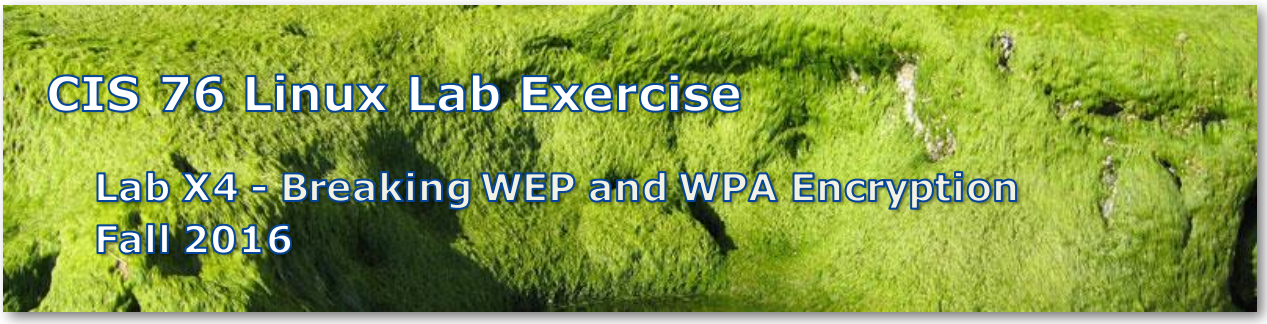
Cabrillo College



Lab X4 - Breaking WEP and WPA Encryption

This lab shows how to examine traffic from wireless networks and crack and decrypt Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab, you have authorization to hack the VMs in the associated Netlab+ pod.

Preparation

1) Reserve a Netlab+ pod for the maximum amount of time for this lab:
   NISGTC Lab 10: Breaking WEP and WPA Encryption
   You can always release it if you finish early.

Part 1 – Wireless Commands and Tools

1) Since Netlab+ doesn't support wireless capture and injections view the YouTube video at https://www.youtube.com/watch?v=ngxzSIsP1JU
2) Write a brief description in your report of what the following commands do:

```
airmon-ng start wlan0
airmon-ng
airodump-ng mon0
airodump-ng -w OURFILE -c 1 --bssid 58:6D:8F:A0:5B:16 mon0
aireplay-ng -0 0 -a 58:6D:8F:A0:5B:16 mon0
aircrack-ng OURFILE-01.cap -w darkc0de.lst
```

Part 2 – Examining Plain Text Traffic

1) Add a screenshot of the CompTIA Security+ Lab 1: Network Devices and Technologies PDF file, extracted from the Wireshark capture, to your report.

Part 3 – Cracking and Examining WEP Traffic

1) Add a screenshot of the CompTIA Security+ Lab 16: General Cryptography Concepts PDF file, extracted from the Wireshark capture, to your report.

Part 4 – Cracking and Examining WPA Traffic

1) Add a screenshot of the CompTIA Security+ Lab 10: Mitigation and Deterrent Techniques PDF file, extracted from the Wireshark capture, to your report.

Submit your work

1) Prepare a report using the word processor and formatting of your choice. Your report should contain the following:

   - Course name, lab assignment name, your name, and date.
   - All the screenshots or command descriptions collected above.
   - Each screenshot should be the full uncropped Netlab window.
   - Each screenshot should be labelled, captioned and readable.

   As an example you can see Benji Simms' report here:
   https://simms-teach.com/docs/cis76/cis76-labX4-simben76.pdf

2) Email your report to: **risimms@cabrillo.edu**

Remember **late work is not accepted.** If you run out of time submit what you have completed for partial credit.

Grading Rubric (15 points)

6 points for Part 1
3 points for Part 2
3 points for Part 3
3 points for Part 4

Document update history

11/29/2016 - clarified that PDFs shown in snapshots must be extracted from Wireshark capture.