CFRS 769 - SEC 001 - Fall 2015
Advanced Topics in Computer Forensics – Anti Forensics
George Mason University

Syllabus

Administrative Information

Instructor: **Tahir Khan**
Email: tkhan9@gmu.edu subject=CFRS 780-AntiForensics-Your name

Office hours: By appointment
Classes: Thursday, 19:20 – 22:00 – Nguyen Engineering Building 4457

Course Description

CFRS 780 - Advanced Topics in Computer Forensics – Anti Forensics (3:3:0)
Prerequisites: TCOM 548 and TCOM 556 or TCOM 562; a working knowledge of computer operating systems (e.g. CS 471 or equivalent) or permission from instructor. Teaches students how to identify anti-forensic techniques through research and hands-on implementation. Students will explore the various methods that can be used to thwart the forensic process, and how to identify what techniques were applied.

Prerequisites

- Working knowledge of TCP/IP and basic networking protocols
- Working knowledge of Linux/Windows
- Familiarity with various software tools such as:
  - Wireshark/Tshark
  - Hex Editors
  - VMWare Workstation / VirtualBox
- Familiarity with various programming concepts such as:
  - Logical operations
  - Program flow
  - Understanding high level view of code
- Familiarity with scripting
  - Bash / Python
  - Windows shell scripting
- Familiarity with file headers / magic numbers/ file signatures

Required items

- Access to a computer with *at least* 6GB RAM
- Two gmail accounts (Please create two test accounts)
- Installed copy of VMWare workstation and VirtualBox
- Installed Android SDK and Genymotion Emulator
- Installed copy of Burpsuite (Free Edition)
- Installed copy of Volatility
- Installed copy of Metasploit
- Installed and configured Windows XP and Windows 7 virtual machines

Textbook

Available Online @ http://library.gmu.edu/ (Search for book title) (Optional)

Title:	File System Forensic Analysis
Author:	Brian Carrier
Publisher:	AddisonWesley
Pub. Date:	March 27, 2005
ISBN-13:	978-0321268174

Topics

- Digital Media wiping
- Steganography
- Rootkits
- Encryption
- Metadata manipulation
- S.M.A.R.T.
- Audit / Log / Network manipulation
- Timestomping
- Slack space manipulation
- Memory manipulation
- Misleading evidence
- Forensic tool vulnerabilities
- Obfuscation / Polymorphism
- Anonymizing

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.

Goals

- To recognize the anti-forensic processes that can be used to thwart the forensic process
- To determine what anti-forensic actions were performed

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 exercises are a factor in the overall grade.

Grading

Weights
(30%) Assignments/Quizzes
(20%) Midterm
(20%) Final Project
(30%) Final

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

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

Assignments/Quizzes

Assignments will be given throughout the class. The material covered will be first discussed in class, and then applied in the homework. Homework may have advanced topics not fully covered in class, but will be discussed in a future class. The homework will be graded on the gradable portions. The advanced problems are for students to go above and beyond. All assignments are due when specified and late submissions will not be accepted.

Midterm

The midterm will consist of using an assigned VM and performing normal usage activities. The deliverable will consist of report that fully documents the steps of every action taken on the VM, and finally, every anti-forensic step taken on the VM. This project will be then passed on to another student in the class as part of the final. You must perform anti-forensic actions on the VM as well as exfiltrate one of the files marked for exfiltration. Please refer to the final project handout for more information.

Final Project

The final project will consist of a forensic report on an assigned virtual machine. The report must detail actions performed on the VM, please be aware the image/disk may not contain any obvious artifacts and try and focus on the anti-forensic techniques used. The package will contain a memory snapshot, multiple pcap files and a disk image. The final report/paper must be done in a professional manner. Utilizing the skills and knowledge you have gained throughout the program create a forensic report detailing all steps taken and the findings. Please refer to the final project handout for more information.

Final Presentation

The final presentation will be an in-class presentation of findings obtained from the forensic analysis of the virtual machine. Please present the findings in a professional manner and expect questions. A soft copy of the PowerPoint (.ppt) file must be submitted prior to the presentation.

Resources

Report templates:

http://www.sans.org/reading_room/whitepapers/forensics/forensic-investigator_1453
http://my.safaribooksonline.com/book/networking/forensic-analysis/9780072226966/writing-computer-forensic-reports/ch17lev1sec3

Software:

http://www.genymotion.com/
http://developer.android.com/sdk/index.html
http://portswigger.net/burp/
https://www.virtualbox.org/
https://github.com/volatilityfoundation/volatility
https://github.com/rapid7/metasploit-framework
http://www.kali.org/downloads/

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

Schedule

Lecture	Date	Topic	Reading Assignments	Assignments Info
			Read up on IP and network protocols http://www.wireshark.org/docs/man-pages/tshark.html http://www.tcpipguide.com/free/t_DNSBasicNameResolutionTechniquesIterativeandRecurs.htm http://technet.microsoft.com/en-us/library/cc957843.aspx Read up on python and basic shell scripting as well as tshark commands.	
Week 1	Sept 3	Introduction and overview of anti-forensics, course overview.	Please read the basics on Bash/CMD/PowerShell scripting @ http://ss64.com/	
Week 2	Sept 10	-Scripting forensic tasks for analysis Students will learn the basics of scripting in windows/linux as well as for-loops, nested commands with forensic tools such as tshark, hexreader.	Read up on basic networking, including ICMP, DNS, routing. 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.defcon.org/images/defcon-16/dc16-presentations/defcon-16-ricks.pdf http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DNS_Exfiltration_2011-01-01_v1.1.pdf Please read Chapter 9 in "Data Hiding"	
Week 3	Sept 17	Lecture will cover a review of network forensics and topics such as Packet manipulation/ICMP & DNS Tunneling/ Protocol misuse/Protocol manipulation	Please read and understand the basics of how to use Volatility: https://code.google.com/p/volatility/wiki/Release23	**Assignment 1 issued**
Week 4	Sept 24	Lecture will cover Encryption (SSL), attacking of the tools/processes used in network forensics. The disadvantages of open wireless networks and the basics of network based logs.	Please read and understand the basics of TrueCrypt: http://www.truecrypt.org/faq Please read the following: http://www.techrepublic.com/blog/data-center/10-commands-you-should-master-when-working-with-the-cisco-ios-104071/#.	**Assignment 2 issued**
Week 5	Oct 1	One student will present assignment 1 Lecture will cover a review of memory forensics, and will go into topics in router forensics and anti memory dumping.	http://support.microsoft.com/kb/314834	
Week 6	Oct 8	Lecture will continue memory dumping anti-forensics and SQL Server Anti-Forensics and disk avoidance.	Please and understand the basics of S.M.A.R.T.: http://en.wikipedia.org/wiki/S.M.A.R.T. Read Chapters 8,9,10 in Brian Carriers book 'File System Forensic Analysis'. See optional textbook in syllabus.	**Assignment 1 due (Before Class)**

Week 7	Oct 15	One student will present assignment 2 Lecture will cover disk anti-forensics, bad block manipulation, S.M.A.R.T., and FAT32 file system manipulation.		
Week 8	Oct 22	Lecture will cover file extension manipulation, alternate data streams, and prefetch manipulation and file system tunneling.	Please read readmes on SETMace, Timestomp.	**Assignment 2 due (Before Class)**
Week 9	Oct 29	Lecture will cover time-stomping, registry time modification, steganography and file stuffing.	Please read and understand obfuscation techniques: http://blog.malwarebytes.org/intelligence/2013/03/obfuscation-malwares-best-friend/ http://blog.malwarebytes.org/intelligence/2013/05/nowhere-to-hide-three-methods-of-xor-obfuscation/	
Week 10	Nov 5	Lecture will cover obfuscation, polymorphism, malware techniques and DNS poisoning.	Read and understand how TOR works: https://www.torproject.org/about/overview.html.en	**Midterm Report due (Before Class)**
Week 11	Nov 12	Lecture will cover application forensics, third party system cleaning tools, crash reports, incognito browsing, proxy servers, live-CDs and TOR	Please have Metasploit configured and installed for next week's lecture. Additionally, please read up on the Event Log schema: http://msdn.microsoft.com/en-us/library/windows/desktop/aa384367(v=vs.85).aspx	**Assignment 3 issued**
Week 12	Nov 19	Lecture will cover, post incident log file review, trail obfuscation, log manipulation, and how to identify through forensic methods what anti-forensic techniques were applied during an incident.	Please view the following videos: http://portswigger.net/burp/tutorials/ Please read the following to learn how to intercept responses: http://portswigger.net/burp/help/proxy_intercept.html	
Week 13	Dec 3	One student will present assignment 3 Lecture will cover anti-forensics in a mobile environment, including in-transit manipulation of data.		
Week 14	Dec 10	Final Presentations: Students will present their reports. Additional review/questions		**Assignment 3 due (Before Class)**
Week 15	Dec 18	Final Presentations: Students will present their reports. Additional review/questions		**Final Project due (Before Class)**

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

Important Dates

Please visit http://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.

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://honorcode.gmu.edu/. 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.

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

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.

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.