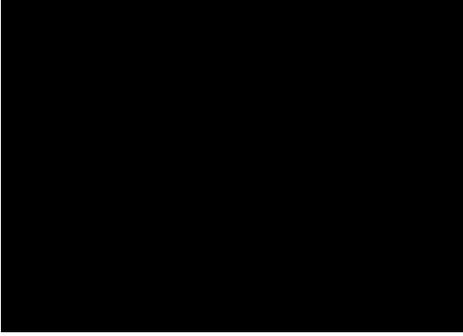


CY3520: Practical Network Operations



Syllabus



Introduction

This course is intended to provide you with an introduction to various aspects of system administration, which will serve as background material for your future war-gaming courses. Much of the war-gaming course involves sys admin tasks: installing operating systems, setting up servers, configuring complex arrangements of software components and locking down and securing machines. In the past, much of the war game has been spent learning these tasks at the expense of more valuable, security-centric activities. Moreover, without having a knowledge of basic system administration, each student rushed to accomplish the one task assigned to him/her without obtaining equivalent knowledge in other fields. As a result this course has been developed. It is hoped that at the conclusion of this course you will have a solid foundation for conducting more involved network and host security tasks.

In support of these objectives, throughout the quarter you will be building, maintaining and securing your own network using virtual machines. Each student will be responsible for putting together their own collection of servers. The majority of server building will take place using Windows Server 2012; however, there will be a small but significant component of the course utilizing Linux. Needless to say this course will not make you an expert but you will walk away with a solid foundation for building a network of computers.

With what you gain here you will have the knowledge you need for continuing to go further in setting up networks of computers and beginning to defend them strategically.

Prerequisites

An introductory networking course is essential. Basic networking concepts will not be explained in depth as it is assumed that you already know them. Also, while not required, it helps to have some experience working from the command line, although this skill can be developed during the quarter. Lastly, a familiarity with basic concepts in computer security is helpful but not required.

Class Schedule

There will be three 50-minute lectures each week along with two lab sessions, one lasting two hours and one lasting 50 minutes.

CY3520 is a very hands-on class with a significant portion focused on our lab assignments. Essentially, class time is intended as the theoretical prep for lab. Lectures will provide the background information necessary for understand the components of the network you build during lab.

Nearly every first lecture of the week, for the first 10-15 minutes of class, there will be a quiz covering the past week's lecture and lab material¹. These quizzes are intended to keep your knowledge current—this is essential as future topics build on previous ones.

Each lab will be accompanied with a write-up². Each write-up will be posted to the Assignment section of Sakai during the first lab session for the week. Lab write-ups will be due before the following week's two-hour lab session, giving you a week to complete each assignment.

Textbook and Resources

No textbook is required for this course. The material covered is too disparate to be covered by one book. However, I will be providing resources throughout the quarter, some of which will be required and some of which

¹The majority of the questions will be based on lecture material, although I reserve the right to ask questions about the lab.

²This is for most part: some labs will just require you to do some work (without any written deliverable), which I will verify from within the virtual lab environment.

are optional. This material will be placed in the Resources section of the course Sakai page in the Lecture Materials folder.

However, what I provide is not exhaustive of the subject matter, so consulting other resources is encouraged. Surprisingly, YouTube is an excellent resource for the topics in this class. In addition, you might also want to check out *Windows Server 2012 Unleashed*. Please do your own Googling and let me know if you find anything worthwhile.

Grading

Your grade breaks down as follows:

- 35% Quiz Average (lowest score will be dropped)
- 45% Labs
- 20% Final Exam

Calendar

Week	Topic
1 July 7	Linux, Routing, Shell Intro
2 July 14	WS2012 Intro and Active Directory Basics
3 July 21	DHCP, DNS, Building a Domain
4 July 28	E-mail via Exchange
5 August 4	Web-server via IIS and dynamic content
6 August 11	Firewall (host-based and for the network)
7 August 18	Proxies, SSL and Logging
8 August 25	Server Hardening via GPOs
9 September 1	Server Hardening via Best Practices
10 September 8	Honeypots, IDSes and Network Monitoring
11 September 15	Final: \approx 50 multiple choice questions on everything above

Some of these topics are subject to change. The above calendar is merely a rough estimate of what we will strive to cover during the quarter. If we get through everything too quickly there are always additional topics to cover. Conversely, if the above schedule is too ambitious, we can adjust accordingly.