A Wifi hack by cracking WEP

Dr.S.P.Rasal
Mudhoji College Phaltan, Satara, Maharashtra, India
(Email:subhashprasal@gmal.com)

Abstract - **A wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Wireless LANs have become popular in the home due to ease of installation, and in commercial complexes offering wireless access to their customers; often for free.In search of fulfilling the wireless demands, Wi-Fi product vendors and service contributors are exploding up as quickly as possible. Wireless networks offer handiness, mobility, and can even be less expensive to put into practice than wired networks in many cases. Wireless LANs have a great deal of applications. Modern implementations of WLANs range from small in-home networks to large, campus-sized ones to completely mobile networks on airplanes and trains. Users can access the Internet from WLAN hotspots in restaurants, hotels, and now with portable devices that connect to 3G or 4G networks. Oftentimes these types of public access points require no registration or password to join the network.**

With the consumer demand, vendor solutions and industry standards, wireless network technology is factual and is here to stay. But how far this technology is going provide a protected environment in terms of privacy is again an anonymous issue. Realizing the miscellaneous threats and vulnerabilities associated with 802.11-based wireless networks and ethically hacking them to make them more secure is what this paper is all about. On this segment, we'll seize a look at common threats, vulnerabilities related with wireless networks. And also we have discussed the entire process of cracking WEP (Wired Equivalent Privacy) encryption of Wi-Fi, focusing the necessity to become familiar with scanning tools like Cain, NetStumbler, Kismet and MiniStumbler to help survey the area and tests we should run so as to strengthen our air signals.

Keywords- **Wi-Fi Hacking, WEP, Kismet, Cain, NetStumbler.**

I. INTRODUCTION

The Institute of Electrical and Electronics Engineers (IEEE) provides 802.11 set of standards for WLANs. The wing ".11" refers to a subset of the 802 group which is the wireless LAN working group. Many industry groups are involved in work with wireless systems, however the IEEE 802.11 working group and the Wi-Fi Alliance came out as key troupes. 'Wi-Fi' is not a technical term. However, the Alliance has generally enforced its use to describe only a narrow range of connectivity technologies including wireless local area network (WLAN). A Wi-Fi enabled device such as a personal computer, video game console, Smartphone, and digital audio player can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more (interconnected) access points — called hotspots when offering public access — generally comprises an area the size of a few rooms but may be expanded to cover many square miles, depending on the number of access points with overlapping coverage. Wireless cracking is the unauthorized use or penetration of a wireless network. A wireless network can be penetrated in a number of ways. These ways vary greatly in the level of computer skill and commitment they require. Once within a network, a skilled hacker can modify software, network settings, other security items and much more. Precautions can however be taken. Ethical hacking is done by taking prior permission and such hackers are named as white hat hackers.

II. NEED TO TEST OUR WIRELESS ARRANGEMENTS

Insecurity of Wireless networks is on track ever since the premature days of the 802.llb standard of 1990s. The standard's initiation, major 802.11 limitations, such as physical security, encryption flaws has been discovered. Because of these, two wireless security standards have come out to help struggle back at the enemy: Wi-Fi Protected Access (WPA): Developed by the Wi-Fi Alliance, served as an intervening standard to fix the well-known WEP vulnerabilities. IEEE 802.l1i (identified as WPA2): An official IEEE standard, that integrate the WPA fixes for WEP with additional encryption and authentication mechanisms.

III. THE DANGERS OUR SYSTEMS MUG

Just going deep into the ethical-hacking process, we should know a couple of terms we'll be using throughout this paper. They are,

Threat: A threat is a sign of target to cause disturbance within an information system. A few paradigms of threat agents are hackers, annoyed employees, and malware such as viruses or spyware that can inflict disorder on a wireless network.

Vulnerability: It is a flaw inside an information system that can be browbeaten by a threat. We'll be seeking out Wireless network vulnerabilities all through this paper.

IV. EVOLUTION OF INTRUDERS

The problem really is not with these wireless networks, in and of themselves. It's with the malicious hackers waiting there for an opportunity over vulnerabilities to make our work thornier. So as to better defend your systems, we have to think like a hacker. Mostly the primary object is an organization having one or two wireless APs. We've found that smaller wireless networks undoubtedly work in hacker's favor, for many reasons. Those are accurately the class of things that elegant hackers make use of. Yet undersized networks aren't the merely vulnerable ones. There are many other flaws that hackers can use in networks of all extents. Hackers usually don't want to lift our information or crash our systems. They habitually just want to prove to themselves and their allies that they can crack in. Sometimes these guys want to use a system for attacking other people's networks under mask.

V.REQUIREMENTS

Ahead of going down the ethical-hacking toll road, it's vital that we plan everything in advance. This take account of:

1. Acquiring permission from our boss or project sponsor or client to carry out our tests
2. Over viewing testing objectives
3. Reconciling what tests to run
4. Grasping the ethical hacking techniques before carrying out our tests.

VI. COLLECTING RIGHT TOOLS

Picking up the appropriate security testing tools is again an important part of the ethical-hacking process. Just for the reason that a wireless hacking tool is premeditated to perform a certain test, but that doesn't signify it will. We may have to nip our settings or locate another tool altogether. Also we should be aware of potential for false positives (screening that there's vulnerability when there's not) and also false negatives (screening that there's no vulnerability when there is). The subsequent tools are some of our likings for performing tests on wireless networks and are crucial for executing wireless hacks:

- Google - yep, a Web site which is a huge tool
- Laptop computer
- GPS satellite receiver
- Network Stumbler - network stumbling software
- AiroPeek - network analysis software
- QualysGuard - vulnerability assessment software
- WEP encryption cracking software

VII. INSPECTING FOR PROTECTION

Once if we get everything geared up, it's time to make our sleeves and dig up our hands dirty by carrying out different ethical hacks against our wireless set-up. There are cluster of security tests we can perform to know how feeble our wireless systems are to bother. The outcomes of these tests will definitely show us what security punctures may or may not be fixed to build a more secure wireless network. We will sketch out various counteract measures we can employ to fix the weaknesses we identify. In the next few segments, we will outline a variety of security attacks to establish the root for vulnerability tests we'll be operating against our wireless network.

A. *Unethical Attacks*

These kinds of attacks take advantage of human weaknesses like lack of consciousness, negligence and ignoring strangers. We also enclose physical vulnerabilities which can make an invader have a chance on firsthand access to our wireless devices. These attacks incorporate,

- Flouting into wireless devices that clients mounted on their own and left unsecured
- Some sort of attacks where a hacker fake as somebody else and persuade users to give out excessively much information about our network
- Unauthorized assessment of APs, antennae and some other wireless infrastructure to reconfigure and confirm data off it. It is essential to test the security system of your PC and so the ethical hacker will follow the same procedure to that of unethical hacker. While scrutinizing your computer system it is essential to look from the point of view of illegal hacker. Hacking your own computer systems will allow you to understand the ability of the system and with this you can further prevent your P from any kind of infringement.

B. *Attacks Concerning Network*

There are a group of techniques the dire guys can use to shatter within our wireless realm or at any rate leave it wilted in a nonworking state. Network based attacks comprise of,

- Mounting mischief wireless APs and dodging wireless clients into linking to them.
- Holding data off the network from a distance by under our own steam etc.
- Attacking the transactions of the client in network by sending up MAC addresses, setting up a medium (Slotting in a wireless system in between an AP and wireless user) and more
- Abusing network protocols
- Carrying Denial-of-service (DoS) attacks.

C. *Attacks Concerning Software*

Since the security harms with the 802.11 protocol weren't adequate, we have to be anxious about operating systems

and utilities on wireless-client machines readily vulnerable to exploit. Now we'll some of the software attacks:

• Hacking the operating system and further applications on wireless-client gear
• Contravening through default settings like passwords and SSIDs that are effortlessly known
• Cracking WEP keys and pattering into the network's encryption scheme
• Getting way in by the use of feeble network authentication methods.

VIII. SIMPLE HACK WITH A DRIVE

Now, we just try to go out and look around scanning for open Wi-Fi hotspots. In many circles, this is deemed as a sport and is increasing in fame crossways the globe. Any Windows machine enabled with Wi-Fi has the ability to scan hotspots by installing either NetStumbler or Cain. Nearly all Windows support scanning utilities make use of a technique of scanning called 'Active scanning' as of the limited access to the hardware. While we scan for Wi-Fi with active scanning, a request has been sent through our device on every channel and records all replies. An immense traffic is produced and it is noisy even.

A. *Going For Tackle*

An active Windows based scanner we normally use for producing the information needed to map Wi-Fi hotspots along with SSID, Encryption and GPS coordinates is the NetStumbler. Because the program continuously yelps out 'ANY ACCESS POINTS ARE AVAILABLE NEAR', the retorts are more copious. NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP. A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system. It is used for Detecting causes of wireless interference and unauthorized (rouge) acesspoints. NetStumbler make use of Windows drivers for accessing Wi-Fi card, ensuing the Wireless Zero Configuration to shut down once run. In WinXP, this Wireless Zero Configuration permits the OS tolocate available Wi-Fi networks. When we go on road, this will become a big problem for connecting to an access point. The simplest mode to resolve this problem is just saving the NetStumbler data, closing program and refreshing the available networks. Cain & Able is the finest one we find as open outstanding auditing program for windows platform. It exercises ARP poisoning, a VoIP logger, password crackers, and also has a built in Wi-Fi scanner. It overcomes the negative aspect that we have with NetStumbler since a third party driver 'WinPcap' (for most low level network programs) is used by this application. The volume of Access points with Cain & Able is not up to the mark as NetStumbler does, so the selection lies on a preference. Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11wireless LANs. Kismet is unlike most other wireless network detectors in that it works passively. This means that without sending any loggable packets, it is able to detect the presence of both wireless access points and wireless clients, and associate them with each other. Kismet is trendy for the reason that it uses 'Passive scanning' schemes and it won't interfere with Wi-Fi signals or network traffic. With a passive scanner, the information is logged only if an access point is transmitted. Mostly it's impossible to spot as giving us flush information than the stated counter parts. Once sufficient traffic is produced or dynamic traffic go by, the IP address range of the AP can be grabbed with no log in. If the network doesn't use DHCP, the access point's IP address can be known very handy.

B. *Area Scan*

The sample of data that may be similar to the data we will also hit upon. We have to be very vigilant that the proportion of Encrypted Vs. Non-encrypted networks will show a discrepancy from place to place. One more significant thing to stare at is the SSID names lists. Most of them are with the default name. The routers of the Broadband using default name will possibly have the default passwords on them too and these are further attention grabbing targets than a concealed SSID.

The NetStumbler file (NS 1), may be uploaded to majority of the Wi-Fi public depositories online for the people to spot like wifunaps.com, wigle.net etc. At the moment we've used NetStumbler, Cain or Kismet to gather the data and now we are able to start our hunt for cracking the WEP. The primary section of the data we should look after to initiate with is the SSID, MAC address and also the Channel.

C. *Congregating Information*

With the desired information, an illicit now starts to hit the WEP or he installs a Warcracker (tiny computer premeditated for automated information gathering and cracking procedure) which is accessed remotely or could be picked up at a short time. Usually to stay legal when involved, it's a fine initiative to build a lab environment among various Wi-Fi AP's as targets and many systems having Wi-Fi cards to intensify the quantity of attractive traffic. This attractive traffic comprises of key negotiation packets and makes us to collect sufficient information by snuffling to crack the WEP key in a lesser span of time. The traffic we are talking about can be produced with

programs like Aireplay and Voidll. These create the necessary WEP initialization vectors to crack. Along with the revealed ones, Airodump is simple to use and assists this process.

D. *WEP Getting Cracked*

After all, we now have the file prepared to be thrown to the massacre. This is the time to consider Aircrack which will do the rest of our work. It uses Airodump data of the file and starts crack process for generating the right key. For the 128 bit WEP to break, the file should hold 200,000 to 700,000 distinctive IV packets. Thinking that we cover a sufficient amount of file, we hit the file to obtain the key. With Aircrack, the command in the root level command line looks as follows,

root@home[l]# aircrack -f 2 -m XX·XX·XX·XX·XX·XX -n 128 -q 3 keygen*.cap

If the key has been revealed, we will see the message 'KEY FOUND!' We've made Wireless Access Point to compromise and now it can be accessed. And finally we've broken Wi-Fi encryption! An equivalent method was employed in Los Angeles ISSA meeting where some local FBI special agents cracked a WEP key of 128 bits in just 3 minutes with the usage of normally found tools available over the Internet. This issue is pointed out only to show that still WEP 128 is an exposed encryption and shouldn't be the one used to secure Wi-Fi hotspots. We should remember that the more computers produce interesting packets, the quicker we can crack the WEP.

IX. CONCLUSION

Wireless networks like Wi-Fi being the most spread technology over the world is vulnerable to the threats of Hacking. It is very important to protect a network from the hackers in order to prevent exploitation of confidential data. The better way to do this is, just think like a hacker. At a glance, we've talked about the whole process of cracking WEP encryption of Wi-Fi in this paper. All this is made only to figure out the necessity in getting touch with some of the scanning tools like NetStumbler, Cain, Kismet, MiniStumbler etc to survey the Wireless locality. The tools that have been stated will give us the ability to break our own WEP key and this may be the time to go to the next rank of security, the WPA. Let us try to hack all the standards of Wireless networks ethically in order to make a system very protected.

REFERENCES

[1] Jeremy Martin, "The art of casual Wi-Fi Hacking," CISSP-ISSAP, 2009.

[2]L. Zhou and ZJ. Haas, "Securing Ad Hoc Networks," IEEE Network, vol. 13, no. 6, 1999, pp. 24-30.

[3] M. Junaid, Dr Muid Mufti, M.Umar Ilyas, "Vulnerabilities of IEEE S02.11i Wireless LAN," Transactions On Engineering, Computing And Technology Vll February 2006 Issn 1305-5313.

[4] Stanley, Richard A."Wireless LAN risks and vulnerabilities," Information systems control Journal, volume2, 2002.

[5] US-CERT, "Using Wireless Technology Securely," produced by USCERT, a government organization, 200S.

[6] Michael Roche,"Wireless Hacking Tools," available at http://www.cse.wustl.edul-jain/cse571-07/ftp/wireless_hackingl

[7] R. Terarnura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, "Breaking WEP with Any 104-bit Keys - All WEP Keys Can Be Recovered Using IP Packets Only," Proc. of SCIS2009, CDROM, 1A2-6, Jan. 2009.

[8] D. Waterman (Eds.), "Interconnection and the internet': Selected papers from the 1996 TC conference.

[10] V. Moen, H. Raddum, and KJ. Hole, "Weaknesses in the temporal key hash of WPA," ACM SIGMOBILE Mobile Computing and Communications Review, vol.S, pp.76-S3, 2004.

[11] IEEE S02 standards, http://standards.ieee.org/getieeeS02