IT444
Network Security Administration II

Chris Kelly

cg.kelly2013@gmail.com

Goal of This Course

- The goals of this course are
  - To teach you multiple theories, background, and abstract concepts about network security.
  - To engage in various practical lessons and types of testing around network penetration and other issues.
- The goal of this lecture is to let you know how this course will be conducted

Format of the Course

- This is a **lab** course
  - I will speak briefly at the beginning of each class
  - but much of the class time you will spend working on various kinds of servers in a simulated environment.
- I will be here to help you with any issues that may arise
- **HINT:** When issues do arise, it is to your great benefit to resolve them sooner, rather than later.
- The bulk of the course will consist of your lab reports for a series of projects, working in teams of two

Format of the Course

- On your personal machines you will be running **VMWare**
  - VMWare is virtualization software
  - You will setup and configure various servers using VMWare
- For now, at least, you will be graded *individually*
- Each of you must keep an ongoing record of what you are doing in the form of ***lab reports***

- Lab report format(s) will be specified in a number of ways.
- There may be some variation in format, depending on the assignment in question

Format of the Course

- In addition to the aforementioned, there will also be:
  - **Individual assignments**
  - **Midterm exam**
  - **Final exam**
- The exams' questions will be taken/derived from material covered in…
  - Lectures
  - The course textbooks

What will you learn

- Social engineering attacks
  - Using Kali built-in SET. This is to duplicate sites like gmail, yahoo and lure users in entering ID and password
  - Leveraging existing vulnerabilities in corporate environment to watch and capture password hashes
  - Using Powershell empire to create payload hidden in a file, presentation and send to users
  - Using Kali MSFVenom to encrypt the payload to avoid anti-virus catch

What will you learn cont’d

- Using nmap to collect device information to prepare for potential attacks
- Using CrackmapExec to enumerate all devices (workstations, servers), user names, and the Microsoft corporate domain.
- Using Armitage to attack servers with vulnerabilities discovered by nmap
- Using Metasploit to inject payload to the victim and learn how easy attackers use keyloggers.
- The last excercise is how to built site-to-site VPN to secure data flow between sites to avoid plain text capture.

Projects

- The core of this course is using VMWare to create a virtual server on the machines for testing and analytical purposes
- In the **first** project, you will deal with basic clients and servers -- along with relevant components
- Through subsequent projects, you will deal with more and more features and vulnerabilities, for testing
- You will become more comfortable and familiar with
  - various servers…
  - and their components

Administrator's Log

- One of the most important things you can learn from this course, is the importance of keeping a written record of what you have done
- A system administrator will usually do this in the form of an **administrator's log**
- When you change a machine you administer - or something significant happens on it - you should make a note in your admin log
- Changes to a machine's configuration can cause problems, that may not appear until *months* afterwards

Administrator's Log

- If you forget what you changed and when, you will struggle figuring out what to do next
- This is particularly important when you *solve a problem*
  - *First*, if the problem occurs again, the existence of a previously documented solution will save you the trouble of looking it up again
  - *Second*, the solution could affect other aspects of the system, making a clear record even more important

Lab Reports

- *For IT444*, you must keep various types of records and logs - which will consist of the "daily entry" portions of your lab reports
- Each lab report will be *due* by a particular date and time - to be eligible for credit.
- All students write their own lab reports *separately*, even if teams are later involved...which they may or may not be.
  - Even if work is later shared, all work submitted for a grade is to be unambiguously individual
  - Duplicated text (other than command line output) between students' lab reports will be considered **plagiarism**

Lab Reports

- You should make an entry in the log for *each day* you work on the machine
    - This work will usually be done during class
        - ...but you may sometimes come in outside of regular class meetings or work remotely
        - Regardless, that day's work should get an entry
    - While working, you may choose to keep rough notes
        - ...but those are to help you remember what you did and recall observations. ***The entries in your lab report should be more refined!***
        - You should complete your entries as soon as possible after.
    - Note: There is no need to include class notes in your log, nor should you do so - except as it pertains directly to project work.

Lab Reports

- *In addition to* the daily entries, at the end of each lab report, you will answer a series of ***discussion questions***.
- Read the lab report specifications for further details
- There is a link to the specifications on the class web page, under the ***Course Components*** section

Individual Assignments

- The assignments are not technically "homework", but you may be able to finish some of them at home
- You will find the list of assignments on the course web page
- You will probably work on the first assignment today (or next class period), after I have finished speaking
- The first assignment is to
  - complete the Unix Apply Process for this course
  - set up a special text file for e-mail
  - send me an introductory e-mail
- I can help you with this, as needed

Working on the Command Line and with Configuration Files

- Since most of you have taken IT 244 (or possess some equivalent), you know that the command line is a user-hostile environment
  - On Linux and Unix machines, almost all system administration work is done at the *command line*
  - Almost all configuration information is stored in *text files*
  - Even some Windows work can be CLI-based
- All of the project work you do in this course, therefore, will be done at the command line

Working on the Command Line and with Configuration Files

- You must be very ***careful*** about what you type at the command line
    - If you *mistype or misspell* a single character, your command will not work the way it is supposed to
    - As such, you must be extremely careful when changing these files
    - *A single typo* could cause a service on your machine to fail
- *You should reconsider taking this course if…*
    - You did not do well in prerequisite courses or struggle it
    - You are unable to quickly and easily recall the material learned in that course

Do You Have Enough Time to Do the Work for This Course?

- Many of you work, either part time or full time
  - This cuts down on the time you have for class work
  - ***You should not be taking this course if you do not have enough time to do all the work***
- In this course, you will be configuring virtual servers
  - As previously mentioned, the command line is user-hostile
  - Moreover, configurations and installations will require considerable attention to many <u>*small details*</u>
  - Project completion will require you to <u>*read and follow given directions*</u> closely.

Do You Have Enough Time to Do the Work for This Course?

  - Finally, you need to understand how individual project tasks relate to the *grand scheme* of things
- In addition, doing well in this class will require a higher quality of submitted work.
  - You must both *understand* the material well and *express* yourself well
  - Do you have the time and energy to bring your work to a level sufficient to achieve your desired grade?
- If you sign up for more work than you can achieve in the time you have, you are cheating yourself
  - Many people in this country rush to get a degree, but haven't done enough work to digest the material
  - Those people invariably set themselves up for failure

Other Considerations...

- How well do you handle minute details? Can you keep track of things like:
  - Uppercase versus lowercase
  - When to use single quotes ' ' versus double quotes " "
  - When to use parentheses ( ) versus curly braces { } versus square brackets [ ]
- How good are you at reading directions and following them specifically? Such as...
  - Coding conventions
  - File names and locations
  - Folder names and locations
  - Assignment specifications

Other Considerations...

- For example, if asked to name a file **homework_09.txt** , that means *none* of the following are acceptable:
  - **Homework_09.txt**
  - **homework09.txt**
  - **homework_9.txt**
  - **homework_09.rtf**
  - **Homework 9.doc**
  - ...
- Small details are especially important, considering how computers work.

Attendance

- At each class I'll take attendance
- I do this to:
  - Learn your names
  - Have a record
- Your attendance will not affect your grade *directly*
- However, if you find yourself struggling with the material and have not been coming to class, *I'll be less sympathetic!*

Course Documents

- Everything I create for this class is made available *online*
  - All of it can be accessed from the Class Page: **http://www.cs.umb.edu/~ckelly/teaching/it444**
  - You should *bookmark* this page because the page will function as our syllabus, instead of a paper syllabus
  - It is a lot of material, but you should at least get to know the *layout*
    - That way, you will *know where to look* for information you need
    - This is much *quicker* than sending an e-mail and awaiting my response

Course Documents

- The ***"Course Policies"*** section will give you a good idea of my rules and expectations. That section also contains some supplementary information you should check out.
- The schedule will feature links to class notes, along with reading assignments - including your chapter summaries
- The ***"Projects"*** section will feature descriptions of each project as they come up
- Similarly, links to assignments may be found in the ***"Assignments"*** section

Course Documents

- Many terms we encounter in this class can be found on the *Definitions* page:

http://www.cs.umb.edu/~ckelly/teaching/it341/local_assets/files/common/data/linux/linux_sysadmin_definitions.html

Taking Notes

- Although I make my notes available in PDF form, I want to encourage you to *take* notes in class
  - Studies have shown that students *learn more* when they take notes, even if they never look at their notes again
  - Other studies have shown that the more activities and senses are *engaged* when you learn something, the greater your likelihood of *remembering*
  - Writing notes engages another part of your brain, which increases *recollection*
- All of you should take notes

Taking Notes

- Probably the best practice would be for you to *print* the notes before coming to class.
- That way, you can *write your own* notes in the margins, along with any questions you may have.
- **Note:** Sometimes PDF content may differ from slides as presented in class!

Cheating

- All students are expected to follow the University's Code of Student Conduct
- You will find this at `http://www.umb.edu/life_on_campus/policies/community/code`
- The Computer Science Department has the following policy on cheating
  - You will be given a score of **zero** if you cheat on any assignment, quiz or test
  - If you cheat a second time you will receive an **F** in the course
  - If you cheat a third time you can be **expelled** from the University

Cheating

- I put a great deal of work into my courses, and I ask you to respect that work by not cheating.
- **Important:** *It is the* ***student's*** *responsibility to know what constitutes academic dishonesty - at this university and in this class. Lack of knowledge that something constitutes an academic honesty violation* ***will not*** *be accepted as a valid excuse.*

Grading Policy

- All homework and exams are subject to the honor code
- Plagiarism is not allowed in any form
- Grades will be computed as follows (or close to this, which is *not yet finalized*):
  - **Lab Reports:** 50%
  - **4 Assignments:** 15%
  - **Chapter Summaries:** 10%
  - **Midterm Exam:** 10%
  - **Final Exam:** 15%

Grading Policy

- Final *number* grades will be translated to *letter* grades as follows:

A	*93.3* and above
A-	*90* to *93.2*
B+	*86.7* to *89.9*
B	*83.3* to *86.6*
B-	*80* to *83.3*
C+	*76.7* to *79.9*
C	*73.3* to *76.6*
C-	*70* to *73.3*
D+	*66.7* to *69.9*
D	*63.3* to *66.6*
D-	*60* to *63.3*
F	Below *60*

Accommodations for Disabilities

- The school is legally obligated to try to accommodate students with disabilities
- If you have a disability you can get help from Ross Center for Disability Services
  - **Location:** Upper Level of the Campus Center, Room 211
  - **Phone:** 617-287-7430
  - **Web Site:** https://www.umb.edu/academics/vpass/disability/
- After you have discussed the matter with them, see me
- They will usually draft a letter explaining any accommodations you should receive.

Accommodations for Disabilities

- You should get this letter to me ASAP!
- If you require extra time for an exam, then it is your responsibility to arrange for this at least a week in advance!
- Also, you may wish to check out the page containing my own notes:

http://www.cs.umb.edu/~ckelly/teaching/common/data/disability.html

Communications

- All communication outside of class will be conducted through ***email***
- For regular contact, we will use your `@umb.edu` email.
    - Even if you e-mail me from another account, I will still e-mail you via UMB
    - The *first* assignment will include setting up email
    - I will use that account when sending you a personal email concerning the class or any class-wide announcements outside of class.
    - If I have sent you an email about something concerning the class, I'll assume that you have been given adequate notice

Communications

- If you have a question, email me at `cg.kelly2013@gmail.com`
- Please be sure to:
  1. Use a descriptive, meaningful subject line
  2. Begin the subject with `IT444:`
- Failing to include #2 is effectively the same as not having sent the e-mail at all!
- Don't hesitate to contact me if you are stuck and/or need help with something.
- Others might be having the same issue!

Office Hours

- My office is **M-3-0201.32** (***CURRENTLY REMOTE***)
- My official office hours will be posted on the course web page
- You do not have to make a special appointment to see me during office hours - just drop in!
- If you need my help and cannot make it to office hours, contact me and we'll work something out