International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

Ethical Hacking and Penetration Testing Using A mini computer

Meghana K R **Associate Professor Suma S**
meghanamegh610@gmail.com suma-mcavtu@dayanandasagar.edu
Dayananda Sagar College of Engineering
Bangalore ,India

Abstract **- This paper is dedicated to the field of network and info-communication defense along the cyber security platform to take a closer look at what is now known as "ETHICAL HACKING", in order to define, analyze, discuss and resolve some of the most common and widely spread threats and their functionalities according to which vulnerabilities are currently at hands in most threat incidents and try to come up with new techniques to more effective resolve such problems.**

Keyword- **Penetration Testing, Reconnaissance and Vulnerability Scanning.**

I. INTRODUCTION

Don't you think internet is becoming very dangerous? The way it's been developing rapidly and that's why we all need protection. An ethical hacker is someone who is certified and legally bound to use special types of skill sets that mimic the same approach used by criminals but the difference is mainly in the word "ethical". It became effective in the field of security very fast and gain approval of the majority. People all over the world are willing to pay any coast for a certified ethical hacker in their team. It identifies a simulation environment i.e., how an intruder may attack the system through white hat attack, cyber security is being strengthen by an acknowledgeable percentile throughout the years and fighting cyber crime was no longer a seemingly impossible issue as it used to be.

II. PENETRATION TESTING

An ethical hacker can apply multiple approaches to achieve security measures, most common ways are of two sorts mainly – analysis and investigation. To analyze the parameters of a network, objectives to look for will need to be pointed out first. In most cases these objectives are mainly being vulnerabilities, also known as "zero days" or "holes", and they open windows for breaches and intrusions that can lead to disasters and the crumbling of an entire enterprises network. After these holes are founds, the expert will try to use them to see if that can help to breach the security parameters of the network. Such method is known as "Penetration Testing" and it has 5 main levels (Fig 1). The levels of Pen testing are mainly 4, when they are combined they construct an affective operation to test the security level of a network. The main idea is to take a hackers approach and think like one, as for hackers mostly use to same steps to breach networks.

Fig. 1. Phases of Penetrating Testing

The use of an organized approach is important because it not only keeps the penetration tester focused and moving forward, but also allows the results or output from each step to be used in the ensuing steps .The use of a methodology allows you to break down a complex process into a series of smaller, more manageable tasks. Understanding and following a methodology is an important step in mastering the basics of hacking. Depending on the literature or class you are taking, this methodology usually contains between four and seven steps or phases. Although the overall names or number of steps can vary between methodologies, the important thing is that the process provides a complete overview of the penetration testing process. For example, some methodologies use the term "Information Gathering", Where as others call the same process "Reconnaissance" or "Recon" or even "OSINT". For the purpose of this article, we will focus on the activities of the phase rather than the name. After you have mastered the basics, you can review the various penetration testing methodologies and choose one that you like best[3-5].

International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

II.RECONNAISANCE AND VULNERABILITY SCANNING

Recon, short for reconnaissance, is the very first level of this operation known as penetration testing, the main goal of Recon is to obtain information about target that can be used as keys to establish an exploitation strategy against the target. There are two types of Recons: Passive and Active (Fig. 2). So, passive reconnaissance, which is almost undetectable, can yield a significant amount of information about the target organization and its users. Active reconnaissance builds on the results of open-source intelligence and passive reconnaissance, and focuses on using probes to identify the path to the target and the exposed attack surface of the target. In Fig. 3 the arrow indicates the usefulness of the data to attacker, however, the more aggressive the scanning is, the easier for the attacker to be detected.

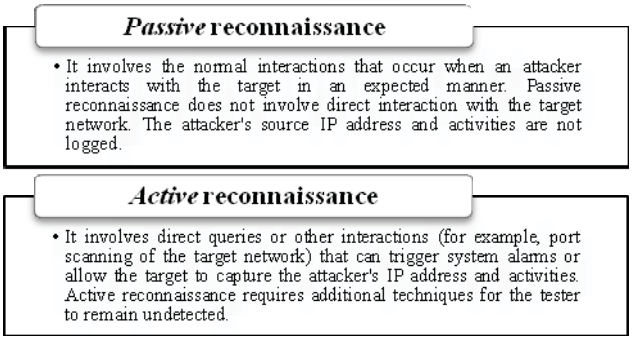

Fig. 2 Types of reconnaissance

Fig. 3 Usefulness of data to attacker

In general, complex systems have a greater attack surface, and each surface may be exploited and then leveraged to support additional attacks. Although active reconnaissance produces more information, and more useful information, interactions with the target system may be logged, triggering alarms by protective devices, such as firewalls and intrusion detection systems. As the usefulness of the data to the attacker increases, so does the risk of detection; this is shown in the following diagram: To improve the effectiveness of active reconnaissance in providing detailed information, our focus will be on using stealthy, or difficult to detect, techniques.

1. Stealth scanning strategies

The greatest risk of active reconnaissance is the discovery by the target. Using the tester's time and data stamps, the source IP address, and additional information, the target can identify the source of the incoming reconnaissance. Therefore, stealth techniques are employed to minimize the chances of detection. When employing stealth to support reconnaissance, a tester mimicking the actions of a hacker will do the following:

- Using camouflage tool signatures to avoid
- detection and triggering an alarm.
- Hiding the attack within legitimate traffic.
- Modifying the attack to hide the source and
- type of traffic.
- Using nonstandard traffic types or encryption
- to make the attack invisible.
- Stealth scanning techniques can include some or
- all of the following:
- Adjusting source IP stack and tool
- identification settings.
- Modifying packet parameters (nmap).

Using proxies with anonymity networks (ProxyChains and Tor network).

1. **Remote Penetration Testing With Raspberry Pi 3 (Minicomputer) And Kali Linux**

Kali Linux, formerly known as BackTrack, is the most widely known Pentest platform; it is a Debian distro from the wide Linux family. Being used by world's security experts, Kali provides every tool need for Penetration, including network scanning, social engineering, zero days exploits and even password cracking and creating backdoors. Raspberry Pi is a very low cost new generation mini- computer that uses HDMI cord to connect to display, it uses MicroSD that act as its hard drive memory and boot instantly into the OS, it's very stealthy and undistinguished due to its small size and un-attractive look (small black box). One can hide it anywhere and it would automatically blend in as a normal battery bank or even a cigarette box. It's very unlikely that people will temper with it or it would cause any kind of

suspicion. That's why to conceal a Raspberry Pi in common office supplies such as clocks, lamps, and printers is an extremely approach for a stealthy Recon and exploitation [7-8]. Main advantages of Raspberry Pi Model B+ are relatively impressive; it has more USB ports to support plugins, Low power draw and Ethernet port with active lights.

1. Combining Kali Linux and Raspberry Pi

Kali can be booted into the Raspberry Pi using light image that are specially made for Raspberry pi known as ARM Rpi image. It can be found and download from offensive-security.com

2. Network scanning

Reconnaissance is generally another interpretation of scanning the parameters around the target, it takes time and it is very important, mainly, because it shapes the whole strategy and the way which the operation is heading, It helps you to get familiar with the target and its activities and the way the target move and operates, eventually scanning the target will help you to decide how to attack and when to attack. The best way to scan a target is to do so quietly; therefore avoiding interaction from the beginning will be a smart decision to make just so you won't raise suspicion.

Eventually contact will be made when you take your first step into the target system after scanning and find an open port that will act as your window into the network through one system from the entire network[9]. Using Nmap as a primary scanning tool is a good idea, this specific tool for scanning among others provide ease and fast of use as well as faster response due to the light interface that it uses to interact with the network. A basic network penetration platform and scan a network let's put the above procedures into practice [10-11]. The Fig. 4 is a flow chart of how can penetration testing be planned and put into action. Finding a good hide spot to put the device so it doesn't raise any alert during the process, because gathering information is relatively time consuming and we don't want anyone to temper with the device during the operation.

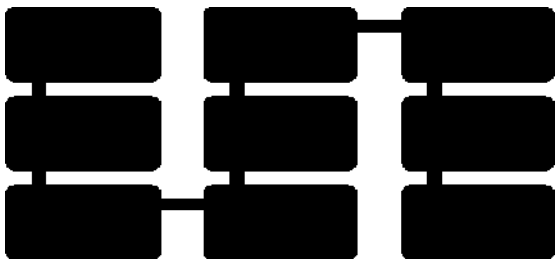

Fig. 4 Penetration Scenario flow chart.

Setting up a Command and Control center is important due to nature of Raspberry Pi and its capacity in performance is not so strong and can handle heavy load, so we use this C&C to capture data to avoid overwhelming the processor. Equipment's then will need to be gathered and assembled, and after the hardware is all set you will need to install your hacking platform, which the Kali Linux Distro, for Raspberry it's an ARM image. Now we prepare to raid the network and we set up the wireless card and connect to the device remotely using putty to gain access into the target network. At last we start the network scanning to obtain information and get the data into the device.

V. CONCLUSION

Ethical hacking is a very effective way to prevent breaches through uncovered holes in your system and networks, through a successful penetration testing and information gathering, patches can be put into place to reinforce your network defense, because the methodology of ethical hacking and penetration testing is taken directly from a hacker point of view, using the attackers strategy and approach to discover the vulnerabilities and eliminate the threats in the system. By using the following phases:

- Strategy planning.
- Recon and network scanning.
- Exploring.
- Information and vulnerability analysis.
- Exploitation and breach.
- Make Analysis report.

Pen testing is one of the most affective approaches to study the security parameters of a network of any size and it helps to analyze the security level of a network or system by filtering out the main holes and vulnerabilities. Pen testing is a security measure because of the following:

- It Implements a virtual environment of how a hacker may attack the system.
- It point out the holes where an intruder or a hacker may take advantage of and use it to attack.
- It protects sensitive data from being threatened by black hats and violation of integrity or theft.

It establishes the margin of the potential risks and threats that a business establishment have or attract.

- It displays clear evidence and proven facts that why it is crucial to have such measures and how important it is to invest into Information and Network security technology to help reinforce the valuable assets and information.

REFERENCES

[1]Patrick Engebretson. The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy Second Edition, Elsevier Inc. 2013.

[2] Beggs Robert. Mastering Kali Linux for Advanced Penetration Testing A practical guide to testing your network's security with Kali Linux, the preferred choice of penetration testers and hackers First published, Packt Publishing Ltd, 2014.

[3] Joseph Muniz and Aamir Lakhani. Penetration Testing With Raspberry Pi Construct a hacking arsenal for penetration testers or hacking enthusiasts using Kali Linux on a Raspberry Pi First published: Packt Publishing Ltd, 2015.

[4] H.M David. "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, 2004.

[5] J. Danish and A.N. Muhammad. "Is Ethical Hacking Ethical?" , International journal of Engineering

Science and Technology, vol 3 no. 5, pp. 3758-3763, 2011.

[6] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala. "Ethical Hacking " , International journal of Computer Applications, vol. 1 no. 10, pp. 14-20, 2010.

[7] Gurpreet K. Juneja."Ethical hanking :A technique to enhance information security" International