Wireless

1.0 Introduction

The purpose of this labs is to get you used to running the common tools that are used in wireless hacking. Although there are certain limits with take-home activities, these aim to get you somewhat associated with targeting WEP, WPA-PSK and WPA-Enterprise networks.

The pcap can be downloaded inside vlab at:
10.12.1.10/pcap

As with previous labs fully document your lab procedures using screenshots and descriptions of your steps.   This is in addition to answering the questions below.

2.0 Watch What You Say

When using hotspots or open wireless networks, communications are sent over the air in the clear. Although some hot spots may require authentication to ensure you've paid for access, they don't protect your traffic. Instead, privacy is only obtainable by hirer level protocols (e.g. SSL, VPN, etc...) so if the service you're using doesn't provide this, you're in trouble! Using Wireshark and the capture file you've been provided, answer the following questions:

Questions:

1) What primary plaintext communication protocol is being used within the capture?

2) Whose server's is the conversation about?

3) What is the administrator username?

4) What is the password?

3.0 Your Key = My Key

Within the capture file is a large amount of WEP encrypted traffic. You're goal is to download aircrack-ng (http://aircrack- ng.org/) and crack the key for the "CrackSmack" wireless network.

Although this capture contains enough data for you to crack the key, in a real world attack you'd have to either:

1)   Capture enough traffic to deduce the key or

2)   Inject traffic so that the AP generates new unique Initialization Vectors (IVs) which can then be used to deduce the key

Questions:

1) What is the WEP Key?

4.0 What Where You Thinking?

WPA-PSK can be adequately secured as long as you pick a strong and complex passphrase. Within the capture file is a WPA-PSK handshake between a client and an AP. You're goal is to use aircrack-ng and a good wordlist to crack the PSK for the "BradsLoveShack" wireless network.

In a real world attack you would have had to wait for a wireless client to connect so that you could capture their handshake, or kick them off so they'll reconnect and then capture their handshake.

If you are doing the lab within VLAB the wordlist can be found at:

10.12.1.10/pcap/9-final-wordlist.zip

You can find the wordlist on the Internet at:
http://www.renderlab.net/projects/WPA-tables/9-final-wordlist.zip

Questions:

1) *What is the pre-shared key?*

2) *Which wordlist did you use?*

3) *How long did it take?*

5.0 You're Using What?

LEAP is an extremely outdated EAP type that is subject to a brute force attack. Within the capture is a LEAP handshake for the "jwright" user. Download asleap (http://www.willhackforsushi.com/?page_id=41) and crack jwright's password.

In a real world attack you would have had to wait for a wireless client to connect so that you could capture their handshake, or kick them off so they'll reconnect and then capture their handshake.

Questions:

1) *What is the user's password*