This is a six week project in which you will explore, test, and verify the presence of known vulnerabilities from the bottom to the top of OSI layer [1] in your network. You will be using the ISIS test bed, ASSET, for this project. The network topology is depicted in figure 2.

The project itself is divided into five sections according to the OSI layers (see figure 1) and you will work on one section every week. For each section you will use the pentest procedure discussed in the class and refine your attack trees. In the sixth week you will present the final attack tree that incorporates all the attack trees you have developed to meet a final goal.

Week 1: Physical Network Survey

In the first week of this project you will test the physical security of the network. In addition, you will gather vital information about the hardware, software, procedures, and tools used in the network and used to maintain the testbed that may come in handy in future. Following is an incomplete list of items you must consider when assessing physical security of a network. In addition, you may cover any other relevant items as part of your pentest process. The list and questions are provided as a guide and by no means exhaustive. Your grades, however, will depend on the comprehensiveness of information you gather.

1. Equipment Security:
   - How are the equipments protected?
   - Who has access to what equipment?
   - What is the process of gaining access equipments in the network?
   - What kind of switches are in the network?
   - Can you access the switch’s console port?
   - What is the physical topology of the network?

2. Network Media Security:
   - What type of network media is used?
   - How can the network media be accessed tapped?

3. EMI from Network Media and Equipment
   - What protection measures are taken to avoid EMI?
   - Is there any EMI from the media?
   - Are there any hardware tools to extract data from EMI emitted by the media, switch or any other networking equipment?

At the end of the week you would have gathered all necessary information relevant to assess physical security of the network. Your report will structure this information in a readable form. In addition, you will create an attack tree with all the information you gathered. Then, verify which attacks are viable on the network and refine your attack tree accordingly. The report you turn should include at least the following information:
• Information you gathered on the network infrastructure, processes, etc.
• An attack tree for the network
• Methods taken to verify the attacks in the attack tree
• Pruned/refined attack tree noting which attacks are viable and which ones are not. This attack tree should include a cost metric so that we can find out the most serious threats immediately.

*Note:* Please note that your report should include two attack trees. One prior to verifying attacks and the other (pruned tree) which has only attacks that are viable on the network. Also, note that this section is concerned only about the physical security of the network.

**Week 2 & 3: Data Link Security**

In this two week exercise you will explore and verify vulnerabilities in layer-2 protocols and mechanisms used in ISIS. In particular, you will be dealing with CAM Tables, VLANs (802.1Q), and Spanning Tree Protocol [2, 3]. From previous week's exercise you already know the type of switches in use and the topology. In the first week you will create three attacks trees, one for each protocol or mechanism, and prune them using the knowledge you gained from last week. For example, you may have attacks in your initial attack tree that are specific to certain switches or software versions, which you could eliminate. You should also create a "Plan of Attack" that you would use to verify your semi-pruned attack tree. Your "Plan of Attack" must at least include the following:

• What "off-the-shelf" tools are planning to use or develop and use?
• A detailed procedures to test each protocol or mechanism and what are expecting to observe in each step
• Backup plans if things go wrong. (Things will go wrong, and you are expected to predict what can go wrong and be prepared for that event. To the best you can)

In the second week you will execute your "Plan of Attack" and prune the attack tree further to reflect the results you observe. The following is a preliminary guide-line for the goals to achieve for each attack:

1. **CAM table:** Make your Net 3 behave like HUB’ed network
2. **STP**: Make all the traffic between R1 and R2 go through Node A

3. **VLAN**: Try to send a packet to Net 3 in victim’s network from your network directly (i.e. *without going through the routers*)

You are free to extend the goals of your attacks but your report must include the verification of at least the attacks above. Your report should include the following items:

- An overview of VLANs, CAMs, and STP.
- An attack tree for the each of the above protocol
- Verification (include source code in all cases) of the goals listed above
- Prune the attack tree accordingly and attach the pruned tree
- Please answer the following questions:
  - Are there any well-known vulnerabilities specific to the switches in ISIS? If so, please describe the vulnerabilities in detail (and cite your source).
  - Are there any well-known vulnerabilities in the protocols and mechanisms in general? If so, please describe the vulnerabilities in detail (and cite your source).
  - How are these CAM tables implemented in switches? Are there separate CAM for each port, VLAN, or for group of ports?
  - List tools available to test vulnerabilities at layer-2?

**Week 4: IP Routing Security**

TBA
Week 5: TCP, UDP, HTTP, FTP, DNS, and SQL security

TBA

Week 6: Final Presentation

TBA

References

