Project 3

WiFi Hacking

Team of 2 (max)

(125 points)

0. Learning Objectives

- Practice WiFi scanning and reconnaissance
- Exploit WEP access points with no connected clients
- Exploit WEP access points with connected clients
- Exploit WEP access points with different key sizes
- Exploit WPA2 access points
- Optional: Teamwork!

1. Project Introduction

The focus of this project is WiFi hacking. You will exploit wireless access points with different settings. This project will require research before performing the exploitation. The success of your technique highly depends on being physically close enough to send and receive access point packets. The access points you are authorized to exploit are present in the 3rd floor server room (Rice 374). There are student seats in front of the 3rd floor server room (Rice 374).

You are encouraged to check-out a Panda PAU07 wireless adapter to use for the exploitation from Michael Benos. Once you check-out a wireless adapter, you will lose 10 points on your Exam 3. Once you return the wireless adapter back to Michael Benos you will get those 10 points back. You are encouraged to return the wireless adapter before Exam 3 to avoid any confusion.

Note: You can work on this project alone or with (ONLY) one other student in the same course.

2. Problem Statement

Find the essid, channel, vendor, and key (a.k.a password) for the following WiFi access points:

- Paris
- Munich
- LONDON
- LUXOR
- Toronto (wordlist)

Good luck!

3. Submission

This project will be scored out of 125 points. Please keep track of the time you spend on performing the attacks. I'll ask you for it later.

You should submit a single PDF that includes:

- A cover page that has
    - (2 pts) The class number and name
    - (2 pts) Semester
    - (2 pts) Title: Project 3 - WiFi Hacking
    - (2 pts) Date of Submission
    - (2 pts) Your name (and your partner's name - if applicable)

- A section named "Section 1: Report on exploiting Paris AP"
    - (2 pts) The bssid for Paris is _________ .
    - (2 pts) The channel for Paris is _________________ .
    - (2 pts) The vendor of Paris is _________________ .
    - (2 pts) The key (a.k.a password) for Paris is _________________ .
    - (2 pts) This attack took me/us _________________ hours to perform.
    - (10 pts) Step-by-step documentation of how you performed the exploitation (including commands and screenshots)
    - (2 pts) A conclusion section discussing how easy/difficult your experience was

- A section named "Section 2: Report on exploiting Munich AP"
    - (2 pts) The bssid for Munich is _________ .
    - (2 pts) The channel for Munich is _________________ .
    - (2 pts) The vendor of Munich is _________________ .
    - (2 pts) The key (a.k.a password) for Munich is _________________ .
    - (2 pts) This attack took me/us _________________ hours to perform.
    - (10 pts) Step-by-step documentation of how you performed the exploitation (including commands and screenshots)
    - (2 pts) A conclusion section discussing how easy/difficult your experience was

- A section named "Section 3: Report on exploiting LONDON AP"
    - (2 pts) The bssid for LONDON is _________ .
    - (2 pts) The channel for LONDON is _________________ .
    - (2 pts) The vendor of LONDON is _________________ .
    - (2 pts) The key (a.k.a password) for LONDON is _________________ .
    - (2 pts) This attack took me/us _________________ hours to perform.
    - (10 pts) Step-by-step documentation of how you performed the exploitation (including commands and screenshots)

    - (2 pts) A conclusion section discussing how easy/difficult your experience was
- A section named “Section 4: Report on exploiting LUXOR AP”
    - (2 pts) The bssid for LUXOR is __________ .
    - (2 pts) The channel for LUXOR is ___________________ .
    - (2 pts) The vendor of LUXOR is ___________________ .
    - (2 pts) The key (a.k.a password) for LUXOR is ___________________ .
    - (2 pts) This attack took me/us ___________________ hours to perform.
    - (10 pts) Step-by-step documentation of how you performed the exploitation (including commands and screenshots)
    - (2 pts) A conclusion section discussing how easy/difficult your experience was

- A section named “Section 5: Report on exploiting Toronto AP”
    - (2 pts) The bssid for Toronto is __________ .
    - (2 pts) The channel for Toronto is ___________________ .
    - (2 pts) The vendor of Toronto is ___________________ .
    - (2 pts) The key (a.k.a password) for Toronto is ___________________ .
    - (2 pts) This attack took me/us ___________________ hours to perform.
    - (10 pts) Step-by-step documentation of how you performed the exploitation (including commands and screenshots)
    - (2 pts) A conclusion section discussing how easy/difficult your experience was
- (5 pts) Citation to any readings, websites, tools, or code you used.

You must upload the PDF as an attachment to the “Project 3” assignment on the UVaCollab site. If two students are working together, each student must submit the PDF as their solution to “Project 3” on UVaCollab before the due date.

Submission link:
https://collab.its.virginia.edu/portal/site/fcd93fce-5826-491e-91d0-3ce3f0dfca14/tool/7c2826ab-8f32-41a2-9091-93d04f8ff9a1?panel=Main

4. Due Date

Sunday 03/31/2019 11:50 PM

5. Late Submission Policy

You can submit your solution to this project up to four days late with a 25% off penalty per 24-hours. No submissions will be accepted afterward.

6. Hints and References

- You can receive up to 5 bonus points if you submit your solution to this project by Sunday 3/24/2019 by 11:50 PM.
- You are highly encouraged to work with another student on this project. You can have one of your machines listening to the wireless communication and the other machine performing the exploitation.
- Exploiting the above-mentioned APs has been tested and verified using this Kali VM and the Panda PAU07 wireless card.
- If you use a different wireless card or OS for the exploitation, we can't guarantee the success of your exploitation.
- Tutorial: WEP Cracking
- Tutorial: Simple WEP Crack
- Tutorial: How to crack WEP with no wireless clients