ELEC 567 Project Part I: Network Penetration Testing (22.5%)

(Due February 24, 2014)

J.D. E-Trading Ltd. is a global e-commerce company with branches in several countries around the world. The company has recently been victim of theft of important trade secrets costing several million dollars in lost revenues. The company suspects that the theft was carried through some insider attack against the company's network infrastructure. Likewise the CEO of the company managed to keep the incident secret and decided to audit the security infrastructure of the branch where the attack occurred. Assume that you are a professional penetration tester hired by E-Trading to perform the audit. No one from the branch under investigation know about your task. In fact only few managers from the IT department at the headquarter know about your task. Your cover is that you are an employee who is going to spend one month of training in this branch. As a trainee you've access only to the public website of the company (available at http://142.104.64.199/index), and no access (during the training period) to the private network.

Phase 1: Information gathering (10.5%)

1.1 Analyze the directory structure of the company website, and locate (in one of the files) the IP address of the company's private network. (3.5%)
1.2 Using scanners, extract the topology information of the company's private network. Identify available hosts, and for each host, find the IP address, Operating System, running services and open ports. Ensure that you specify the exact versions. (3%)
1.3 Identify vulnerable services; briefly explain why you think these services are vulnerable. (3%)

Phase 2: Exploitation (12%)

2.1 Review the *network* scanning results and other information obtained in the previous phase, and exploit one or more of the vulnerable services to gain access to the private network. (6%)
2.2 After gaining access to the private network, collect one of the following company confidential files (6%):
(i) Employees personal records (e.g. SIN, address, bank accounts from database server)
(ii) Source code of the company new mobile application (from the GIT code server)

Important Notes:

- Ensure to target only machines behind the J.D. E-Trading NATP.

- Document your answer using screenshots of your scanning activities and explain the scanning methods you used. Report both your successful and failed attempts.

Appendix: Additional Information (i.e. Hints)

During your first week at the target branch you were able to collect various information, some related to work obtained during the training sessions and personal information gathered during lunch and coffee breaks. Assume that by the end your first week you were able to collect the following information:

1. Mark Twain is the branch database administrator. He is hard worker, always on call and sometimes works from home, especially during the week-end when a problem occurs in the database server. He is a big fan of Harry Potter and his best Harry Potter book is “Harry Potter and the prisoner of Azkaban”.
2. Michael Phelps is a quality assurance engineer. He was hired initially as a co-op student to test the company public web site, and was later offered a full-time position. In his opinion ultimate security is all about authentication. He told you that BCRYPT is too expensive for password storage and MD5 or SHA is enough for password storage.
3. Peter Adams is a software developer who is currently very busy. He is working in a team that is developing an innovative mobile app that will give the company a head start over their competitors in the mobile-commerce space. He experienced before the week-end a problem with the Git server when he was trying to push his code. He will try to push his code from home. He is a big fan of Apple products and is unhappy about the fact that the company does not provide any Mac machine to the developers. He loves soccer and usually plays it every weekend.