**Lab Report**

**Lab Completed: Breaking WEP and WPA Encryption**

**Objective:** Complete the lab presented. Using your textbook, the written lab, and the hands-on activity, use the lab report to demonstrate understanding of the concept presented.

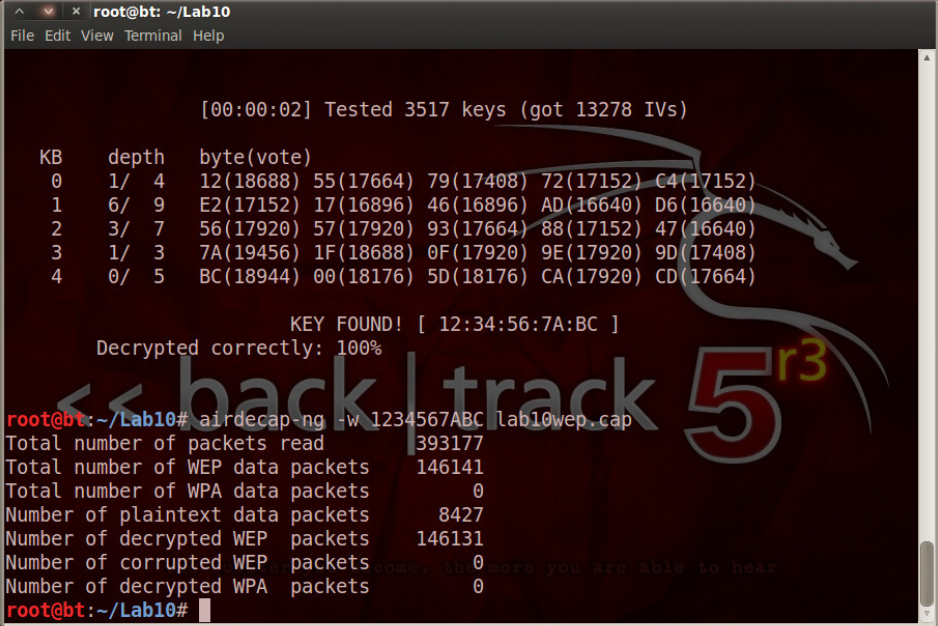
**Part 1: Lab Activity**

Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

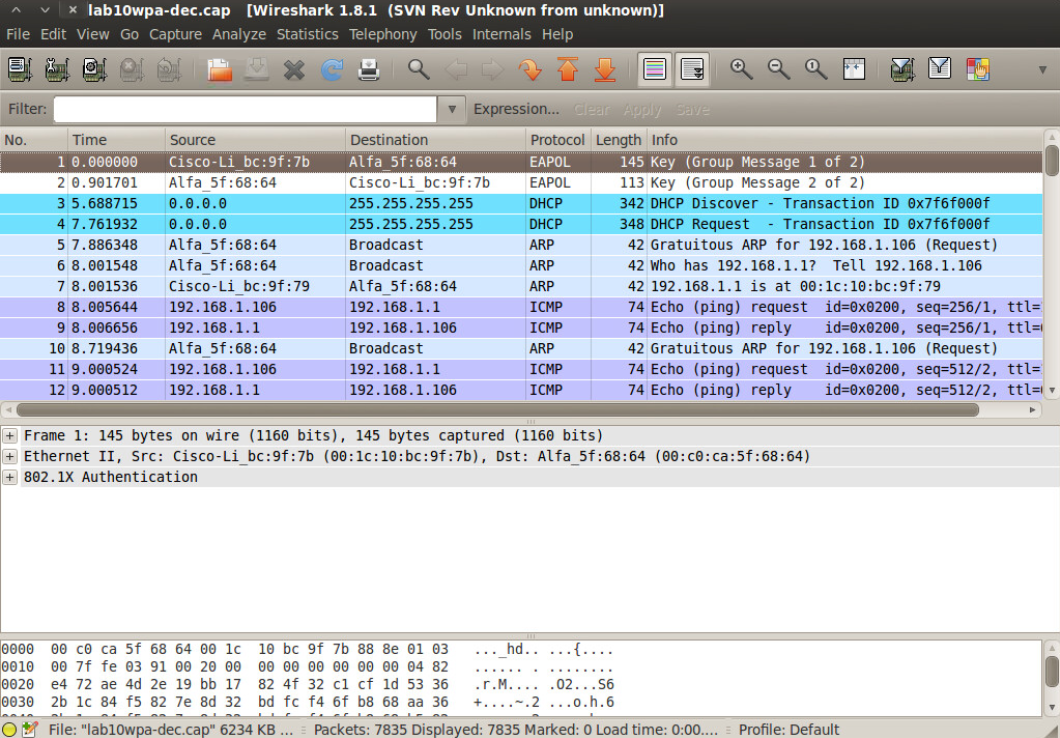
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we did the following: used wireshark to view unencrypted traffic from an open network, used aircrack-ng to break the encryption on WEP and WPA networks, then using airdecap-ng to decrypt the captured traffic from those networks and wireshark to view the decrypted traffic.

**Q2:** Provide 2 screenshots that demonstrate lab completion. For each screenshot, include 1-2 sentences explaining what the screenshot is demonstrating.



In this screenshot I had just used aircrack-ng to obtain the wireless encryption key and then airdecap-ng to decrypt the captured packets from that network using the key.



This is a screenshot of the decrypted traffic from the compromised WPA network being viewed in Wireshark.

**Part 2: Critical Thinking**

**Directions**: Complete the following questions. Provide an explanation of your reasoning for each answer.

The answers should address the lab you just completed.

Suggested length for Part 2: 1-2 pages

**Q1**: What vulnerability(s) are demonstrated or found in this lab? Vulnerabilities may occur during the lab as part of the lab activity.

The open network that traffic was captured on is inherently vulnerable. The WEP encrypted network is vulnerable due to the weakness of the WEP protocol implementation, and the WPA encrypted network was vulnerable in this case because the key used is found in a common dictionary, and is therefor weak.

**Q2:** How might this (these) attack(s) be utilized during a penetration test?

You could run aircrack-ng against the access points(rogue or otherwise) provided on-site by the company that has hired you to do the pentest. Assuming you find one with weak encryption that can be broken, you could then decrypt traffic on that AP and possibly view plenty of juicy information in plaintext.

**Q3:** Explain your reasoning as to what phase of the attacker methodology this lab falls under.

I think the majority of activities in this lab fall pretty firmly in the system hacking phase with the very beginning where they were explaining enumeration of APs and Stations with aircrack-ng being in the enumeration phase. We were using tools to actively break dismantle the security of a network and then actively exfiltrating information from that network.

**Q4:** Research how the attack(s) in this lab can be mitigated or prevented. Cite any sources used. (APA)

This one is pretty straightforward: Don’t use WEP, don’t expect traffic on an open network to be secure without some additional security implementation, and don’t use weak dictionary passwords.

**Q5:** What ethical or potentially problematic issues should a penetration tester consider if they plan on implementing this (these) attack(s) by exploiting a vulnerability?

They could be compromising a network with sensitive data traveling on it. They could possibly put an important network into lockdown if they are detected as an intruder. Whether or not this is allowed by the company, the network being breached could be an employee’s personal ap (a rogue access point) and they could be intercepting traffic that is intended to be personal and not business related.