**Group Project Name: Penetration Test**

**Student: Gagneet Sahota**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Design:**

Design and document a penetration test.

Feel free to utilize the reference documents (located in Blackboard) (from SANS).

Within your design, incorporate the following components:

Example profile (type of industry and scale) of the organization that has enlisted you to conduct the pen test (not their name).

Detailed plan (2-page report).

Within your plan, be sure to include any particular vectors that you believe will be successful due to type of industry or any observations that you have made within similar industry segments.

In lab next week, we will present and review the plan(s) and follow through with tests of example infrastructure.

**Important Note:**

When you are designing and executing a pentest, documentation can be of great help as replicating exact configurations can at times be challenging. Note: When we do not replicate a configuration exactly, we can end up creating security issues (assuming we had a “secure” or robust design initially). Another reason to develop good documentation is that it gives a good idea of what should be happening with systems and it can be reviewed and refined over time so that the quality of your designs and configurations increases as you practice.

**Questions to Answer:**

Explain the relevancy of a pentest to an organization’s overall security? -

* A pentest can find a potential vulnerability before they get exploited and determine if the security practices of a firm need to be improved.

Said differently, what benefits does a pentest offer?

* Find holes in the security before the bad guys find it.

How long are the results of the pentest “good for”?

* I believe pentest are good for as long as the security is still up to standards and the time frame hasn’t been more then 6 months as security and technology is constantly changing.

Said differently, assuming your organization fared well, what would be an example frequency for testing?

* For my organization the best method would be using social engineering

Explain how your previous usage of the Social Engineering Toolkit (SET) can play a role within your test.

* The organization’s website could be spoofed to get credentials from employees who have elevated system privileges allowing access to the system.

What, if any, nuances does the popularity of Public Cloud computing add to your plan? Explain.

* If the organization uses the cloud then it’ll be difficult to gain access to any hardware they use in the cloud as it wont be as simple as penetrating the security of the locations network.