# Hack a Wireless Network with Wifite

Contents

[Hack a Wireless Network with Wifite 1](#_Toc196026416)

[Hacking Wireless Networks 1](#_Toc196026417)

[Logon to Kali Linux 1](#_Toc196026418)

[rockyou.txt 2](#_Toc196026419)

[Wifite 2](#_Toc196026420)

[Assignment Submission 4](#_Toc196026421)

Time required: 60 minutes

# What I Want You to Do

This proof of concept lab is designed to give you hands-on experience with wireless network hacking and dictionary attacks.

# Why I Want You to Do This

Understand how wireless encryption can be circumvented. Older wireless encryption protocols along with simple shared keys allow your network to be vulnerable. You can protect your network by using good password and shared key practices, as well as using the most up to date encryption protocols.

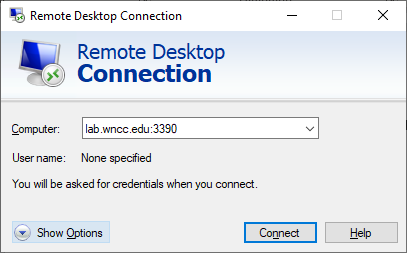
# Hacking Wireless Networks

Hacking wireless networks requires a special wireless chipset.

We are using a [ALFA AWUS036NHA](https://www.alfa.com.tw/collections/wifi-indoor-802-11n-usb-wifi-adapter) wireless adapter.

This adapter supports promiscuous mode, which is for packet sniffing. It also supports monitor mode which allows packets to be captured without having to associate with an access point or ad hoc network first. Monitor mode only applies to wireless networks, while promiscuous mode can be used on both wired and wireless networks.

# Logon to Kali Linux

You will be logging into an older Dell laptop computer in D1 at the WNCC Scottsbluff campus. Please be patient!

You will use **Remote Desktop Connection** on your Windows computer (not the virtual machine) to connect to the remote Kali Linux laptop.

1. Go to **Start,** type **Remote Desktop Connection.**
2. Computer from outside D1: **lab.wncc.edu:3390**   
   In D1: **172.16.1.3:3390**
3. Username: **user**
4. Password: **ToweringFence2344**

# rockyou.txt

**rockyou.txt** is a dictionary attack file containing passwords from data breaches. It contains real passwords used by real users.

1. Google **rockyou.txt**. You can download it on your Windows computer and look at it in Notepad. It will take a while for Notepad to load the file. Look at what is inside it.
2. Describe **what rockyou.txt is and what it contains.**

Click or tap here to enter text.

# Wifite

Wifite is a Python script that can capture an WPA2 authentication hash and decrypt it using a dictionary file. Deauthenticate a client to make it authenticate again, grab the hash of the shared key authentication password, and decrypt the hash.

1. Open a Terminal session: **sudo wifite --kill**
2. Enter the password: **ToweringFence2344**
3. **wifite** will scan for wireless networks.
4. Press **CTRL+C** when you see **WildWest** has some clients.
5. Select the target number of WildWest.
6. Wifite will attempt to find PMKID. Press **CTRL+C.**
7. Type **c** to continue
8. **wifite** will automatically deauthenticate and try to crack the password.

A screenshot of a computer program

AI-generated content may be incorrect.

1. **Insert a screenshot of your successful attack.**

Click or tap here to enter text.

1. What was the key?

Click or tap here to enter text.

1. Remove **cracked.json** This file stores the cracked password.

|  |
| --- |
| rm cracked.json |

## Assignment Submission

1. Type 🡪 **sudo reboot** to restart Kali.
2. Write a 200 word reflection on what you learned in this assignment.  
   For instance, what could you have done to make this wireless network more secure?

Click or tap here to enter text.

1. Attach this completed document to the assignment in BlackBoard.