**Checkpoint 3 –** **6%**

Demonstrate the following:

|  |  |
| --- | --- |
| **Service** | **Method of testing/expected results** |
| Wireshark\TCPDUMP | Run tcpdump on your router, listen on all interfaces and capture all traffic into a PCAP file. **After completing all of the tasks in this checkpoint**, move the tcpdump capture file to your client. Filter it through wireshark to display only the following data:  An SSH packet to your router from your client  An SSH packet from your router to your client  A MYSQL packet from your Client to your Linux Server  A MYSQL packet from your Linux Server to your Client  **Export this data into a new PCAP file. This file will be included in your documentation upload.** |
| SSH (Router) | Connect to your router from your client via SSH on the non-default port specified. |
| SSH (Linux Server) | Connect to your SSH (Linux) server from your client and download a file. |
| FTP | Connect to your FTP service installed on your Windows Server and download a file. |
| E-mail | You will create two e-mail accounts on your mail server called user1 and user2. From your client machine you must be able to access these e-mail accounts from your client machine. You will send an e-mail from user1 to user2 and then have user2 reply to it. |
| MYSQL | Access the MYSQL server from the client **using an account that you have created that has read-only privileges.** You will then attempt to perform an action that requires write privileges (ex. Drop database test;) This action should fail due to the user having insufficient rights. |
| IPTABLES/Firewall | You will create a script that **I will refer to as Scenario 1A.** It will configure your firewall to do the following:   * **Allow** only traffic for services specified in the **“Network Standards and Specifications”** document. **All other requests to servers will be dropped.** * All accepted traffic must be sourced from/destined to your client’s subnet * All accepted traffic must be part of a NEW, ESTABLISHED or RELATED session   You will create a script that **I will refer to as Scenario 1B.** It will configure your firewall to do the following:   * **Do not allow** requests from your client to your IIS server. * **Do not allow** responses from your Apache server * **Allow** all other traffic for the assignment as specified in Scenario 1A |
| IPTABLES Logging | You will submit a text file that contains the following packets from your **IPTABLES LOG**:  **A dropped request** from your client to your IIS server  **A dropped response** from your Apache server to your client |
| NMAP | You will perform a network scan of all of the ports in use on your Windows server for this assignment. **The results of these scans will be included in your documentation submission.** |

**Documentation required for BlackBoard submission:**

Step by step instructions on how to complete the checkpoint

Filtered Wireshark capture file

Filtered iptables log

NMAP scan results