Automated Wi-Fi Penetration Testing

S.P. Kadam, Bhagyashree Mahajan, Mariya Patanwala, Prajakta Sanas, Shruti Vidyarthi
Computer Engineering
Bharati Vidyapeeth's College of Engineering for Women
Pune, India
bcmbhagyashree@gmail.com, mariya52.mp@gmail.com

***Abstract*—Wi-Fi is a local area wireless networking technology that is widely used for different purposes such as data transmission and wireless communication. Wi-Fi connection will most often result in faster, more reliable internet access and it is cheap. A penetration test on Wi-Fi is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Several operating system distributions like Kali Linux, pentoo are taken to the penetration testing. These systems require highly skilled technical users. Our approach is to convert these into a complete automated tool which eliminates manual effort and provides a complete solution for assessing Wi-Fi security. The proposed automated tool is implemented as a mobile application it would provide a handy Wi-Fi analysis and penetration suite mobile application which aims to be the most complete and advanced toolkit for IT security experts to perform network security assessments on from a mobile device. Issues and challenges related to the proposed mobile app have been discussed in this paper.**

Keywords— DNS, Penetration Testing, Spoofing, Wi-Fi, Traceroute.

I. INTRODUCTION

Wi-Fi is a local area wireless computer networking technology that allows electronic devices to connect to the network, based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. Wi-Fi is a single technology that makes all connections seamless. It has industry standard security protections on which the customers can rely on. Wi-Fi can be less secure than wired connections.

Penetration testing is a method used to test the Wi-Fi network. It looks for network vulnerabilitiess which gains accessibility to the network and flowing data. Penetration testing for Wi-Fi is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit network and system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are also useful in validating the efficiency of network security mechanisms, as well as end-users' adherence to security policies.

There are tools available to assess Wi-Fi networks. There are operating systems which combine these tools in a single suit. But disadvantages of using these tools and operating systems is the user requires to manually enter commands and keywords for each attack and user needs deep technical knowledge about networking, attacks and penetration testing methods. For accessing these tools we need to boot our laptop with these operating systems and carry along. In our approach we are combing all tools and methods and are implementing as a mobile app. Hence anyone can do penetration testing of available Wi-Fi networks easily.

The remaining paper organized in various sections, various attacks possible on a Wi-Fi networks (section A), existing tools and operating systems used by pentesters for Wi-Fi analysis and its limitations (section B), combination of these tools into an automated tool (section C), an approach towards developing an mobile applications (section D) and benefits and limitations of an automated tool.(section E).

II. ATTACKS ON WI-FI NETWORK

A. Eavesdropping

Basically, eavesdropping is term which is used to describe a situation where the person listens to the speaker without his knowledge. In cyber security the term is used more often as it happens on a wider scale on the network.

Usually the communication over a network takes place in an unsecured format hence it is easy for an attacker to interpret the traffic. Therefore a strong encryption is required especially in an enterprise.

B. Data Modification

An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if re confidentiality is not required for all communications, we do not want any of our messages to be modified in transit.

C. Identity Spoofing (IP Address Spoofing)

Every computer on a network is identified by its IP address. For an attacker, it is quite easy to modify the IP Address and gain the access. Once we gain access to the required network, we can do changes to greater extent without letting the actual user to know about it.

D. Password-Based Attacks

A common conception of almost all operating system and network security is to deal with its password-based access control. It means it checks for the authentication for the authentic user.

978-1-4673-9939-5/16/$31.00 ©2016 IEEE

E. Denial-of-Service Attack

The denial-of-service attack hinders the normal use of network by actual users. Once obtaining the access to the network, the attacker can perform following attacks:

- Randomize the centre of focus of internal Information Systems users so that they cannot notice intrusion immediately.
- Send data which is not valid to network services.
- Overload the network traffic till the network breakdown

F. Man-in-the-Middle Attack

A man-in-the-middle attack is an attack where attacker is in between the sender and the receiver of the data. With this attack, monitoring, capturing, modifying and controlling communication throughout .It is an active attack. Man-in-the-middle attacks are like using someone's identity to attack the other user.

G. Compromised-Key Attack

A key is numerical secret code which is necessary to interpret in order to fetch the secured information. However, to obtain a key is a difficult task and also resource intensive process for attacker. Although, it is possible. Once the attacker obtains the required key, that key is only known as compromised key. On obtaining the compromised key, the attacker can absolutely modify the data and try to compute additional keys which can alter the data too.

H. Sniffer Attack

To sniff a network is to get the entire knowledge of the packets passing through the network. A sniffer can read, monitor, and basically capture data communications over the network .So detailed information of the packet can be gained if it is not well encrypted. Also with the help of a sniffer, an attacker can analyze the user profile and alter the data which might cause the system crash or data corruption.

I. Application-Layer Attack

An application-layer attack is basically done by deliberately creating faults in servers of the Application layer servers which can bypass the normal access controls. The attacker takes advantage by gaining control of the application, system, or network and it can perform:

- Read or modify data
- Induce a virus program that can hamper the network, using computers and software applications.
- Can use sniffer program to gain information of the network
- Terminates the data applications or operating systems abnormally
- Make network vulnerable for attacks

III. Existing Wi-Fi Testing Tools

Following are the Wi-Fi testing tools which are used widely by network security administrators or managers:

A. Acunetix

It tests on SQL injection and gives a report of it. It also does Cross Site script testing and comes with the art crawler technology which has a client engine of script analyzer. This tool generates a report which gives detailed information of the network vulnerabilities. The latest edition is Acunetix WVS version 8.It includes various paradigms of security such as a module testing slow HTTP DoS(Denial of Service).

B. Cain & Abel

Cain & Abel is a password recovery tool. It allows a pentester to recover various types of passwords just by sniffing. It helps in cracking the encrypted passwords by usage of a dictionary or brute-force attacks. This tool can record the VoIP communication .It is used to analyze routine protocols, if used correctly, with the help of expertise. It identifies weakness and loopholes in the network but not actively participates in exploitation of any vulnerability.

C. Ettercap

It is a free and open source network security tool .It is used for man-in-the-middle attacks on LAN. This tool is used to analyze the network protocols of the system within a security auditing context. Ettercap has following functions:

- Security scanning by filtering of IP based packets and MAC-based packets(done by the gateways)
- ARP-based scanning is also performed by using ARP poisoning
- Public ARP is uses ARP poisoning to sniff on a switched LAN from a victim to all other hosts.

D. John the Ripper

It is one of the most popular tools available for password cracking and breaking through the password in order to get the access. Initially it was designed specifically the UNIX system but currently it works well on almost all operating systems. It is able to identify password hash types through its own cracker algorithm. It is freely available and was developed by Black Hat Pwnie Winner Alexander Peslyk.

E. Metasploit

It is used by every ethical hackers and pentesters in the world as it comes with the easy- to-use procedures and is developed by Rapid7.It gives details about the security vulnerabilities. It helps in pentesting and intrusion detection. It also comes as an open source project known as Metasploit framework which is used by highly skilled security professionals to execute exploit code in just any remote machine.

F. Nmap

It is another massive tool of a security tool which has been around for forever and is probably the best known. It is written in C, C++, and Python by Gordon Lyon starting from 1997, Nmap stands for Network Mapper is the existing security scanner which can be used to discover hosts and services on a network. To discover hosts on a network Nmap sends specially built packets to the target host and then analyzes responses. The program is a little complex because

unlike other port scanners out there, Nmap sends packets based upon network conditions.

Several operating system distributions are geared towards penetration testing. Such distributions typically contain a pre-packaged and pre-configured set of tools. The penetration tester does not have to hunt down each individual tool, which might increase the risk complications, such as compile errors, dependencies issues, and configuration errors. Also, acquiring additional tools may not be practical in the tester's context.

Popular penetration testing OS examples include:

- Kali Linux (which replaced BackTrack in December 2012) based on Debian Linux
- Pentoo based on Gentoo Linux
- WHAX based on Slackware Linux

IV. Proposed Approach

A. Combination of tools

Combining various tools under a single Wi-Fi testing toolkit simplifies the task of security analysts/administrators to assess the risk level of a Wi-Fi with a push of a button .Following are list of tools which can be combined into an automated Wi-Fi testing application:

1) Traceroute: It is a diagnostic tool for the network,used to track routes taken by a particular packet on an IP network from source to destination. It also records the time taken for each hop the packet makes during its path to the destination. It utilizes the Internet Control Message Protocol , echo packets time to live (TTL) values which is variable. The response time of each hop is calculated. To assure accuracy, each hop is questioned or say queried various times atleast three times for better response of a particular hop. It is a utility that records the route (the specific gateway computers at each hop) through the Internet between your computer and a specified destination computer. It also calculates and displays the amount of time each hop took. Traceroute is a handy tool both for understanding where problems are in the Internet network and for getting a detailed sense of the Internet itself.

2) Port Scanner: A port scanner is basically a software application which is designed especially to probe a host to check for the open ports present in a network. This is often used by administrators or security professionals to verify security policies of their networks .It is also used by attackers to identify services running on a host.On identifying,it tries to exploit vulnerabilities.It is basically a process that sends all clients requests on the network requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself.Most of the port scanner are not attacks ,but are very simple probes to determine the services they provide on an network.

SYN scan is also one of the forms of TCP scanning. Rather than use the operating system's network functions, the port scanner builds a raw IP packets automaticallyfor its self use, and monitors for responses. This scan is also referred to as half-open scanning because it never opens a TCP connection(full connection). It generates a SYN packet and if the target port is opened, it responses with a SYN-ACK packet and an RST packet is responded by the scanner host, closing the connection before the handshake is completed. But if the port is closed and not filtered, the target will be responded by with an RST packet immediately.

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan works against any compliant TCP stack . It also allows clear, reliable differentiation between the open, closed, and filtered states.

3) Local Network Mapping: The field of automated network mapping has taken on greater importance as networks become more dynamic and complex in nature. Network mapping is the study of the physical connectivity of networks. Internet mapping is the study of the physical connectivity of the Internet. Network mapping discovers the devices on the network and their connectivity. It is not to be confused with network discovery or network enumerating which discovers devices on the network and their characteristics such as (operating system, open ports, listening network services, etc.)

Many organizations create network maps of their network system. These maps can be made manually using simple tools such as Microsoft Visio, or the mapping process can be simplified by using tools that integrate auto network discovery with Network mapping. Sophisticated mapping is used to help visualize the network and understand relationships between end devices and the transport layers that provide service.

Several tasks could be done using Network Mapping as mentioned below:

- Which computers are running on the local network
- What IP addresses is being used on the local network
- What is the operating system of target machine
- Finding out what ports are open on the scanned machine
- Finding out if the system is infected with malware or virus.

4) DNS Spoofing: All devices and computers connected to the internet have IP address and DNS helps people to remember the human friendly names instead of large numbers. Spoofing is a deceptive practice that is used to mislead the target to mistake one thing for another. Spoofing is done on the internet with emails that appear to be from a sender other than the real sender. It is done for fraudulent websites that use every possible means to prove that they represent a real organization.

A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively.

5) Exploit Finder: In computer security, vulnerability is point where a system lacks immunity to attacks.Vulnerability is the combination of three elements: a system flaw, attacker accessibility to the flaw, and attacker efficiency to exploit the flaw. Once vulnerabilities are discovered the suite can run some exploits to gain access at which point you can then trigger various actions.

6) MITM: An MITM attack is one in which the attacker secretly intercepts and relays messages between authenticated users who are supposed to communicate directly with each other. It's a form of eavesdropping but the entire conversation is controlled by the attacker, who even has the ability to modify the content of each message. Often abbreviated to MITM, MitM, or MITMA, and it has a strong chance of success if the attacker can pretend each party to the satisfaction of the other. MITM is a serious scourge to online security because they give the attacker the sole power to capture and modify the sensitive information in real-time while posing as a trusted party during transactions, conversations, and the transfer of data.

The man-in-the middle attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read and modify the data in the intercepted communication.

7) Packet Forger: It is also termed as packet crafting. Packet crafting is one of the techniques which allows network administrators to probe firewall rule-sets and find loopholes into a targeted system or network. It is done by generating packets manually to test network devices and behaviour, instead of using the existing network traffic. Packet crafting is a task that is methodically carried out to penetrate into a network's infrastructure. Crafting is typically used to invade into firewalls and intrusion detection devices, but can also be used to attack Web servers and other application gateways.
The act of packet crafting can be divided into four stages: Packet Assembly, Packet Editing, Packet Playing and Packet Decoding.

8) Kill Connections: Established network connections can be broken using the suite. Kill connections by preventing target to reach any server or destination address. So, one can face situation like no internet connection is there. In computing, DoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is the attack source is more than one–and often number of-unique IP addresses.

Criminal perp of DoS attacks generally attacks on target sites or services which is hosted on high-profile larceny web servers as banks, credit card payment gateways.

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two forms of DoS attacks: those that destroys the services and those which flood services. The most serious attacks are distributed and in many or most cases involve forging of IP sender addresses so that the location of the attacking machines cannot easily be identified, nor can filtering be done based on the source address.

B. Mobile Application

It is necessary to build some tool which has a very user friendly GUI and which can use the same techniques with more effective approach. If we think about today's technology then 2 factors are affecting over world computer industry. First is Smartphone and another is the operating system which is used into those Smart phones. Android is the largest installed base of any mobile platform and is growing rapidly. Every day another million of users powers up their Android devices for the first time and start looking for apps, games, and services (other digital content. Android provides a world-class platform for various usage such as creating apps and games for users everywhere around the world.

Benefits of using Android platform:

- Global partnerships on large installation base
- Rapid innovation
- Powerful development framework
- Open market for apps distribution

Most of the current existing systems have terminal screen for testing purposes. The user / tester need to memories commands to perform various penetration tests. While proposing a solution for our problem statement we wanted to make it user friendly and enhance penetration testing experience. There is a need of simple interface where users don't have to memorise commands to perform tests. We want it to be one click experience for the users. Hence we wanted it to be a GUI based application, where the users need to connect to the WLAN network and then the entire connected device will be visible in a list format. User will select one device and then next he just has to click on the list of test that he wants to perform on the selected device. Application will run its magic in the backend and generate the test result which can be mailed by user for further research purpose.

V. BENEFITS OF PROPOSED AUTOMATED TOOL

Benefits of the tool are listed below:

- It provides user friendly GUI which allows making use of each and every available feature in the App.
- No need of having deep knowledge about networks and security aspects as it provides comparatively easy to use techniques but with the same effectiveness.
- It can actually save our time and efforts.
- Our features will be appearing in the form of smart GUI as a list of Menus.
- Most phones have Wi-Fi capability, cameras, mass storage capability and a persistent internet connection via 3G and 4G and allow a wide number of applications and if rooted provide many of the same tools as a computer, but with more hardware and network capabilities.
- These conveniences also carry over to make them a very powerful tool to use in penetration tests, more powerful than a laptop, as a mobile device can be easily hidden with the person, or inside of an office building.

VI. CONCLUSION

In this paper, we have investigated the possible approach of developing an automated Wi-Fi testing tool which can be implemented in an android application. We have explained the concepts related to each tools in terms of computer network security. Possible attacks on the network and general exploit finders for those attacks are discussed briefly. Purpose behind using specific techniques and resources has been explained in details with respect to network penetration testing tools.

References

[1] M. Domenico, A. Calandriello, G. Calandriello and A. Lioy. Dependability in Wireless Networks: Can We Rely on WiFi?. IEEE Security and Privacy, 5(1):23-29, 2007

[2] Charles J. Kolodgy Gerry Pintal, "Automated Penetration Testing: Can IT Afford Not To?," Sponsored by: Core Security Technologies, January 2007

[3] Pranav S. Ambavkar, Pranit U. Patil, Dr.B.B.Meshram, Prof. Pamu Kumar Swamy, WPA Exploitation In The World Of Wireless Network, IJARCET, vol. 1., Issue 4, June 2012

[4] Md Sohail Ahmad, WPA Too!