**FootPrinting Report**

**Introduction:**

Maintaining a proactive approach on security requires that an organization perform its own hacking footprinting to see how much information is available to potential hackers. Some organizations do this using internal staff; however, it is much more common to see organizations hire external security consultants to perform these types of security reviews. This allows a truly unbiased outsider to attempt to gather as much information as possible to formulate an attack.

Assume that you have been selected as the security consultant to perform a comprehensive security review for an organization of your choosing. Ensure that the organization that you select has a public website that you can access and at least one web application that you can use for this task. You will review the security of the organization’s website and any related web applications and consider security risks such as structured query language (SQL) injection and social engineering techniques.

To complete this task, you will need to perform a footprinting analysis of your selected company. Your comprehensive security review will involve a series of tasks that are described in detail below.  
  
*Note: You are* ***ONLY ALLOWED TO DO*** *“Passive” Footprinting.* ***At no time during the execution of this task should any connection be made to the Footprinting target****. If you have any questions please contact your instructor.*

**TO CLARIFY: YOU ARE NOT ATTACKING ANYONE! THIS IS USING ONLY PASSIVE METHODS. THIS WILL BE FURTHER DISCUSSED DURING CLASS.**

**Task:**

A.  Create a report (*suggested length of 2 – 5 pgs*) in which you do the following:

1.  Summarize your findings of a footprinting analysis you performed on your chosen organization.

2.  Discuss how the information gathered during your footprinting analysis could be used to initiate an attack against the organization.

3.  Discuss social engineering techniques that could be utilized to gather information regarding the organization’s computer systems.

a.  Present appropriate countermeasures that should be used to combat such social engineering techniques.

4.  Prescribe a series of countermeasures and remedies that could be utilized to counter this type of footprinting attack.

6.  Present common threats against web applications that pose the greatest risk to the organization’s web applications.

B.  When you use sources, include all in-text citations and references in APA format.

*Note: When using sources to support ideas and elements in a paper or project, the submission MUST include APA formatted in-text citations with a corresponding reference list for any direct quotes or paraphrasing. It is not necessary to list sources that were consulted if they have not been quoted or paraphrased in the text of the paper or project.  
  
Note: No more than a combined total of 30% of a submission can be directly quoted or closely paraphrased from sources, even if cited correctly.*