ClubHACKMag

1st Indian "HACKING" Magazine

Can you cage a wifi signal???

Issue 17 | June 2011
www.clubhack.com

TechGyan Pentesting Your Wireless | **LegalGyan** Copyright and Cyberspace |
ToolGyan Wi-Fi Tools | **Mom's Guide** Best Practises for Wi-Fi Networks |

Can you cage a Wi-Fi signal? You may or may not... discover it for yourself in this issue.
This issue is specially dedicated to wireless network security. Learn about attacks and penetration testing on wireless networks. Additionally we have some demos for the same and best practises for Wi-Fi network security. I am sure these would be of great value to network admins. By understanding the methods used by attackers in compromising Wi-Fi networks, network admins can redefine their strategies required to secure their networks.

Pankit Thakkar

This issue covers Pentesting Your Wireless in Tech Gyan, Best Practises for Wi-Fi Networks in Moms Guide, Wi-Fi Tools in Tool Gyan, Copyright and Cyberspace in Legal Gyan and Forensics with Matriux - Part 2 in Matriux Vibhag.

What topics would you like to be covered in the upcoming issues of CHMag? Feel free to write us at **info@chmag.in** and do check out the new look of **http://clubhack.tv** Hope you'll like it.

ClubHACKMag

Issue 17, June 2011.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

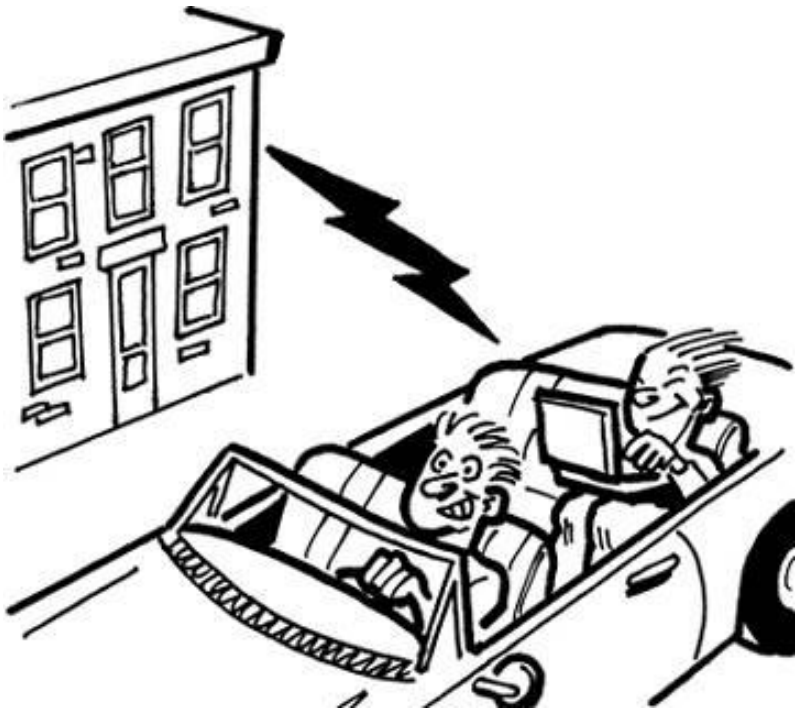
Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS



Pentesting your own Wireless Network

Introduction to IEEE 802.11

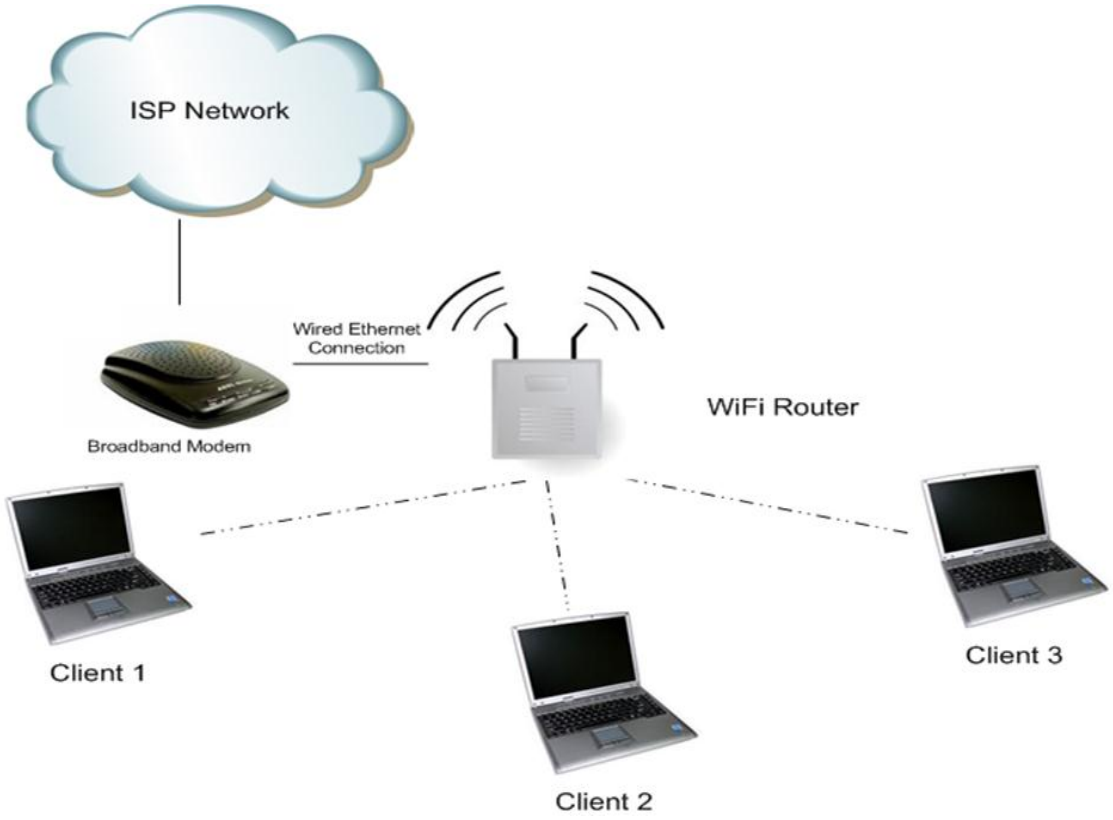
IEEE 802.11 is a set of protocols used for implementing wireless LAN. IEEE Protocol standards are created and maintained by IEEE LAN/MAN Standard Committee.

WLANs operate in 3 different frequency ranges that is2.4Ghz (802.11b/g/n), 3.6Ghz (802.11y) and 4.9/5.0Ghz (802.11a/h/j/n). Each of these Frequencies are further divided in to multiple channels. Every country has permissible channels and maximum power levels. However, wireless card can be easily configured to disregard these policies. One can make the wireless NIC hop on different channels, but at any given period of time a wireless NIC will be connected only to a single channel.

Different Wireless Architectures & Implementations

Wi-Fi implementation as any other technology is needed to drive Business. It's very important to get an optimum ROI with required security & controls in place. Keeping this in mind, the Home implementation of Wi-Fi network differs as compared to SOHO or Enterprise implementation.

1. **Wi-Fi Network at Home:**
   In a usual home environment multiple clients connect to an AP which is connected to a broadband (DSL / Cable) modem. Wi-Fi at home is mainly used for internet access and all the users have same privileges.



Wi-Fi network at Home

The following is typical of a Wi-Fi implementation at home's:

- Clients connecting to AP / Wireless Routers
- Wireless Router connected to a broadband modem for internet service
- Security – WEP or WPA/WPA2 Personal
- SSID broadcast
- MAC Address filtering
- Paraphrases/passwords to access Wi-Fi service never changed and at times easy to guess

Due to the nature of work and the type of information, it is not feasible to implement Enterprise class security for home users. The home networks are easier to compromise but again it's a tradeoff between security and ease of use.

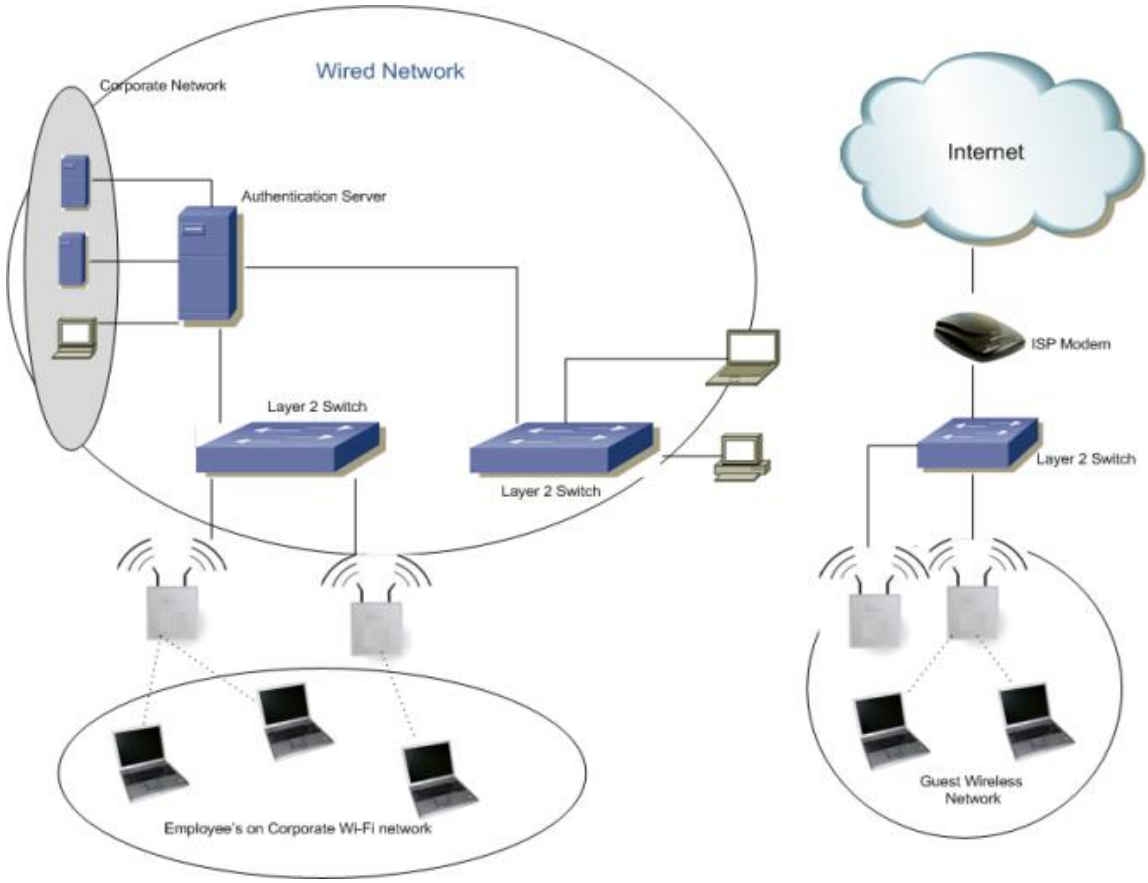
However, there are good practices which if implemented correctly would deter and make it difficult for an attacker to break into the home Wi-Fi network.

2. Corporate / Enterprise Network:

In a Corporate enterprise network, stronger security controls are required. Wi-Fi is used by employee's to access the corporate network and by the guests / visitors to access the internet.

Access to Corporate network through Wi-Fi requires the employee's to authenticate to the authentication server before the access is granted to the corporate network. They key features of this network setup are:-

- Restricted to employee's
- Involves authentication using authenticating server
- Stronger encryption protocols



Corporate/Enterprise Network

- Access on need to know basis
- Security – WPA2 Enterprise along with EAP-TTLS, MSCHAPv2 etc. is used

In a corporate environment there is usually a 'Guest' wireless network for guests and visitors. This network is only for internet access and is supposed to be isolated from the Corporate Wi-Fi network.

Encryption & Authentication used in IEEE 802.11 Environment:

Wired Equivalent Privacy (WEP) – WEP uses RC4 encryption algorithm which has several weaknesses. IEEE 802.11i was ratified in 2004 and is the primary means of wireless security. In spite of known vulnerabilities due to the oldest and easiest configuration WEP is still widely deployed at least on Home Networks

Wi-Fi Protected Access (WPA) – WPA protocol implements majority of IEE 802.11i standard requirements. WPA makes use of Temporal Key Integrity Protocol (TKIP) instead of RC4 used in its predecessor WEP. To offer greater security, CCMP, an AES based encryption protocol was released in the final IEEE 802.11i standard (referred to as WPA2).

WPA Personal – Commonly referred as WPA – Pre shared key (PSK). The clients authenticate with the AP's using the 256 bit keys. It's mainly used at homes and in SOHO environment

WPA Enterprise – Mainly designed for Enterprise networks and requires authentication using RADIUS server. Extensible Authentication Protocol (EAP) is used for authentication, which comes in different flavors (EAP-TLS, EAP-TTLS). It is also referred as WPA-802.1x mode

RADIUS protocol inherently only allows for password based authentication i.e. the password is sent as MD5 Hash or response to a challenge (CHAP-password). EAP enriches the authentication feature of RADIUS.

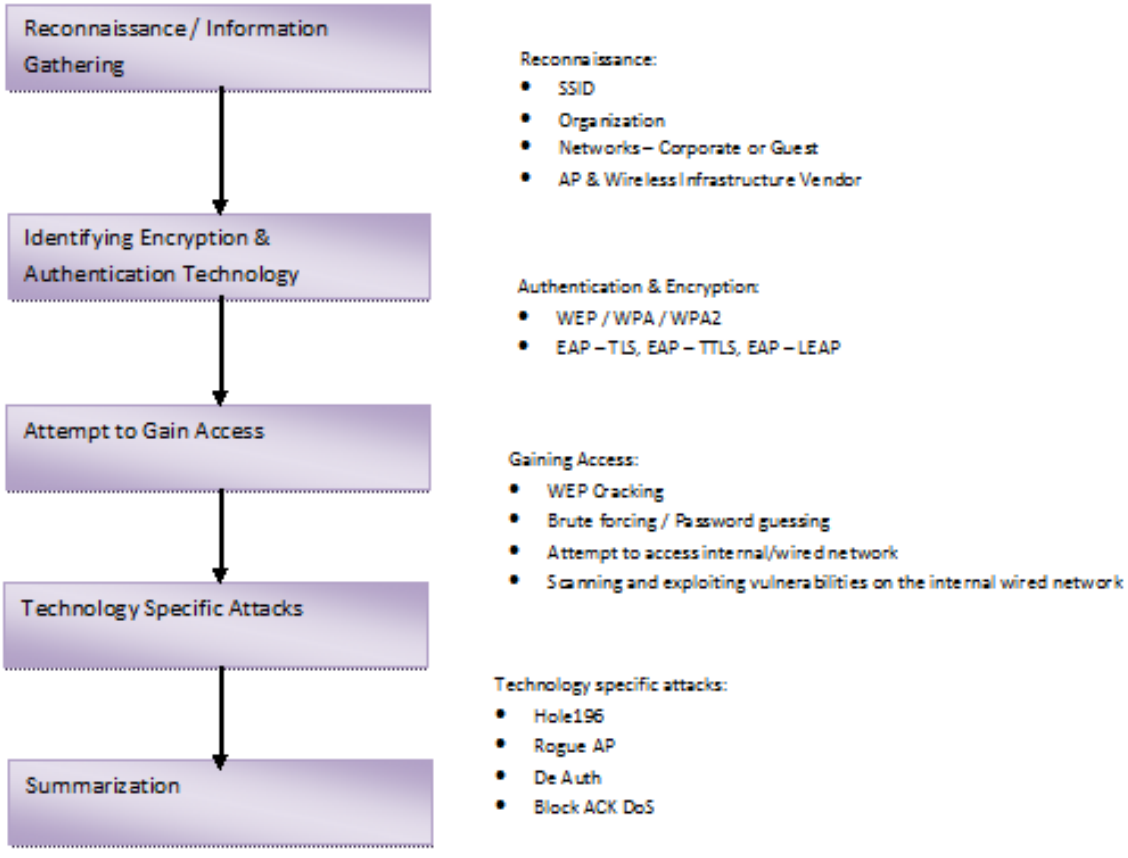
VA&PT of Wireless Networks

Approach for conducting VA&PT of a wireless network is similar to traditional connected network but there are added risks and vulnerabilities specific to Wi-Fi network that need to be looked into. To conduct VA&PT of wireless network it is very important to get the objectives clear.

Wireless network if compromised can lead to unauthorized access to the corporate infrastructure which might be on the traditional connected network.

Approach:-

1. Reconnaissance
2. Identifying the Encryption & Authentication Technology
3. Attempt to Gain Access
4. Brute Forcing / Guessing Passwords
5. Identifying weakness in the Wi-Fi Technology
6. Attacks specific to Wi-Fi Technology
7. Summarization & Reporting



Phase I: Reconnaissance

This is the most important phase whereby the attacker gains most of the information required for further directed attacks. Intelligent sniffing can help in gathering good amount of information on the wireless network, technology being used and the deployment.

Beacons are used to relay important information like weather conditions, navigation details, status reports etc. Beacon frames in an IEE 802.11 WLAN contain important details like SSID, type of the network, encryption details, supported data rates, manufacturer of AP etc. It is transmitted periodically to make the presence of WLAN known.

Tools like Kismet, NetStumbler, Wireshark can assist in reconnaissance. With the help of these tools details like SSID, Type of encryption & authentication, access point MAC Address along with approximate location, signal strength, channels being used etc. can be obtained.

The information obtained in this phase is what dictates the further course of wireless security testing.

Exploiting the Authentication Protocol:

Due to the inherent nature of Wi-Fi networks i.e. without wires and theoretically no boundaries; security has always been a prime concern. Authentication, Encryption, Authorization are a must in a Wi-Fi setup. In 802.11X network EAP gives RADIUS the capability to work with variety of authentication schemes like Kerberos, PKI, Smart Card etc.

In a typical and common implementation of EAP like TLS, MD5 and MSCHAPv2 (used in most of the Windows clients) the user ID/Login ID (active directory/domain) is sent in clear text during handshake.

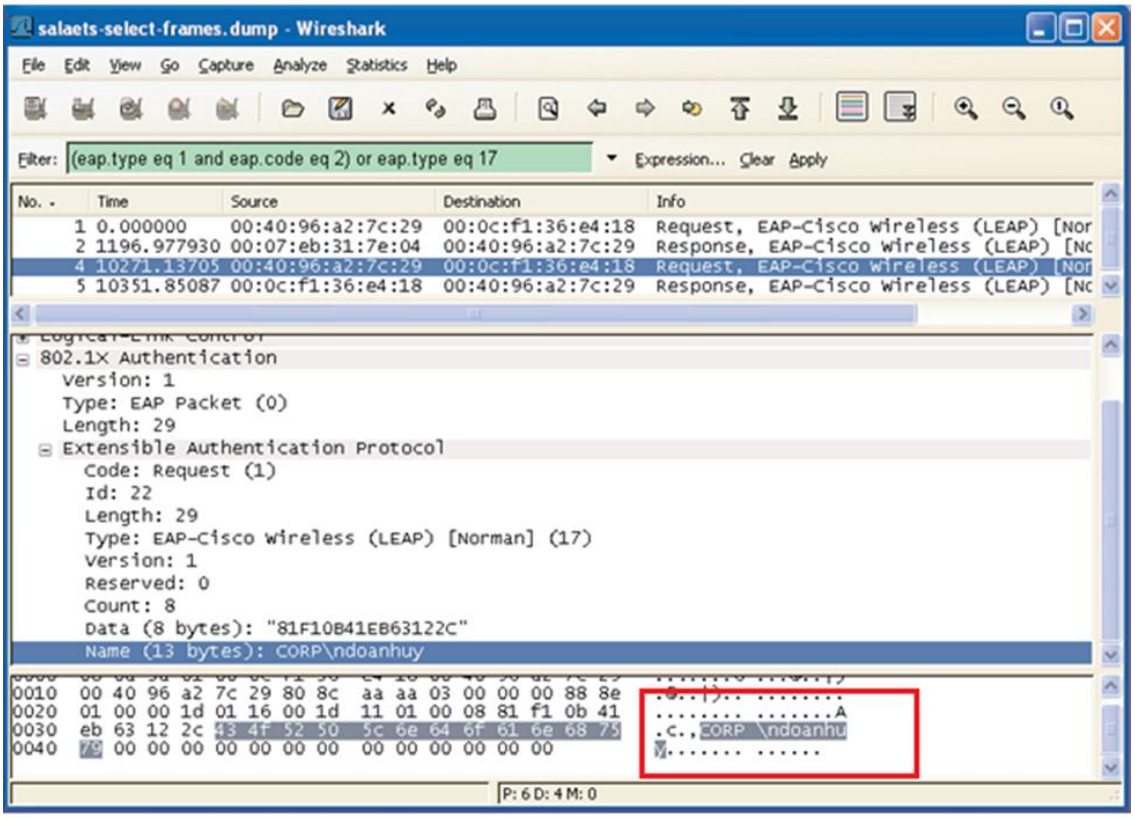


Figure 1: LEAP Handshake [1]

Compromise of Login ID can further lead to brute force attempts for the passwords leading to unauthorized access. In Figure 1 it can be seen that the User / Login ID is displayed in clear text. Wireshark is used to sniff the EAP – LEAP packets.

Phase II: Attacks on Guest Wireless Networks

Organizations these days have an isolated wireless network for guests & visitors to access the internet. The 'Guest' network is supposed to be an isolated network with no connection / interface to the corporate network.

The following is common in a typical implementation of a 'Guest' wireless network:

- WEP
- WPA2 with pre-shared key (PSK)
- Internal IP Address assigned to the guests
- The 'Guest' client part of 'Guest VLAN' hypothetically isolated from the corporate / enterprise network; in many cases it is not
- For accessing the 'Internet' resources; login credentials (username & password) required to be entered in the browser
- Pre-Shared Keys are common for all 'Guests' and are seldom changed
- Login Credentials used for accessing the internet are common for all the 'Guests'
- Outsiders, contractors, vendors, guests, over sea / travelling employees etc. given access through the same 'Guest' network
- 'Guest VLAN' is not isolated from the corporate VLAN

Consider a scenario where an attacker sitting in the organization's premises gains access to the 'Guest' network's IP Address. Irrespective of if he/she can access the internet assigning of organization's internal IP Address to the attacker's machine is a major threat.

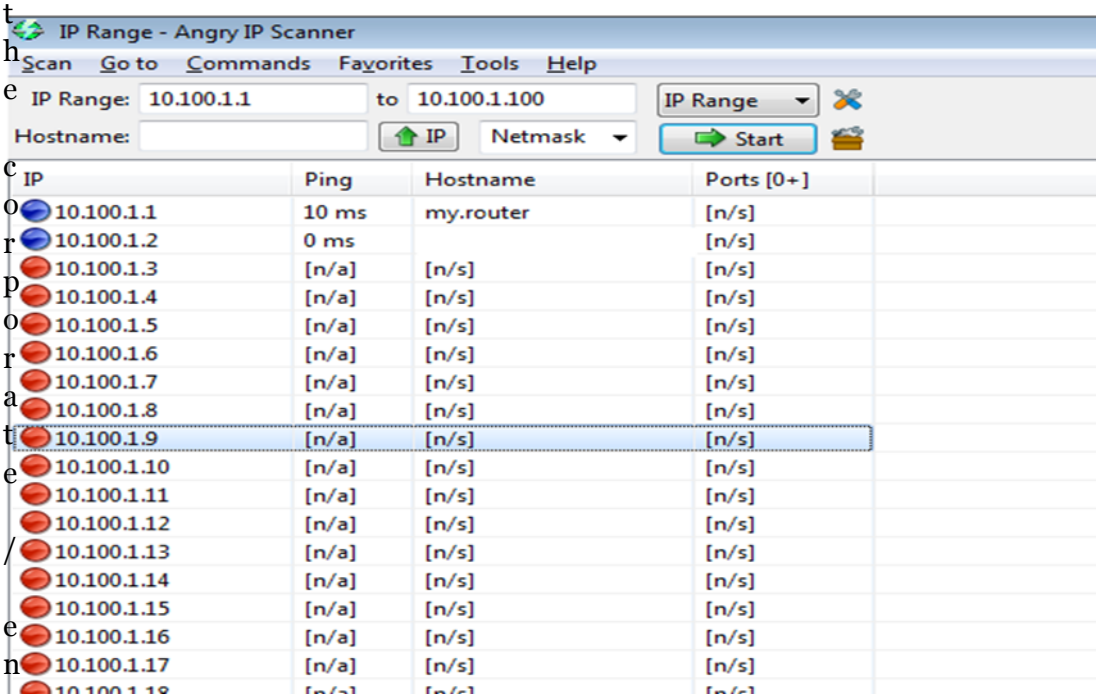


Figure 2: Scan for 10.100.1.1 to 10.100.1.100 range showing two hosts are up

The attacker can use tools like 'Angry IP Scan' to scan the entire range of IP Address to find out the host that is 'UP'. Once the host is identified traditional VA&PT tools like Nessus, nmap, Metasploit etc. could be used to identify and exploit the vulnerabilities.

Phase III: Implementation specific Attacks

Attack on WEP:

Attack Scenario 1: Cracking Wep Key Using airmon-ng

Boot your favorite Linux distribution and initialize command console, Make sure you have the following tools installed:

1. **Aircrack-ng:**Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.
2. **Macchanger:**A GNU/Linux utility for viewing/manipulating the MAC address of network interfaces.

Part A: Setting up your Machine

1. Let's start with setting up your machine with required software's and libraries. You can install the above mentioned software's from your linux distributor's online repositories.
2. For Debian Based Linux Distribution (Eg: Debain, Ubuntu, linux mint etc.):-

```
sudo apt-get install aircrack-ng
sudo apt-get install Macchanger
```

For Redhat Based Linux Ditribution (Eg: RHEL, Centos, Fedora, Opensuse):-

```
yum install aircrack-ng
yum install Macchanger
```

3. This command will list the current network adaptors in your system in detail; see what name has been assigned to your Wi-Fi adaptor. For E.g: wlan0, wlan1, etc.

```
ifconfig
```

4. This command will stop the card and disable's the broadcast and reception, as system won't allow you to change the MAC address when card is in use:

```
airmon-ng stop [Wi-Fi Card name]
```

5. Macchanger utility will change the original MAC address to any MAC address you desire.

```
macchanger  - -mac [Desired MAC
address] [Wi-Fi card name]
```

6. This command will activate the wireless network adaptor for broadcast and reception, In some Linux distributions you may also witness the following error, as shown in the snapshot below:

```
Airmon-ng start wlan0
```

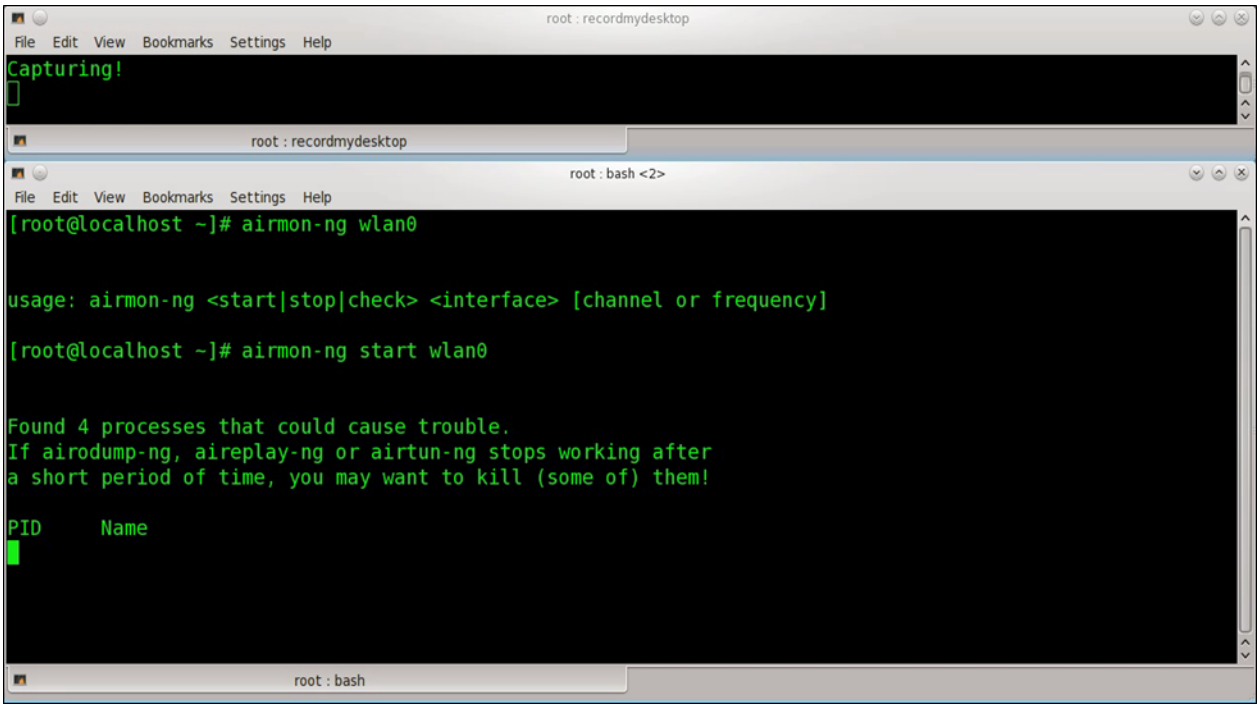


Figure 3: (step 6) Starting airmon-ng

7. If you see this error coming up on your console, you don't need to lose your heart, it's just that few services are already using your wireless adaptor or it's associated files, you will also see the process names and PID's, you can stop those process by using the following command's:

```
Kill - kill [PID ] - process
```

```
airmon-ng start [Wi-Fi Card name]
```

mono, use that adaptor in further commands where – '[Wi-Fi card name]' appears

PART B: Start Capturing Data Packets

1. This command will initialize the Wi-Fi network monitoring & will show wireless network's in range with encryption cipher being used like Wep, WPA or WPA2 and more.
2. As you execute the following command, you will see a certain number of beacons and data packets that will be stored in the filename you have given. The file will be stored in the root of the system drive (Click on Computer and you will see the file). The file will be present in two formats: *.cap, *.txt.

```
airodump-ng-c [Channel Number] -
w [Desired Filename for later
decryption] - - bssid [BSSID]
[Wi-Fi Card name]
```

Part C: Speed up the Process Data Packet's Capturing

Open a new console after the first data packet has been stored. Type the command in the new console and execute it

```
airreplay-ng -1 0 -a [BSSID] -h
[FAKED MAC ADDRESS] -e [Wi-Fi
name] [Wi-Fi card name]
```

the data packets required for breaking the key will increase dramatically thereby saving you a lot of time.

PART D: Cracking/brute forcing Wep Key

Open another console once you have around 20,000 data packets and type the following command to reveal the WEP key.

```
aircrack-ng -n 64 -b [BSSID]
[Filename without the extension]
```

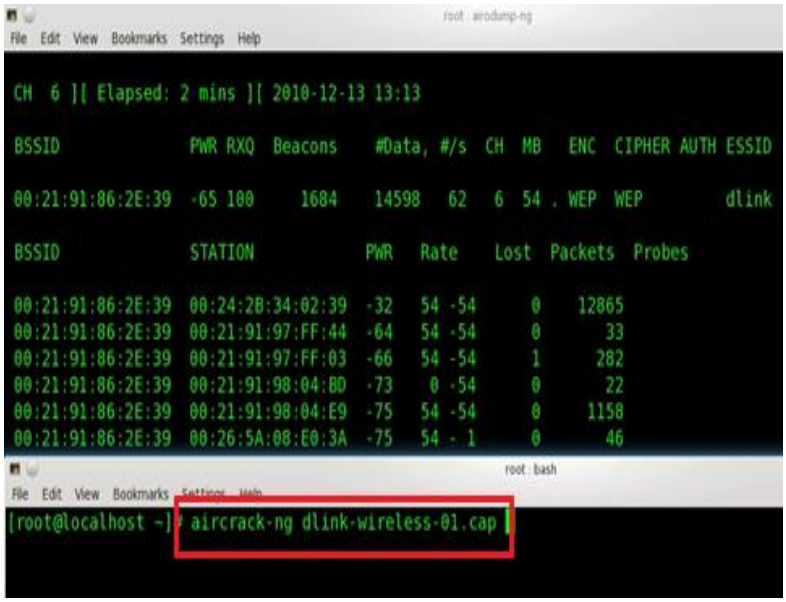


Figure 4: Aircrack-ng in action

It is not necessary that the key should have exactly the same digits as shown above so please don't freak out if you see a 10 digit or 14 digit key.

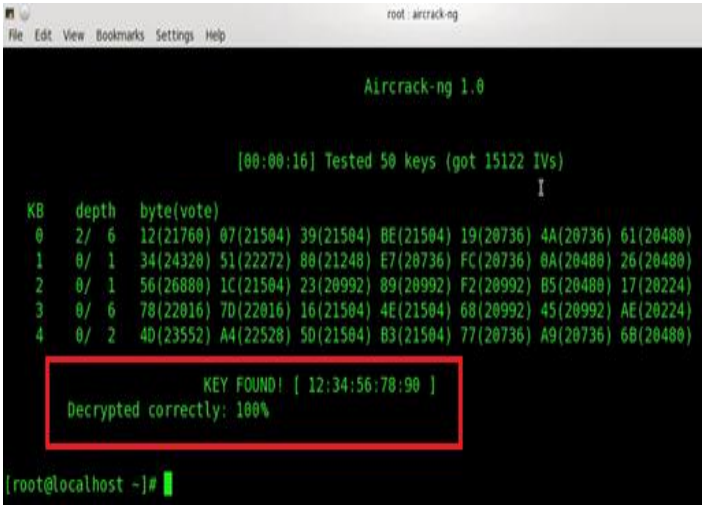


Figure 5: Brute force attac completed. Key decrypted.

Also if the decryption fails, you can change the bit level of the decryption in the command:

```
aircrack-ng -n [BIT LEVEL] -b
[BSSID] [Filename without
extension]
```

Remember, the bit level should be a number of 2^n where n = 1,2,3,4...

Rogue Access Points

Rogue Access Point is a wireless access point that has been illegally installed within a range of secure wireless network without the consent of the administrator of that wireless network. The sole purpose behind creating the Rogue access points is to capture the secret key used to by the clients to authenticate them to the legitimate wireless access point. Attacker's exploits the loophole and setup their own access point with the same SSID's to fool the clients in a way so that instead of connecting to legitimate access point they may connect to the Fake Access point created by the attacker. Once the attacker gain's access to

the secured wireless network he may also use sniffing and man in the middle attacks to capture the juicy information travelling throughout the network like login credentials, credit card details other important information.

Airsnarf [1]

Itis a simple rogue wireless access point setup utility which can found in Backtrack a popular security distribution for penetration testers. Airsnarf is specially designed to demonstrate how rogue access point can actually steal usernames and passwords from publically available hotspots. It exploits the vulnerability in 802.11b hotspots by confusing the users with DNS and HTTP redirects from a competing legitimate wireless access point.

Airsnarf is very user friendly. It contains a configuration file `./cfg/airsnarf.cfg` file in which details like local network, gateway & SSID can be configured. The clients associated with the Fake / Rogue AP will receive the IP, DNS and gateway details from the Rogue AP. Also, it is possible to configure Airsnarf 'splash page' as dummy login page and capture the login credentials of the users. These details would be mailed to root@localhost.

Rogue AP is in a way a Social Engineering attack where in the attacker exploits the human tendency of 'trust'.

Other tools available for creating Rogue access point are freeradius WPE, karmetasploit a module in Metasploit (which is a combination of famous tool called karma), Hotspotter, Fake AP, VOID11 and wifitap.

hole196 [2]

Please note this vulnerability was identified and presented by MdSohail Ahmad from AirTight Networks at BlackHat 2010.

Background:

Man-in-the-Middle Attack or what is popularly known as MITM is very common in wired networks. But, now it's very much possible in WPA2 networks as well.

WPA2 uses two ncryption keys:

- Pairwise key (PTK)
- Group Key (GTK)

GTK – GTK is broadcasted by the Access Point (AP) to all the clients and remains common for all the clients.

PTK – It's a unique to each client and is used to protect unicast data frames. It changes with each session.

As per IEEE 802.11 standard PTK has inherent capability whereby it can detect MAC Address spoofing and data forgery. GTK has not been designed with this feature. These details are mentioned on the page 196 of IEEE 802.11 standard and hence the vulnerability was named as 'Hole196'. Once again the flaw in the inherent design of the protocol has been used to exploit this vulnerability.

'hole196' does not lead to cracking of WPA2 keys or discovering the passwords. It is a threat by the malicious insider which can act as a legitimate Access Point and affect the other clients i.e. Man-in-the-Middle Attack.

Attack:

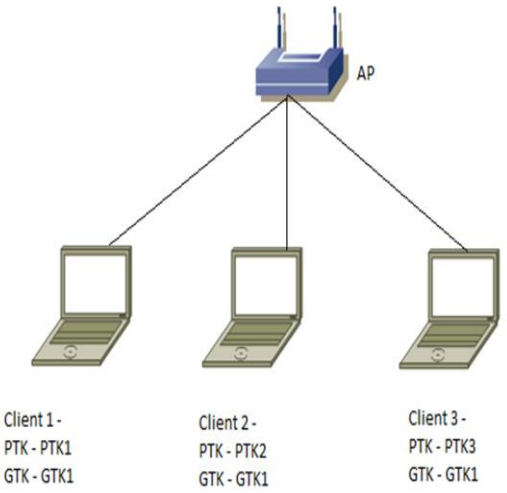


Figure 6: Three connected Clients

The Access Point (AP) shares the same GTK with all the connected clients. So, GTK is known and is common to all connected clients. GTK is used as an encryption key by the AP and decryption key by the client.

```
EAPOL: External notification - portValid=1
State: 4WAY_HANDSHAKE -> GROUP_HANDSHAKE
RSN: received GTK in pairwise handshake - hexdump(len=18): [REMOVED]
WPA: Group Key - hexdump(len=16): [REMOVED]
WPA: GTK key: 7b:41:d1:bb:2e:65:b6:b4:99:3c:56:32:dd:78:51:7b
WPA: Installing GTK to the driver (keyidx=1 tx=0 len=16).
WPA: RSC - hexdump(len=6): 00 00 00 00 00 00
nl_set_encr: ifindex=6 alg=3 addr=0x808fcad key_idx=1 set_tx=0 seq_len=6
WPA: Key negotiation completed with 00:1b:11:50:3b:1e [PTK=CCMP GTK=CCMP]
Cancelling authentication timeout
State: GROUP HANDSHAKE -> COMPLETED
```

wpa_supplicant software log file

Figure 7

The log of wpa_supplicant software running on wireless clients shows that GTK key is known to the client devices.

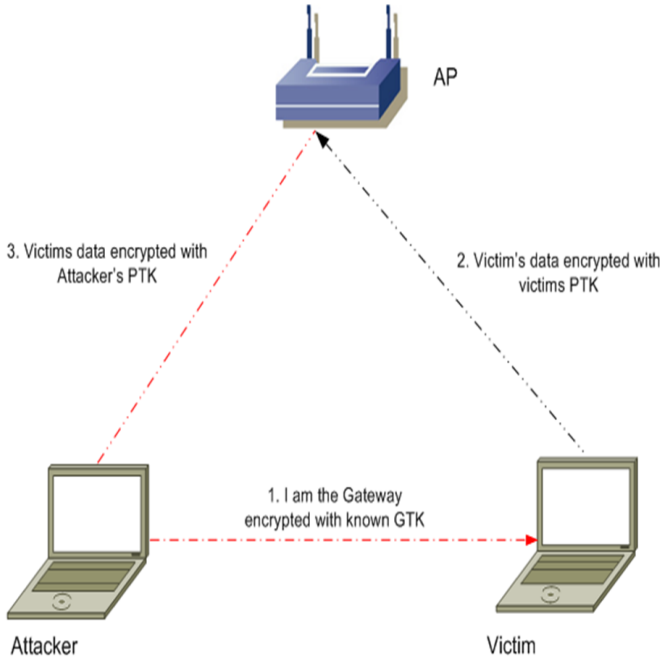


Figure 8

- Attacker injects fake ARP Request packet to poison client's cache for gateway. For the victim the attacker's machine becomes the client gateway.
- Victim sends all traffic encrypted with its PTK to the AP, with Attacker as the destination (gateway)
- AP forwards Victim's data to the Attacker encrypting it in the Attacker's PTK. So Attacker can decrypt Victim's private data.

Spoofed ARP packets are never sent to AP and they never go over the wire and hence cannot be detected by wired IDS/IPS.

Block ACK DoS [3]

All of us are familiar with TCP Sliding Window flow control concept. On the similar lines IEEE 802.11e and IEEE 802.11n are designed to acknowledge a block of packets instead of sequential transmit/acknowledge. The AP sends the client Add Block Acknowledgement (ADDBA) indicating the starting of the transmission, window size, sequence numbers etc. Anything outside the window is dropped by the recipient. So here is the catch!

There is no security on the control frame and hence ADDBA frame can be impersonated and spoofed.

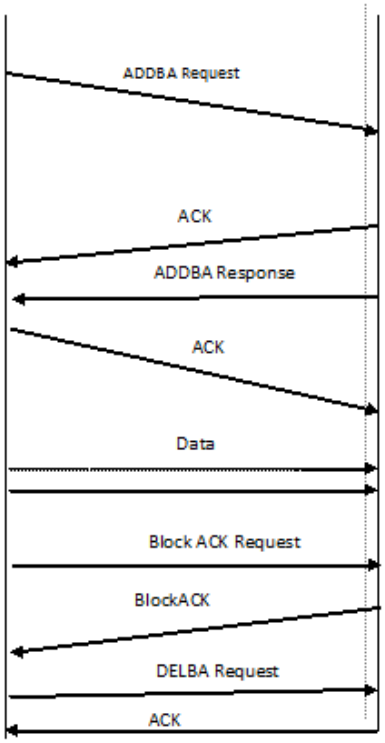


Figure 9

Ideal Scenario:

- AP sends the ADDBA request to client identifying the window size, starting sequence number etc.
- Client responds with ACK followed by ADDBA response
- AP sends an acknowledgement (ACK)
- Clients starts receiving the frames defined in the ADDBA control frame and ignores all the frames that fall outside this range
- The AP sends BlockACK Request frame to client to know the status of the received frames
- Client reverts with a BlockACK if all the frames were received alternatively client can request for a retransmission or selective transmission of lost packets
- AP sends a delete block acknowledgement (DELBA) Request to release the buffers of both AP and Client.

Vulnerability in Block ACK Handling & DELBA frame:

- Since the control frames are not protected a malicious user / attacker can spoof the ADDBA frame and tamper the sequence details causing the recipient (in this client) to drop some or all the frames
- This would result in re transmission or can also lead to DoS
- Alternatively malicious DELBA messages can be sent to untimely free the sender and receiver buffers causing disruption of service

References:

[1] http://airsnarf.shmoo.com/

[2] MdSohail Ahmed from AirTight networks.

- http://www.airtightnetworks.com/WPA2-Hole196
- BlackHat 2010

[3] High Speed Risks in 802.11n Networks by Joshua Wright from Aruba Networks presented in RAS Conference 2008.

Note: By the time of this writing, a very good tutorial series has been launched by VivekRamachandranOn SecurityTube.net.

Ishan Girdhar

Ishan Girdhar working as a Information Security consultant. Ishan loves exploring different linux distributions. He is currently working with AKS IT Services Pvt. Ltd Noida.

Vishal Kalro

Vishal is an Information Security Consultant specializing in Infrastructure & Network Security. He has also published articles on Cloud Computing Threat & Security, Measuring WAN Performance & Social Engineering. He loves playing Badminton and reading fiction novels.

Wi-Fi Tools

This section in itself may look incomplete, to have full flavor read Tech Gyan.There are many Wireless Testing tools in the wild for the different OS flavors right from Windows, Unix to Smart Phone OS. Unix based tools remain the most popular among them.

Unix

Backtrack which is a Unix distribution for Ethical vulnerability assessment & penetration testing (VA&PT) has an impressive collection of tools for reconnaissance, vulnerability assessment, cracking keys & passwords, penetration testing etc.

To name a few:

1 **Kismet** - Kismet is a powerful analyzer for analyzing the wireless traffic at a glance.

The following features are supported by Kismet:

- 802.11b, 802.11g, 802.11a, 802.11n sniffing
- Standard PCAP file logging (Wireshark, Tcpdump, etc)
- Client/Server modular architecture
- SSID detection (including hidden SSID's)
- Distributed remote sniffing with Kismet drones
- XML logging for integration with other tools
- Linux, OSX, Windows, and BSD support (devices and drivers permitting)

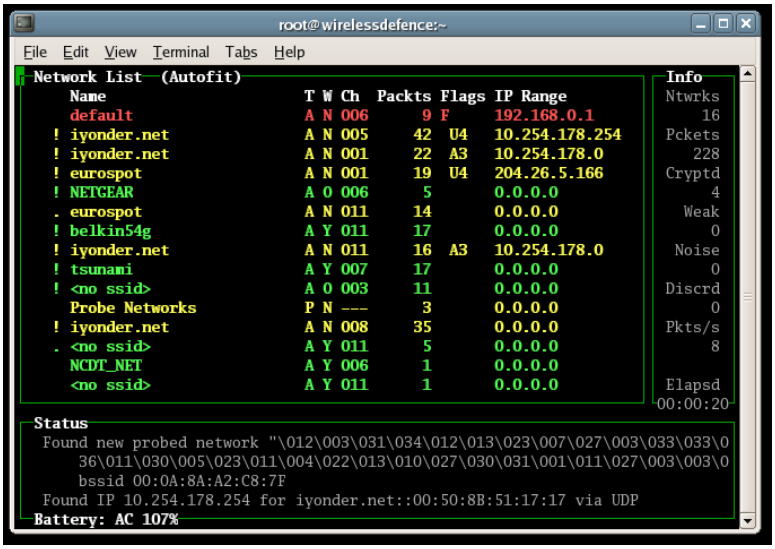


Fig 1: Kismet showing the Network List & Details [1]

2. **Air Crack** – It assists in cracking WEP & WPA-PSK and recovers the keys being used. It contains tools like Air Decap& Air Replay (802.11 packet injection utility), Airodump (used to capture 802.11 packets) etc. thus making it a suite containing tools and utilities for auditing of wireless networks.

3. **Airsnort**– It recovers encryption keys.

4.**CowPatty**– It is used to audit WPA-PSK keys

5. **FakeAP** – Used to generate spoofed/ counterfeit 802.11 b access points

6.**Karma** – KARMA once again is a popular suite of tools used for Wireless Auditing. It can discover the clients and the wireless networks as per client preference. Rogue AP's can be created to capture client credentials or exploit the vulnerabilities on the client side.

7. **GerixWiFi Cracker**– Once again a very good GUI based tool comes pre-installed in BackTrack 4. It can be used for WEP & WPA cracking, to create Fake AP's etc.
There are lots more. For more details on BackTrack refer to – http://www.backtrack-linux.org/

Fig 2:Gerix, a GUI based security tool

Windows

NetStumbler:

NetStumbler also known as Network Stumbler is an excellent Windows based tool for Wi-Fi reconnaissance.

Usage of NetSumbler:

- Ward-riving
- Identifying SSID's
- Identifying rogue Access Points (AP)
- Assistance in determining the location of the AP's
- Determining signal strength etc.

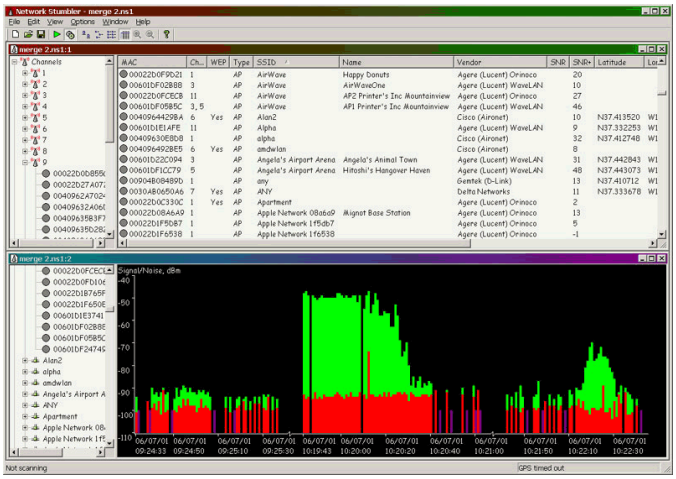


Fig 3 NetStumbler [2]

Wi-Fi Scanning using Smartphone

Classically for War Driving the following items were needed:

- Laptop with Wi-Fi card
- GPS Module for mapping the location of the Access Points

What you need today is only a Smart Phone!

There are quite a few Wi-Fi Scanning / War Driving applications for all breeds of Smart Phones. They not only detect the Wi-Fi network but help in disclosing the SSID's, type of encryption, channels, signal strength and mapping the position of the access points on Maps giving the approximate real time location of AP's.

WiGLEWifi War driving:

This is a FREE application available on Android Market and is a good to have. It not only lists the Wi-Fi network in range along with SSID's but also discloses the encryption and authentication protocol being used. It also plots the approximate location of the Access Point on a map.

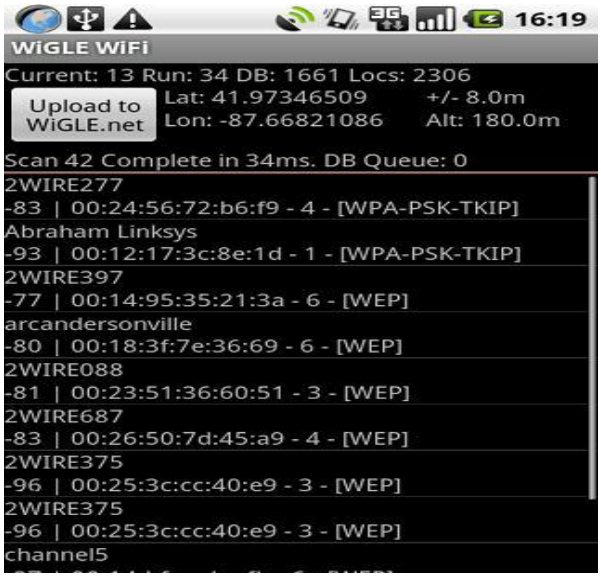


Fig 1: WIGLE WiFi, Android based Utility [3]

The details like channel used, signal strength, latitude & longitude etc. are also captured.

The other commonly used tools for Android platform are:

- Wardrive
- WiFi Buddy etc.

Then there is **MiniStumbler** which is called the little brother of NetStumbler for Pocket PC's (Windows) platform.

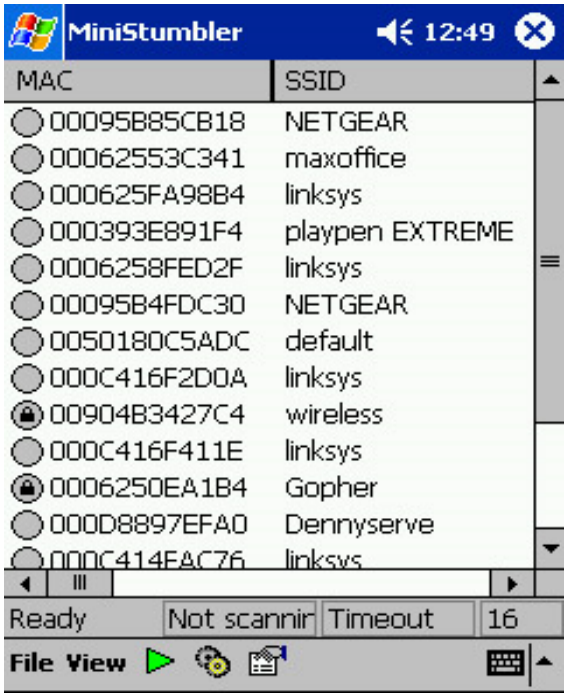


Fig 5 MiniStumbler Windows Utility [4]

MiniStumbler helps in:

- Detecting SSID's
- MAC Address of the AP / Wireless router
- Encryption type
- Channel & signal strength
- Plots co-ordinates if a GPS device is attached / present on the handheld etc.

Similarly there are tools / utilities available for other mobile platforms as well.

References:

[1] http://www.wirelessdefence.org/Contents/kismetMain.htm

[2] http://www.networkuptime.com

[3] http://www.androidapplicationspro.com/wigle_wifi-wigle_net-1_12-download.html

[4] http://flylib.com/books/en/1.323.1.17/1/

Vishal Kalro

Vishal is an Information Security Consultant specializing in Infrastructure & Network Security. He has also published articles on Cloud Computing Threat & Security, Measuring WAN Performance & Social Engineering. He loves playing Badminton and reading fiction novels.

IshanGirdhar

IshanGirdhar working as a Information Security consultant. Ishan loves exploring different linux distributions. He is currently working with AKS IT Services Pvt. Ltd Noida.

Wireless Security - Best Practices

This article is about different kind of Best Practices that should be followed when using Wireless LAN.

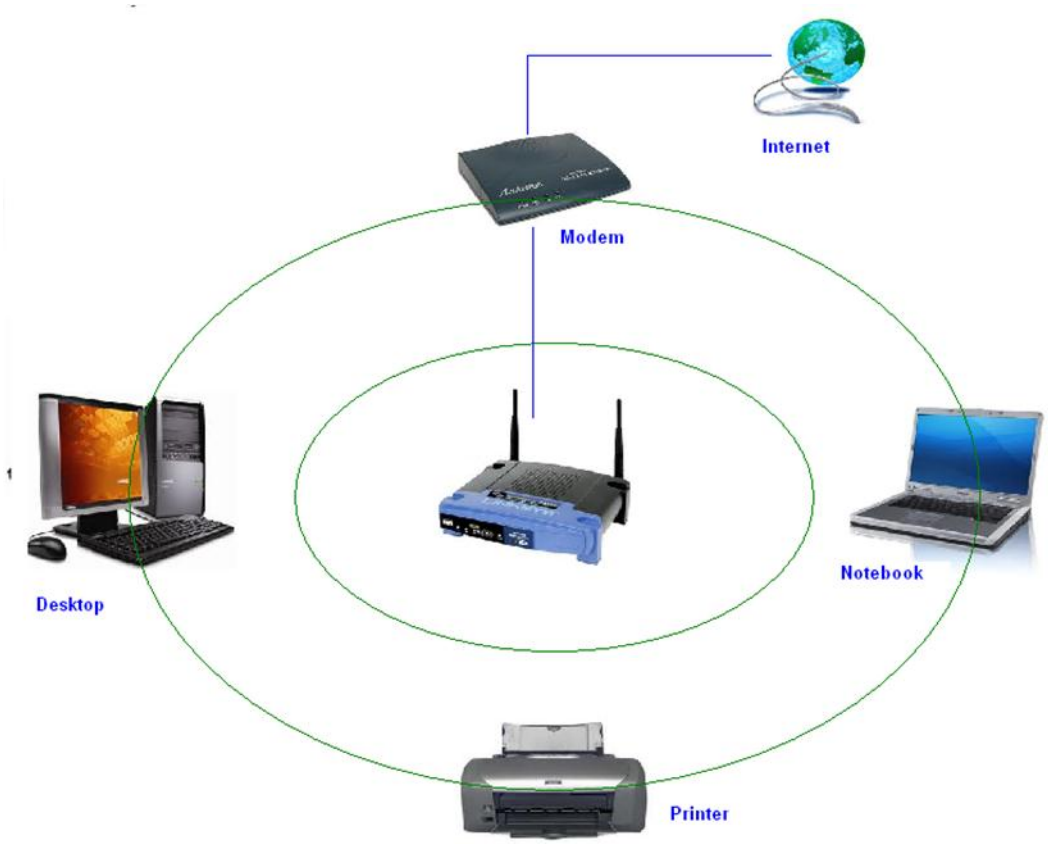
What is Wireless LAN

The Wireless LAN or WLAN is becoming a popular way to connect devices such as computers these days. In offices and homes, WLAN has become an alternative way of communication compared to wired LAN. The convenience to connect different devices is both cost effective and easily maintainable.

The Wikipedia says: "Wireless LANs have become popular in the home due to ease of installation, and the increasing to offer wireless access to their customers; often for free."

The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables. You can roam around freely in office premises, home or around.
2. WLANs are cost effective. Cabling all the way in the offices, hotels etc are not needed. So its cheap and provide same quality of service.
3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.
4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.
5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.



A typical wireless network

Major issues with WLAN

Having said that, WLAN are also as prone to various attacks as their counterpart wired LNAs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack, can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), Deauthentication attacks, War driving etc. As this paper is not focused on attacks, we shall mainly concentrate on best practices- how to install and use WLAN securely which can thwart a number of above mentioned attacks.

Secure WLAN

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used.
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing.

Wi-Fi at home

I believe using a Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it?

Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to fend for herself. So make sure, your network is secured from being maliciously used.

There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

1. **Use most secure possible encryption:**
   The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel. Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access -2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.
   Attacks mitigated: WEP Key cracking, Sniffing, Capturing/Eavesdropping

2. **Use Firewall:**
   All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.
   Attacks mitigated: Fingerprinting, System compromise

3. **Have a monitoring system in place:**
   There's a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.
   Attacks mitigated: Scanning, DoS

4. **Don't use default credentials:**
   Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ " ".
   Attacks mitigated: Unauthorized access, War driving

5. **Disable Auto-connect feature:**
   Some devices or the computers/laptops have 'Let this tool manage your wireless networks' or 'Connect automatically to

available network'. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as 'HotSpot', 'SecureConnect', 'GovtNetworks' etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.
Attacks mitigated: Phishing, Sniffing, Rouge AP association

6. **Don't use public Wi-Fi spots to surf sensitive websites:**
Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. Recently to demonstrate these types of attacks one researcher developed a tool Firesheep.
[http://codebutler.github.com/firesheep/]. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked. I had blogged about this tool and its countering tool Blacksheep [ZScalar] here: http://nileshkumar83.blogspot.com/2010/11/firesheep-session-hijacking-tool.html.
Attacks mitigated: Sniffing, Session Hijacking

7. **Change the default SSID:**
Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?
Attacks mitigated: War driving

8. **Restrict access by assigning static IP addresses and MAC filtering:**
Disable automatic IP assigning feature and use private static IPs to the legitimate devices you want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering-router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.

9. **Turn off your router when not in use:**
Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

Wi-Fi in a Corporate/Enterprise Network

Due to the nature of activity and criticality of information, it is very important that Corporate / Enterprise networks have a higher degree of security.

The following are good to have:

- Defining an adequate organization wide Information Security policy & procedures for wireless network
- SSID's should not be associated with the organization, AP vendor or any other related information which would be easy to guess or associate with the current organization
- Enable WPA2 Enterprise encryption with RADIUS authentication and use of EAP protocol like EAP-TTLS, TLS etc.
- Implementation of PKI infrastructure. CA signed certificates to authenticate the server to client and vice versa
- Filtering of clients based on unique identifier like MAC Address
- Isolated 'Guest' wireless network with no interface / connection to the corporate network
- Limiting the radius of Wi-Fi network by reducing the power output of the AP
- Allocating IP Address to the employee and guest machines only after successful authentication
- Periodically changing the keys & passwords
- Use of VPN while accessing corporate information from Public Wi-Fi network
- Client side utilities like DecaffeintIDcan help in detecting changes in ARP table and serve as common man's IDS to protect against attacks like 'hole196' and DoS.
- Implementation of Wireless IDS. Wireless IDS is a new concept. The key features of Wireless IDS are:

✓ Prevention against Rogue AP's
✓ Detection & prevention against DoS attacks
✓ Assistance in locating the approximate physical location of the attacker
✓ Assistance in enforcing the Organization's Information Security policy on wireless networks
✓ Detection of use of scanning tools like Kismet &NetStumbler

Snort-Wireless & WIDZ are examples of the open source Wireless IDS

Nilesh Kumar

Nilesh Kumar is working as a Senior Engineer-Security Analyst with Honeywell Technology Solutions Lab, Bangalore, India. He is mainly focused on Application Security, Network Security and Wireless Security. Apart from that he shows interest in Reverse Engineering.

His blog:
http://nileshkumar83.blogspot.com/


ClubHACK
free wifi with
coffee
compromise

Copyright and Cyberspace

Copyright in cyberspace primarily exists at two levels

- Computer Source code.
- Computer database.

Copyright

[This concept is explained using simple fictional illustrations involving Revati, who has created easyPDF, a computer program for converting documents into PDF (Portable Document Format)] According to Section 14 of the Copyright Act, "Copyright" means the exclusive right to do (or authorize the doing of) any of the following:-

1. To reproduce a computer programme in any material form including the storing of it in any medium by electronic means,

Illustration 1

Revati has the exclusive right to reproduce the easyPDF program on CD, DVD and other storage media.

Illustration 2

Revati has the exclusive right to upload the easyPDF program onto her website.

2. To issue copies of the computer programme to the public.

Illustration 1

Revati has the exclusive right to provide the easyPDF program along with computer magazines so that the general public can use the software.

Illustration 2

Revati has the exclusive right to upload the easyPDF program onto her website so that people around the world can download it.

3. To perform the computer programme in public, or communicate it to the public.

   Illustration 1
   Revati has the exclusive right to give a public demonstration of the workings of the easyPDF program.

4. To make any cinematograph film or sound recording in respect of the computer programme.

   Illustration 1
   Revati has the exclusive right to make a promotional film depicting the working of the easyPDF program.

   Illustration 2
   Revati has the exclusive right to make a promotional sound recording depicting the working of the easyPDF program.

5. To make any translation of the computer programme

   Illustration
   Currently the easyPDF program has all the menu commands and help files in English. Revati has the exclusive right to make a version of the easyPDF program that has the menu commands and help files in Hindi.

6. To make any adaptation of the work.

7. To do, in relation to a translation or an adaptation of the computer programme, any of the acts specified above.

8. To sell, give on hire, offer for sale, or offer for hire, any copy of the computer programme.

   Illustration 1
   Revati has the exclusive right to offer the easyPDF program for sale.

   Illustration 2
   Revati has the exclusive right to act as an Application Service Provider for the easyPDF program e.g. a user will be charged a small fee for every document that he converts to PDF using the easyPDF program.

Term of Copyright

Illustration 1
Ketaki creates a computer program in 2008. She dies on 12th March, 2010. The copyright in the computer program will subsist for 60 years from 1st January 2011.

Illustration 2
Ketaki and Rajan together create a computer program in 2008. Ketaki dies on 12th March, 2010 while Rajan dies on 13th July, 2014. The copyright in the computer program will subsist till 60 years from 1st January 2015.

Copyright Infringement

The copyright in a computer program is deemed to be infringed when any person without a license or in contravention of the conditions of a license:-

- Does anything, the exclusive right of which is conferred upon the owner

of the copyright by the Copyright Act, or
- Commercially permits any place to be used for the communication of infringing work to the public.

The following are also deemed to be infringement:-

- Distributing, selling or hiring out infringing copies,
- Exhibiting infringing copies in public,
- Importing infringing copies into India.

There are several acts that are not deemed to be infringement of copyright.

These are explained using the following simple illustrations given below. In these illustrations, I have used the fictional illustration of Revati who has created the easyPDF software. Sameer has purchased a CD containing the easyPDF software.

Illustration 1

Sameer can make a backup copy of the easyPDF software on another CD so that in case the original CD gets damaged, he can reinstall from the CD ROM.

Punishment for copyright infringement

Knowingly using the infringing copy of a computer program on a computer is punishable with:-

- Imprisonment for a term between 7 days and 3 years and
- Fine between Rs. 1 lakh and Rs. 2 lakh.

In case the infringement has not been made for commercial gain, the Court may impose no imprisonment and may impose a fine up to Rs 50,000.

The offence can be tried by a magistrate not below the rank of a Metropolitan Magistrate or a Judicial Magistrate First Class.

In case of offences by companies, persons in charge of the company are also liable unless they prove that the offence was committed:-

- Without their knowledge or
- Despite their due diligence to prevent it.

Understanding Computer Software

According to Section 2(ffc) of the Copyright Act, a computer program is a "set of instructions expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve particular results".

The essential elements of a computer program are:-

It is a set of instructions expressed in:-

- Words,
- Codes,
- Schemes or
- In any other form, including a machine readable medium.

Which is capable of causing a computer to:-

- Perform a particular task or
- Achieve a particular result.

Computer software is "computer program" within the meaning of the Copyright Act. Computer programs are included in the

definition of literary work under the Copyright Act.

Computer Database & Law

According to Section 43 of the Information Technology Act (IT Act), a "Computer data base" means,

a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

Essential elements of "computer database":-

A. Computer database is a representation of

- ✓ Information,
- ✓ Knowledge,
- ✓ Facts,
- ✓ Concepts or
- ✓ Instructions

B. This representation can be in

- ✓ Text,
- ✓ Image,
- ✓ Audio,
- ✓ Video

C. This representation must be such as

- ✓ Being prepared in a formalized manner or
- ✓ has been prepared in a formalized manner or
- ✓ has been produced by a computer, computer system or computer Network

D. Computer database is intended for use in a computer, computer system or computer network.

Illustration 1

Sameer has prepared an online database of all Hindi movies. This database is searchable by movie name, director name, lead actor etc.

Illustration 2

The Noodle Ltd website contains several password protected web-pages. The usernames and passwords of all authorized users are contained in a Microsoft Access database.

Illustration 3

Noodle Telecom Services Ltd creates a CD ROM containing the names and phone numbers of all their subscribers.

Illustration 4

Noodle School has an automated system for student administration. This system is powered by a database that contains detailed student information.

Roll no.	Name	Address	Phone	Email

One table of this database is titled "basic_info" and contains the following categories of information

Another table is titled "student_marks" and contains the following categories of information:-

Roll no.	Test 1	Test 2	Test 3	Final

When a student's report card is to be prepared, the system automatically takes the marks from the "student_marks" table and the name and contact information from the "basic_details" table. It then collates the information and prepares the final report card.

Illustration 5

Noodle Law Firm has prepared a computerized database of all their client companies along with the relevant contact persons.

An interesting element of computer databases is that copyright can exist in two levels.

- Firstly, the information contained in the database may be the subject of copyright
  E.g. A list of computer vulnerabilities and the relevant security measures.

- Secondly, the actual representation of this information may be the subject of copyright protection
  E.g. the above mentioned information in a searchable online database.

Diljeet Titus case

- **Diljeet Titus vs Alfred A. Adebare and Ors.**

130(2006) DLT330, 2006(32) PTC609 (Del)

This case involved two counter suits filed by a group of legal professionals. Diljeet Titus (the plaintiff) is the proprietor of Titus and Co.

His colleagues Alfred Adebare, Seema Jhingan, Alishan Naqvee and Dimpy Mohanty (hereinafter referred to as defendants) had left Titus and Co.
While leaving Titus and Co, the defendants had taken with them computer data (from the computers of Titus and Co) relating to:-

1. proprietary drafts of precedents, agreements, forms, presentation, petitions, confidential documents, legal opinions, legal action plans, and

2. Computerized database containing client information, proprietary client list, proprietary potential client list and other related information.

Titus claimed to have copyright over the above. The defendants claimed to be the owners of the copyright in what they had created. It was their contention that the creation was independent and was created by advising and counseling the clients.
The defendants sought a decree of declaration that they were the owners of the copyright in what they had created and sought a permanent injunction against Mr. Titus and his firm from using and parting with the same.
The question was whether there was exclusive right of any of the parties in what they had created or it was a joint right.

Conclusion

The Court held that Titus and Co. was a sole proprietorship concern and not a partnership. It held that the defendants did not have a right over the subject matter of the suit.

Sagar Rahukar
sr@asianlaws.org

Sagar Rahukar, a Law graduate, is Head(Maharashtra) at Asian School of Cyber Laws. Sagar specializes in Cyber Law, Intellectual Property Law and Corporate Law. Sagar also teaches law at numerous educational institutes and has also trained officials from various law enforcement agencies.

Forensics with Matriux - Part 2

Hi readers,
In the Part I of the article on Forensics with Matriux, we had highlighted the forensic acquisition techniques using Matriux distribution. In this second part, we will cover the tools that focus on analysis techniques.

Forensic Analysis techniques can be used to discover Deleted Files, Cloaked files, Encrypted files, Fragmented files, PDF, Browser, V irtualisation, Memory and etc.

Vinetto:

This is a basic introduction more advanced details can be found in official vinetto documentation.

Vinetto can be seen in Aresenal> Digital Forensics >Analysis> vinetto

Windows Systems stores images as Jpeg, Jpg, png, Gif etc. image file format and html as thumb nails. Windows creates thumbs.db files to store these entries to minimize the CPU usage to process the images. Thumbs.db file stores images previews as an Alternate Data stream in the file system;the file size depending on the number of images stored in the folder. We can enable / disable the feature of thumbnail caching from folder options in Windows Explorer. Thumbs.db files are created every time when a file added to the folder.

Even if folder/files is encrypted by Microsoft EFS an image preview will be available in thumbs.db and hence these can be analysed.

Figure 2

Vinetto works in three modes as:

Elementary mode

It extracts thumbnails information from a thumbs.db file

Directory mode

It will report the thumbnails that are not associated to a file into the directory.

File System mode

It will check for the data in whole File system (FAT/NTFS)

How vinetto can be useful for a forensics expert:

While carrying out an investigation, the forensics expert can have a quick review of all the images in a browser and can proceed further easily. Mostly investigations into Thumbs.db files are used in Child pornography cases.

Installation in ubuntu:

Through synaptic

```
sudo apt-get install vinetto
```

Pre requisite :Python, Python Imaging Library

Usage:

vinetto path of thumbs.db

vinetto--version shows version number of vinetto

vinetto -h, --help show this help message and exit

vinetto -o DIR path to the thumbs.db write thumbnails to DIR

vinetto -H write html report to DIR

ex:

```
vinetto /home/matriux/Desktop/Thumbs.db

vinetto-
o/home/matriux/Desktop/vinetto_output
/home/matriux/thumbs.db

vinetto -H -o /home/matriux/html
/home/matriux/thumbs.db
```

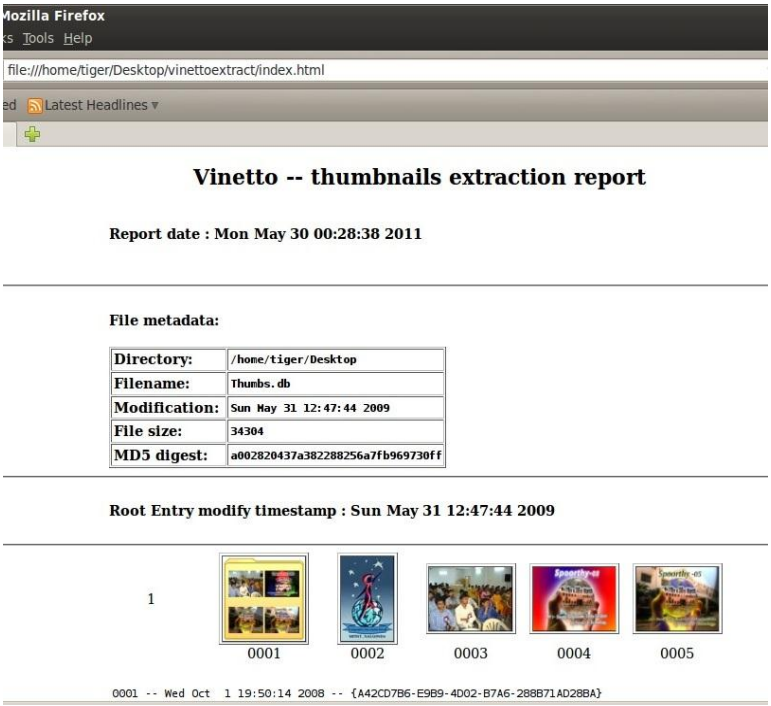


Figure 3

Fig. 3 represents the Report generated, it consists of Report date the report generated date

File Metadata information of the thumbs.db file as directory and modification, Filesize

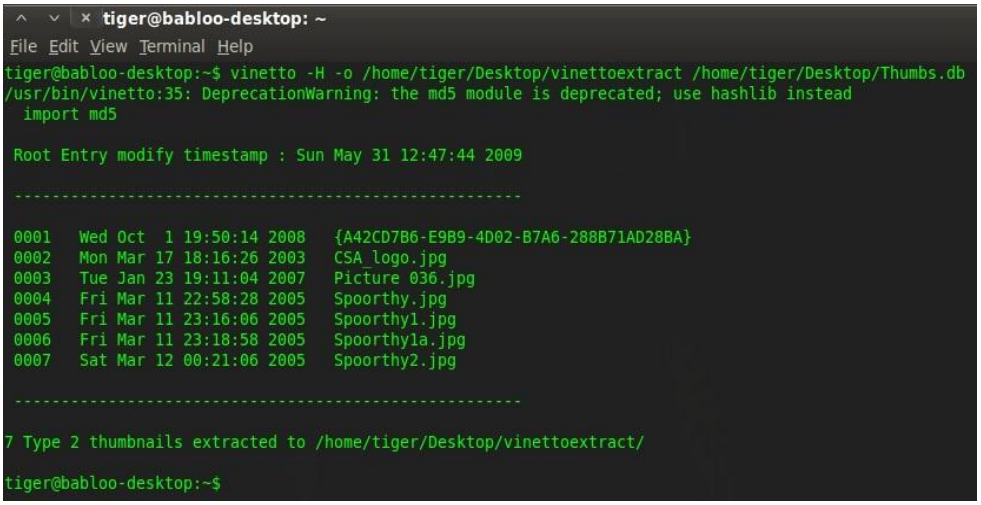


Figure 2

Root Entry modified timestamp - this is the time stamp of the thumbs.db file modified

And thumbnail previews with time stamps

Other Analysis tools will be covered in next issue.

References

http://vinetto.sourceforge.net/

More details please check http://vinetto.sourceforge.net/docs.html

For any further details/queries mail @ pardhu19872007@gmail.com .

TEAM MATRIUX

http://www.matriux.com/

follow @matriux on twitter.

ClubHACK

Can you cage a wifi signal???

Issue 17 | June 2011
www.clubhack.com

Design: pankit@chmag.in