# Cybersecurity

**Activity 3.3.4 Analyzing Wireless Authentication**

Copy and paste screenshots and/or answer questions from the activity.

#5

|  |  |
| --- | --- |
| 80211\_beacon: Fixed parameters | |
| Beacon Interval | 0.102400 |

#6

|  |  |
| --- | --- |
| 80211\_beacon: Tagged parameters | |
| SSID Parameter Set (the network name) | TESLA |
| Supported Rates (speed of transmission) | 1(B) 2(B) 5.5(B) 6 12 24 36 [Mbit/sec] |
| DS Parameter Set (the channel) | 11 |

What are some recommendations you could make to a security specialist who manages wireless networks and Wi-Fi devices?

I would probably be careful by the multiple speeds in the system. Also know the names and the channels of each to acquire packets and diagnosing a problem.

#29 Aircrack-ng requires one more piece of information—the target (the WAP) to analyze. Enter the number that indicates the desired device.

Why is it easy to crack a weak password even with strong encryption?

It’s a weak password, no numbers and no special characters. It’s a common word as well

Conclusion:

#3 How do you protect against a wireless password exploit? (list at least 3 ways)

Use a very difficult password not common to the language/wordlist

Change your password every now and then.

Don’t make it keep your information, don’t do the remember me if you have such powerful information about the company.