NOTES FROM PROF KABAY ABOUT PREPARING FOR PENETRATION TESTING

1) **There is little point in penetration testing BEFORE we have provided**
   a) assurance that the pen-testers fully agree that their goal is to FIND PROBLEMS, not to show that there are none;
   b) awareness & training for all employees about the planned tests;
   c) role-playing exercises to prevent trauma if social-engineering techniques are part of the pen testing;
   d) assurance that individual mistakes will not be pinned to named individuals (mistakes do not include deliberate malfeasance);
   e) plans for positive (not negative) reinforcement such as prizes, honorable mentions and so on for low-vulnerability groups and systems;
   f) AUDIT to locate obvious technical and procedural problems that are to be FIXED before the pen-testers begin their work;
   g) post-test analysis plans similar to incident-response planning so that the best possible use can be made of the information.
2) **In addition, we should discuss the importance of legally-valid contracts authorizing the pen-testers to perform their work without being charged with violations of the CFAA [18 USC 1030(a)].**
3) **Any information gathered by the pen-testers that includes personally-identifiable data must be protected according to legal requirements (e.g., HIPAA or FERPA or GDPR) and corporate policies.**
4) **Pen-testers must be required to protect the confidentiality of all results of the exercises to protect the client-corporation's safety against illegal use of the discovered vulnerabilities and damage to their reputation.**
5) **External pen-testers should be bonded to prevent bad actors from infiltrating the systems under test.**

You may find the following articles interesting:

< http://www.mekabay.com/nwss/059_social_engineering_v03.pdf >

< http://www.mekabay.com/nwss/599_social_engineering_in_penetration_testing--1_(orlando).pdf >

< http://www.mekabay.com/nwss/600_social_engineering_in_penetration_testing--2_(orlando).pdf >

< http://www.mekabay.com/nwss/601_social_engineering_in_penetration_testing--3_(planning).pdf >

< http://www.mekabay.com/nwss/602_social_engineering_in_penetration_testing--4_(postmortem).pdf >

< http://www.mekabay.com/nwss/607_social_engineering_in_penetration_testing--5_(schumacher).pdf >

< http://www.mekabay.com/nwss/608_social_engineering_in_penetration_testing--6_(schumacher).pdf >