



Ethics in IT

Class 10

Lab 3



Lab Objectives:

- Wireless Hacking

Ethical Hacking - Wireless Hacking

A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range.





The devices in a wireless network have the freedom to be in motion, but be in connection with the network and share data with other devices in the network.

One of the most crucial point that they are so spread is that their installation cost is very cheap and fast than the wire networks.

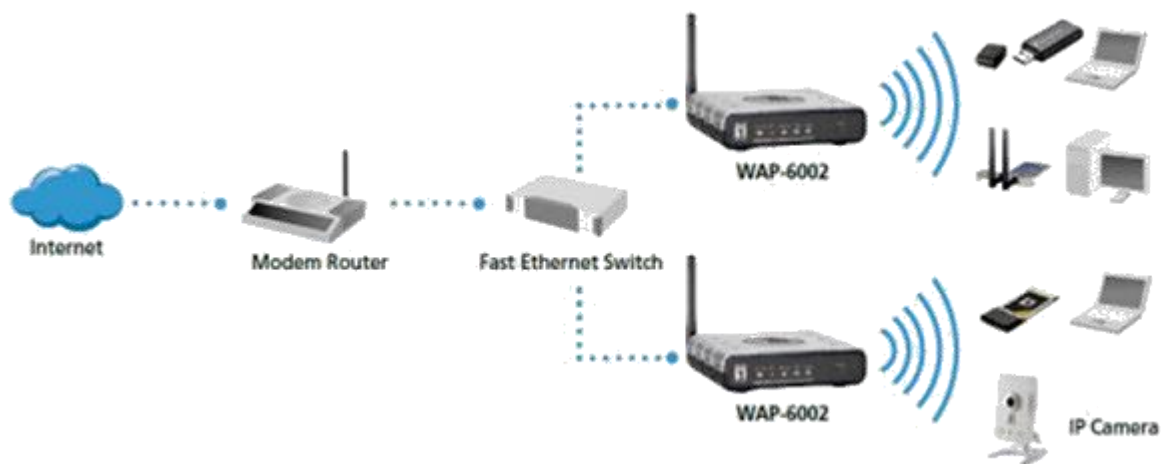
In a wireless network, we have Access Points which are extensions of wireless ranges that behave as logical switches.



A Wireless Router



Although wireless networks offer great flexibility, they have their security problems. A hacker can sniff the network packets without having to be in the same building where the network is located. As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location.



Most attackers use network sniffing to find the SSID and hack a wireless network. When our wireless cards are converted in sniffing modes, they are called monitor mode.



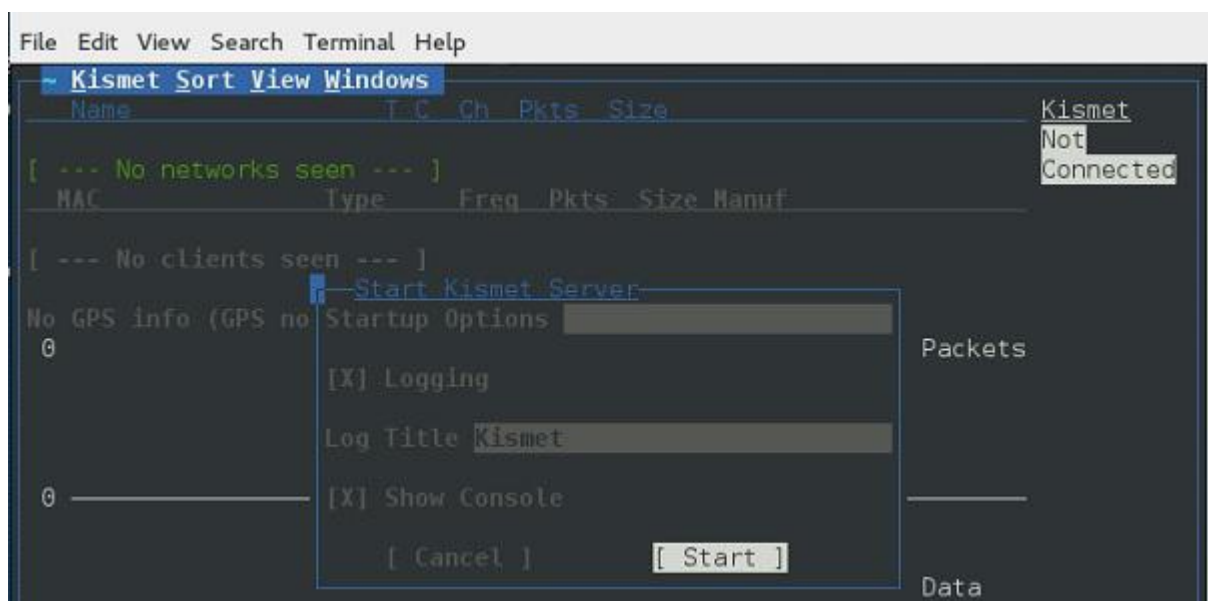
Kismet

Kismet is a powerful tool for wireless sniffing that is found in Kali distribution. It can also be downloaded from its official webpage – <https://www.kismetwireless.net/index.shtml>

Let's see how it works. First of all, open a terminal and type kismet. Start the Kismet Server and click Yes, as shown in the following screenshot.



As shown here, click the Start button.





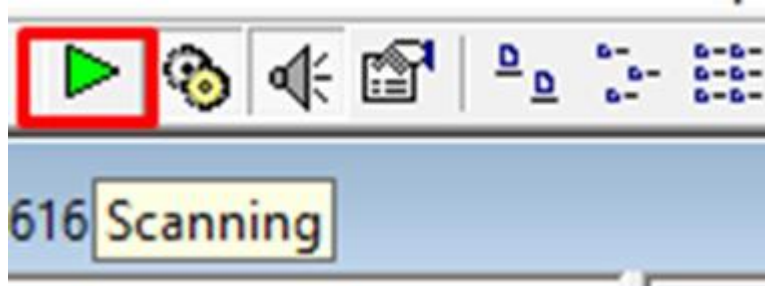
Now, Kismet will start to capture data. The following screenshot shows how it would appear –



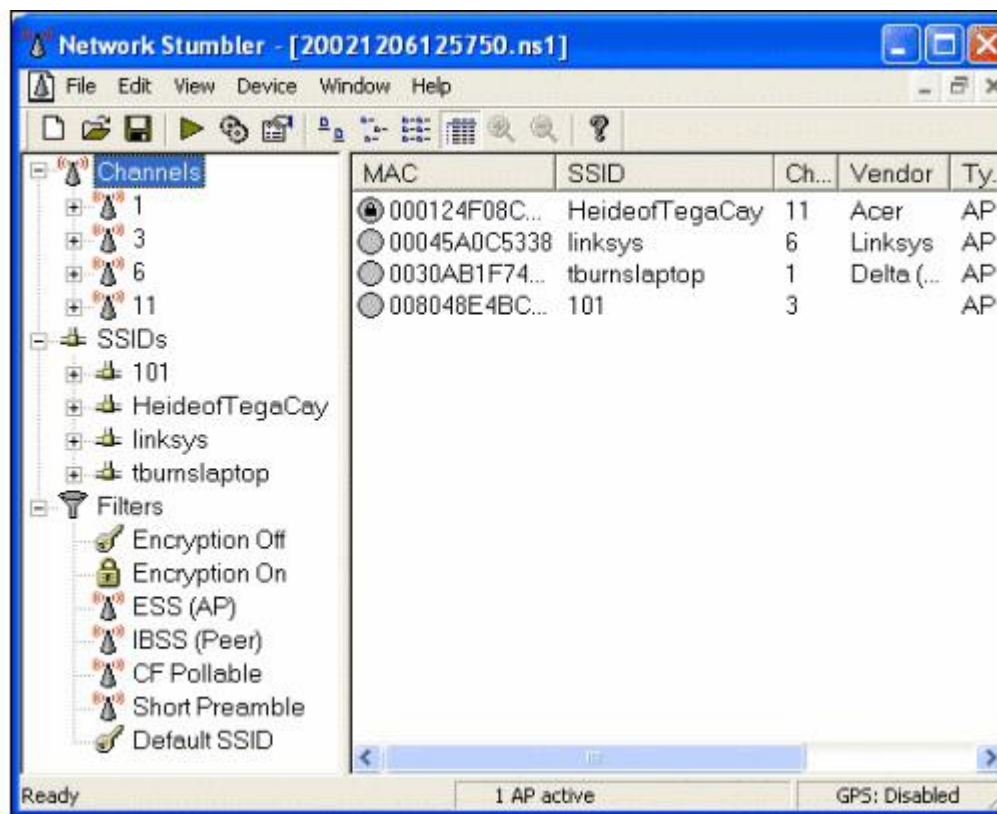
NetStumbler

NetStumbler is another tool for wireless hacking that is primarily meant for Windows systems. It can be downloaded from <http://www.stumbler.net/>

It is quite easy to use NetStumbler on your system. You just have to click the Scanning button and wait for the result, as shown in the following screenshot.



It should display a screenshot as follows –



It is important to note that your card should support monitoring mode, otherwise you will fail to monitor.



Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security protocol that was invented to secure wireless networks and keep them private. It utilizes encryption at the data link layer which forbids unauthorized access to the network.

The key is used to encrypt the packets before transmission begins. An integrity check mechanism checks that the packets are not altered after transmission.

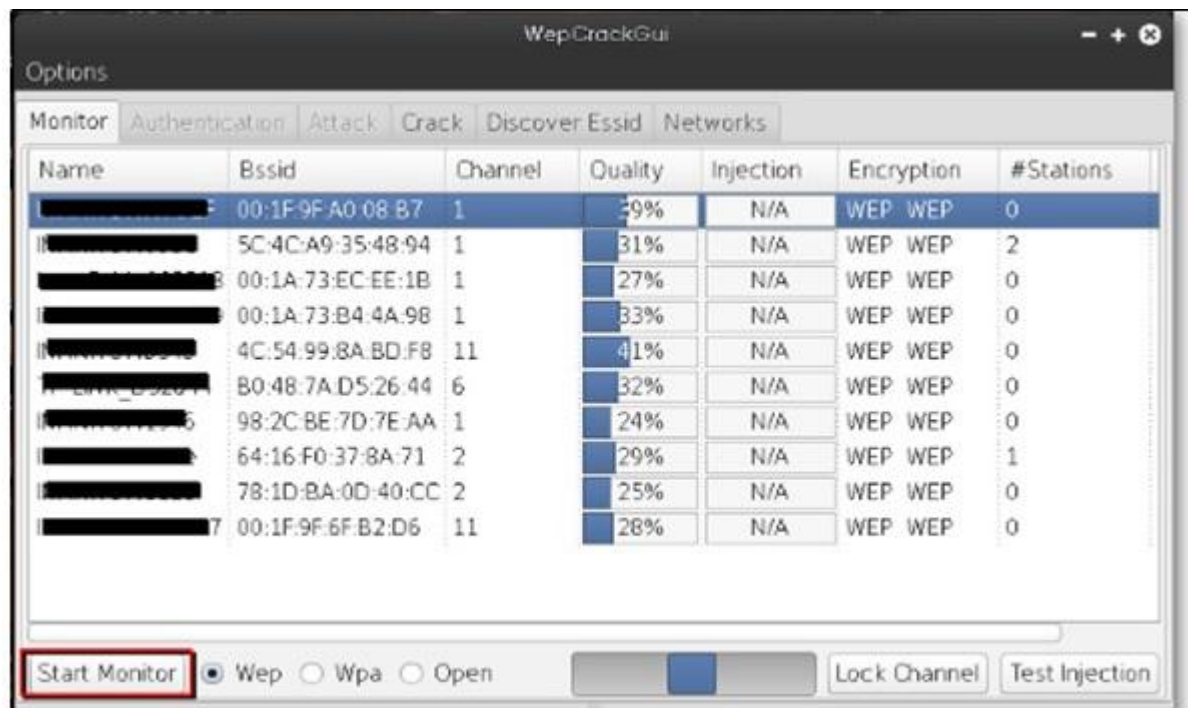
Note that WEP is not entirely immune to security problems. It suffers from the following issues –

- CRC32 is not sufficient to ensure complete cryptographic integrity of a packet.
- It is vulnerable to dictionary attacks.
- WEP is vulnerable to Denial of Services attacks too.



WEPCrack

WEPCrack is a popular tool to crack WEP passwords. It can be downloaded from – <https://sourceforge.net/projects/wepcrack/>



Aircrack-ng

Aircrack-ng is another popular tool for cracking WEP passwords. It can be found in the Kali distribution of Linux.



The following screenshot shows how we have sniffed a wireless network and collected packets and created a file RHAWEP-01.cap. Then we run it with aircrack-ng to decrypt the cypher.

```
File Edit View Terminal Help
root@bt:~# aircrack-ng RHAWEP-01.cap
Opening RHAWEP-01.cap
Read 44315 packets.

# BSSID            ESSID            Encryption
1 98:FC:11:C9:14:22 linksys          WEP (7565 IVs)

Choosing first network as target.

Opening RHAWEP-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 7565 ivs.

Aircrack-ng 1.1 +1899

[00:00:02] Tested 38039 keys (got 7565 IVs)

KB  depth  byte(ivote)
0   3/ 7    C3(11264) 59(11008) 5B(11008) EC(11008) 52(10752) 54(10496) 82(10496) D6(10496) 46(10240) 92(10240) C5(10240) 16(9728)
1   6/ 4    6E(13056) D8(13056) B9(12032) 4D(11776) BB(11008) 11(10752) 68(10752) 69(9984) 7F(9984) 96(9984) 97(9984) E3(9984) E6
2   2/ 16    E8(10752) 09(10752) ED(10496) 3C(10496) 50(10496) 69(10496) 6A(10240) FE(9984) 12(9984) FB(9728) FC(9728) 07(9728) 5E
3   7/ 10    AB(10240) 04(9984) 10(9984) 25(9984) 44(9984) 4E(9984) C9(9984) CA(9984) 0A(9728) 30(9728) 42(9728) 8B(9728) CC(9728)
4   3/ 9     82(11264) C7(11264) F5(11008) 24(11008) AC(11008) 5F(10752) 67(10496) 1B(10240) 37(10240) 16(9984) 6E(9984) F6(9984)

KEY FOUND! [ C3:6E:E8:F7:82 ]
Decrypted correctly: 100%
```

Wireless DoS Attacks

In a wireless environment, an attacker can attack a network from a distance and therefore, it is sometimes difficult to collect evidences against the attacker.

The first type of DoS is Physical Attack. This type of attack is very basic and it is in the base of radio interferences which can be created even from cordless phones that operate in 2.4 GHz range.



Another type is Network DoS Attack. As the Wireless Access Point creates a shared medium, it offers the possibility to flood the traffic of this medium toward the AP which will make its processing more slow toward the clients that attempt to connect. Such attacks can be created just by a ping flood DoS attack.

Pyloris is a popular DoS tool that you can download from – <https://sourceforge.net/projects/pyloris/>

Low Orbit Ion Cannon (LOIC) is another popular tool for DoS attacks.





Quick Tips

To secure a wireless network, you should keep the following points in mind –

- Change the SSID and the network password regularly.
- Change the default password of access points.
- Don't use WEP encryption.
- Turn off guest networking.
- Update the firmware of your wireless device.