Computer System Security Analysis and Investigation Techniques**– ITEC 465**

**Credits: 3**

Radford University – Spring 2024

**Instructor:** Rick Joyce

**Phone:** 540 831 5306

**Email:** [rjoyce9@radford.edu](mailto:rjoyce9@radford.edu)

**Website: https://www.radford.edu/rjoyce9/classes/itec465**

**Office Hours:** Davis 218, T/TH 12:30-13:45, W 13:00-15:00, and scheduled

**Course Time & Place:** T/TH 11:00 – 12:15, 142 Reed-Curie Hall

Syllabus Contents

[About This Class 2](#_Toc523124470)

[Course Requirements 2](#_Toc523124471)

[Course Objectives/Learning Outcomes 2](#_Toc523124472)

[Optional Text(s) and Course Materials 2](#_Toc523124473)

[Course Topics 3](#_Toc523124474)

[Tentative Schedule 3](#_Toc523124475)

[Computer Resource Acceptable Use Policy 4](#_Toc523124476)

[Grade Calculation 4](#_Toc523124477)

[Letter Grades 4](#_Toc523124478)

[Attendance Policy 4](#_Toc523124479)

[Classroom Behavior Expectations 5](#_Toc523124480)

[Netiquette Policy 5](#_Toc523124481)

[Communication 5](#_Toc523124482)

[Response Time 6](#_Toc523124483)

[Homework/Project Policy 6](#_Toc523124484)

[Office Hours 6](#_Toc523124485)

[Classroom Recording Policy 7](#_Toc523124486)

[Academic Honesty and Plagiarism Policy 7](#_Toc523124487)

[Accommodations Policy 7](#_Toc523124488)

[Final Exam 8](#_Toc523124489)

[Appeal of Grades 8](#_Toc523124490)

[Exceptions to Policies 8](#_Toc523124491)

## About This Class

Students will learn ethical hacking, conduct formal security analysis of computing infrastructure; apply investigation techniques to detect vulnerabilities and threats in software and hardware including reverse engineering program binaries for malware analysis, memory and disk analysis; systems analysis of embedded devices.

## Course Requirements

Prerequisites: ITEC 352, ITEC 371, and ITEC 445 with a grade of “C” or better

## Course Objectives/Learning Outcomes

|  |
| --- |
| Students who complete this course will be able to: |
|  |
|  |
|  |
|  |
| Explain the wide array of offensive techniques used to attack a computing infrastructure |
| Explain the underlying kernel data structures of at least one standard operating system such as: Windows or Linux |
| Demonstrate an ability to analyze the current state of a kernel through memory and file dumps on at least one standard operating system such as Windows or Linux. |
| Demonstrate an ability to reverse engineer compiler generated code using tools such as disassemblers, de-compilers, and debuggers. |
| Explain obfuscation techniques used by malicious software to confuse tools and analysis. |
| Develop networked applications using secure coding techniques. |

Additionally, more fine grained skills acquired will include:

* Recognize commonly used binary file formats
* Use a debugger to attach to, monitor, and control program execution
* Disassemble code segments using the linear sweep and recursive descent disassembly algorithms
* Construct basic blocks and calling graphs
* Identify conditional execution constructs, loops, switch statements, and commonly used function calling conventions in disassembled files
* Perform data flow analysis
* Safely execute malware samples in a sandboxed environment
* understand and manipulate symbol tables
* Recognize and exploit/overcome commonly used anti-disassembly techniques, anti-debugging techniques, anti-virtual machine techniques, buffer overflow vulnerabilities, commonly used encoding algorithms, commonly used obfuscation techniques, packing methods, and malware mechanisms

## Optional Text(s) and Course Materials

1. SLEIGH, Ghidra's processor specification language

*Available online at: https://github.com/NationalSecurityAgency/ghidra/blob/master/GhidraDocs/languages/html/sleigh.html*

2. [Eagle] The IDA Pro Book, 2nd Edition: The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle, No Starch Press , ISBN-13: 978-1593272890

ISBN-10: 1593272898

*Available in e-book format through the McConnell library at:*

[*https://radforduniversity.on.worldcat.org/atoztitles/ebooks?searchType=matchAll&btitle=The+IDA+Pro+Book*](https://radforduniversity.on.worldcat.org/atoztitles/ebooks?searchType=matchAll&btitle=The+IDA+Pro+Book)

3. [Lions] Lions' Commentary on Unix 6th Edition, with source code by John Lions, Peer-to-Peer Communications, ISBN-10: 1573980137, ISBN-13: 978-1573980135

*This will be available as a reference text, checked out using the algorithm we will discuss in class*

## Course Topics

Many topics from computer architecture, organization, language translation, and other central CS topics come to bear during process of reverse engineering and so will be covered to the degree necessary as a precursor. The full set of topics include:

The computer + HID’s, a byte-level view

The shell, libc, the kernel

Common base data types, byte, char, short, int, float, double, boolean and implementation: signed magnitude, 1’s and 2’s compliment, IEE754 fps

The address space, C vs OO vs assembly

Church-Turing, models of computation

Gate-level model of the computer

Pipelining principals and the memory hierarchy

Building an executable

The compilation process

Chomsky hierarchy, lexical, syntactical, semantic analysis

Macro preprocessor, asm, relocatable object, linker, loader, static/dynamic libs

Common relocatable object and executable file formats

Binary patching

Debugger, truss/strace, other common libraries

Instruction set architectures

Assembly crash course

8052, X86, ARM

General introduction to software reverse engineering

static analysis, dynamic analysis, symbolic execution approaches, and limitations

## Course Topics, con’t

Disassembly principals and techniques

linear sweep, recursive descent

Recognizing high-level constructs (if-then-else, loops, switch)

source code to assembly and back

Function recognition, calling conventions

Control flow and data flow analysis

Malware

Classification

Network Signatures

Automatic classification based on dynamic analysis

Covert Launching

Analyzing Malicious Windows Programs

Packers and Unpacking

Obfuscation and anti-signature techniques

Challenges of disassembly techniques

Anti-Disassembly, debugging, VM techniques

Memory Forensics

Reverse engineering of network protocols

The rise of lightweight, embedded web servers and cross channel scripting (XCS)

Legal and Ethical issues of Reverse Engineering

Tools

Ollydbg, windbg, gdb, IDA Pro, hex-rays, Ghidra

## Computer Resource Acceptable Use Policy

Some of the work in this course will require reverse engineering and understanding and defeating various security measures. Individual servers and software targets will be made available for these assignments and must be used exclusively. Using these tools and techniques outside of the targets provided may cause a broad spectrum of responses from being frowned-upon to legal prosecution depending on context. Many ***Acceptable Use Policies*** specifically prohibit reverse engineering, e.g.

*You agree to comply with this Acceptable Use Policy when using the --- Website. Unacceptable uses include, but are not limited to:*

*a) Intentionally or unintentionally violating any applicable law or regulation;*

*…*

*l)* ***Attempting to decipher, decompile, disassemble or reverse engineering any of the software*** *comprising or in any way making up a part of the RVC Website; m) Interfering or attempting to interfere with the access of any user, host or network, including without limitation, sending a "virus" to the RVC web site, overloading, "flooding," "spamming," "crashing," or "mailbombing" web sites; or*

and, from the Payment Card Security and Confidentiality Agreement at Radford University:

*I acknowledge that I have no right to use, reproduce,* ***reverse engineer****,*

On the other hand, there are acceptable uses which have been recognized by courts of law, e.g.:

From a Lexmark vs SCC lawsuit:

*The court ruled that "copyright law shouldn't be used to inhibit interoperability between one vendor's products and those of its rivals. In a ruling from the U.S. Copyright Office in October 2003, the Copyright Office said "the*[*DMCA*](http://ethics.csc.ncsu.edu/intellectual/electronic/dmca/)*doesn't block software develpers* [sic] *from* ***using reverse engineering*** *to access digitally protected copyright material if they do so to achieve interoperability with an independently created computer program."*

I am not a lawyer and nothing in this course should be construed as legal advice. Before taking any action based on or enabled by this course, you should consider your personal situation and seek professional advice before any such action. So, to keep things simple(r) and legal, for the purposes of this course, use only the hardware/firmware/software provided for the purpose of completing assignments.

Violating this policy may be violation of the Universities acceptable use policy. You can find the RU Acceptable Use and other security policies in the Division of Information Technology website at: https://www-pprd.radford.edu/content/dam/departments/administrative/policies/InformationTechnologyPoliciesandProcedures/IT-PO-1500\_AcceptableUsePolicyforUniversityComputersandInformationTechnologySystems.pdf

## Grade Calculation

Points can be earned from assignments (~30 points), a midterm exam (15 points), a final exam (25 points), a final project (~30 points), and extra credit (~10 points). The two exams will be the midterm, just beyond ½ way through the course, and the final, at the regular time and place as scheduled by the university. Assignment details and definitive due dates will be posted on the class website and announced in class. It is your responsibility to keep track of due dates. “I forgot”, “I didn’t realize it was yesterday” etc. are not valid reasons for missing an exam/project (see Homework/Assignment/Project Policy below).

The final exam will be held at its regularly scheduled time and place, and will be comprehensive.

## Letter Grades

To figure out your grade, simply add up all the points you have earned throughout the course. Your total number of points maps to your letter grade in the usual manner, so if **S** is your point total, then:

A: 93 <= S

A-: 90 <= S <93

B+: 87 <= S <90

B: 83 <= S <87

B-: 80 <= S < 83

C+: 77 <= S < 80

C: 73 <= S < 77

C-: 70 <= S < 73

D+: 67 <= S < 70

D: 63 <= S < 67

D-: 60 <= S < 63

F: S < 60

Information about the grade point system at Radford can be found in the Academic Policies section of the Undergraduate Catalog here:

[http://catalog.radford.edu/content.php?catoid=35&navoid=1311#Grades\_and\_Credit](http://catalog.radford.edu/content.php?catoid=35&navoid=1311%23Grades_and_Credit)

## Attendance Policy

This course will require consistent effort and commitment. Missing class can quickly avalanche into I’m-lost territory due to the complexity and layered dependencies of much of the material. Students who are absent are responsible for getting the class notes and homework assignment for the class(es) missed. **There will be no make-up projects or exams** unless the absence is due to health problems or other emergencies. Health related absences require a physician-supplied statement. Further details regarding attendance policy can be found in the Academic Policies section of the Undergraduate Catalog here:

[http://catalog.radford.edu/content.php?catoid=39&navoid=1476#Class\_Attendance](file:///C:\cygwin64\home\rjoyce9\cl\cs2771.f17\catalog.radford.edu\content.php%3fcatoid=39&navoid=1476#Class_Attendance)

## Classroom Behavior Expectations

All students and staff of Radford University are members of a unique educational community; whose goal is to enable each student to tap his or her full potential for success. Such a challenging goal requires tremendous individual effort on the part of each student and cooperative effort on the part of each member of the community. The guiding principles of the community include hard work, respect for others and oneself, honesty, personal accountability, and careful organization of time and materials.

Come to class on time, follow normally expected patterns of social interaction and, in particular, cell phones/laptops/game players/your-favorite-gadget-here, are to remain off during class time. If you need to have a running conversation with a third party or achieve the next level in Idle Miner Tycoon, do it elsewhere.

## Netiquette Policy

What is Netiquette? Simply stated, it is network etiquette -- that is, the etiquette of cyberspace. And "etiquette" means "the forms required by good breeding or prescribed by authority to be required in social or official life." In other words, Netiquette is a set of rules for behaving properly online.

The following Netiquette rules will apply to this course.

Rule 1: Remember the Human

Rule 2: Adhere to the same standards of behavior online that you follow in real life

Rule 3: Know where you are in cyberspace

Rule 4: Respect other people's time and bandwidth

Rule 5: \*Make yourself look good online\*

Rule 6: Share expert knowledge

Rule 7: Help keep flame wars under control

Rule 8: Respect other people's privacy

Rule 9: Don't abuse your power

Rule 10: Be forgiving of other people's mistakes

## Communication

In addition to the learning management systems of Radford University I will maintain a website for this class at: **https://www.radford.edu/rjoyce9/classes/itec465**

All class materials will be posted there. We will use and reference this website often during class, so it should rather quickly become second nature to look there. That said, it is your responsibility to check the site on a regular basis - daily at a minimum. In particular, the *assignments* page of the site above contains a calendar of all assignments and their due dates, and said web page will be the definitive source for due dates. Remember that no late work will be accepted.

Another channel for communication is email, and you can also find me on discord: rj2718#7565. I will occasionally use the D2L email broadcast to send information to everyone. Again, it is your responsibility to check for such emails on a daily basis. 24 hours after I send any such email, the information therein will be deemed to be in your possession. If something is not clear, ask without delay.

**Use your Radford university email for communication for this class, do not use a personal email**. Some assignments are automated in various ways and so rely on your Radford email address.

Assignments will have explicit instructions on how to turn them in. Generally they will be submitted in electronic form via a setuid bit program which I will provide. You must read the instructions on the assignments and follow them explicitly. Software I have written will collect and stage assignments for grading. If you do not follow the submission instructions exactly, then I will not see your work and you will not get a grade (or rather you will get a grade of zero).

This will not feel good, especially if you have invested a lot of time and effort. We would then have to forensically track down the missing assignment, verify it was completed on time, and so on. To save the effort and bad feeling, again: carefully read and follow the assignment instructions exactly.

## Response Time

I am typically online at some point every day, and in most cases you will receive a response to any contact within 24 hours. There may be rare occasions however when I do not check in for 2 or even 3 days, so response time may be longer. You can use my office hours or schedule a meeting if you need certainty of availability.

## Homework/Project Policy

All projects are due by the deadline stated on each, NO LATE WORK WILL BE ACCEPTED (hence the terms “due” and “**dead**line”). Turn in what you have when it is due. The only exceptions to this are if you have a physician signed statement attesting to a bona fide medical reason for the late submission, meet other criteria set out in the attendance policy referenced above, or if you have died. Once more, just so we are clear from the beginning: NO LATE WORK WILL BE ACCEPTED, do not ask for exemptions.

## Office Hours

Office hours are listed at the beginning of this syllabus. Any deviations, temporary or permanent, will be announced in class. Office hours will be held in my office: Davis 218.

## Classroom Recording Policy

For the purposes of private academic study and review, students may record class lectures and discussions using analog or digital technology, including audio, video, still photos, and other forms of capture technology. Students who wish to make such recordings must first let me know.

## Academic Honesty and Plagiarism Policy

Effective evaluation of student work can occur only in an environment in which intellectual honesty is respected. Academic dishonesty is a clear violation of academic integrity and academic responsibility.

Academic dishonesty would include but is not limited to inappropriate giving or receiving of aid during tests and plagiarism of programming assignments. Discussion with others regarding programming assignments is encouraged, but taking a copy of code is not. The exams questions ask you to write code as well. People who have done their own programming, synthesizing algorithms and code from their own mind usually do well on the exams. The converse is also true.

Academic integrity and responsibility are important in the classroom and are inherent in the honor system at Radford University which each student has committed to uphold without compromise or exception. In cases of Academic dishonesty, a conversation with the student and professor will convene and the University policy for Academic dishonesty will be followed. This policy can be found at:

[http://catalog.radford.edu/content.php?catoid=35&navoid=1311#Honor\_System](http://catalog.radford.edu/content.php?catoid=35&navoid=1311%23Honor_System)

## Accommodations Policy

Federal law discusses a variety of mitigating measures used to normalize instruction and assessment of students with certain physical or mental impairments. If you are seeking academic accommodations under the Americans with Disabilities Act at Radford University, you are required to register with the Disability Resource Office (DRO). To receive academic accommodations for this class, please submit your documentation to the DRO in the lower level of Tyler Hall Suites 54-69, by fax to 540-831-6525, or by email to dro@radford.edu. After submitting documentation to their office, you will set up an interview with a Disability Services Specialist to discuss accommodations. You will be notified via email once your accommodation package is complete and ready to be picked up. Once you have picked up your accommodation package, you will need to meet with each course professor during their office hours to review and discuss your package. For more information and/or for documentation guidelines, visit www.radford.edu/dro or call 540-831-6350

## Covid-19 Policy

Students who have been diagnosed with COVID-19, who demonstrate COVID-19 symptoms, or who have been exposed through close contact to a person confirmed as COVID-19 positive should contact the Dean of Students Office for guidance.  The Dean of Students Office will provide resources and consultation to the student and will notify the faculty of the student if the student's absence from class is verified along with the dates of the verified absence from class.

If you are experiencing symptoms of COVID-19 and believe you have been exposed, please consider getting tested before you return to class. In the event that you test positive for COVID-19, please follow University protocols.

## Digital Devices

This class is far more interesting and a better learning environment when everyone is engaged, listening, and contributing. We are all challenged (myself included) by the ways in which our digital devices—laptops, tablets, and phones—can steal our attention away from our immediate surroundings. In this class we will have a device policy that is designed to support your attention to one another and to the course material. I have developed this policy for three reasons:

* A significant body of research demonstrates that when students engage in off-task behavior on their devices, **it hurts the learning of peers sitting near them**. In one study, students who were *not* using a device in a class lecture, but were seated *within view of a peer with a device*, performed 17 % worse on an exam based on that lecture material than students who were not within view of someone else’s device. (Glass, A.L. & Kang, M. (2019). Dividing attention in the classroom reduces exam performance. *Educational Psychology, 39*(3), 395-408.)
* This class depends upon everyone’s active engagement. Your ideas about the material in this class will become richer when they are articulated and engaged in dialogue with the ideas of your peers. If you are focused on your device, instead of our work, **you are missing an opportunity to learn and depriving your classmates of the opportunity to learn from you**. Your attention contributes to *all* of our learning.
* Finally, since so much of the course depends upon discussion, I want to make sure that we all **show respect for one another by listening to each other**. We all have likely had the experience of trying to speak with someone who was focused on their phone, and feeling hurt by their lack of attention to us. In this class, I want us to respect everyone’s voices by being present and listening to each other.

To achieve those objectives, the digital device policy is as follows:

1. You may use laptops to read course material and take notes as needed. If you use a laptop, **close any tabs that are not related to the course**. Remember, off-task behaviors can hurt the learning of your classmates.
2. You may have your phone out on your desk, but **keep it facedown and silent so you are not continually seeing and hearing new notifications** that steal away your attention and the attention of your classmates. Those notifications have been engineered to hijack your attention and can hurt your and your classmates’ learning.
3. There will be times in class when I want everyone to put their devices away and focus on some activity. In those activities, we will all be device free.
4. Finally, in order to show everyone that we are listening respectfully to one another, please remove any AirPods, earbuds, or headphones from your ears at the start of class.

## Student Support Services:

### Center for Accessibility Services:

If you are a student with special needs or circumstances, I invite you to contact me early in the course so appropriate supports and scheduling can be addressed. *Students seeking academic accommodations under the Americans with Disabilities Act must register with Radford University’s Center for Accessibility Services (CAS).* The policies regarding students with disabilities may be found at <http://www.radford.edu/content/cas/home.html>.  You may also contact the CAS office at: 540-831-6350; ASL users 540-922-1176;

### Harvey Knowledge Center:

The Harvey Knowledge Center is a Radford University resource to explore class content, learn new skills, prepare for your exams, or receive individualized academic coaching. In the HKC you can:

* Work one‐on‐one with an academic coach to discuss course content, study strategies, or college success skills
* Get your classmates together and form an online facilitated study group
* Reserve a single-use room for Zoom coaching or for working on your online class
* Access tips and guides for taking your learning to the next level

Call us at: 540‐831‐7704 | Email us at: [hkc@radford.edu](mailto:hkc@radford.edu)

Visit our website: Radford.edu/HKC | Schedule an appointment through Starfish

### Technology Support:

The Technology Assistance Center provides a number of options for students to find answers to common questions and request assistance.

* Find common answers or submit an online support request: [www.radford.edu/itonestop](http://www.radford.edu/itonestop)
* Phone Support: (540) 831-7500; Monday - Thursday 8 a.m. – Midnight, Friday 8 a.m. - 5 p.m.
* Walk-in Support (Appointment Recommended); Walker Hall 1st floor lobby; Monday through Friday 8 a.m. – 4:45 p.m.

Each student has an account on rucs.radford.edu (137.45.192.100), which you will need for this course. The password is the same one you use for other Radford University computing activities. You will also need the Cisco AnyConnect VPN software. I do not administer this computer, nor do I have root access. Any issues will need to be addressed through the Technology Assistance Center. Additionally, I will provide additional accounts on other computers from time to time. Details will be provided in class.

## Counseling

Mental wellness is essential to your intellectual and physical growth. RU offers counseling support to students. Please see their webpage for information on how to make an appointment: <https://www.radford.edu/content/student-counseling/home.html>

## Final Exam

The final exam will be comprehensive, will be held at the regularly scheduled exam time and place.

## Appeal of Grades

Final grades (but not individual assignments) may be appealed, the process for which is initiated by completing a [Notice of Intent to Formally Appeal a Grade form (PDF)](https://www.radford.edu/content/dam/departments/administrative/registrar/content-files/forms/Grade-Appeal.pdf). The grade appeal procedures contemplate a narrow range of applicable reasons for appeal focused on “arbitrary or capricious” behavior resulting in an injustice to the individual. In particular not liking your grade, ‘needing’ a better grade, etc. are not valid reasons.

## Exceptions to Policies

From the undergraduate student handbook:

The Radford University Undergraduate Catalog is the basic authority for academic requirements at Radford University. All students are expected to follow the catalog in the pursuit of their degrees. On occasion, extraordinary circumstances may, however, justify minor departures from the catalog requirements. Students who believe their situation warrants a deviation from academic policy may petition for an exception. Students should consult with their advising coordinator to explore the feasibility of petitioning for an exception to academic policy.

For the rest, see:

[catalog.radford.edu/content.php?catoid=35&navoid=1311#Exception\_to\_Academic\_Policy](file:///C:\cygwin64\home\rjoyce9\cl\cs2771.f17\catalog.radford.edu\content.php%3fcatoid=35&navoid=1311#Exception_to_Academic_Policy)