DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Syllabus

Administrative Information

Instructor:	**Tahir Khan**
Email:	mailto: tkhan9@gmu.edu / subj: DFOR767-PTF
Office hours:	By appointment
Classes:	Tuesday, 16:30 - 19:10

Course Description

CFRS 767-001 - Penetration testing forensics (3:3:0)
Prerequisites: CFRS 780 (Forensic Artifact Extraction) and CFRS 660/CFRS 661; working knowledge of computer operating systems (e.g. CS 471 or equivalent), networking or permission from instructor. This course will cover the full life cycle of penetration testing ranging from passive and active reconnaissance, vulnerability assessment, exploitation via various methods, post-exploitation and pivoting, reporting writing and post incident forensics.

Required Skills and Hardware/Software

Students **must** have a **working understanding** of the following items:

- TCP/IP and its underlying protocols including
  - Routing and other basic networking knowledge (DNS, ICMP, etc)
- HTTP Protocol including methods, status codes and parameters
- Various encoding formats used in a web environment
- Windows / Linux command line knowledge
- Scripting (Bash, **python 3*** or powershell) ** You will need to program
- A Mac/PC that can run VMWare (v11+) **AND** VirtualBox (6+) with **6GB** minimum

DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Tools used during the course

- Nmap
- Hydra
- Sqlmap
- Metasploit*
- Nikto
- Burpsuite*
- Commix
- Kali Linux*
- Amass

Please have these installed and working before the first class.

Textbooks

N/A

Topics

- Ethics / Scoping
- Passive / Active reconnaissance
- Mobile app reconnaissance
- Vulnerability assessment
- Exploitation
- Brute forcing
- Header modification
- Parameter tampering
- Command execution/injection
- File inclusion / Web shells
- SQL Injection
- Cross site scripting (XSS)
- Credential Gathering
- Privilege escalation
- Pivoting
- Broken authentication
- Report writing
- Post incident log review

This syllabus is subject to changes and revisions throughout the course.

DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Technology

Because this is a computer classroom, we will frequently be using the internet as a means to enhance our discussions. We will also be using the computers for our in-class lab assignments. Please be respectful of your peers and your instructor and do not engage in activities that are unrelated to the class. Such disruptions show a lack of professionalism and may affect your participation grade.

Goal

The goal of this course is to teach students the basics of penetration testing and post incident forensics. Students will learn a variety of methods to test the security and protection mechanisms of systems as well as how to bypass them. By learning how to “attack” a system, students will learn to identify the various artifacts that are left behind after a real world “attack”.

External Resources

Please set up an amazon aws account. This process is easy and will allow us to run several tools in a cloud based environment. Please sign up for https://aws.amazon.com/education/awseducate/apply/

Please download and try out various vulnerable machines located on http://www.vulnhub.com. These machines will give you valuable experience and can be used to practice for the midterm.

This syllabus is subject to changes and revisions throughout the course.

DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Grading

Weights		Letter Grades	
(50%)	Assignments	A	92-100
(25%)	Midterm & Report	A-	90-91
(25%)	Final & Report	B	83-86
		B-	80-82
		C	70-79
		F	0-69

Assignments

Assignments and quizzes will be given throughout the course. They are due on the date presented on the syllabus. Each assignment will be relevant to the current topics. Upon receipt of all the assignments, they will be covered in class. It is imperative that students turn assignments on time as they are covered in class on the day they are due. Assignments may consist of a virtual machine with a vulnerability.

Midterm Test

A midterm test will be an assigned virtual machine that the student will have to compromise. Exploitation of the system will rely on knowledge gained from the first seven weeks of class. Students are advised to use alternate resources to practice before the take home exam. See www.vulnhub.com for practice VMs.

Final Test

The final project will consist of two virtual machines running unknown operating systems and unknown services. Students must successfully bypass security mechanisms of the virtual machines and exploit the systems utilizing the techniques and skills learned throughout the semester. Additionally, the students must create a video detailing the approach and findings as well as a presentation of the post incident forensic artifacts left behind on the virtual machines issued. The presentation should be in PowerPoint format and must be professional. See the final attachment for further details.

This syllabus is subject to changes and revisions throughout the course.

DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Participation

Throughout the semester there will be hands on exercises and labs to demonstrate the various tools and techniques covered in class. Students are expected to participate in the exercises. In-class assignments are a factor in the overall grade.

Presentation of Final (If time allows)

Each student must present their group presentation. Students are expected to know the material they are presenting and to expect a question and answer session. A soft copy of the presentation (.pdf) file must be submitted prior to the presentation.

This syllabus is subject to changes and revisions throughout the course.

DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Schedule

			Read up on HTTP, IP and network protocols http://net.tutsplus.com/tutorials/tools-and-tips/http-the-protocol-every-web-developer-must-know-part-1/ http://www.tutorialspoint.com/http/ http://www.tutorialspoint.com/http/http_messages.htm http://www.tutorialspoint.com/http/http_methods.htm http://www.tutorialspoint.com/http/http_header_fields.htm http://www.tutorialspoint.com/http/http_status_codes.htm http://www.tutorialspoint.com/http/http_message_examples.htm	
Week 1	Aug 23	Introduction and overview of penetration testing. Scoping / Ethics / Basics Basic Skills needed for class	Please have installed for next week: Kali Linux	Assignment 1 issued
Week 2	Aug 30	Passive reconnaissance – Lecture will cover ways to obtain data on targets utilizing passive techniques.	Install Kali Linux and Burpsuite Pro Install and configure BWAPP	
Week 3	Sept 6	Active reconnaissance – Lecture will cover active scanning to gain information about targets utilizing open source tools.	Download and install --> Tenable for Education	**Assignment 1 due @ 16:20** Assignment 2 issued
Week 4	Sept 13	Vulnerability assessment – Students will use open source / free tools to assess the weaknesses and vulnerabilities of systems. Exploitation – Students will use open source tools to perform brute force attacks on username		

This syllabus is subject to changes and revisions throughout the course.

		/ passwords. An intro to Metasploit will also be done.		
Week 5	Sept 20	SQL Injection - Students will learn what SQL Injection is, how to potentially identify it, and how to use it to exploit a system.	https://www.owasp.org/index.php/SQL_Injection http://resources.infosecinstitute.com/sql-injection-http-headers/	**Assignment 2 due @ 16:20** Assignment 3 issued
Week 6	Sept 27	SQL Injection - Part II students will learn advanced SQL injection techniques, and how they can bypass WAF's and other security mechanisms in place to prevent SQL injection.	https://www.owasp.org/index.php/Command_Injection	
Week 7	Oct 4	SQL Review	http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion http://securityxploded.com/remote-file-inclusion.php	
Week 9	Oct 18	Command Injection - Students will learn what command injection is and how to determine if a system is vulnerable. Students will take knowledge from previous classes to learn where command injection is possible, and how to automate the scanning process.		**Assignment 3 due @ 16:20** Assignment 4 issued Group Project Issued
Week 10	Oct 25	Midterm Take Home	https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/ http://www.offensive-security.com/metasploit-unleashed/Pivoting http://www.offensive-security.com/metasploit-unleashed/Persistent_Backdoors	Midterm Issued
Week 11	Nov 1	Maintaining persistence - Students will learn how to maintain persistence within a network after successful exploitation. Students will learn various techniques that	https://hashcat.net/hashcat/ http://www.openwall.com/john/	Assignment 5 issued Assignment 6 issued

		will allow them to add users, create backdoors, etc. Optional: File Inclusion - Students will learn the different types of file inclusion vulnerabilities (Local and Remote) and how to perform advanced attacks utilizing file inclusion, including uploading web shells, backdoors, etc.		**Assignment 4 due @ 16:20**
Week 11	Nov 8	Pivoting and lateral movement - Students will learn how to pivot from one system to the next and move laterally across a network to further the penetration test.	https://phoenixts.com/blog/types-of-wireless-network-attacks/ https://resources.infosecinstitute.com/wireless-attacks-unleashed/	Final Issued **Midterm Due**
Week 12	Nov 15	Passwords - Various methods for cracking passwords will be demonstrated. Including john the ripper, hashcat and using the cloud. Privilege Escalation - Various methods used to escalate privileges will be covered. Cross site scripting - Students will learn what cross site scripting is, and how XSS can be used to further the attack process.	https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)	**Assignment 5 due @ 16:20** **Assignment 6 due @ 16:20**
Week 13	Nov 29	Final Review - Techniques, and other questions can be asked. Homework 5 & 6 review		
		~~Final Presentations - Students will present their reports. Additional review/questions.~~		**Final due @16:20**

This syllabus is subject to changes and revisions throughout the course.

		~~Final Presentations – Students will present their reports. Additional review/questions.~~		

DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Important Dates

Please visithttp://registrar.gmu.edu/calendars/ and view important dates for the current semester.

Call 703-993-1000 for recorded information on campus closings (e.g. due to weather).

Attendance Policy

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account. Lecture slides are complements to the lecture process, not substitutes for it – access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

DFOR 767 – 001 - Fall, 2022
Penetration Testing Forensics / George Mason University

Academic Integrity

GMU is an Honor Code university; please see the Office for Academic Integrity for a full description of the code and the honor committee process. The principle of academic integrity is taken very seriously and violations are treated gravely. What does academic integrity mean in this course? Essentially this: when you are responsible for a task, you will perform that task. When you rely on someone else's work in an aspect of the performance of that task, you will give full credit in the proper, accepted form. Another aspect of academic integrity is the free play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. When in doubt (of any kind) please ask for guidance and clarification. Students are required to be familiar and comply with the requirements of the GMU Honor Code @ http://oai.gmu.edu/the-mason-honor-code-2/. All assessable work is to be completed by the individual student. Students must **NOT** collaborate on the project reports or presentation without explicit prior permission from the Instructor.

Disability Accommodations

If you have a learning or physical difference that may affect your academic work, you will need to furnish appropriate documentation to the Office of Disability Services. If you qualify for accommodation, the ODS staff will give you a form detailing appropriate accommodations for your instructor. In addition to providing your professors with the appropriate form, please take the initiative to discuss accommodation with them at the beginning of the semester and as needed during the term. Because of the range of learning differences, faculty members need to learn from you the most effective ways to assist you. If you have contacted the Office of Disability Services and are waiting to hear from a counselor, please tell me.

Diversity

George Mason University promotes a living and learning environment for outstanding growth and productivity among its students, faculty and staff. Through its curriculum, programs, policies, procedures, services and resources, Mason strives to maintain a quality environment for work, study and personal growth.

This syllabus is subject to changes and revisions throughout the course.

An emphasis upon diversity and inclusion throughout the campus community is essential to achieve these goals. Diversity is broadly defined to include such characteristics as, but not limited to, race, ethnicity, gender, religion, age, disability, and sexual orientation. Diversity also entails different viewpoints, philosophies, and perspectives. Attention to these aspects of diversity will help promote a culture of inclusion and belonging, and an environment where diverse opinions, backgrounds and practices have the opportunity to be voiced, heard and respected.

The reflection of Mason's commitment to diversity and inclusion goes beyond policies and procedures to focus on behavior at the individual, group and organizational level. The implementation of this commitment to diversity and inclusion is found in all settings, including individual work units and groups, student organizations and groups, and classroom settings; it is also found with the delivery of services and activities, including, but not limited to, curriculum, teaching, events, advising, research, service, and community outreach.

Acknowledging that the attainment of diversity and inclusion are dynamic and continuous processes, and that the larger societal setting has an evolving socio-cultural understanding of diversity and inclusion, Mason seeks to continuously improve its environment. To this end, the University promotes continuous monitoring and self-assessment regarding diversity. The aim is to incorporate diversity and inclusion within the philosophies and actions of the individual, group and organization, and to make improvements as needed.

Privacy

Students must use their MasonLive email account to receive important University information, including messages related to this class. See http://masonlive.gmu.edu for more information.