

Forum:[Hack Forums](#)

Thread: [Advanced attacks on WiFi infrastructure and its clients - Tutorial - part 4](#)

2xTheTap115 - April 28, 2020, 7:30 am

6. HIRTE TYPE ATTACK

This attack is an extended version of the caffe latte attack. Its basic premise is to use the packet fragmentation technique, which allows any packet to be used to carry out an attack, not limiting itself to ARP protocol packets (it can also be an IP packet). However, in this attack, we generate packages in such a way that the client responds to them (and we generate the packages themselves based on packages from the client). Each packet, whether ARP or IP has specific fields such as the client's IP address and destination MAC address. Our goal is to "transfer" the source address to another item in the package. Normally we are not able to change the position of bytes in packets because such a packet would be invalidated (the checksum of the packet would not match and would be rejected as incorrect). So to do this we divide the package into two parts and then send it to the customer. I know it sounds quite complicated, so let's try to conduct such an attack in practice. If you would like to know more about this attack, I invite you to visit the aircrack-ng package page where this attack is described in detail.

Using the aircrack-ng command, create a WEP access point exactly as we did during a caffe latte attack. The only change is that instead of the "L" option, use the "N" option, which causes a hirte attack.

```
Code aircrack-ng -c CHANNEL -a BSSID -e ESSID -W 1 -N INTERFACE
```

Then open a new console window where we run the airodump-ng command which will collect packages from the access point:

```
Code airodump-ng -c CHANNEL --bssid BSSID_EVIL_AP --write  
/PATH/TO/SAVE/FILE/IN/PACKAGES.CAP INTERFACE
```

Just like during a caffe latte attack, as soon as the client connects, aircrack-ng will start the hirte attack. Now just run the command aircrack-ng which after processing the appropriate number of packages will break the WEP key.

7. MAN-IN-THE-MIDDLE ATTACKS

MITM attacks are probably the most effective and most common attacks on wireless networks. There are many configurations for such attacks. We will focus on the most common type, when the attacker connects to the Internet via LAN and creates a fake access point. Such an access point broadcasts a WiFi network whose SSID is the same as the identifier of the attacked nearby network. An authorized user of the attacked network may accidentally connect to such a false access point (or such a connection may be "forced" by using the stronger signal theory, which we discussed earlier). I described the implementation of such an attack earlier in point 3 so I will not repeat myself, and I will only describe this attack in theory and I'll leave it to you. The first step will be to create an access point to which customers will connect. Later you need to create a bridge between the access point and the cable interface (the original network interface). After creating the bridge, run all interfaces (it's also worth giving the IP address to our bridge, you can do it with the ifconfig command) with the ifconfig command. The next step will be to enable packet forwarding. If you follow all the steps correctly, you should be able to eavesdrop on the exchange of packets in both directions (between the AP and the cable interface). All you have to do is start the sniffer and save

everything that flies online.

- SESSION CAPTURE

One of the many attacks that can be carried out using a MiTM attack is interception of application sessions. An interesting element of this process is the ability to modify data in forwarded packets (if they are not encrypted or do not use other data integrity safeguards). In practice, this means that the attacker can modify, damage and in extreme cases even selectively remove selected packages. In this attack vector, I will show you how to capture a DNS session using a Man-in-the-Middle attack. And then, based on the captured DNS session, it will show you how to capture a browser session trying to connect to google.com (or any other host). Let's assume that we successfully used the MiTM attack in the attacked network. Let's start the sniffer (in this case it will be Wireshark) with the dns filter enabled (just enter the phrase "dns" in the filter field to display only packages of this protocol). Now just use the dnsspoof tool and show him the interface on which to work. In addition, let's create a text file called hosts.txt in which we will put an entry redirecting to the ip address of the attacker all queries regarding the google.com domain. Then issue the command:

```
Code dnsspoof -i INTERFACE -f hosts.txt
```

After executing this command, all DNS queries sent over the network will go through dnsspoof. Now if the victim tried to visit www.google.com they would receive an error message. This is because dnsspoof sends fake dns responses to the attacker's computer on which the google service is not running (that is, it simply does not find the service on the attacker's computer, exactly on port 80). For the purposes of this example, start the apache server that will replace the google service. So let's give the command:

```
Code apache2ctl start Or
```

```
Code service apache2 start
```

From this moment, when the victim sends a dns query about the google site, he will be redirected to the address of the attacker where the apache server is running. Based on this example, we can clearly see the possibilities of MiTM attacks. This is one of the simplest attacks that can be carried out, I leave the exploration of the more advanced ones to you. The internet is full of information on this subject. Just search well.