NWEN 405 "Security Engineering"

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

Report is due September 10th
Submit as a PDF, report should include diagrams and can include screen captures

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.

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.

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.