AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

www.ajcse.info

Asian Journal of Computer Science Engineering 2017; 2(3):11-16

RESEARCH ARTICLE

Wireless Network Security Software

[1]Ameya Kisan Mohape*, [2]Vinit Shankar Bhoye, [3]Archana Ganesh Mhatre, [4]Prof. Smita Bhoir, [5]Prof. Prashant Lokhande

Computer Science Department, RAIT, Nerul, India

Received on: 17/02/2017, Revised on: 25/03/2017, Accepted on: 20/05/2017

ABSTRACT

Wireless networks are more vulnerable than wired networks due to omnidirectional nature of electromagnetic radiation and no physical connection. Some of these networks are secured using cryptographically broken Wired Equivalent Privacy (WEP) while most are based on the newer Wi-Fi Protected Access (WPA/WPA2) encryption which is still vulnerable to a certain degree. Security of a Wi-Fi Access Point (AP) may be compromised due to user's lack of technical knowledge, inbuilt flaws or an intentional attack. We have developed an application called Wireless Network Security Software – software with the capability to detect AP vulnerabilities and suggest prevention mechanism to increase security. The software detects AP vulnerabilities by performing attacks such as Man in the Middle (MITM), Denial of Service (DOS), MAC (Medium Access Control) address spoofing and DNS (Domain Name System) spoofing. It also automatically captures 4-way handshake and tries to crack the AP password using dictionary and custom wordlist attack. Prevention techniques are recommended based on the results of performed attacks on AP.

Keywords—WPA, WPA2, aircrack-ng , cowpatty, eviltwin, handshake, spoofing, DOS.

INTRODUCTION

Wireless Networks are more vulnerable than wired networks. This is because in wired networks nature of data transmission can be unicast, multicast or broadcast depending on the requirement. However, in wireless networks data is transmitted using radio waves that can be captured by anyone using a proper receiver and software. Hence, data is broadcast while tranmission no matter what kind of delivery it corresponds to. This application analyses the captured data, tests the network for vulnerablilites and recommends prevention techniques for the listed attacks.

The various attacks are as follows:

- MITM
- DNS spoofing
- DOS
- MAC spoofing

The application is useful in performing penetration testing and network security analysis on home, work or public networks that are setup in infrastructure mode. It detects vulnerabilities and flaws in Access Point setup and recommends prevention techniques to avoid possible attacks. It also checks the network password strength with respect to entropy.

1. WPA
   WPA was developed in 2003 and provides better security than WEP. It has a wide range of target users: WPA-Personal for personal use, WPA-Enterprise with additional security for commercial networks and Wi-Fi Protected Setup (WPS) for simple key distribution. WPA is vulnerable to dictionary and brute force attacks.
2. WPA2
   WPA2 and WPA have a lot in common. Firstly, WPA2 is an improvement over WPA in which it uses Advanced Encryption Standard (AES) based encryption for stronger security. WPA2 is also vulnerable to dictionary and brute force attack however this might take a lot of time.

RESEARCH PAPER SURVEY

1) An Experimental Study Analysis of Security Attacks at IEEE 802.11 WLAN [1]

In this paper, we have worked an experimental

***Corresponding Author:** Ameya Kisan Mohape**, Email**: mohapeameya@gmail.com

analysis to study some of the well-known attacks pertaining to IEEE 802.11 WLAN. IEEE 802.11 wireless networks have become one of the most widely used networks. Due to open nature of wireless medium, hackers and intruders can make utilization of the loopholes of the wireless communication; as a result, there are many security threats associated with Wireless Local Area Network (WLAN).

2) A comparative analysis of wireless security protocols (wep and wpa2) [2]
This paper is a comparative analysis of WEP, WPA and WPA2. We have tried to perform and check authentication of all 3 protocols by implying the legendary attack vector scripts i.e. Air crack set of tools. The test was conducted on Back Track operating system which is considered as dedicated penetration testing operating system. In the test result, we found out that WEP is the weakest, to which WPA was a temporary solution and WPA2 is a very solid and long term solution.

Present system includes network testing tools such as NetStumbler that offer only a few functionalities and are outdated. Another solutions are firewalls and antivirus systems. These are real time application. These do not provide prevention mechanisms to avoid the attack in the first place. Also antivirus is a heavy application and most of them don't support Unix and Linux systems. These systems lack functionalities such as penetration testing and vulnerability analysis.

Drawbacks of current systems:

- Only real time attack detection,
- No attack prevention mechanisms,
- Don't support Unix and Linux systems,
- Lack vulnerability analysis.

PROBLEM STATEMENT

Now-a-days the need for Wi-Fi access points has increased greatly. Routers come with preconfigured settings that need little to no understanding of the system. These systems come with default settings and can be vulnerable to a number of attacks. These attacks include password bruteforcing, default password guessing, no or poor security protocol, encryption protocol exploitations, etc. which makes these vulnerabilities dangerous. Sometimes, the user might lack knowledge regarding the working of the system. The user might configure the system incorrectly leaving behind vulnerabilities that could be exploited. The user might not configure the system at all as many latest systems can be used without any configuration and work out-of-the-box. This creates vulnerabilities that have potential for attacks such as MITM, DOS, MAC spoofing, and DNS spoofing. Also router firmware might have vulnerabilities or in-built flaws that can be used by an intruder to attack the system. An application is described to detect these vulnerabilities and to prevent attacks that exploit them.

TOOLS NEEDED TO SCAN WPA/WPA2 NETWORK

- Kali Linux operating system
- Wireless Access Point with WPA/WPA2 security
- Wireless network card capable of monitor mode and packet injection with Atheros chipset (TP-LINK TL-WN722N 150Mbps High-Gain)

IMPLEMENTATION

Handshake Capture

The 4-way handshake[1]used to crack the password contains the hash of the WPA/WPA2 password and is calculated using network name as salt value.

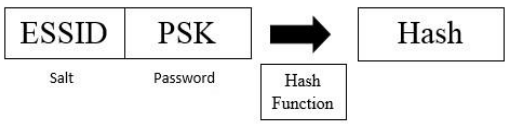

Fig. 1: WPA Handshake hash calculation.

Step 1: Use "airmon-ng start wlan0" where "airmon-ng" [2] is a program to put interface in monitor mode and "wlan0' is the name of the wireless interface.
Step 2: Capture packets in monitor mode. Use "airodump-ng wlan0mon" to capture packets where "airodump-ng" [2] is a program to capture wireless packets and "wlan0mon" is interface name. Wait for some time to get a list of access points. Use Ctrl+C to stop packet capture.
Step 3: Search for the target network name under Extended Service Set Identification (ESSID) column. Note down ESSID, Basic Service Set Identification (BSSID) and channel number of the network.
Step 4: Monitor and capture packets going through the target network. Use "airodump-ng –channel X –bssid XX:XX:XX:XX:XX:XX –w nname" where "X" is the channel number, "XX:XX:XX:XX:XX:XX" is the BSSID or

Medium Access Control (MAC) address of target network and "nname" is the name or ESSID of the network.

Step 5: De-authenticate all clients and force them to reconnect to the target access point. 4-way handshake can be captured by "airodump-ng" [2] during this process. Use "aireplay-ng -0 10 –a XX: XX: XX: XX: XX: XX wlan0mon" in another terminal to de-authenticate clients. Program "aireplay-ng" [2] is used to send de-authentication frames. Successful handshake capture will be shown at the top-right corner of "airodump-ng" [2] window.

Step 6: Crack the password using Aircrack-ng [2] and a password list. Use "aircrack-ng –w /path/to/password_file.lst –b XX: XX: XX: XX: XX: XX /path/to/capture file/nname-01.cap"

Fig. 2: Cracking password using Aircrack-ng.

Aircrack-ng [2] goes through the password list and compares its hash with one in 4-way handshake. If found, the password would be shown besides "KEY FOUND". We can speedup this attack by calculating in advance the hash of network name and passwords using Cow patty [3].

Observed cracking speed using Aircrack-ng: 862 keys/sec. Observed cracking speed using Cow patty using pre-calculated hash: 184623 keys/sec. This shows an approximately 214 times increase in cracking speed.

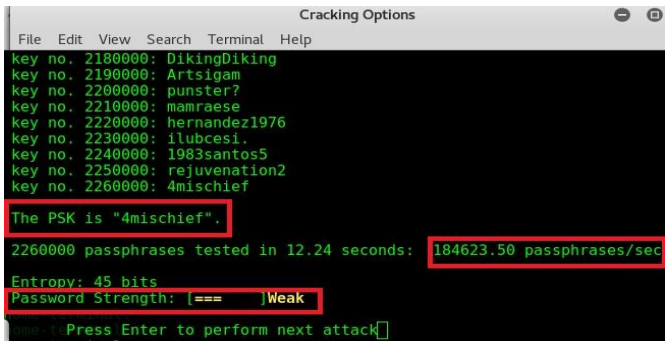

Fig. 3: Cracking password using Cowpatty using pre-calculated hash.

Password strength or Entropy of a password depends on the length and character set used to create the password. Entropy of a password of length L is calculated using the formula:

$E = L.\text{Log}_2 \sum$ (size of character CSi set used)

Where CSi is the i^{th} character set.

E.g. 1. For password "JohnAnderson@123" :
Entropy $E = 16.\log_2(26+26+10+33) = 105.12$ bits

E.g. 2. For password "Password123" :
Entropy $E = 11.\log_2(26+26+10) = 65.5$ bits
Therefore password "JohnAnderson@123" is cryptographically stronger than "Password123".

Such a network has weak security and can be secured by using a strong passphrase. Passphrase must not be a common language word. It must be a random combination of alphabets, numbers and special symbols which makes it hard to guess. Available wordlists won't contain such random password.

The table below shows the password strength in terms of entropy and its grade with respect to security.

Password Entropy (in bits)	Password Grade
<40	Very Weak
>40 and <60	Weak
>60 and <80	Reasonable
>80 and <120	Strong
>120 and <150	Very Strong
>150	Overkill

Table 1: Password Grades based on Entropy.

Evil Twin

Attack uses Man in the Middle (MITM) and Domain Name Server (DNS) spoofing attacks along with social engineering.

Step 1: Extract details of target network such as ESSID, BSSID and channel number using methodology similar to Handshake Capture.

Step 2: Setup fake access point using "airbase-ng –essid nname –channel X wlan0mon" where "airbase-ng" [2] is a program used to setup access point, "nname" is ESSID or name of the network, "X" is the channel number and "wlan0mon" is the name of the interface in monitor mode.

Step 3: Airbase-ng [2] creates interface "at0" by default. Give subnet and Internet Protocol (IP) address to this interface.
"ifconfig at0 10.0.0.1 netmask 255.255.255.0",
"route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1", where "10.0.0.1" is the IP address of "at0", "255.255.255.0" is the network mask, "10.0.0.0" is the network address and "gw" is the gateway.

Step 4: Give firewall rules

"iptables -t nat -A PREROUTING -j DNAT --to-destination 10.0.0.1"
"iptables -t nat -A POSTROUTING -j MASQUERADE"
where "iptables" [4] is used to set firewall rules

Step 5: Enable IP forwarding
Use "echo 1 > /proc/sys/net/ipv4/ip_forward"

Step 6: Configure Dynamic Host Configuration Protocol (DHCP) server for subnet 10.0.0.0, netmask 255.255.255.0 and DNS server IP 10.0.0.1 along with IP pool.

Step 7: Setup appropriate fake webpage in directory /var/www/html to resemble target router administrator page.

Step 8: Setup mysql database to store harvested password through fake webpage.

Step 9: Start services
Use "/etc/init.d/mysql start" to start MYSQL [5] server.
Use "/etc/init.d/apache2 start" to start Apache [6] web server.
Use "service isc-dhcp-server start" to start DHCP [7] server.

Step 10: Start fake DNS server using "dnschef –fakeip=10.0.0.1 –i 10.0.0.1 -q" where "dnschef" [8] is used to setup fake DNS server.

Step 11: De-authenticate all users using "aireplay-ng –c X –a XX:XX:XX:XX:XX:XX wlan0mon" where "X" is the channel number and "XX:XX:XX:XX:XX:XX" is the ESSID of target network.

Step 12: If a targeted client connects to the fake access point it would get a socially engineered webpage asking for WPA password to upgrade router firmware.

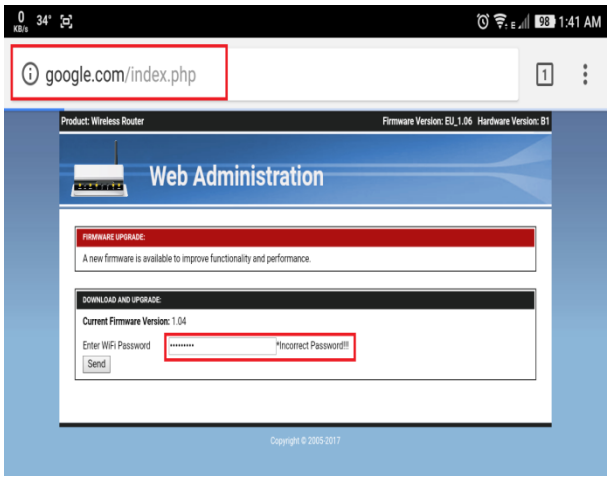

Fig. 4: Fake socially engineered webpage.

If the client enters the password, it is stored in database on attacker's machine and client is redirected to a fake firmware upgrading page.

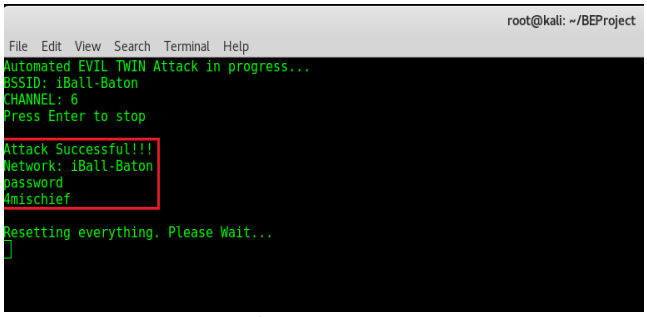

Fig. 5: Successful Eviltwin attack.

If handshake of target network is available then it is also possible to verify harvested password in real time using the Aircrack-ng [1] suite. This attack thus exploits client's lack of knowledge about the wireless system through MITM and DNS spoofing attacks. Such attack can be avoided by educating user about social engineering, phishing and security issues of open Wi-Fi.

MAC Spoofing

Access points might have filtered MAC addresses. MAC spoofing attack uses MAC address of authentic users to gain access to networks with such increased security.

Step 1: Extract details of target network such as ESSID, BSSID, channel number and target client MAC address using methodology similar to Handshake Capture.

Step 2: Use following commands to spoof MAC address:
"ifconfig wlan0 down"
"macchanger –m XX:XX:XX:XX:XX:XX wlan0"
"ifconfig wlan0 up"
where "macchanger" [9] program is used to spoof MAC address and "XX:XX:XX:XX:XX:XX" is target client MAC address.

Step 3: Create wpa_supplicant [10] file for connecting to the target network manually. Use "wpa_passphrase ESSID Password /path/to/wpa_file.conf" where "ESSID" is the network name, "wpa_passphrase" [11] is used to generate wpa_supplicant configuration file and "Password" is the known network password.

Step 4: Try to connect to the target network manually. Use "wpa_supplicant –D wext –i wlan0 –c /path/to/wpa_file.conf" where "wext" is the wireless driver.

Step 5: Run DHCP client program to get IP for the connected interface. Use "dhclient wlan0" where "dhclient" [12] is used to configure client IP address.

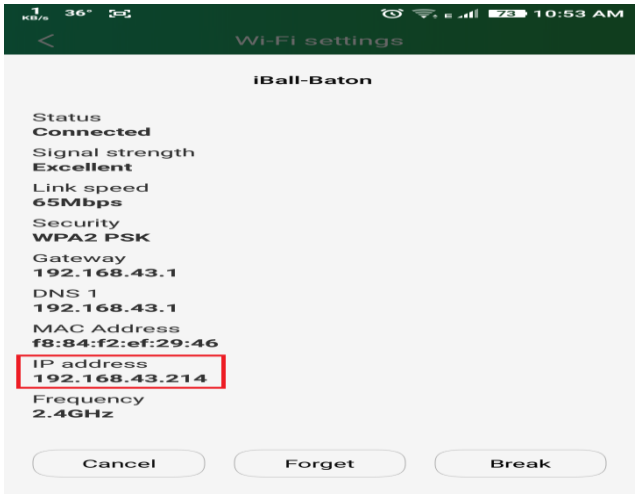

Fig. 6: Target client connection details.

If successful, wireless interface "wlan0" will get an IP address same as the target client. Using "ifconfig" we can see the IP address.

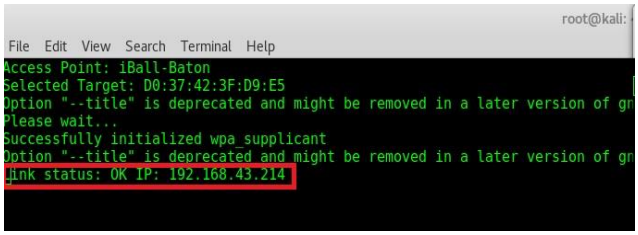

Fig. 7: Stolen IP address based on MAC.

If target client is continuously transmitting or receiving data then frame collision takes place due to IP conflict slowing down the attack considerably.

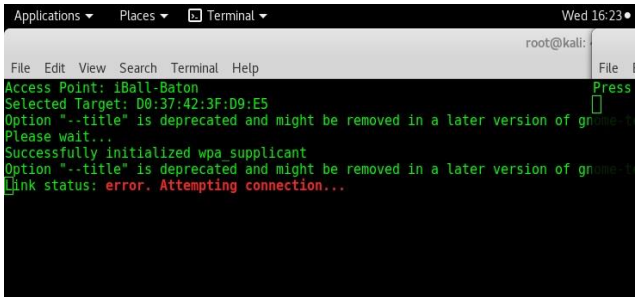

Fig. 8: Connection status during IP conflict.

However, neither client nor attacker can get proper connection. But if target client is not transmitting or receiving any data then attacker's machine gets continuous access to the network. This attack can be slowed down by continuously checking connection with the AP.

Wireless Denial of Service (DOS)

Wireless DOS attack uses de-authentication frames to continuously disconnect all clients connected to target network.

Step 1: Capture packets using monitor mode similar to Handshake Capture using "airmon-ng". Collect MAC address of clients connected to target network from packet capture file.

Use "readarray -t value < <(grep -i -e XX:XX:XX:XX:XX:XX /path/to/capture_file-01.cap | cut -b -17)" where "XX:XX:XX:XX:XX:XX" is the target ESSID.

Step 2: Continuously unicast and broadcast de-authentication frames for all clients.

Use "aireplay-ng –c X –a XX:XX:XX:XX:XX:XX wlan0mon" to broadcast de-authentication frames where "X" is the channel number and "XX:XX:XX:XX:XX:XX" is the ESSID of target network.

Use "aireplay-ng –c X –a XX:XX:XX:XX:XX:XX –c YY:YY:YY:YY:YY:YY wlan0mon" to unicast de-authentication frames where "YY:YY:YY:YY:YY:YY" is the client of target network.

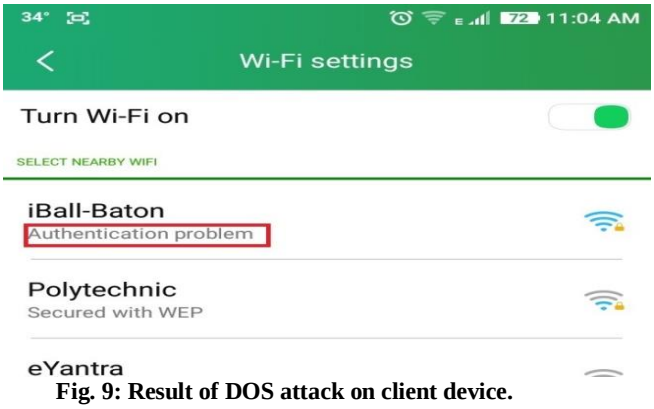

Fig. 9: Result of DOS attack on client device.

Wireless DOS attack can be stopped only by physically locating attacker and taking the attacker machine offline because the de-authentication frames used for DOS are part of IEEE 802.11i standard.

RESULT

WPA/WPA2 provides nominal security when used as WPA-Personal. Network security depends entirely on the password strength and user's knowledge about the wireless system.

Handshake Capture

Captured handshake can be used to crack network password only if the password is weak. If password is a random combination of ASCII characters then it is highly unlikely that it would be present in any precompiled wordlists. This can prevent dictionary attacks. Also using passwords of length greater than 10 characters makes brute force attacks impossible as number of possible

passwords increase exponentially with password length.

Evil Twin

Evil Twin attack tricks target client into entering network WPA password using socially engineered webpage. This attack works due to user's lack of knowledge about the wireless system. It can be avoided by educating users about phishing and social engineering and also about security issues of open Wi-Fi.

MAC Spoofing

In MAC Spoofing client's MAC address is spoofed to get his IP address associated with attacker's machine. MAC spoofing is difficult to detect and avoid as it might require custom firmware on access points.

Wireless DOS

Wireless DOS de-authenticates all users connected to target network. IEEE 802.11 offers no specific protection against DOS attack on Wi-Fi access points. The only way to stop this attack is to locate attacker in vicinity and stop it.

CONCLUSION

In this paper, we have shown some potential attacks on Wi-Fi networks and possible solutions for some of them. The principle idea is to expose the vulnerabilities of insecure networks and try to secure the flaws. We have seen four types of attacks. Handshake capture attack exploits weak passphrase of a network. This can be stopped by using strong random password. Evil Twin attack focuses on social engineering a fake webpage to get Wi-Fi credentials. This attack can be avoided by educating users about phishing, social engineering and security risks of open Wi-Fi. MAC Spoofing disconnects legitimate user and spoofs its MAC to get its IP from access point. This attack can be slowed down by continuously checking network connection and connecting to the network but cannot be avoided. Wi-Fi DOS attack de-authenticates all connected clients with unicast and broadcast frames. This attack can be stopped by locating attacker physically and stopping the attack.

REFERENCES

1. https://en.wikipedia.org/wiki/IEEE_802.11i-2004
2. https://www.aircrack-ng.org
3. http://tools.kali.org/wireless-attacks/cowpatty
4. http://ipset.netfilter.org/iptables.man.html
5. https://dev.mysql.com
6. http://httpd.apache.org/docs
7. https://linuxconfig.org/what-is-dhcp-and-how-to-configure-dhcp-server-in-linux
8. http://tools.kali.org/sniffingspoofing/dnschef
9. https://linuxconfig.org/change-mac-address-with-macchanger-linux-command
10. https://w1.fi/wpa_supplicant
11. https://linux.die.net/man/8/wpa_passphrase
12. https://linux.die.net/man/8/dhclient