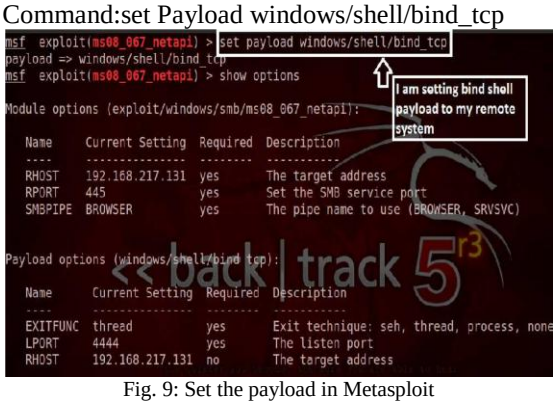


Fig. 9: Set the payload in Metasploit

Step 7: To get the shell on the target computer, use the command "exploit".This command runs the payload against the target system.Then you will get a remote shell on the target system.
Command:exploit

Fig.10:Exploit the target system using Metasploit[3]

Thus, the test was performed successfully.

PROPOSED DESIGN

The design will be the basis for further implementation. The design will include the Lifecycle model and the Use-Case diagram.

1.Lifecycle model:

The Spiral Lifecycle model can be used to develop the Penetration-testing Application.The most important advantage of this model is that it helps to analyze the risks that we can encounter during the development cycle.

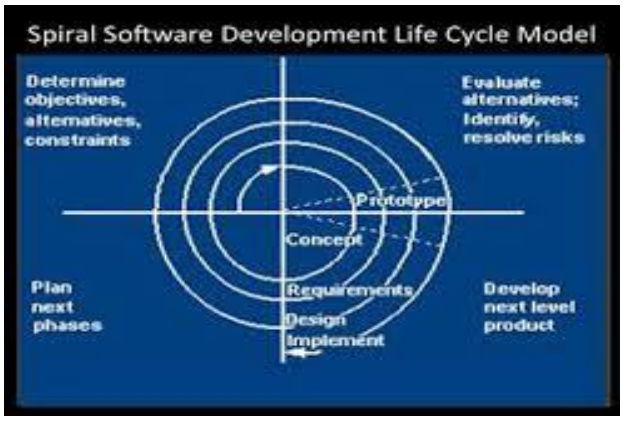


Fig. 11: Spiral Lifecycle Model[7]

2. Use-Case Diagram:

The proposed use-case is from the user's point of view for his better understanding of the application. The application is a penetration testing application which helps to find the system vulnerabilities.

The clients of the application must inform the pen-tester about what type of test he wants to do on his system.The type of test can be Web, Social, Wireless, Client-side, Network tests.

The selected type of test is performed by the application. The Test results are generated by the pen-tester which can be viewed by the client.The client comes to know about the vulnerabilities in his system.

The pen-tester gives suggestions on fixing the vulnerabilities.The security expert can be concerned to fix the vulnerabilities.

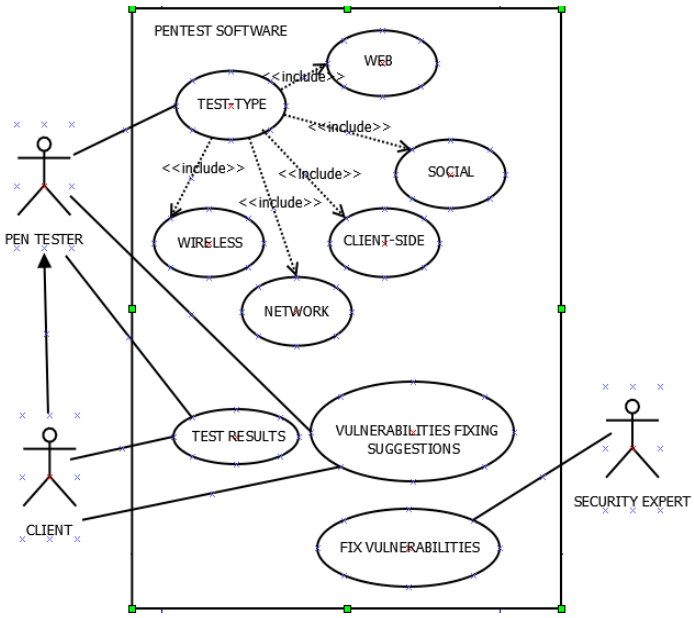


Fig.12: Proposed Use-case diagram for Penetration testing

IMPLEMENTATION

The frameworks like Nmap, Wireshark and Metasploit will be used to perform Penetration Testing on the Web-application. The Scenario is as follows:

User A is the victim user and User B is the attacker. Now User A uses the Web Application to perform some activity on the Internet. The various steps that will be required to perform the attack are as follows:

1.User B will try to find the IP Address of the User A using tool like Zenmap. The only pre-requisite is that both of them should be in the same network either wireless Wi-Fi or through LAN.

2.User B will try to find out the various details about theUser A like its Operating System, Services used, etc. This will give brief idea about the User A's environment. Nmap tool will be used with its various features for OS detection, Version detection, etc.

3.User B will now try to find packets that will be transferred between the User A and the Web Application. The various credentials like Username, Password, etc. can be obtained. The tool called Wireshark will be used. Its packet capturing capability can be used.

4. User B will try to perform various attacks using the Metasploit framework. The severity of the attack will vary depending on the amount of User A's information the User B will be successful to access. The various exploits of Metasploitframework will be used to attack.

Thus, User B if becomes successful to attack User A, then various vulnerabilities in User A's system can be found out which can be taken care by using proper security measures. On a more broader basis, this scenario can be extened to the example of the Shopping Complex with Open Wi-fi access. Any User can login to the system. So an attacker can perform any malicious activity by using the IP Addresses of any other user.

CONCLUSION

With the advent of sophisticated hacking tools and the exponential growth rate of cyber crimes, there is an urgent need for penetration testing as a field of research and study. Pen-testing as a process can be used to determine the vulnerabilities that a system possesses and the potential threats it is likely to suffer from in the near future. In no way is it possible to take care of all the threats that a system may encounter and hence a comprehensive analysis of security measures needs to be carried out. Penetration testing is one of the many options available to a cyber security professional to make up for the flaws in Firewalls and regular security protocols. With this report, we conclude that though no system is completely secure, penetration testing can provide the user with a different perspective regarding the susceptibility of his own system, thereby enabling him to take the necessary steps to prevent intrusion carried out with a malicious intent.

REFERENCES

[1] http://en.wikipedia.org/wiki/Penetration_test
[2] http://en.wikipedia.org/wiki/Nmap
[3] http://190.90.112.209/http/MetasploitGuide.pdf
[4] http://en.wikipedia.org/wiki/Wireshark
[5] p03_StealingPasswordsWithWireshark_ch3-10
[6] Syngress'sMetasploit Toolkit-For Penetration Testing,Exploit Development and Vulnerability Research.
[7] http://techiconsolutions.com/deliverymodel.html