# CRJ 475 Project Proposal Form

## Spring 2022 – Professor James C. Brown

1. **Your name**: Joseph (JT) Cavallaro (jocavall)
2. **Your major (CYB, CRJ, CIA, or FFCI)**: CYB
3. **The number of credit hours you are registered for CRJ 475 (1–6)**: 3

## 4. Executive Summary

*Please provide a summary of the information detailed throughout this project proposal*. What is the problem that you desire to study (summary), what is the purpose of your project (summary)?

With this project proposal, I will be showing how simple it is for hackers to preform reconnaissance and malicious attacks using a coding language called Python. I will be doing this by showing a Python Hacking tool I created. We will cover (not in order), the history of python and how it has changed over time, hacking tools and how they evolved, the exploits that Python can take advantage of, how the tool I created works as a whole, how each sub-tool works and what they do, the kinds of attacks preformed and how they work. This tool could also be used by organizations for white-hat hacking and reconnaissance. We will also cover how Python can be used by companies to protect against attacks.

*More will be added in the final paper*

## 5. Statement of Need

*Discuss the needs or opportunities to be addressed by this project. Why is it necessary to know the information you propose to research?*

It is necessary to know this kind of information because it can help to gain a better understanding of Python, how hackers use it, and the exploits that are commonly used in attacks. It can also help protect your own company or home network from these types of attacks. Not only that, but it will also serve its educational purpose of showing a "real" example of the power Python has.

## 6. Project Goals

*Identify the goals of the project. Discuss what is to be achieved and the expected/desired outcomes of this project. Who would benefit from this study and how?*

With this project, I hope to finish my hacking tool, show how easy it is for attackers to get information and preform an attack using Python, and how to protect networks from/prevent attacks like this. As well to help organizations protect/prevent from attacks like this.

## 7. Constraints

*Talk about constraints that could affect the development, implementation, and/or end outcomes of this project. Consider such factors as time, experience, knowledge, skill sets, budgetary resources, competitive environment, and existing investments.*

The constraints that I have with this project are that most of these vulnerabilities are already taken care of (in today's age some of this is outdated), the tool only works on a virtual machine and tools that preform malicious attacks should only ever be used on a fake target (another virtual machine). The purpose of this is to not break any laws and to stay ethical.

## 8. Requirements

*Given your operational context, describe what needs to be in place during the project and afterwards in order for the project to be successful. In your discussion, consider the constraints you identified above and, if necessary, define requirements to compensate for constraints.*

For this hacking tool to work successfully on any machine, there are a few things that will need to be installed on your computer. First is VMWare Workstation Pro 16.x or higher. This program allows an operating system to run within another (like inception) and runs them as Virtual Machine's (VMs). Which brings us to our next step of getting our two VMs Ubuntu (Linux) 20.04 Focal or higher and Metasploitable2 Linux. The Ubuntu VM will act as the home

computer and where the program is coded. The Metasploitable2 VM will act as the target for the malicious attacks as it was created to be hacked. As well the difficulty can be changed for beginners, moderate, and advanced leveled hackers.

On the Ubuntu VM we will need to install the latest version of the programs and all of their dependances, which consist of: Python 3.10.0 or higher & all its dependencies; Pip; Snort & all its dependencies; Nmap & all its dependencies; Mechanize & all its dependencies.

Python has all of its own modules which allow it to preform functions. These modules have their own dependencies (other modules) and are needed in order to work. Most programs in this tool require third-party modules which need to be installed with all of their dependencies. These are listed below:

- sys
- os
- time
- PyPDF2
- PdfFileReader from PyPDF2
- mechanize
- random
- randint from random
- http.cookiejar
- CookieJar from http.cookiejar
- DefaultCookiePolicy from http.cookiejar
- urllib.request
- re
- bs4
- BeautifulSoup from bs4
- time as time_module
- scapy[complete]
- IPy
- IP as IPTEST from IPy
- nmap
- ipaddress

## 9. Time Line

*A. In order for this project to meet CRJ 475 requirements, satisfy the needs and opportunities outlined above, and achieve your stated project goals, what is the desired timeline for the project?*

- By the end of Week 3 the hacking tool will be "fully" complete (can never really be finished).
- By the end of Week 4 the full draft paper will be almost complete as well the PowerPoint.
- By the end of Week 5 the full draft paper and PowerPoint will be complete.
- By the end of Week 6 the project and PowerPoint will be completed.
- By the end of Week 7 any changes/fixes will be made to wrap up the project.

*B. What do you think is the longevity or useful life of the solution?*

This longevity or useful life of the solution is that it could benefit small or large organizations defend against these types of attacks, help beginners learn about Python and its capabilities, as well history of Python and how its changed overtime.

## 10. Impact: Costs and Risks (to you and others)

*Discuss the expected impact of the project and its expected outcomes. Provide detail on expected and potential costs and risks. If you believe there are none, explain why.*

The cost and risk of this project is that someone decides to use the tool for malicious activity that is illegal and does so outside of the VMs. This could cause a large-scale attack on a large organization; however, this tool was made to not have this capability. It is when the person decides to change the code to make it malicious. Ethical hacking is huge in the world of cybersecurity as it could result in being fired from your job or jail time, even if it is an accident.

## 11. Impact: Benefits and Opportunities

*Discuss the expected impact of the project and its expected outcomes. Provide detail and opportunities. Wherever possible, quantify the impact of the solution.*

The benefits and opportunities that come from this project is to teach about the coding language Python, to show the power that it really has, and to protect companies from future or current attacks that may be taking place.

## 12. Project Fit

*Discuss how this project fits within the goals of CRJ 475 and your major program of study (CYB, CRJ, CIA, or FFCI).*

This project idea would fit both the goals of CRJ 475 and my major CYB. This fits to the goals of CRJ 475 as it covers how an organization can use Python to protect from hackers, and teaching students by using this tool for white-hat hacking, to using Python for penetration testing, or to just gain more knowledge on Python.

This project fits my major of Cybersecurity because it is focused on coding, hacking, and the use of a coding language to exploit vulnerability's in a network/computer system, gain access, and gather information or preform a malicious attack on a target.

## 13. Evaluation and Measurement

*Propose criteria that might be used in defining and evaluating the success of this project and its end outcomes. What measurement standards are available to determine if the project is a success and the impact of its end outcomes? What benchmarks can be set up to determine the short-term and long-term efficacy of the project? Consider in your discussion the goals, requirements, and impact defined above.*

To measure the success of this project, the hacking tool would have to successfully preform reconnaissance and malicious attacks on a target, people are able to learn about Python from the written portion of the project, and the project as a whole could help an organization protect from malicious black-hat hackers.

Benchmarks could be set up for the short-term efficiency of this project as well the long-term. A short-term could be to compare my tool to another hacking tool. The long-term benchmark could be using this tool within a company to assess the vulnerabilities that need to be fixed.

## 14. Potential Solution

*At a high level, describe a potential solution that would satisfy the goals and requirements defined above.*

A potential solution, like described above could be using this tool within a company to assess the vulnerabilities that need to be fixed. This could be penetration testing, nmap port scanning, finding hidden data in a PDF, tricking the intrusion detection system, flooding the network with SYN packets, and more. However, this means that someone could use this tool for malicious reconnaissance and attacks as the tools in this tool will be mainly for reconnaissance.

If a company were to use this tool to do white-hat reconnaissance, they would be able to find vulnerable information and fix the issue. Even simple things like an employ's PDF file contains metadata that contains classified information like usernames, passwords, emails, etc. As well, a company could use the HTML Grab or the Link Parser (for 'href' links) tool to see if there are any classified links or data on a webpage, as well within a cookie (using the Cookie Grab Tool).

The TTL Pkt Parser Tool can be used by a company to spot packets picked up while browsing the internet. If the packet is spoofed it will also be printed. This means that any website that is visited by a user will be shown. The company can use this to find malicious activity internally and externally. As well a hacker could use this, while connected to the targets internet, to traffic live internet usage and gather packet flow data.

## 15. Human Subjects Approval

*Research conducted by Utica College faculty and staff must be pre-approved by UC's Institutional Review Board (IRB)* ***when that research involves collection of data from living people.*** *The IRB process requires a background experience in social science research methodology as well as time to complete the application process and gain IRB approval. Please review UC's IRB policy (click here), and confirm there that you will not be collecting data from (living) human subjects or going through the IRB.* **You should contact Professor Brown immediately if you have any plans to collect data/surveys etc. from human subjects.**

I will not have a Hauman Subject in this project.

## 16. Subject Matter Expert/Mentor

*If applicable, describe your subject matter expert (SME) and what role that person expects to play in your project. If you will not be taking advantage of a SME, explain why.*

I will not have a Subject Matter Expert/Mentor for this project.

## 17. References

*Identify—in full APA 7th bibliographic format—at least* ***four*** *scholarly/academic and/or professional/industry resources that are relevant to your proposed topic. If you are not able to identify these resources, you might not have an appropriate topic for the timeframe available.*


O'Connor, T. (2012). *Violent python: A cookbook for hackers, forensic analysts, penetration testers, and security engineers*. *BryteWave*. Elsevier Science. Retrieved 2021, from https://brytewave.redshelf.com/.

Mohit. (2015). Python penetration testing essentials : employ the power of python to get the best out of pentesting. Packt Publishing. Retrieved January 25, 2022, from https://uclibraryts.on.worldcat.org/search/detail/903957504?queryString=python%20hacking&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false.

Duffy, C. (2016). Python : penetration testing for developers : unleash the power of python scripting to execute effective and efficient penetration tests : a course in three modules (Ser. Learning path). Packt Publishing. Retrieved January 25, 2022, from https://uclibraryts.on.worldcat.org/search/detail/962192181?queryString=organization%20

hacked%20with%20the%20use%20of%20python&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false.

Babcock, J. (2016). Mastering predictive analytics with python : exploit the power of data in your business by building advanced predictive modeling applications with python (Ser. Community experience distilled). Packt Publishing. Retrieved January 25, 2022, from https://uclibraryts.on.worldcat.org/search/detail/958874809?queryString=python%20exploits&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false.

I have a lot more references when including non-scholarly refences like instructions for Python modules and other third-party programs used in the making of this tool, websites for this tools and modules, research for information, resources and help with these tools, and modules. As well, research on error solutions for all the sub-tools in this hacking tool.

## 18. Additional Information

*Provide below any additional considerations or information in support of this proposal*.

This project idea may be rough around the edges in this project proposal; however, I believe that this hacking tool could be used (if programed successfully, marketed correctly, and made to be used on more platforms) by an organization to preform security tests, internal/external reconnaissance, and white-hat hacking (on itself) to protect itself, and evade from future malicious hackers and the attacks they bring with them.

## 19. I acknowledge that I have reviewed the sample Senior Project Proposal in our online classroom prior to submitting my proposal.

Yes____x_____ No_____

**This must be checked yes**. Review the full sample proposal before your final submission. Ask yourself this simple question; does my proposal look like the sample in terms of content/substance?