M00: Course Overview and Requirements

To-Do Date: Apr 27 at 11:59pm

Course Project Overview

This is a "project-based" course. Working with a team partner and a lab environment, you will build a working IPv4-networked IT infrastructure, consisting of three security zones:

1. "secure" (highest trust—sensitive server assets will be deployed in this zone.)
2. "inside" (ordinary trust—regular user machines would go in this zone.)
3. "dmz" (semi-trusted "demilitarized zone"—assets that must be Internet-accessible will be deployed here.)
4. "outside" (untrusted—alas, the rest of the Internet does not belong to you, so it is not yours to create or control.)

You will configure two firewalls as perimeter devices between your zones:

- A Palo Alto NGFW will serve as the default router to the "outside."
  - In other words, it will be your team's Internet-facing firewall.
- A "VDOM" (virtual domain) on a FortiGate firewall will be the default router for your "secure" zone.
  - In other words, it will be your team's secure-facing firewall.

Your firewalls will enforce network security policies for various virtual machines, which you will also deploy and configure:

- Internet-facing hosts in your "dmz" for web, proxy, load-balancing, and other services.
- Protected "secure" hosts for database, network monitoring, and other services.

By the end of the semester, your lab architecture will enable and satisfy each of the following requirements:

1. Every host in your team's dmz, inside, and secure zones will have a private (RFC 1918) address.
2. Every host in the dmz and inside zones will have access to Internet (outside) resources, using network and port address translation (NAT/PAT) configuration on your Internet-facing firewall.
3. Every host in the secure zone will have access to (outside) web resources through proxy services deployed in your dmz.
4. Internet clients will have limited access to selected services in your dmz, using static NAT configuration on your Internet-facing firewall.

5. You will deploy a three-tier web application. This application will serve web-browser clients from the (outside) Internet, using load-balancing and server middleware in your dmz, and with a database back-end in your secure zone.

6. Your team and another team will be able to access an account on selected hosts in each others' dmz, by way of an IPsec site-to-site VPN.

7. Your team will be able to access your inside zone's hosts from the Internet, by way of a remote access VPN service.

8. A network intrusion detection system (NIDS) will monitor network traffic to and from your dmz hosts, and will produce alerts when it detects traffic that might be hostile.

9. An SNMP-based network traffic monitor will measure bandwidth usage of your Internet-facing firewall's routed interfaces.

10. A security information event manager (SIEM) will manage logs and alerts from selected equipment in your lab infrastructure.

11. At a particular time during the course, your team will deploy a vulnerability scanner and a pentest toolkit in your dmz, and use them to conduct a simple penetration testing ("pentest") exercise.

In addition to the requirements listed above, motivated students will have "above-and-beyond" opportunities to practice additional skills and delve deeper into their learning. Eight such opportunities are presented in the course materials. If you have other creative ideas to go above-and-beyond, you are welcome to welcome to propose and accomplish your own challenges. (Please get approval **by email** from your instructor before pursuing your own "above-and-beyond" projects or tasks.)

NOTE: Just like many real-world projects, these requirements are somewhat vague and incomplete. This is on purpose! It's for your learning and benefit. (It makes teaching this class harder for your instructor, so it certainly isn't for their benefit!) The aim is to let you practice eliciting and clarifying project requirements. Most of the interaction among your classmates will involve conversations and analysis that should help you figure out and better understand what you need to do.

Overall Course Requirements and Grading

1. This course project consists of the 11 milestone tasks listed above, which are further detailed in **M00: Semester Project Tasks and Requirements (https://byui.instructure.com/courses/295222/pages/m00-semester-project-tasks-and-requirements)** .
   - Team milestone deliverables:
     - For the first milestone task, each **individual** will deliver a separate document, to be evaluated and scored by your instructor.
     - For every milestone task thereafter, **your team** will submit one report document (a multiple page illustrated memo, authored jointly) to be evaluated and scored by your instructor.
   - Team milestone requirements, grading, and detailed rubrics:
     - To complete each task, you and your teammate(s) must successfully meet every requirement of that task.

- Meet all requirements, and your team will earn a **"passing"** score for that task (one point).
- Any unmet requirement will result in a **"failure"** score for that task (no points).
- **NOTE**: this means that your instructor will give you **zero points** on any task you haven't passed, even though you will notice partial points awarded in a scoring rubric. In this class, rubrics are used to convey information on how to complete each task satisfactorily, but are not used for grading, since task scoring is **binary** (either pass or fail).
  - If your team doesn't pass the milestone task before its due date, you can take your instructor's feedback, make corrections, and resubmit your report, until you receive **full credit** by meeting all requirements.

2. You will also complete three peer evaluations, in which you will provide a short status report of you and your teammates' working relationship. Please watch the following two videos to get some ideas about the "soft skills" you will evaluate:
   - Human skills, useful skills, real skills … soft skills, by IT marketing executive and author Seth Godin.
     - **"Human skills, useful skills, real skills ... soft skills, by IT marketing executive and author Seth Godin"** ⮑ **(https://vimeo.com/297182889)** (4:02 mins)
   - DevOps Soft Skills, by cybersecurity expert Mayur Rele.
     - **"DevOps Soft Skills, by cybersecurity expert Mayur Rele"** ⮑ **(https://vimeo.com/693019243)** (03:14 mins, **"DevOps Soft Skills, by cybersecurity expert Mayur Rele" Transcript** ⮑ **(http://mayurrele.com/devops-soft-skills/)**)
   - At three separate times during the course, each **individual** student will write a peer evaluation, which your instructor will read and score.
   - In each peer evaluation, you should identify team-building "soft skills" you have learned to recognize and improve.
   - As long as you complete each part of your peer evaluations sincerely and provide supporting evidence, your instructor will award full credit.

3. You are required to complete **all** of the milestone tasks and peer evaluations to pass this class. By doing so, you will earn a *C* for your final grade.

Above and Beyond

4. If you are interested in going above the average, you can complete "Above and Beyond" tasks to earn a *B* or even an *A* for your final grade.
   - Report each above-and-beyond project task with a multiple-page written and illustrated memo, just like the team milestones.
   - Above-and-beyond project tasks can be team or individual efforts. However, jointly-authored reports will **not** be acceptable for above-and-beyond credit. Each individual must submit her or his own original writing to attempt to earn above-and-beyond points.
   - Just like the team milestones, each above-and-beyond project task earns either a "passing" (one point) or "failure" (no points) grade.

- Each passed above-and-beyond task enhances your grade by one +/- mark: pass one to earn a *C+*, two to earn a *B-*, three for a *B*, four for a *B+*, five for an *A-*, or pass six above-and-beyond project tasks to earn an *A* grade for the course. There are eight separate above-and-beyond opportunities in the course, so if you are unable to complete one or two of them, you will still have ample opportunity to earn your *A* grade.
  - Nonetheless, **no amount of above-and-beyond effort will compensate for failing any of the team milestones**—those must all be passed before any credit for above-and-beyond projects will be considered.

Groups

5. You will work together in pairs or trios (groups of two or three students) to complete the semester project.
   - This is to give you experience working with others to complete work, just as you would do in the workplace.

Starting the Course

6. In order to unlock Module 01 and start this class, you will need to read this overview, **M00: Semester Project Tasks and Requirements (https://byui.instructure.com/courses/295222/pages/m00-semester-project-tasks-and-requirements)**, and the **course syllabus (https://byui.instructure.com/courses/295222/assignments/syllabus)**, then complete the Module 00 Quiz: Course Overview with a 100 percent score (unlimited retakes).

7. To begin the class, you will also need to complete **Module 00 Quiz: Group Signup (https://byui.instructure.com/courses/295222/quizzes/4612123)**.

8. Please note that *although you cannot start this class without completing these quizzes*, neither quiz counts towards your final grade.