Wireless Lab

Purpose: The purpose of these 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.

Activity 1: 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:
Note: The pcap file 802.11_Fundamentals_and_Hacking_Labv1.1.cap can be downloaded from 10.12.1.10/pcap from the backtrack machine also from vital.poly.edu/release/labs/802.11 Fundamentals and Hacking - Lab v1.1(1).cap

Question	Response
What primary plaintext communication protocol is being used within the capture?	
Whose server's is the conversation about?	
What is the administrator username?	
What is the password?	
What movie is the conversation from?	

Activity 2: 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

Question	Response
What is the WEP key?	

Activity 3: 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.

Hint some good wordlists can be found here:

- http://www.renderlab.net/projects/WPA-tables/9-final-wordlist.zip
- ftp://dl.openwall.com/pub/wordlists/
- http://www.packetstormsecurity.org/Crackers/wordlists/
- http://www.cotse.com/tools/wordlists1.htm

Question	Response
What is the pre-shared key?	
Which wordlist did you use?	
How long did it take?	

Activity 4: 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.

Question	Response
What was the user's password?	