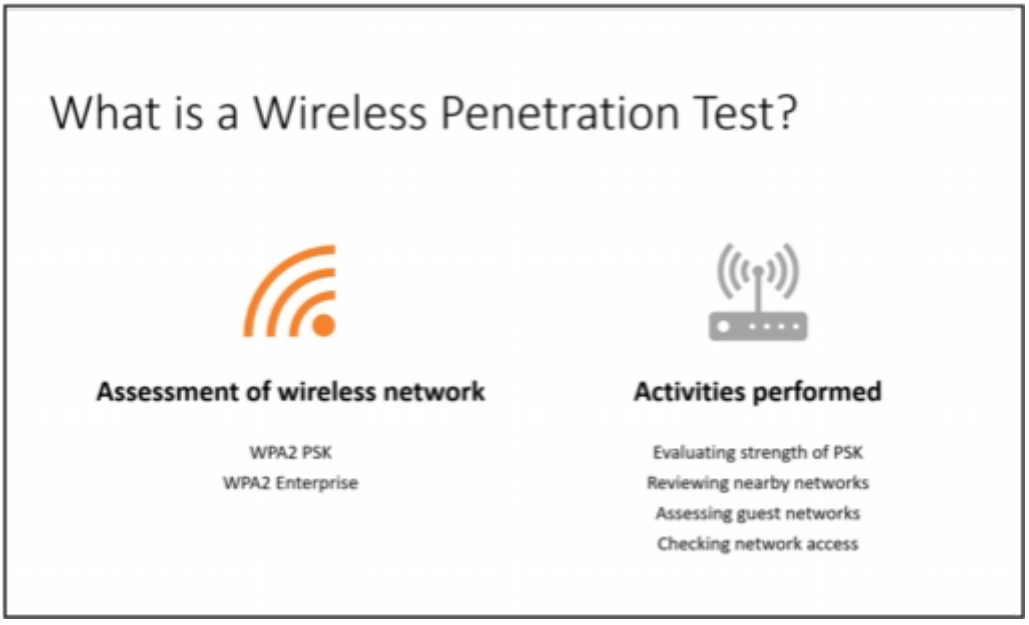
# 001 - Wireless Penetration Testing Overview

What is it?

Essentially, it is the assessment of a wireless network.

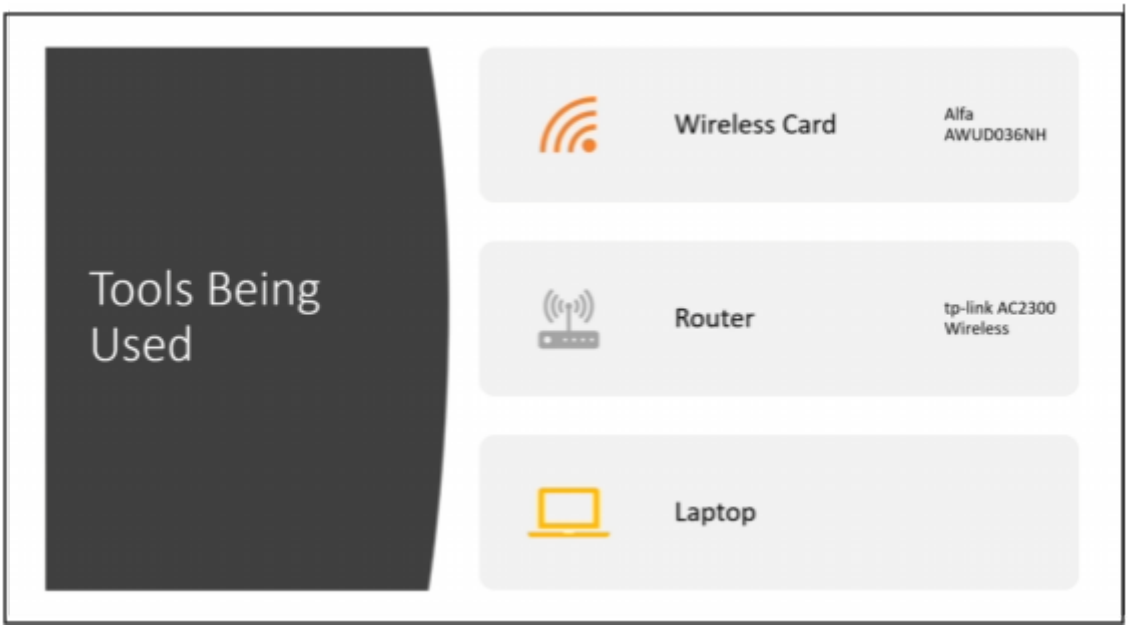
We have two types most viewed.

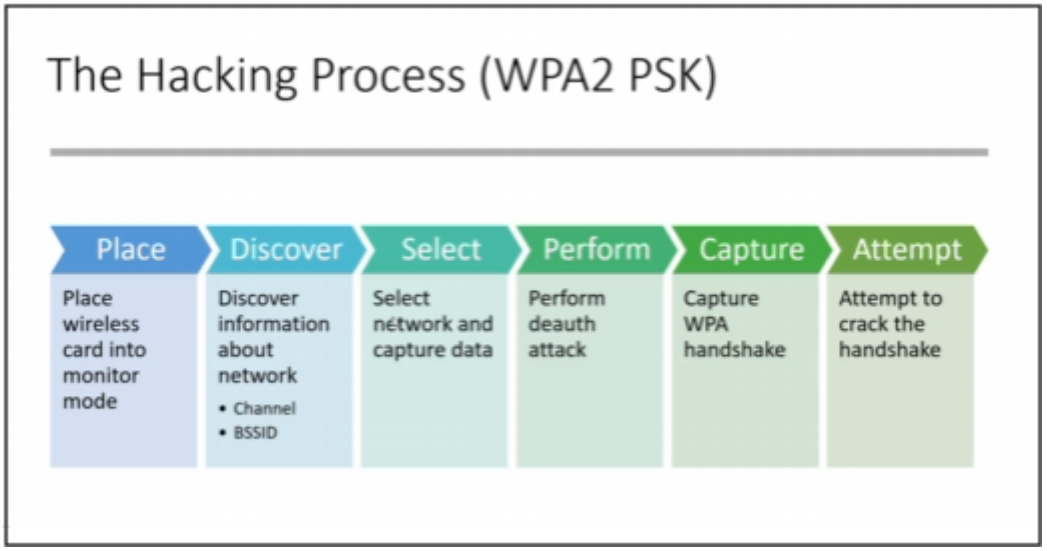



We are going to be focusing on the WPA2 PSK, which is more likely to be a home, small business, or maybe even a medium size business network.

To do pentesting in the WPA2 Enterprise, we would need to set one up, and that can get very cost.

War walking.






We are going to need a Wireless Card. We can find out the latest Wireless Card in Kali Linux website.

This is basically a beefy card that is used to inject packets and listen to packets.

Wirelesshack.org

We need a card that does both 2.4 GHz and 5.0 GHz.

https://www.ceos3c.com/security/best-wifi-adapter-for-kali-linux/

This is another good source.

Some of the supported chipsets that qualify as WiFi adapter for Kali Linux are:

- Realtek RTL8812AU
- Realtek 8187L
- Ralink RT5370N
- Ralink RT3572
- Ralink RT5572
- Ralink RT3070
- Ralink RT307
- Atheros AR9271
- MT7610U
- MT7612U

| Adapter Name | Chipset | Frequency | Protocol | Where to buy |
|---|---|---|---|---|
| ALFA AWUS036NEH | Ralink RT3070 | 2.4GHz | 802.11N | **Amazon** **WiFi-Stock** **eBay** |
| TP-LINK TL-WN722N 2.4GHz (V1) | Atheros AR9271 | 2.4GHz | 802.11N | **Amazon** (DYOR) **eBay** |
| ALFA AWUS036NH | Ralink RT3070 | 2.4GHz | 802.11N | **Amazon** **eBay** |
| ALFA AWUS036NHA | Atheros AR9271 | 2.4GHz | 802.11N | **Amazon** **Alfa Networks** |
| Panda PAU09 | Ralink RT5572 | 2.4GHz | 802.11N | **Amazon** **eBay** |
| ALFA AWUS036ACH | Realtek RTL8812AU | 2.4GHz / 5GHz | 802.11AC | **Amazon** **Alfa Networks** |
| ALFA AWUS036H | Realtek 8187L | 2.4GHz | 802.11b/g | **Amazon** **eBay** |
| ALFA AWUS036ACHM | MT7610U | 2.4GHz / 5GHz | 802.11AC | **Amazon** **eBay** |
| ALFA AWUS036ACM | MT7612U | 2.4GHz / 5GHz | 802.11ac/a/b/g/n | **Amazon** **eBay** |
| ALFA AWUS1900 | Realtek RTL8814AU | 2.4GHz / 5GHz | 802.11ac/a/b/g/n | **Amazon** **eBay** |
| ALFA AWUS036AC | Realtek RTL8812AU | 2.4GHz / 5GHz | 802.11ac/a/b/g/n | **Amazon** **eBay** |
| ALFA AWUS036ACS | Realtek RTL8811AU | 2.4GHz / 5GHz | 802.11ac/a/b/g/n | **Amazon** **eBay** |
| ALFA AWUS036EAC | Realtek RTL8812AU | 2.4GHz / 5GHz | 802.11ac/a/b/g/n | **Amazon** **eBay** |
| ALFA AWPCIE-1900U | Realtek RTL8814AU | 2.4GHz / 5GHz | 802.11ac/a/b/g/n | **Amazon** **eBay** |

ALFA AWUS1900 why does it not work "out of the box"?

The **ALFA AWUS1900** Wi-Fi adapter doesn't work "out of the box" on many Linux distributions, including Kali Linux, due to driver and firmware issues. Here's why:

### 1. Driver Support

- The **AWUS1900** uses the **Realtek RTL8814AU** chipset, which is not included in the default Linux kernel.
- Most Linux distributions, including Kali Linux, do not ship Realtek drivers by default due to licensing issues.

### 2. Manual Driver Installation Required

- You need to manually install the **RTL8814AU** driver for it to function properly.
- The driver is available from the community via GitHub and needs to be compiled from source.

### 3. Lack of Native Monitor Mode and Packet Injection Support

- While the adapter supports **monitor mode** and **packet injection**, not all driver versions work well with tools like `airmon-ng` and `aireplay-ng` without additional patches.
- Some users report issues with dropped packets and inconsistent performance.

### 4. Secure Boot Conflicts

- If you have **Secure Boot** enabled, it might prevent the driver from loading.
- You may need to disable Secure Boot in your BIOS settings.

### 5. Kernel Updates Can Break It

- Since the driver is not in the official kernel, a Linux kernel update may cause compatibility issues, requiring you to reinstall the driver.

## How to Fix It on Kali Linux

**Step 1: Install Required Packages**

bash Copy Edit

```
sudo apt update
sudo apt install -y dkms build-essential libelf-dev linux-headers-$(uname -r)
```

**Step 2: Clone and Install the Driver**

bash Copy Edit

```
git clone https://github.com/morrownr/8814au.git
cd 8814au
sudo ./install-driver.sh
```

**Step 3: Reboot and Verify**

bash Copy Edit

```
sudo reboot
```

After rebooting, check if your adapter is recognized:

bash Copy Edit

```
ip link show
iwconfig
```

This is definitely something we want to do and make it work, but not right now. I am learning a lot, and taking the time to set up the correct drivers is something I do not have the time for right now.

To install  ALFA AWUS1900:

https://www.youtube.com/watch?v=SSLRDERuCkg

After researching a little more, I found out this one should work "out of the box".

ALFA AWUS036ACM.

The **ALFA AWUS036ACM** Wi-Fi adapter **does** work "out of the box" on most Linux distributions, including **Kali Linux**, because it uses the **MediaTek MT7612U** chipset, which has built-in kernel support.

### ✅ Why It Works Out of the Box

1. **Uses the MediaTek MT7612U chipset**, which has native support in the Linux kernel (since version 4.19+).
2. **No need for manual driver installation**—just plug it in and use it.
3. **Supports monitor mode and packet injection** without additional patches.

### 🔍 How to Verify If It's Detected

After plugging in the adapter, check if it's recognized:

bash Copy Edit

```
ip link show
iwconfig
```

### 🛠️ If It's Not Working Properly

- Update your system and install additional firmware (just in case):

bash Copy Edit

```
sudo apt update && sudo apt upgrade -y
sudo apt install firmware-misc-nonfree -y
sudo reboot
```

- Check if the interface is listed using:

```bash
lsusb
dmesg | grep usb
```

## How to Check If It Works Out of the Box

To determine if it works without additional setup:

1. **Plug it in and check if it's recognized**

```bash
ip link show
iwconfig
```

2. **Check the chipset it uses**

```bash
lsusb
```

- Look for the chipset name (e.g., **Realtek RTL8812AU, MediaTek MT7612U, Atheros AR9271**).
- If it's a **MediaTek** or **Atheros** chipset, it likely works out of the box.
- If it's a **Realtek** chipset (especially RTL88XX series), manual driver installation is likely required.

For other penetration testing tools we can visit:

https://shop.hak5.org/collections/implants

https://shop.hak5.org/collections/wifi-pentesting