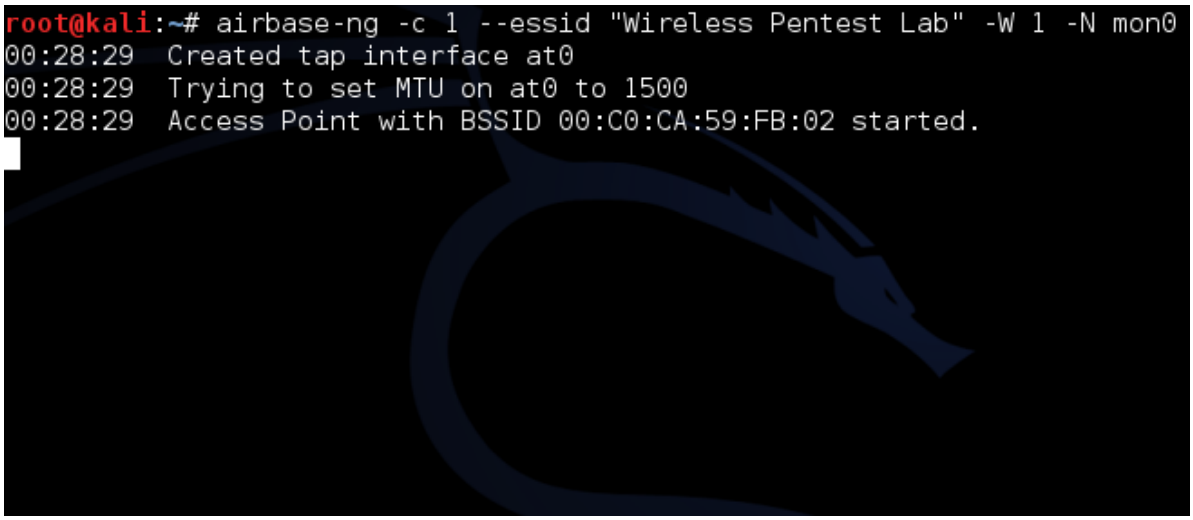
Hirte Attack

pentestlab.blog/category/wireless

February 3, 2015



Hirte is a type of attack that aims to crack the WEP key of wireless networks that are not reachable but the client device (laptop, mobile, etc.) is in the area of the attacker. This can be achieved because the WEP key and the configuration details are still stored in the wireless device.

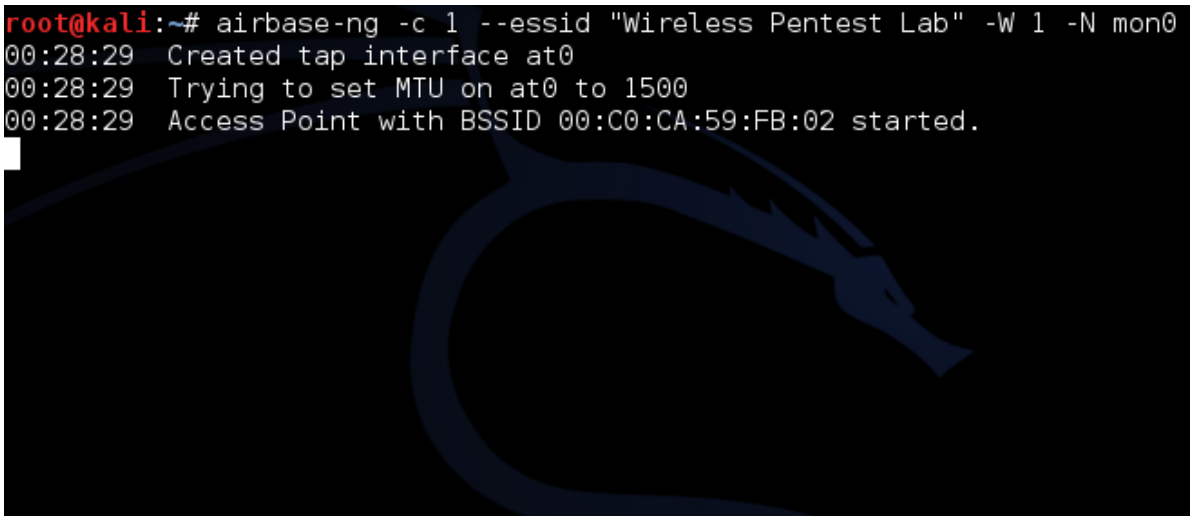
The only requirement for this attack is to setup a fake access point with the same SSID of the WEP network. When the client device will try to connect automatically then ARP packets will be sent from the fake access point (attacker machine) to the device and the other way around which they will contain part of the keystream.

Breakdown of the Hirte Attack

1. Setup a fake WEP AP and waits for a client to connect
2. Upon connection of a client waits for auto-configuration IP address
3. Client sends an ARP packet
4. Obtain the ARP packet and converts it into an ARP request for the same client
5. Client replies
6. Collect these packets
7. Crack the WEP key

Deployment of Hirte Attack

The first step is to create the WEP access point with the use of the tool airbase-ng. The -c variable defines the channel, the -W sets the encryption bit, mon0 is the interface and the -N enables the Hirte attack mode.

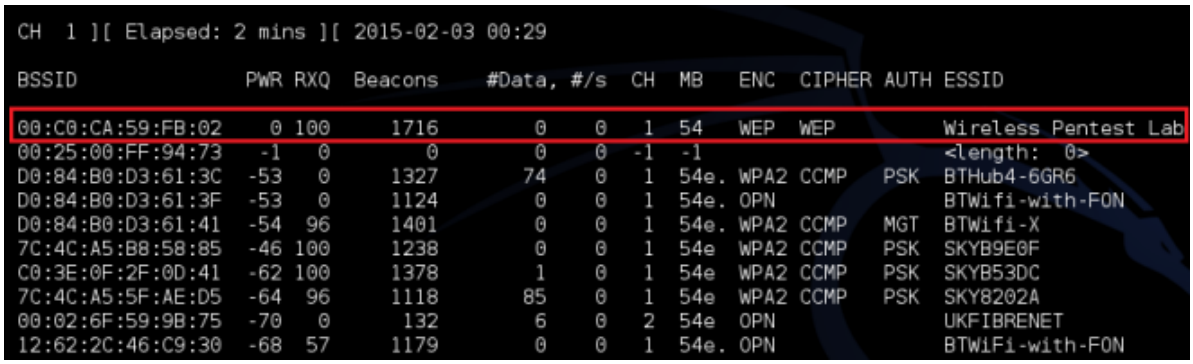


Creation of Fake Access Point

The next step is to configure airodump-ng to capture packets and to write those in a file called Hirte.

Initiate Packet Capturing

As we can see the fake access point appears on the list of the available wireless networks.

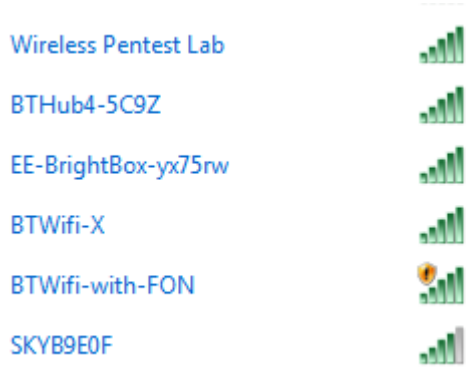


Rogue Wireless Network

The same network will appear and on the victim device.

The victim device will connect automatically on the Wireless Pentest Lab as it is a network that it was connected previously when the genuine Wireless Pentest Lab was in range. The Hirte attack will start and ARP packets will be sent as the device will try to

obtain an IP address. However this will not be possible as there is no DHCP server running but the collection of IVs will start.



Victim – Fake Wireless Network Available

```
root@kali:~# airbase-ng -c 1 --essid "Wireless Pentest Lab" -W 1 -N mon0
02:23:13  Created tap interface at0
02:23:13  Trying to set MTU on at0 to 1500
02:23:13  Access Point with BSSID 00:C0:CA:59:FB:02 started.
02:23:48  Got 140 bytes keystream: 84:3A:4B:14:91:A2
02:23:48  SKA from 84:3A:4B:14:91:A2
02:23:48  SKA from 84:3A:4B:14:91:A2
02:23:48  Client 84:3A:4B:14:91:A2 associated (WEP) to ESSID: "Wireless Pentest
Lab"
02:23:48  Starting Hirte attack against 84:3A:4B:14:91:A2 at 100 pps.
02:25:08  Starting Hirte attack against 84:3A:4B:14:91:A2 at 100 pps.
```

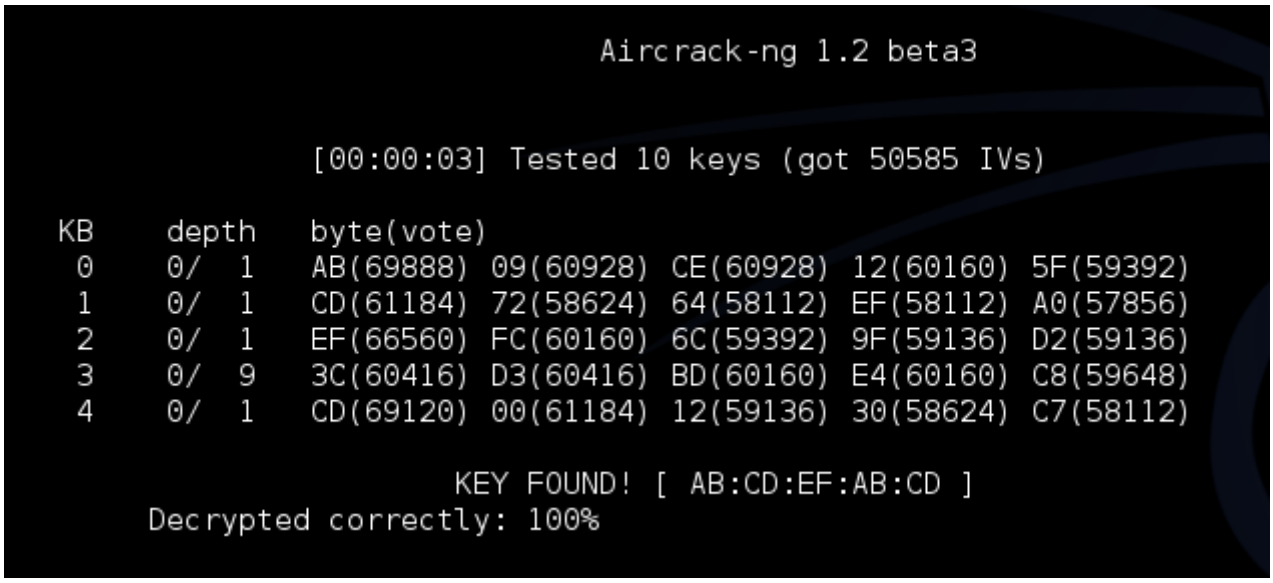
Hirte Attack Running

The final step is to start the aircrack-ng in order to crack the WEP key from the packets that have been captured on the file called Hirte.

```
root@kali:~# aircrack-ng Hirte-01.c
Hirte-01.cap  Hirte-01.csv
root@kali:~# aircrack-ng Hirte-01.cap
Opening Hirte-01.cap
Read 7219559 packets.
```

Read the packets

As we can see from the image below the WEP key has been cracked for a wireless network that it was not even in the range of the attacker.



WEP Key Found

Conclusion

As we saw with the Hirte attack someone is able to crack the WEP wireless key from a network just by exploiting a roaming client and without attacking the access point at all. This happened because the wireless configuration including the WEP key was stored on the device and client had the option to connect automatically to this wireless network when it was found in range. In a summary this attack uses the following principles:

- It is a fragmentation attack
- Targets isolated clients
- Collects ARP packets that contain the WEP key