ITEC345 2013fall-ibarland

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

Due 2013.Dec.06 (Fri) 17:00

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; ***please work in teams of (at most) three***.Submit only one solution for your entire team. **All team members must be physically working together** for all parts of each problem.[[1]](#footnote-1) If you are looking for others to work with, post a request on the discussion boards. Before starting, decide which team-member’s Windows XP workstation you will use, from the [hw07-windows-VM-login instructions](http://www.radford.edu/~itec345/2013fall-ibarland/Homeworks/hw07-windows-admin/hw07-windows-VM-login.html). Please try not to use multiple workstations per team, as resources are limited.

**ONLY ONE SUBMISSION PER EACH TEAM REQUIRED. Please state the names of all team members so everyone gets credit. Also please state the team number you used as this is necessary for me to check your solutions.**

**Team Member A: \_\_\_\_\_\_\_\_\_\_\_\_@radford.edu**

**Team Member B: \_\_\_\_\_\_\_\_\_\_\_\_@radford.edu**

**Team Member C: \_\_\_\_\_\_\_\_\_\_\_\_@radford.edu**

**Virtual machine used: team\_\_-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):   6. secunia.com: |
| 1. Identify the network path between your team’s workstation and Radford’s DNS server (the one you identified in #1).   **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 DNS 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: have Wireshark running; start up secunia; see what IP address(es) it is communicating with, and which of those might be the database.  **Deliverable**:   1. List of application layer protocols being used. 2. The IP address of secunia database 3. Screenshot showing wireshark. |

1. Should you want to add a team member after having already completed problems, you’ll have to *re*-complete those steps with them (presumably letting them ‘drive’ the keyboard). [↑](#footnote-ref-1)