# NWEN 405 "Security Engineering"

# Penetration Testing, Intrusion Detection and Interception Lab: 18-19 August, 2017

**Report is due September 10th**

## 1. Overview

### 1.1 Penetration Testing, Intrusion Detection

In this lab you will set up a firewall running a typical business configuration, connect a bank server (referred to as Ray's Bank) and run external penetration testing tools from the external side of the firewall. Next, you will introduce a command line version of SNORT on the internal network such that you can monitor suspicious traffic arriving at Ray's Bank. Then you will introduce a full commercial GUI IDS engine (SNORBY) and examine in much more detail the traffic reaching Ray's Bank – this stage is equivalent to a formal pen test and intrusion analysis carried out by an IT security engineer in practice.

### 1.2 Traffic Interception

In this section of the lab you will commence by extracting private data from an *http* connection using interception tools. Then you will move on and do the same thing with an *https* connections. This demonstrates how security services can pull data from encrypted https sessions. This tool is NOT to be used outside this lab.

## 2. Lab Report

1. Provide a brief introduction including an equipment interconnection diagram. Next provide a summary of the facilities of the three pen testing tools that you will use from the external side of the firewall – Zenmap, FileZilla, Nessus noting the similarities and differences between these tools.

2. Describe the use of the SNORT engines that you use for Intrusion Detection on the trusted side of the network alongside Ray's Bank. Very briefly explain how the command line version functions but then discuss the monitoring and reporting facilities in SNORBY.

   Where you identify any remote services in operation (clue: there are *four* main ones which require your attention) you are to recommend that either they be shut down - or if required for online services - to recommend secure methods of operation. Note that if you recommend that all ports/services be closed down (hardly realistic!) for this bank then you will need to explain how the systems staff will carry out software maintenance, how patches and updates are to be handled, how new developments are to be installed for clients and how Cloud Services will operate in practice.

3. Interception of encrypted http traffic – introduced by Black Hat. Provide a brief summary of how the interception engine works and how it is possible to extract personal data out of https connections. Note that we are only interested in the IT engineering side of such an interception system that could be used by intelligence agencies – not the legal nor ethical issues.

## 3. Marking Guide

*Presentation (10%):*

Include course and project name in the report title, your name and date.
Don't include an abstract for this report.
Do not double space, use a font size of at least 11 and choose a serif-font such as Times Roman for body text.

Use APA referencing or another widely accepted style (e.g. IEEE or Harvard) and include a biblography. Use citations to support claims. Use footnotes to indicate websites where tools can be found[1]. Avoid use of Wikipedia (or use it find things and locate the original source to reference).
Report submitted as a PDF.
No more than 10 pages, aim for 5 pages.
Spell checked.
Basic grammar checked (possession, subject-verb agreements, tense, punctuation).
Assumes reader wants an easy to read report and reader is someone else doing this course, has attended the lectures.
Correct use of terminology from the literature.
C grade: problems following presentation guidelines, readable but spelling or grammar mistakes.
B grade: followed all presentation guidelines, no spelling mistakes but some grammar problems.
A grade: as for B but minimal grammar issues.
A+ grade: well-written for the intended audience and well structured.

***#1 Brief introduction (30%)***

Draw your own network diagram (for example, https://www.lucidchart.com/pages/examples/network-diagram).
Describe each component's role.
Compare each tool in terms of features and it's advantages and disadvantages.
C grade: basic diagram, describes the function of tools at high-level.
B grade: diagram plus good explanation, comparison of functions and some pros and cons.
A grade: as for B but excellent presentation (perhaps a table) plus discussion in accompanying text of pros and cons with consideration of how they might be used by different types of penetration testers and at what point in penetration testing process.
A+ grade: as for A but included analysis of another pen testing tool not used elsewhere, perhaps even tried it out and include evidence of this in the report.

***#2 Snort and Snorby (30%)***

Comparison of Snort and Snorby.
Analysis of risks related to vulnerabilities identified related to theremote functions and proposed mitigations for these risks.
C grade: brief high-level comparison of Snort and Snorby without any real summary or analysis of differences, vulnerabilities in remote services identified correctly.
B grade: as for C but summary/analysis of differences between Snort and Snorby and basic mitigations for risks identified.

A grade: as for A but discussion of mitigations explicitly considers tradeoff between functional requirements of the bank and the need for safety, consideration of the potential effectiveness of mitigation against hackers with different levels of skill and motivation.
A+ grade: research another intrusion detection system and compare its capabilities with Snorby.

***#3 Interception of encrypted http traffic (30%)***

How does this work?
C grade: brief high-level description of how the man-in-the-middle manages to decrypt the traffic (use a diagram to help your explanation).

B grade: as for C but explain why it works (what's the vulnerability here) and how it became man-in-the-middle.

A grade: as for B but explain how you would prevent it and give an example showing how it would work in practice.
A+ grade: research another method to intercept what is meant to be sent via http.

---

[1] Study & Learning Site, RMIT *Referencing – Footnotes*, https://www.dlsweb.rmit.edu.au/lsu/content/1_studyskills/study_tuts/footnotes_ll/electronic.html Accessed: 19th August 2017