COMP 4337/9337

Project Component

Portable Penetration Testing Station for Wi-Fi Networks

T1, 2019 – V 1.1 (DRAFT)

Submission Deadline: 24 April 2019

ALL project related materials are posted under Project folder in main Resources section on Moodle.

The project component weight is 20/100.

Dates may change within the next 7 days.

Introduction:

Penetration testing involves performing various attacks against a target to observe where the target is lacking in security, and is an important aspect of securing modern networks. This project will introduce you to penetration testing by asking you to perform various attacks against devices connected to a Wi-Fi network. Your penetration testing setup will be *portable* and can be used, in theory, to penetration-test any Wi-Fi network; however, you will use it to test only an experimental and not shared Wi-Fi network[1]. The portability aspect of this project is achieved by using Raspberry Pi, a very small computing device, to host your attacks.

Objective:

After successfully completing this project, you should be able to:

1. Set up a portable, purpose-built penetration-testing station using a Raspberry Pi;
2. Penetration-test any network and discover how easy it is to infiltrate, as well as the security-savviness of its users;
3. Think how you can defend your own networks against common network attacks.

[1] **Note: if you live in shared accommodation and/or your Wi-Fi connection is shared with other residents, please set up a personal hotspot to be used as the target network. Under no circumstances whatsoever, students should target networks or devices not fully owned by them. UNSW, The School of Computer Science, and the course staff are not liable for any attempted attacks by students against protected networks not fully owned by students and/or any associated damages and costs and legal issues.**

Tasks Required

In this project you are required to develop a portable penetration-testing station to test the security of your home Wi-Fi network.

Using a small portable computing device (Raspberry Pi) and an external Wi-Fi adapter, you will conduct an Evil Twin Access Point attack by setting up a fake Access Point (AP) that impersonates your home Wi-Fi and attempts to force users connected to the original AP to instead connect to your fake AP. You will then attempt to trick the users into revealing the original AP's password; once you know the password, you can join the AP as a client and perform various web-based attacks from within the LAN. Finally, you will suggest defensive mechanisms to detect and/or prevent the attacks you have performed.

Table 1 below summarises the tasks you will be assessed on. Details of each task follow in the sections below.

Task 1	Setup Portable Pen-Testing Station: Install Kali Linux on Raspberry Pi and connect ALFA wireless adapter.
Task 2	Evil Twin AP Attack: Set up a fake AP impersonating the target AP, and force target AP users to connect to it.
Task 3	Password Capture of Target AP: Set up a captive portal to trick users into handing over the password of the target AP.
Task 4	Web-based Attacks: Use your portable pen-testing station to perform various web-based attacks on users connected to the fake AP.
Task 5	Defence: Suggest defensive measures against the attacks performed in Tasks 2 – 4.

Table 1: Summary of tasks required in this project.

Task 1: Setup Portable Pen-Testing Station:

In your lab assignments you have conducted an Evil Twin AP attack using a Kali Linux VM and a Wi-Fi adapter. For this project, you need a setup that is portable and *in theory* can be used to perform penetration testing on any Wi-Fi network anywhere. You will set up your penetration testing tools on Raspberry Pi, a portable, credit-card sized computer. You can connect your own peripherals to a Raspberry Pi (mouse and keyboard via USB and monitor via HDMI), use a micro SD card as its memory, and any micro USB cable (such as a phone charger) to power it up. You can install any Linux flavour on a Raspberry Pi; we recommend Kali Linux for this project, as it comes with many of the penetration testing tools that you will need built in. While you may use a different OS if you can get it to work, you will then be expected to solve any installation issues you run into by yourself without help from tutors.

You can borrow the hardware (Raspberry Pi and Wi-Fi adapter) from the course tutor-in-charge, Uzma Maroof, or you may choose to use your own. However, you must register as a group indicating that you are doing this project (and not the research report). Once committed, no change will be allowed mid-way.

A Kali Linux version written specifically for Raspberry Pi can be downloaded from the Offensive Security website here.

OS installation and instructions for the initial configuration of your Raspberry Pi can be found here.

Once your Raspberry Pi is up and running with your chosen OS, you can simply connect the Wi-Fi adapter via USB. Test that it is running by executing the command "ifconfig" in a terminal before and after connecting the adapter; it should show an additional interface after connecting the adapter.

Task 2: Evil Twin AP Attack:

If you have correctly set up the hardware in Task 1, this step is very similar to Lab 2, Assignment 2, which you have already completed. The only difference is that you will be executing the attack on your Raspberry Pi instead of a VM on your lab PC. Specifically, you will perform the following sub-tasks:

1. Create an Access Point having the same SSID as your home Wi-Fi network.
2. Perform a deauth (deauthentication) attack on devices connected to the target Wi-Fi network which forces them to disconnect from the network.
3. Ensure that they join your fake AP by jamming the target network (for example by continuously deauthenticating any devices that connect to it).

You can use any available tool for this task or write your own code. Many existing tools that automate this attack sinkhole the traffic of users that connect to the fake AP, not routing it to the internet. Thus, a user is sure to suspect malicious activity when they are unable to access the internet. For bonus credit (1 extra mark), you may carry out this task in a way that ensures that users' traffic is still successfully routed to the internet (i.e., the fake AP forwards their traffic to the internet) so that they do not suspect that they have been compromised.

Task 3: Password Capture of Target AP

This task requires you to trick users of the target AP into revealing the password of the AP. You are required to accomplish the following sub-tasks:

1. Design a Captive Portal that asks for the Wi-Fi password when the users connect to the fake AP. Make the portal convincing, for example, present it as a router administration page that can trick a user into handing over the password by masquerading as a necessary router update required for internet access to be re-established.
2. Once a victim has handed over the password, save it in a text file and verify that it is correct (some tools exist that check the given password against a previously captured handshake).

After this you are required to tear down the fake AP immediately and stop jamming the original network so that the users can re-join the original network and access the internet as usual.

Task 4: Web-based Attacks

Now that you have successfully lured users into connecting to your fake AP and tricked them into revealing the password of the original AP, you can now connect as a client to the target AP. Being inside the target AP gives you an ideal opportunity to carry out many different attacks that require attacker and victim to be on the same LAN. For example, you can now carry out any number of web-based attacks as users browse various websites. You are required to demonstrate the following two attacks:

Task 4 Part 1: Credential harvesting for a social media website

This requires you to present users with a fake login page when they browse to a targeted website, for example facebook.com. The page should be identical to the real login screen of the website, so that it is hard for a user to notice that they are actually putting their login credentials into a fake page. In truth, the fake login page will send the user's entered credentials to a server under your control (i.e. running on your Raspberry Pi). Thus, you will first need to set up a fake login page that sends any data entered to your machine, and then ensure that users visit that page. The easiest way to do this is using DNS poisoning, so that when the user enters the name of the website, it resolves to your machine that is hosting the fake page.

You may use a readily available tool for this attack. Writing your own code is also acceptable as long as the main goal is accomplished, i.e. the user is presented with a fake login page when they browse to the targeted website, and the credentials entered by the user are visible to you as the attacker.

Task 4 Part 2: Web exploit for remotely controlling victim machine

A common end-goal of attackers using web exploits is to allow arbitrary code execution in a victim machine. For example, attackers first use web exploits to open a shell in the victim machine, connect it to the attacking machine, and then send arbitrary code to be executed in the shell. There are countless exploits that can be used to spawn a shell on a victim machine, and different browsers offer different vulnerabilities that can be exploited.

This task is open-ended and you may use any web exploit (or multiple exploits together if required) to ensure that you gain remote access to a victim machine on your target AP and are able to execute arbitrary code in it. To demonstrate the success of your exploit, you should create a temporary file on the victim machine's Desktop and be able to delete it via the attacker shell. Similar to previous tasks, you may use a toolkit or framework that automates much of this task for you.

Task 5: Defence

The final task of this project involves discussing defence (detection and/or blocking) mechanisms against the Evil Twin AP attack you carried out in Task 2 and the social engineering attack and web exploits you carried out in Tasks 4A and 4B. You are not required to actually implement these defences, although doing so will earn bonus credit. However, you must come up with practical solutions for detecting (and if possible, preventing) all three of the attacks. How would you secure your home Wi-Fi against these attacks so that you, the network administrator, are warned when any of these attacks is attempted? If it is possible to block these attacks, please outline how it can be accomplished.

Note: Vague answers such as "by using an Intrusion Detection System (IDS)" are not acceptable – if you think an IDS is the solution, you must provide details of which IDS you might use, how it would work and how you would configure it to detect the particular behaviour you are trying to catch.

Project Guidelines:

Group Formation

SWN project groups are composed of three students (unless explicit authorization from the course admin). ALL groups (whether same as lab or changed) must follow the below policy:

- Send an email to eng.cse.comp4337@unsw.edu.au with email subject "SWN'19 Project Group". The body of email must include all students name and ZID.
- You will receive a confirmation email from the same email account which includes your group name. The group name must be mentioned in all correspondence and when preparing the project report.
    - Note: no change is required to groups formed on Moodle for the labs, whether you keep the same group or change it.
- Deadline to send the email for your project group is **Monday, 25th of March at 9:00 AM**. Any group request after this time will incur penalty in the project mark for both group members.

Device Allocation

A limited number of ALFA and IoT devices are available for students who wish to attend the practical project. These will be made available on a first come first served basis.

Device List

Following devices will be provided to each group:

1. Raspberry Pi
2. ALFA Wi-Fi adapter
3. HDMI cable
4. SD card
5. Raspberry Pi case

Step to acquire Devices:

To acquire the devices follow these steps:

1. Make an appointment on the scheduler available on Moodle.
2. Download and fill device loan form, also available on Moodle.
3. Visit to School of Computer Science and Engineering (K17), 5th floor, room 501 during your booked slot to acquire the devices.

If you take any of the devices on loan, all group members will be responsible to return the device in working conditions on Monday 29th of April at 3 PM. Students will be responsible for any damage to the borrowed devices, otherwise.

Using own device:

Groups can also propose to use their own device subject to approval by tutor-in-charge, Uzma Maroof. You may contact the tutor-in-charge by booking a slot on moodle, as described above, and get approval for using your own device. If no slot is available contact tutor-in-charge by email.

Submission Format and Marking Criteria

You will demonstrate your project with a video, and describe your method, including all code, tools and commands used for Tasks 1 – 5, in a detailed technical report to be submitted along with the video. Both the report and the video will be marked out of 10, for a total of 20 marks for the complete project.

The video should be a screen recording showing running of each step of the project and must include the following each of the following segments against Tasks 1 – 5.

Task	Segment	Description
Task 1	Segment 1	A screen recording of running "ifconfig" in a terminal window in your Raspberry Pi before and after connected your Wi-Fi adapter to show that the Wi-Fi adapter is up and running.
Task 2	Segment 2-A	A screen recording of the commands you run for executing each of the sub-tasks described in Task 2 (Page 3 of this document).
	Segment 2-B	A screen recording of one victim device (e.g. another laptop or smartphone etc.) that shows the device being disconnected from the original AP and connecting to the fake AP.
	Segment 2-C	**(Optional, for bonus credit)**[2] Show victim device connected to fake AP and still able to access internet.
Task 3	Segment 3-A	A screen recording of the commands you run on your Raspberry Pi for executing both sub-tasks.
	Segment 3-B	A screen recording of one victim device that shows the user being redirected to a captive portal on connecting to the fake AP and entering the password.
	Segment 3-C	A screen recording of the password saved in a text file on your Raspberry Pi.
Task 4, Part 1	Segment 4_1-A	A screen recording of disabling the fake AP from Raspberry Pi, and of connecting to the original AP as a client.
	Segment 4_1-B	A screen recording of one victim machine also reconnected to the original AP.
	Segment 4_1-C	A screen recording of all the commands or tools you execute on Raspberry Pi to set up a fake login page for your target website and trick victims into browsing to your fake login page instead of the original (for example, if you use DNS poisoning, show all steps performed to execute the attack).
	Segment 4_1-D	A screen recording of one victim machine browsing to your fake login page and entering login credentials.
	Segment 4_1-E	A screen recording of the victim's login credentials appearing on Raspberry Pi.
Task 4, Part 2	Segment 4_2-A	A step-by-step screen recording of the commands and tools you run on your Raspberry Pi to open a shell on a victim machine.

[2] **Condition for Bonus Marks: Please note that you can only receive bonus marks (up to 2 marks for carrying out both bonus tasks) if you do not already have full marks in the practical component of this course (i.e. your bonus marks + your total mark for the practical component of the course cannot exceed 60). If you have already achieved full marks for the practical component, your bonus marks will not be added to your final exam marks.**

	Segment 4_2-B	A screen recording of the victim machine showing a particular file on the Desktop (that you will later remotely delete).
	Segment 4_2-C	A screen recording of the shell code you run in the remote shell you have opened on the victim machine, to delete the targeted file.
	Segment 4_2-D	A screen recording of the victim machine showing the file is no longer on the Desktop.
Task 5	Segment 5	**(Optional, for bonus credit).** You do not need to show any defences in the video unless you have carried out an implementation to actually block the attacks you have carried out in Tasks 2 – 4. If you have carried out any such implementation, you may show it in this segment of the video as screen recordings as you see fit and earn 1 bonus mark.

The report must include the following:

1. Title. Name of the project, group name and all the team members.
2. Executive summary that gives a brief introduction to the attacks performed in tasks 1 – 5 .
3. Description of methods for tasks 1 – 4, including a step-by-step description of all commands/scripts/code and tools used.
4. Discussion of defences against attacks performed (Evil twin AP, credential harvesting and web-based exploit for remote arbitrary code execution); include all possible countermeasures that you can apply to secure your network.
5. Project Diary: Each group is also required to attach a 1-page project diary to the report. This diary should maintain a weekly log of activities conducted by each group and should explicitly indicate the part played by each team member in these activities. You may use any format (Gantt chart, table, etc.) for maintaining the diary. The diary is not marked. However, if the diary is not submitted, a penalty of 2 marks will be applied. Please attach the diary at the end of the report. Do not submit it as a separate file. Unless specified otherwise, contribution from all members will be considered equal. Any difficulty in working with team members must be reported to the tutor-in-charge at the earliest.

Both the report and video are to be submitted together via Moodle (submission link will be under Week X material on Moodle).

Submission Deadline for report and video: _____

Late Submission Penalty

Late penalty will be applied as follows:

- 1 day after deadline: 20% reduction
- 2 days after deadline: 40% reduction
- 3 or more days late: NOT accepted

Plagiarism

Much information about the attacks in this project, as well as about defences against them, is available on the Internet. However, any direct cut-paste of material will be considered plagiarism. Please make sure that you use your own words, diagrams etc and make proper reference to any material that has been used in your report.

In addition, since we use TurnitIn, each submission will also be checked against all other submissions of the current semester and past submissions. Please note that we take this matter quite seriously.

The LIC will decide on appropriate penalty for detected cases of plagiarism. The most likely penalty would be to reduce the project mark to ZERO and reported to school plagiarism register.

Forum Use

We are aware that a lot of learning takes place in student conversations, and don't wish to discourage those. You are free to discuss (and are in fact strongly encouraged to do so) generic issues relevant to the project on the course forum. However, refrain from posting specific code-fragments or scripts on the forum. Students will be heavily penalized for doing so.

Warning: The attacks implemented in this project are for strictly educational purposes. Please do not perform these attacks against networks or devices not owned by you unless you have express permission from all users to do so.