Advanced Offensive and Defensive Strategies

Syllabus (*Tentative and subject to change)

Administrative Information:

Instructor: Gordon Long
Email: glong8@masonlive.gmu.edu
Office Hours: By appointment

Course Description:

This course aims to teach students attack methodology from recon, to initial access, basic malware development and attacker tradecraft. It will also cover defensive strategies which can be employed to slow down or stop attackers, and potentially strike back. It will cover tradecraft employed by both red and blue teams. It will cover the legal aspects of the best ways to set up deceptive defense technologies, and what defenders are - and are not - allowed to do to intruders in their network.

Required Skills/Hardware

Decent scripting knowledge very helpful - C++, C#, python, bash, maybe powershell
CODING: this course will prove difficult for those with no experience in programming. It is strongly suggested that students familiarize themselves with at least python and C++ before taking this course. The instructor will attempt to help students in this regard, but students will have to work hard to familiarize themselves with coding if they have no prior experience.

Hardware: will likely need a machine with at least 50GB of free space on it, 16GB RAM is preferred. Likely will use around 3 VMs in this course: Kali, Ubuntu, and Windows 10.

Students should have a working understanding of TCP/IP and its underlying protocols, including routing and other basic networking knowledge (DNS, ICMP, HTTP/HTTPS, etc) as well as Windows and Linux command line knowledge

Tools used during this course (this may change)*

1. Nmap

2. Visual Studio
3. Metasploit
4. Various open source projects

5. VMware or some other virtualization software

Textbooks:

Offensive Countermeasures, The Art of Active Defense by John Strand 2nd Edition
Note: I have several of these book copies available

Technology:

As this will be taught online, please be respectful of your peers and your instructor and do not engage in activities that are unrelated to class. Such disruptions show a lack of professionalism and may affect your participation grade.

Grading:

Grading Breakdown:
25% HW
10% Attendance/Participation
30% Midterm
35% Final Project

Letter Grades:

A	92 - 100
A-	90 - 91
B+	87 - 89
B	83 - 86
B-	80 - 82
C	70 - 79
F	0 - 69

Assignments

Assignments will be given throughout the course. They are due on the date presented on the syllabus/assigned on blackboard. Each assignment will be relevant to the current topics. Upon receipt of all of the assignments, they may/may not be covered in class. It is imperative that students turn assignments in on time.

Midterm

The midterm will be an individual coding project focused on attacker methodology/windows development. There will be a subsequent report on how defenders could recognize and defend against the code being used. More explanation will follow in class. This code will be expected to be published to GitHub, which we will also go over. Students will be expected to present their tools in class. A soft copy of the PowerPoint file must be submitted prior to the presentation.

Final

The final will also be an individual coding project, focused on building a defensive countermeasures tool. Students will need to have their project approved beforehand, and will be assigned a project if they cannot come up with any ideas. These projects will also be expected to go on GitHub, and students will present on the tools they have built during the final week of class. A soft copy of the PowerPoint file must be submitted prior to the presentation.

Participation and Attendance

Students are expected to participate during class, ask questions, and contribute to discussions. Students are also expected to be present in class, unless for extraordinary circumstances in which the instructor will be notified beforehand. If students miss class without notifying the Instructor, they must consult with the Instructor to explain the reason behind this absence, or risk being penalized.

Communications

Communications on issues relating to the individual student should be conducted using email if possible.

Week	Date (Estimated)	Topic	Homework (More detail on blackboard)
1	1/18	Introduction to Course/Syllabus + Setup (VM's, textbooks, etc)	None

2	1/25	Legal Cases, explain the world of Cyber Deception from legal standpoint	Find an interesting Legal case involving Active Cyber Defense and write a summary of what it is/what happened, make sure Visual Studio is installed. Due 2/1
3	2/1	Scripting Basics, cmdline, Visual Studio debugger review, Annoyance tools	HW: Create basic reverse shell and compile in VS as a video, upload to blackboard Due 2/8
4	2/8	Initial Recon explanation from attacker perspective, passive and active recon explanations	HW: Create a Word macro which fetches the current working directory, and then echoes out the term “You should not have clicked this macro!!!” Due 2/25
5	2/15	Sysmon + Windows Event Logs, setup, delve into specific honeypot tools	Activity: Perform some rule writing for logging tools, start honeypot tools and check how certain attacks look in event/tool logs Due 2/22

6	2/22	Low level user recon as attacker inside network, your steps, commands you can run, objectives domain recon, persistence, etc	HW: Write a guide of helpful recon commands for low level user on both Linux and Windows systems, 1 page each. Due 2/29
7	2/29	More honeypot tools and fake account setup to catch attackers, discuss theory of separate honeypots or production honeypots.	Midterm Assigned. Due 3/21
8	3/7	SPRING BREAK, NO CLASS	Work on midterm
9	3/14	C2 Frameworks	Work on midterm.

10	3/21	Midterm due. Midterm presentations. 10 minutes cap. If time, either c2 or web depending on week 9.	TBD as well as Make sure GitHub repository is set up, submit idea for final. Due 4/4
11	3/28	Process Hacker, Api Monitor, building your own EDR	HW possibly on using EDR to detect malicious API call for chose NtFunction

12	4/4	Kerberoasting, Whitelist evasion, theDonut, other advanced attacker techniques (syscalls). Discuss final.	Analyze given binary to discover malicious behavior, such as strange API calls. Due 4/11
13	4/11	Wireless Countermeasures + Attribution Tools/Techniques (aka Watermarking documents digitially, etc). OR Web Exploitation/Privilege Escalation from attacker perspective, detection discuss depending on methods. DVWA setup	Work on Final.
14	4/18	More attack back tools for defenders.	Work on Final.
15	4/25	GitHub final project presentations.	None