James Madison University

Integrated Science & Technology (ISAT)

ISAT 460 Networking & Cyber-Security II

Implementation of TACACS+ and Vulnerability Assessment

Semester Project Lab Instructions

Author(s):
Troy Gamboa
Isaac Sumner

Submitted to:
Dr. Emil Salib

April 23, 2017

Honor Pledge:I have neither given nor received help on his lab that violates the spirit of the JMU Honor Code.

Troy Gamboa	Isaac Sumner
Signature	*Signature*
Date	*Date*

Contents

1 Learning Objectives

- What is TACACS+?
- What is AAA?
- What is the different between TACACS and RADIUS?
- What is gns3?
- What is gcc?
-
-
-
-

2 Equipment & Software

Each team should have access to

- A desktop (9020 Dell) Linux 16.04 LTS (username: checkout, Password: hellocheckin)
- VMware Workstation 12 on Linux
- Virtual Machines Base (to be used for cloning and copying) are in /home/checkout/Base_VMs folder: Ubuntu Desktop 16.04 (x64), Ubuntu Server16.04 (x64), Windows 10 (x64) and Kali-Linux 2016.2 (x64)
- Access to iMac (OSX 10.11.x) with VMware Fusion 8.x (username admin3022, password: 3022$3022)
- Access to the Lab private network and to the public network (not simultaneously)
- Access to ShareLatex online
- Ethernet network connection
- Windows 7 VM
- access to TACACS+ Server executable downloaded from TACACS.net

3 Best Practices (Trouble Shooting is How You Learn Networking!)

- To obtain the names of the available network interfaces use the following command: ls /sys/class/net.
- Get used to applying tcpdump for quick packet capturing: A good cheat sheet can be found in http://www.rationallyparanoid.com/articles/tcpdump.html
- Make sure that you have your SSD drive in every class. All your VMs should be on your SSD drive. Clone or copy the baseline VMs to your SSD drive. Never make use of the baseline VMs unless you are given a permission to do so.
- Lab Desktops are set up for weekly deep freeze, that is, every weekend, the desktops will be restored to their original image state. Whatever documents, VMs, etc. left will be wiped out with no way to be restored!
- Do not leave the lab without copying all materials (including VMs) that you care not losing!
- Make it a habit to look up protocol definition and specifications in the appropriate RFC and IEEE standards documents.
- We will be using ShareLatex in creating the Lab Reports. ShareLatex is available online for free.

- Take many screen-shots even if you decide later to drop some.
- Make it a habit to look up a new Linux command description using man ¡command¿.
- Check Firewall: Ubuntu #sudo ufw status, Fedora #sudo /etc/init.d/iptables status, Windows: Check firewall status.
- If you have problems connecting to the Internet, sometimes it's as simple as checking whether the Ethernet Network interface is registered with JMU registration server or whether the Ethernet Network interface adapter (real or virtual) is connected and/or configured correctly (manual versus DHCP).
- When you're working on remote desktop access, make sure that the PC you are trying to access remotely is configured to allow remote desktop access.
- Check reachability/connectivity between two PCs using the ping command.
- Power off or suspend all unused VMs to maintain a decent performance on the Host. The more VMs are powered on, the more demands on the Host's CPU and RAM.
- Check if the software application/program you need is installed.
- As a last resort, you could always reboot (power off/on).
- You should always check Edit ¿ Virtual Network Editor and make sure that vmnet0 is set up for bridged/Auto-bridging, vmnet1 is configured for Host-only and vmnet8 is configured for NAT. These vmnets configurations should not be changed unless instructed to do so.
- In the case that the Asus AP (Access Point) acts sluggish or becomes non responsive, make sure to reset the AP by unplugging the power, press the RED button. While still pressing the RED button, plug back the power and wait for 1 min before releasing the RED button. When asked to enter username and password enter admin, admin, and admin or root, root and root.
- If one of two connected devices has the automatic MDI/MDIX (Medium Dependent Interface/Meduim Dependent InterfaceCrossed) configuration feature there is no need for crossover cables. Introduced in 1998, this made the distinction between uplink and normal ports and manual selector switches on older hubs and switches obsolete.
- If you are working with one or more VMs on an exercise and you need to stop and continue at another time, you can always freeze the VMs in a state that would allow you to continue from where you left off. That is, instead of selecting Power Off you should select Suspend!
- If you get Error binding to port for 0.0.0.0 port. Check lsof i:1812. If you get a response, then you have hung up port. Kill port kill 9 pid. You may also check netstat unpl. However, the easiest way is to execute sudo pkill 9 radius.
- Check the following site for mysql commands:
  http://cse.unl.edu/~sscott/ShowFiles/SQL/CheatSheet/SQLCheatSheet.html
- tcpdump the easy tutorial http://openmaniak.com/tcpdump.php
- Note that // means COMMENTS
- Use clear!
- In a command line shell, you can scroll up using shift+pg up

4 Exercises

MAKE SURE TO PROVIDE NETWORK DIAGRAMs AND TABLEs CONTAINING INFORMATION ABOUT THE MACHINES INVOLVED (SUCH AS, IP ADDRESSES, MAC ADDRESSES, ETC.)

4.1 Exercise 1: Setup of TACACS+, Creating Test Users, and Configuration

4.1.1 Introduction

- You are required to setup an IT department in which all the routers, switches, firewalls, access points and other hardware devices are all to be accessible through a single network. After some research, you find that there are protocols dealing with Authentication, Authorization, and Accounting (AAA), which seem to be highly useful for the job. Of those protocols, you find RADIUS and TACACS+ at the top of the list. As you have already investigated RADIUS, you begin to study TACACS+.
    - Q1 - What does TACACS+ stand for, and what is it used for?
    - Q2 - What is the difference between TACACS+ and TACACS?

  ALL INVOLVED VMs SHOULD HAVE THEIR NETWORK ADAPTORS BE CONFIGURED FOR NAT or HOST-ONLY CONNECTION MODE (IF YOU DO NOT KNOW HOW, PLEASE ASK YOUR INSTRUCTOR OR TA). In this Exercise, let us try NAT.

4.1.2 Step 0: Preparation (see Appendix A)

- For this exercise, you will need
    - VMs: Windows 7 VM/NAT, Ubuntu Server VM/NAT
    - TACACSSetup_v1.3.2 executable file provided.
    - Access to GNS3 Software.
    - GNS3 network saved files, with access to Cisco 3600 router.
- Make sure that the VMs you are utilizing are located locally on your host machine, rather than on an external drive. GNS3 has a hard time using VMs that are not local.

4.1.3 Step 1: Setup of TACACS+ Server on Windows 7 VM

- In this step, we will run through the setup of the TACACS+ server, provided to us by TACACS.net.
- Launch the Windows 7 VM. It might be a good idea to increase the RAM and processing power before powering on the VM, as this is where we will set up the main server.
- During the installation process, the wizard will ask you to input a shared secret to make use of when logging onto the server. Enter:

  testsecret

  when prompted. (This may be changed at a later time in the configuration files, as noted.)

- Begin the installation, and click Finish when complete. You have now successfully put the TACACS+ Server on your windows 7 vm! By default, the process should have automatically been started and running.
    - Q1 - Provide 2 forms of proof that the TACACS+ server is up and running on the windows 7 vm.
    - Q2 - What port does the tacacs.net tacacs+ server run on by default?
    - Q3 - Show evidence that the tacacs+ server can be started and stopped with `net stop tacacs.net` and `net start tacacs.net` in an administrative terminal.
- Validate that TACACS+ Server installed correctly, and all configuration files are free of errors. This is done by navigating in the gui file explorer to C:\Program Files\TACACS.net, and selecting

  tacverify
- FROM HERE ON OUT, MAKE SURE YOU ARE RUNNING ALL APPLICATIONS OR SERVICES AS ADMINISTRATOR.
- All of the changes of configuration done by this TACACS.net TACACS+ server are through XML files. To access these files, navigate to C:\ProgramData\TACACS.net\config.
- Here, you will be presented with 5 separate files.
    - Q4 - Verify that the list of configuration files include: authentication, authorization, clients, googleotp, and tacplus.
- Now that we have confirmed that all is working with the server, we will now begin to test connectivity, both remotely and locally.

4.1.4 Step 2: Local /Remote Connectivity Testing

- To first test the TACACS+ Server locally, we will create a test user, and attempt to connect to the server with the given credentials.
- With the text editor of your choice, (we used atom), open the "authentication.xml" file located at C:\ProgramData\TACACS.net\config, and uncomment the following lines as seen below in figure 1 (lines 44 and 61 in figure 1.) If you are not able to edit these files with the text editor of your choice, select all of the cofiguration files, and verify that they are not set to "read only".

```
40
41      <UserGroup>
42        <Name>Network Engineering</Name>
43        <AuthenticationType>File</AuthenticationType>
44  <!--
45      <Users>
46        <User>
47          <Name>user1</Name>
48          <LoginPassword ClearText="somepassword" DES=""> </LoginPassword>
49          <EnablePassword ClearText="" DES=""></EnablePassword>
50          <CHAPPassword ClearText="" DES=""> </CHAPPassword>
51          <OutboundPassword ClearText="" DES=""> </OutboundPassword>
52        </User>
53        <User>
54          <Name>user2</Name>
55          <LoginPassword ClearText="somepassword" DES=""> </LoginPassword>
56          <EnablePassword ClearText="" DES=""></EnablePassword>
57          <CHAPPassword ClearText="" DES=""> </CHAPPassword>
58          <OutboundPassword ClearText="" DES=""> </OutboundPassword>
59        </User>
60        </Users>
61  -->
62      </UserGroup>
63
```

Figure 1

- Replace the field between the Name tags of "user1" to `testuser1`. Replace the field between the LoginPassword ClearText="somepassword" to `testpassword`. Save the file.
- To test that the adding of another user was successful, first navigate to "tacverify" as you did before from the start menu, All Programs, TACACS.net, "TACverify".
- If no errors were found in the configuration, you can then run "TACTest", in the same directory as "TACverify".

- When you click on "TACTest", you will be presented with a terminal. To initiate the test, log onto the server using the credentials of the test user "testuser1" that you just made in alteration of the authentication.xml file earlier with these commands:

  tactest -k testsecret -u testuser1 -p testpassword
  tactest -k testsecret -u checkout -p checkout

  - Q1 - What do the -k, -u, and -p flags mean?
  - Q2 - How are we able to execute the `tactest` on the user "checkout" if we did not manually set the user up?
  - Q3 - Did the `tactest`s work? Provide screenshots for evidence.

4.1.5 Setting up gns3

We might move this to exercise 2

- Install gns3 on the Host machine, and launch.

  sudo apt-get install gns3-gui
  sudo gns3

- When asked to select a server for gns3 to run on, select **"Local Server"**.
- Add the cisco router image provided to the gns3 network topology. This can be done either through the preference menu on GNS3, or upon startup of GNS3. Follow the default settings, and when done, drag the router to the empty space in the middle.
- Right-click the router and click start, then right click the router again and select console. Here we will set up the router to have a static ip address of 10.10.10.2.
- Issue the following commands in the console of the cisco router.

  show run
  show ip interface brief

  ◦ Q4 - What do the previous commands show / do?

- It is a good thing to note that when the router returns a long list of values, you can use the Enter key to move down line by line, Spacebar to go to the end, and any other key to cancel.
- To set a static ip in the cisco router, initiate these commands:

  config t
  interface FastEthernet0/0
  ip address 10.10.10.2 255.255.255.0
  no shutdown
  end

- check that the ip had been successfully been set with these commands once more:

  show run
  show ip interface brief

- Add an Ubuntu Server VM to the GNS3 Topology, in a similar manner of how the router was added.
- Assuming you have knowledge of setting a static ip address on the ubuntu server, make an interface of vmnet3 in the VMware virtual network editor, and set it to host only with a subnet IP of 10.10.10.0 (netmask 255.255.255.0). Add a network adapter to the Ubuntu Server VM of which you just launched and set it to vmnet3, with an ip address of 10.10.10.100.
- Create a link between the cisco router and the ubuntu server VM using the link icon on GNS3 (The last one on the left panel).
- Select FastEthernet0/0 on the router, and drag it to Ethernet1 on the Ubuntu Server VM.
- At this point, the network topology should look similar to the figure 2 below.

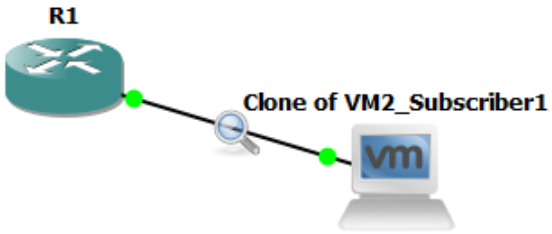

Figure 2: Preliminary network topology

- GNS3 has wireshark packaged in upon installation. To test this, right click on the ubuntu server vm in the network topology, and select capture.
- An instance of wireshark should then launch. To test this, you should ping 10.10.10.100 from the cisco router to receive icmp packets. Close wireshark, and export the packets as "test_icmp.pcapng".

4.1.6 Testing tacacs server on preliminary topology

- Go to Exercise 2, and install the tac_plus daemon on the ubuntu server you have connected to your gns3 topology. Once done, return to this step to test the tacacs connectivity.
- Console into the cisco router once more, and apply the following commands:

```
config t
tacacs-server host 10.10.10.100
tacacs-server directed-request
tacacs-server key tac_test
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization config-commands
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 7 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 7 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network 0 start-stop group tacacs+
aaa accounting network 15 start-stop group tacacs+
aaa accounting connection 0 start-stop group tacacs+
aaa accounting connection 15 start-stop group tacacs+
aaa session-id common
```

- Exit, and verify that these commands were successful with the `show run` command once more.
- To test the tacacs+ server, Start capturing packets on the ubuntu server vm (using the same method as before). We will now tail the tacacs+ log files on the server,

and telnet into the router, providing the verification of the user johnathanm we set in the tacacs+ configuration file.

- On 2 new terminals on the Ubuntu Server VM (CTRL + ALT + F2 (or F3)), run:

  tail -f /var/log/tac_plus.log
  tail -f /var/log/tac_plus/tac_plus.acct

- Restart the tacacs+ server with:

  sudo /etc/init.d/tac_plus stop
  sudo /etc/init.d/tac_plus start

- With the log files being tailed, and wireshark still running, we will test that you have connectivity to the server. Go back to the first terminal in the ubuntu server vm with CTRL + F1.
- Telnet to the router's ip address, and enter the necessary credentials that you set in the file located at /etc/tacacs/tac_plus.conf.

  telnet 10.10.10.2

- You have now successfully connected to the tacacs+ server via cisco router! Stop wireshark and export the specified packets, as well as the log files that were being tailed.
- To prove that you are in the cisco router of which you had previously set up, issue:

  show run
  show ip in br
  show users

4.1.7 Step 3:Comparison to RADIUS

- **Extra Credit (5 points each)**

4.2 Exercise 2 - TACACS on Ubuntu Comparison to Windows

4.2.1 Step 1: Preparation

- For this exercise we will need a single Ubuntu Server VM, configured for NAT. We will refer to this machine as VM1
- On VM1 run `sudo su` to become the root user.
- This version of TACACS relies on four dependencies: gcc, bison, flex, and libwrap0-dev. Check to see if they are installed by running

  dpkg -s gcc bison flex

  ◦ Q5 - What is gcc?
- Use `apt-get install` to install the packages that aren't already installed.
- Now we need to install TACACS+. Download by running

  wget ftp://ftp.shrubbery.net/pub/tac_plus/tacacs+-F4.0.4.26.tar.gz
  tar zxvf tacacs+-F4.0.4.26.tar.gz
- Navigate to the `tacacs+-F4.0.4.26` directory and use `cat` or `less` to view the contents of INSTALL.

  ◦ Q6 - What does the `--prefix` option do?
- Now run

  ./configure -help

  to view all the installation options.
- Next, run

  ./configure –enable-acls –enable-uenable make install
- Now, we must make sure that necessary library links are installed. Execute `nano /etc/ld.so.conf`. Add the line `/usr/local/lib`, and reload the libraries using the `ldconfig` command.

4.2.2 Step 2:

- Now, we will be creating the two user groups: sys_admin and network_admin. Let's first create the tac_plus.conf file.
- Execute `mkdir /etc/tacacs`, then change into that directory. Run `touch tac_plus.conf` and `chmod 755 tac_plus.conf`.
- Next, we shall make a file for the accounting logs.
- `mkdir /var/log/tac_plus`
- `touch /var/log/tac_plus/tac_plus.acct`
- Now, add the text in Appendix (appendix here) to the `tac_plus.conf` file
- Let's take a look at the file:
- Under `Encryption Key` we see `key = "tac_test`. This is used to encrypt packets between the server and clients.
- Now, look under the comment `Set where to send accounting records`. We have the lines `accounting syslog;` and `accounting file = /var/log/tac_plus/tac_plus.a` This tells the tacacs daemon where to write log information.
- Let's take a look at the text under the `ACL for network_admin group` and the `ACL for sys_admin group` comments.

  ◦ Q5 - Compare the permissions under each ACL group.
- Now let's look at the sys_admin group configuration, specifically the sections that begin with `cmd =`

- Q6 - Which commands for the sys_admin group are only allowed with certain options?

- Let's look at the at the specific users that are defined in our config file. These configurations can override those for the group specified.
- Under the user jonathanm, notice the `login =` and `enable =` fields. These are passwords generated with `tac_pwd`. Instead of using the ones in the template let's make our own.

  tac_pwd

  Password to be encrypted: your password here

- The output you receive is a DES encrypted password. Add your password to the config file (the one you just generated and two more).

4.2.3 Step 3:

- We need a couple more steps to give tac_plus the normal start/stop abilities (using service)
- Execute:

  touch /etc/default/tac_plus

  chmod 755 /etc/default/tac_plus

  nano /etc/default/tac_plus

- Now copy the script text in Appendix(blah) into `/etc/default/tac_plus`
- Start the service by executing:

  /etc/init.d/tac_plus start

- Verify tac_plus is in fact running.

  ps aux — grep tac_plus

  netstat -an — grep :49

4.3 Exercise 3(?): Vulnerability Assessment of TACACS+ Server

4.3.1 Step 1: Setup and DOS

- While a TACACS+ Server can be useful in the field of network access control, there are certain vulnerabilities that are in place that must be looked at. There are 7 of these vulnerabilities that must be assessed. Of these include:
    - Lack of intergrity checking
    - Vulnerability to replay attacks
    - Forced session_id collisions
    - The birthday paradox and session_id's
    - Lack of padding
    - MD5 context leak
    - Packet body length DoS and/or overflow
- While it is not feasible to implement all of these vulnerabilities at this time, we will only be looking into a few in this exercise.
- The first Tacacs+ vulnerability we will examine is a DOS via an older version of tac_plus that doesn't error check payload length. Instead of downloading this older version, we can instead make a trivial change to the source code to simulate this insecure version.
- From the home directory where you downloaded Tacacs, cd into the `tacacs+-f4.0.4.26` directory. Now open the packet.c file using nano, and scroll down until you find the `/* get memory for the packet */` comment. Now comment out the lines so the file now looks like this:
- Now look at the following line:

  len = TAC_PLUS_HDR_SIZE + ntohl(hdr.datalength);

    - Q5 - What does the len variable represent? (No need to be overly technical)
- The lines we commented out basically does a sanity check on the length of the encrypted data contained within the Tacacs+ packet. Now look at the line directly after the comment:

  pkt = (u_char *)tac_malloc(len);

- This statement allocates memory for the packet structure called `pkt`. It is important to note that, if tac_malloc fails it returns null.
- By commenting out the length sanity check we are simulating an old version of Tacacs+. This code was added after a major vulnerability was discovered.
- Next, we need to open up the Kali-Linux VM. Let's make sure that scapy is installed by executing:

  dpkg -s scapy

- Now create an empty text file named tacacs_scapy.py and fill it with the script in Appendix ?. Make it executable with:

  chmod 755 tacacs_scapy.py

- Now run the script (`./tacacs_scapy.py`). Now we can interact with scapy. Execute:

  tac=Tacacs()
  tac.display()

- This is a Tacacs+ layer header populated with default values. For our attack we mostly care about the length.

- Q6 - Why did we need the script to examine a Tacacs+ packet with scapy? Hint: Look online for a list of protocol layers that scapy knows by default.

4.3.2 Step 2: Tacflip.py? (Using kali)

- Here, we will use the same network configuration as we did in exercise 1 when we set up gns3. However, this time, we will add an instance of kali linux as a "Man in the middle" between the router and the tacacs+ server.
- Add and open a kali linux vm in VMware Workstation through gns3 and add another network adapter in the virtual network editor. Set this adapter to vmet3. (Make sure that you configure all vms in gns3 to use any configured gns3 adapter).
- Assign kali a static ip address of 10.10.10.123/24 in the /etc/network/interfaces file. Make sure that you can ping to the tacacs+ server (10.10.10.100) and the cisco router (10.10.10.2).
- For this step we will need to obtain the tacotaco-master zip provided and extract it into the Downloads folder.
- The end goal of this attack is to simply bypass all required authentication and authorization techniques provided to us by the tacacs+ server. In short, the tacflip python file makes use of a man-in-the-middle and bitflip attack on the tacacs+ server, and grants users with invalid credentials full access to the server.
- The man-in-the-middle attack will be performed by use of ettercap, a software built into kali linux. In partucular, we will make use of ARP poisoning to trick the router that the attacker (in this case, the kali vm) has the MAC address of the tacacs+ server.
- First, open a terminal and cd to where you extracted the tacotaco-master folder.
- Run this command:

  python tacoflip.py -t 10.10.10.100 -v
- on another terminal, launch ettercap.

  ettercap -G
- Under "Sniff", select "unified sniffing" and set it to the interface of which you assigned the static ip to kali (Most likely eth1).
- Scan for Hosts under "Hosts" and select the ip / MAC addresses of the TACACS+ server and the Cisco router. (10.10.10.100 and 10.10.10.2, respectively)
- Initiate ARP Poisioning, and select the option to "Sniff Remote connections" under the "Mitm" tab.
-

4.3.3 Step 3:

4.4 Exercise 4(?): Extra features of TACACS (Single Sign On, etc.)

4.4.1 Step 1: Preparation

4.4.2 Step 2:

4.4.3 Step 3:

5 Additional Questions

6 Deliverables

7 References

8 Appendices

8.1 Appendix A - TimelineMilestones

1. 10/10/2016 - Announcement
2. 10/12/2016 - 3 ideas: a list of 3 ideas and brief description of each and why you are interested in each of them)
3. 10/17/2016: SP Status 1- Definitions of 2 of 4 exercises, identifying resources, lab instruction (outline, network configuration) draft, Lab report draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
4. 10/24/2016: SP Status 2 -Definitions of 4 of 4 exercises, identifying resources, Lab instruction (Ex 1) draft, Lab report draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
5. **1**0/31/2016: SP Status 3 - Demo of Exercise 1, ShareLatex Lab Instruction (Ex 1, 2) draft, ShareLatex Lab Report (Ex 1) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
6. 11/9/2016:SP Status 4 - Demo of Exercises 1, 2, ShareLatex Lab Instructions (Ex 1, 2, 3) draft #1, ShareLatex Lab Report (Ex 1, 2) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
7. 11/16/2016:**S**P Status 5 -Demo of Exercises 1, 2, 3, ShareLatex Lab Instructions (Ex 1, 2, 3, 4) draft #1,ShareLatex Lab Report (Ex 1, 2, 3) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
8. 11/30/2016: Dry Run 1 -Demo of Exercise 1, 2, 3, 4, ShareLatex Lab Instruction (Ex 1, 2, 3, 4) draft#2, ShareLatex Lab Report (Exercise 1, 2, 3, 4) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
9. 12/7/2016: Dry Run 2 - Demo of Exercise 1, 2, 3, 4,ShareLatex Lab Instruction (Ex 1, 2, 3, 4) close to final,ShareLatex Lab Report (Exercise 1, 2, 3, 4) close to final (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
10. 12/14/2016 (1:00 am - 3:00 pm) : Final Demo - (Live or Video/Videos) for scenarios based of the exercises during the finals,ShareLatex Final Lab Instructions,ShareLatex Final Lab Report, Final Double-Sided OnePager (including draft of final demo), Final 5-Slide Presentation (include scenarios of final demo).

8.2 Appendix B - Weekly Status Updates

Status #3 TO Do List - 10/31/2016

(a) **Pre-class - Status of Last Week's Action Items and/or Milestone due this week**

i. TACACS+ Server is successfully set up on Windows 7 vm, done by BOTH.

ii. Demo will involve showing the instructions, some of the report, and the majority of the 1st exercise. This includes the editing of the authentication xml file, showing proof of the service, etc.

(b) **Post-class - Action Items for Next week and/or Milestones due next week**

i. Find a way to allow remote login from another vm.

ii. Think about using GNS3 to emulate a cisco router

iii. Get the lab report up to date with the lab instructions.

iv. (TROY) Finish Exercise 1. Add step (or exercise) for comparison of RADIUS and TACACS+. Integrate wireshark.

v. (ISAAC) Finish Exercise 2. Work on exploiting the vulnerabilities associated with the tacacs+ server.

vi. Begin Exercise 3. This will have all of the extra features that TACACS+ has, such as OTP, and verification/troubleshooting.

vii. Begin Exercise 4. This will have a comparison between running an tacacs+ server on windows and linux.

viii. INSTALL LO INTERFACE ON WINDOWS 7 to be able to capture packets.

Status #4 To DO List - 11/9/2016

(a) **Pre-class - Status of Last Week's Action Items and/or Milestone due this week**

i. Show instructions of the 4th exercise, and add it to template on the lab report.

ii. Still cannot find out how to integrate wireshark to capture tacacs+ packets.

iii. how to emulate cisco router and connect to it

iv. Finished up setting up tacacs on ubuntu. Write this up

v. find out how to work gns3 (Am having a hard time with it)

vi. fix lo interface on windows

(b) **Post-class - Action Items for Next week and/or Milestones due next week**

i. Assess vulnerability. Finish Exercises 1 and 4? (Instructions and Lab report)

ii. make video demo for next status

Status #5 To DO List - 11/9/2016

(a) **Pre-class - Status of Last Week's Action Items and/or Milestone due this week**

i. (Troy) - Show video demo that is put on youtube. Work on screenshots of the exercise shown in the video.
ii. (BOTH) Finalize exercise 1 and 2 (almost done) by adding questions where noted.
iii. (BOTH) Explain the different types of vulnerabilities that we found (MitM w/ arp spoofing DOS overflow)
iv. (Isaac) Learned Scapy to initiate vulnerability
v. (Troy) Learned GNS3 / cisco router configuration

(b) **Post-class - Action Items for Next week and/or Milestones due next week**

i. (BOTH) Work on Lab report exercises. Up until this point, we have been focusing on the instructions.
ii. (BOTH) initiate actual vulnerabilities
iii. (BOTH) Think about order of exercises. Exercise 4 has been defined, but nothing has been written up. (Look at documentation)
iv. (BOTH) Finish Network Diagrams for all exercises
v.