ITEC345 2013spring-ibarland

**Hw08 answer sheet** (submit on D2L):
Network security basics.

The primary instructions are at [hw08.docx](http://www.radford.edu/itec345/Homeworks/hw08/hw08.docx). Use *this* document to record your answers.

**Note: The table below enumerates the tasks that need to be accomplished. Please record your answers next to each task. The instructions to accomplish the tasks and the motivation for the tasks are provided after the list of tasks.**

**Note: This is a group project. You are encouraged to team up with 1 other student. ONLY ONE SUBMISSION PER EACH TEAM REQUIRED. Be sure to complete all 3 of the following lines:**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Name of teammate: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Virtual Machine used: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (e.g. “team99\_WinXP”)**

**Assignment Deliverables**

|  |  |
| --- | --- |
| **Task category**  | **Task description (please record your answers after each task in this table)** |
| **Basic network administrative tools** |
| **Casing a network.** | 1. Identify the IP address of your computer.

Deliverable: enter the IP address here:  |
| 1a. Identify the *network* of your workstation – that is, the first 3 octets (e.g., if IP address is *X*.*Y*.*Z*.*W*, network is *X*.*Y*.*Z*).**Deliverable: Enter the network address here:**  |
| 1. What is the IP address of Radford University’s domain name server.

 **Deliverable**: Enter the IP address here.  |
| 1. Reverse engineer the firewall: the network you are working on is protected by a very restrictive firewall. Using **ping** determine if the network is blocking or allowing traffic to and from the following servers. Record your answer in the deliverables by entering either the word “blocked” or “allowed”. An example is provided for [www.google.com](http://www.google.com) below :

 **Deliverable**: * 1. [www.google.com](http://www.google.com): **blocked**
	2. [www.radford.edu](http://www.radford.edu):
	3. 137.45.26.80:
	4. 137.45.192.187:
	5. [www.google.com](http://www.google.com):
 |
| 1. Identify the network path between your team’s workstation and Radford’s DNS server.

**Deliverable**: Screenshot showing the IP addresses of systems in the path (or “\* \* \* Request timed out.” for silent nodes).  |
|  | 1. Identify the Operating system of the firewall server.

**Deliverable**: Enter the screenshot that shows the name of the OS on the firewall server. |
| 1. Identify the open ports on all the workstations on your network.

**Deliverable:** Partial screenshot of the results. Entire screenshot is difficult to capture due to the resolution of the terminal.  |
| **Checking for out-of-date software.** | 1. Identify the programs that are up-to-date and those that aren’t.

**Deliverable**: screenshot of Secunia PSI screen.  |
| **Packet sniffing** | 1. When connecting with Secunia PSI’s website, identify:
	1. All the application layer protocols that are being used.
	2. The IP address of secunia database that the Secunia PSI software is connecting to.

Hint: you may need to use Wireshark for this. **Deliverable**: 1. List of application layer protocols being used.
2. The IP address of secunia database
3. Screenshot showing wireshark.
 |