CSC 432-Z1

Lab – Week 6

Professor: Ronny Bull

April 18, 2022

Joseph (JT) Cavallaro

Abstract

This proposal idea works to aim at protecting organizations by using this hacking tool for server and network security and security testing. In doing so I will be able to show how hackers use Python to preform reconnaissance and malicious attacks. To demonstrate this, I will be using my hacking tool, which I created using Python, within a CORE network topology that contains one router, two hubs, and three PC nodes that I also have set-up. It will be conducted like previous labs as PC1 will attack PC2 and PC3 will capture the traffic that is being sent.

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. This type of information is absolutely necessary to understand as it can help protect organizations large or small, schools, health care facilities, and even personal WI-FI networks. As well, it will grant a better understanding of the Python language, how ethical and malicious hackers use Python, as well the common attacks preformed using Python.

Introduction

With this project, I hope to expand not only my hacking tool, but also my knowledge of Python, Scapy, and computer, server, and network security and security testing. Showing how hackers use Python in attacks can be used to protect networks from attacks like this as well could train new employees on how to stop attacks like this. The main problem with this project is that that a lot of this may be out-of-date as it does not have the capability to stop zero-day-attacks, however it does possess the ability to attack a target as well collect data which could contain vulnerabilities. This is what would help an organization protect themselves from attacks. Another constraint is that as of now, this hacking tool does not have a windowed user interface but is used within the terminal, as well only can be run on a Virtual Machine. I have not tested this tool on Windows or Mac and have kept it within an Ubuntu VM. This is because if this tool is used on an actual target, it could cause actual damage even if the intent is not there. This is why we would use a fake target, in old projects, a Metasploitable2 Linux VM. However, this time the target will be a node within our CORE network topology. This was done to stay ethical and not break any laws related to cyber-attacks. This is very interesting to me as I have not been able to see the packets being sent by my tool and would love to test it out on a simulated network.

The main cost and risk to this project is that if someone were to download this tool and use it solely for malicious intentions. This could cause a large-scale attack on a desired target if used correctly. To rate the success of this project, My Hacking Tool would have to successfully send packets and these packets must be captured. This would only be for the manicous attacks, not the reconnaissance biased ones. This could help teach about types of attacks, Python, as well how an organization can defend from these attacks. In other case, this could be used to teach a in-training network analysis on how to spot these attacks as well defend against them.

Topic Idea & Proposed Solution

For this proposal, I was hoping to use the hacking tool that I created and used for two previous classes Final Projects and add Scapy scripted sub-tools to it and expand on it. When first starting this tool on October 20, 2021, it was a final project for CYB 339 with Professor Ish Morales. The name of this class was Cyber Operations Tools, and I was taught how to use Python to preform Cyber Operations like reconnaissance and malicious attacks. At the end of this course, my hacking tool only had a total of nine different sub-tools.

The second class that I used this for was CRJ 475, also known as the Senior Project and this was with Professor James Brown. I started this on March 3rd, 2022, which was the first eight weeks of this semester. In this class, I used my hacking tool to show how it could be used to help protect an organization from malicious attacks and Black Hat Hackers. It also discussed: the Python Coding Language; White, Black, Grey Hat Hackers and their methodologies; Ethical Hackers and Hacking as well their methodologies; Hacking Tools and their attacks; Ways organizations defend against attacks; My Hacking Tool; and finally, how organizations could use my tool to hello defend from attackers and preform security testing. The tool can even be used to find internal and external threats. At the end of this course, I was only able to add three scripts from the five made because of errors and time restraints, so this means the total number of tools after this class was 12.

In this class, I would be expanding on my tool, not by fixing the two other scripts I did not get to add from the last class but add new scripts to the tool that use Scapy. This would be so stay in the guidelines for this assignment. As well, I would test this tool within a CORE network topology. This would be a more complex topology compared to the ones created in this class however this is done to display what it would be like for a real Network Analysis watching an organizations network. These networks would have hundreds of computers and devices, as well wired and wireless connections. This would also include devices not in the building but connected to another network (like someone's Wi-Fi at home) but are still connected to the organizations servers. For this project however, it will be much simpler so we can show exactly how the hacking tool works and functions.

For my idea, I would like to expand on my hacking tool once again by adding more tools that use Scapy and the base module. After creating Python scripts in this class, I feel I could add a few more tools to my hacking tool that use Scapy. I want to add scripts that send packet and receive packets, monitor traffic, send fuzzing packets, and much more. I would use commands from our previous lab as well more that were left out from the report. The interactive tutorial was very effective in helping me learn how scapy could be used and I would love to be able to expand my knowledge of this. I would be able to display the use of this tool by setting up a CORE network topology and use this tool to target one particular node. I would set up a network with one router, two hubs, and three PCs. This would allow PC1 to attack PC2 on one part of the network, and the Network analysist (PC3) would be watching and capturing the network traffic from the attacks. This would show how my hacking tool could be used for security testing as well training.

The reconnaissance tools could be used to collect data on the target, or node two (PC2). The malicious tools could be used to attack the target (PC2). The network admin watching the traffic on PC3 could be a new employee in training on how to stop these kinds of attacks, or they could be an employee preforming these attacks on the system (in a virtual environment), like we are here, to test how secure the network really is and find flaws before any malicious attackers can.

Required Materials

The list of materials needed for this Hacking Tool as well the new modules and programs added with this class will be extensive. Because of this, I will be listing out the dependencies for my hacking tool to function correctly.

- VMWare Workstation Pro
- Ubuntu 20.04 Linux VM
- Metasploitable2 Linux VM
- CORE – Common Open Research Emulator & all its dependencies
- Python 3.10.0 & all its dependencies
- pip – The newest version available
- Snort & all its dependencies
- Nmap & all its dependencies
- Mechanize & all its dependencies
- Scapy & all its dependencies
- Python Modules & All Their Dependencies:
    - 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
  - Scapy
  - Ipaddress

- My Hacking Tool: will be available, and is now in its current state, on my GitHub page as well on my Google Drive, which are listed below:

https://github.com/JT-Ca/JT-Ca

https://drive.google.com/drive/folders/1Obge_KUuQ4DJuSfVicKp5PRJL_2MJPO7

Timeline

For this project, we have three weeks to work on the final project. The first week is working on this proposal, however, I have turned this in early to try and get a head start on this project. If this topic is approved and I can continue to work on this, because we have almost three weeks, I feel I have a lot of time to work on this project and get it done. The first week, which is this week, I will be focusing on this topic proposal, as well if this is approved, will start to work on the sub-tools within my hacking tool. These will consist Scapy commands that send and receive packets, send Fuzzing packets, sniffing, SYN Scans and much more.

Plan #1: If everything goes as planned, by Monday of Week 7, I will have four through six new sub-tools, which would make the totals 16, 17, or 18 total sub-tools. This gives me a full week (if needed) to collect results and write the report. If these scrips are all added to my hacking tool by Monday of next week, I will use Monday – Tuesday to collect results from using the tool within CORE network topology. This would be command and script outputs as well the traffic captured when using TCPDump or other sniffing programs (My Hacking Tool). This means that I have Wednesday – Sunday of that week (Week 7), to write the lab report. As well, if this all goes as planned, this gives me an extra full week to work on the report and fix all errors and make sure it is all organized correctly.

Plan #2: As a backup plan which covers in my other class takes up too much time, or the errors I am getting prove to take up too much time, or even if typing the report takes up too much time. I would have to stretch these time frames longer to give myself more time and to plan accordingly. The most amount of time that I can spend on each part of this is six days. This is because if I stretch these for more time, I could have the possibility of not completing this on time.

Benchmarks can be set-up as well for short- and long-term goals or efficiency of this project. The first, short-term, could be to compare my hacking tool to others that are created, an example could be Scapy, Nmap, or John the Ripper. A long-term benchmark could be using this tool within an actual organization and doing this to assess the network or servers for vulnerabilities that need fixing or monitoring activity to locate a possible attack.

Both the previous plan as well this one will be listed below in a table which shows what days I will be doing what within the upcoming weeks. (NOTE: X = Day off)

Final Project Timeline						
Plan #1						
4/17	4/18	4/19	4/20	4/21	4/22	4/23
Proposal	Proposal	X	Scripts or X	Scripts	Scripts	Scripts
4/24	4/25	4/26	4/27	4/28	4/29	4/30
Scripts or Collection	Collection	Collection	Collection or Report	Report	Report	Report
5/1	5/2	5/3	5/4	5/5	5/6	5/7
Report	Report & Organize	Report & Organize	Report & Organize	Report & Organize	Report & Organize	X
Plan #2						
4/17	4/18	4/19	4/20	4/21	4/22	4/23
Proposal	Proposal	X	Scripts or X	Scripts	Scripts	Scripts

4/24	4/25	4/26	4/27	4/28	4/29	4/30
Scripts	Scripts	Collection	Collection	Collection	Collection	Collection
5/1	5/2	5/3	5/4	5/5	5/6	5/7
Collection	Report & Organize	Report & Organize	Report & Organize	Report & Organize	Report & Organize	X

References

CSC 432 References:

Class Textbook: Dulaney, E. A., & Easttom, C. (2018). CompTIA Security+ deluxe study guide: Exam SY0-501. ISBN: 978-1-119-41685-2.

CSC 432 Labs Week 1 – 5

CYB 339 – Final Project References:

CYB 339 Labs from weeks 1 – 7

Class Textbook: Violent Python A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers by TJ O'Connor. PRODUCT INFORMATION: Sold By: Elsevier Science. ISBNs: 9781597499576, 9781597499576, 9781597499644, 1597499641. Language: English. Number of Pages: 289.

VMWare Workstation:

https://www.vmware.com/

https://www.vmware.com/products/workstation-pro.html

https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

Ubuntu 20.04 Focal VM:

https://ubuntu.com/download/desktop

Metasploitable2–Linux VM:

https://sourceforge.net/projects/metasploitable/

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

- Alternative to VM

https://linuxhint.com/install_metasploit_ubuntu/

https://blog.eldernode.com/install-and-use-metasploit-on-ubuntu/

Ubuntu VM Dependencies:

https://pypi.org/project/pip/

https://pip.pypa.io/en/stable/

https://kifarunix.com/install-and-configure-snort-3-nids-on-ubuntu-20-04/

https://upcloud.com/community/tutorials/install-snort-ubuntu/

https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/008/108/original/Snort_3_on_Ubuntu_18_and_20.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20211023%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211023T224202Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=eaaaf69ee92ba2d4b951d951adb3e27e62505e2b5ac52004da993c7508b4c674

https://nmap.org/

https://linuxhint.com/use-nmap-command-ubuntu/

https://manpages.ubuntu.com/manpages/xenial/man1/nmap.1.html

https://mechanize.readthedocs.io/en/latest/

https://github.com/python-mechanize/mechanize

https://pypi.org/project/mechanize/

Python 3:

https://www.python.org/

https://www.python.org/downloads/

Python 3 Modules:

https://docs.python.org/3/library/sys.html

https://docs.python.org/3/library/os.html

https://docs.python.org/3/library/time.html

https://pythonhosted.org/PyPDF2/

https://mechanize.readthedocs.io/en/latest/

https://docs.python.org/3/library/random.html

https://docs.python.org/3/library/http.cookiejar.html

https://docs.python.org/3/library/urllib.request.html

https://docs.python.org/3/library/re.html

https://www.crummy.com/software/BeautifulSoup/bs4/doc/

https://scapy.readthedocs.io/en/latest/installation.html

Tool #1 – #9:

https://pypi.org/

https://pypi.org/project/dpkt/

https://dpkt.readthedocs.io/en/latest/_modules/examples/print_packets.html

https://jon.oberheide.org/blog/2008/10/15/dpkt-tutorial-2-parsing-a-pcap-file/

https://mechanize.readthedocs.io/en/latest/

https://www.rubydoc.info/gems/mechanize/Mechanize:set_proxy

https://coderedirect.com/questions/215632/pythons-mechanize-proxy-support

https://sectigostore.com/blog/13-vulnerable-websites-web-apps-for-pen-testing-and-research/

https://stackoverflow.com/questions/1186789/what-is-the-best-way-to-call-a-script-from-another-script

https://pypi.org/project/IPy/

https://www.tutorialspoint.com/python/python_if_else.htm

https://stackoverflow.com/questions/20591385/bad-operand-type-for-unary-str

https://docs.python.org/3/tutorial/errors.html

https://stackoverflow.com/questions/12519554/invalid-syntax-in-except-handler-when-using-comma

https://coderedirect.com/questions/165494/invalid-syntax-in-except-handler-when-using-comma

https://stackoverflow.com/questions/20844347/how-would-i-make-a-custom-error-message-in-python

https://stackoverflow.com/questions/11329917/restart-python-script-from-within-itself

https://stackoverflow.com/questions/855493/referenced-before-assignment-error-in-python

https://careerkarma.com/blog/python-local-variable-referenced-before-assignment/

https://www.delftstack.com/howto/python/python-local-variable-referenced-before-assignment/

http://net-informations.com/python/err/local.htm

https://newbedev.com/how-to-make-a-python-program-automatically-restart-itself

https://stackoverflow.com/questions/23294658/asking-the-user-for-input-until-they-give-a-valid-response

https://codefather.tech/blog/validate-ip-address-python/#:~:text=To%20validate%20an%20IP%20address%20using%20Python%20you%20can%20use,IP%20address%20is%20made%20of.

https://stackoverflow.com/questions/36018401/how-to-make-a-script-automatically-restart-itself

https://www.codegrepper.com/code-examples/python/how+to+reboot+a+python+script

https://stackoverflow.com/questions/19782075/how-to-stop-terminate-a-python-script-from-running/34029481

https://stackoverflow.com/questions/73663/how-to-terminate-a-script

https://www.delftstack.com/howto/python/python-run-another-python-script/

https://stackoverflow.com/questions/45384429/how-to-execute-a-python-script-in-a-different-directory

https://datatofish.com/one-python-script-from-another/

https://www.edureka.co/community/50712/possible-call-one-python-script-from-another-python-script

https://www.codegrepper.com/code-examples/python/import+script+from+another+folder+python

https://newbedev.com/how-to-execute-a-python-script-in-a-different-directory

https://www.geeksforgeeks.org/how-to-run-multiple-python-file-in-a-folder-one-after-another/

https://www.geeksforgeeks.org/python-import-module-from-different-directory/

https://stackoverflow.com/questions/52577047/run-another-python-script-in-different-folder

https://www.geeksforgeeks.org/sys-path-in-python/

https://stackoverflow.com/questions/2333400/what-can-be-the-reasons-of-connection-refused-errors

https://stackoverflow.com/questions/2333400/what-can-be-the-reasons-of-connection-refused-errors/2361762

https://stackoverflow.com/questions/11585377/python-socket-error-errno-111-connection-refused

https://github.com/rgerganov/py-air-control/issues/21

https://resources.infosecinstitute.com/topic/port-scanning-using-scapy/

Targets:

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

https://twitter.com/

https://www.facebook.com/

https://www.google.com/

Other:

https://pythontutor.com/visualize.html#mode=edit

https://towardsdatascience.com/top-6-python-libraries-for-visualization-which-one-to-use-fe43381cd658

lolcat:

https://github.com/busyloop/lolcat

https://www.youtube.com/watch?v=8EGDxMgNRs0&ab_channel=AlexLynd

CRJ 475 Senior Project References:

A. H. Lashkari, B. Li, T. L. Carrier and G. Kaur, "VolMemLyzer: Volatile Memory Analyzer for Malware Classification using Feature Engineering," 2021 Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS), 2021, pp. 1-8, doi: 10.1109/RDAAPS48126.2021.9452028, from https://ieeexplore.ieee.org/abstract/document/9452028

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). Ransomware detection and mitigation using software-defined networking: The case of WannaCry. Computers & Electrical Engineering, 76, 111-121, from https://eprints.whiterose.ac.uk/144194/1/WannaCry_SDN_Akbanov_et_al.pdf

Argaw, S.T., Bempong, NE., Eshaya-Chauvin, B. et al. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med Inform Decis Mak 19, 10 (2019), from https://doi.org/10.1186/s12911-018-0724-5

Aziz, Shallaw M., "Ransomware in High-Risk Environments" (2016). Information Technology Capstone Research Project Reports. 1, from https://scholar.valpo.edu/itcrpr/1

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

Bemardo, D. A. G., & Miroslav, S. (2022). Sqlmap®. Retrieved February 10, 2022, from https://sqlmap.org/

Bennetts, S., Pereira, R., & Mitchell, R. (2022). *Owasp zap*. OWASP. Retrieved February 9, 2022, from https://owasp.org/www-project-zap/ & https://www.zaproxy.org/

Broersma, M. (2016). Python-Based Malware Infects European Companies. EWeek, 1, from https://uclibraryts.on.worldcat.org/search/detail/6033208475?queryString=python%20malware&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false

Canonical, U. (2022). *Enterprise open source and linux*. Ubuntu. Retrieved February 10, 2022, from https://ubuntu.com/

Capano, D. E. (2019). Understand the cyber-attack lifecycle. Control Engineering, 66(7), 32–33 & 66(11), 41–43, from https://uclibraryts.on.worldcat.org/search/detail/8212949150?queryString=Understand%20the%20cyber-attack%20lifecycle%3A&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false

Cavallaro, T. J. (2021). CYB 339 – Final Project Report – jocavall.docx [Unpublished Paper]. Cybersecurity Department, Utica University, from https://drive.google.com/drive/folders/1Obge_KUuQ4DJuSfVicKp5PRJL_2MJPO7

Cavallaro, T. J. (2021). CYB 339 – Final Project Code – jocavall. MHT Folder [Unpublished Code]. Cybersecurity Department, Utica University, from https://github.com/JT-Ca/JT-Ca & https://drive.google.com/drive/folders/1Obge_KUuQ4DJuSfVicKp5PRJL_2MJPO7

Cielen, D., Meysman, A. (2016). Introducing Data Science: Big Data, Machine Learning, and More, Using Python Tools. United States: Manning, from https://books.google.com/books?hl=en&lr=&id=bTozEAAAQBAJ&oi=fnd&pg=PT14&dq=how+can+python+benefit+a+large+organization&ots=-ilVFog81M&sig=AJuYBcNAtE8Uf4z47WhkSqNwhSY#v=onepage&q=how%20can%20python%20benefit%20a%20large%20organization&f=false

Cisomag, C. I. S. O. M. A. G. (2021, October 18). *How to build a career in ethical hacking in 2021 and Beyond*. CISO MAG | Cyber Security Magazine. Retrieved February 12, 2022, from https://cisomag.eccouncil.org/how-to-build-a-career-in-ethical-hacking-in-2021-and-beyond/

CSIS, -. (2022). *Significant cyber incidents*. Significant Cyber Incidents | Center for Strategic and International Studies. Retrieved February 17, 2022, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cusack, G., Michel, O., & Keller, E. (2018, March). Machine learning-based detection of ransomware using SDN. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (pp. 1-6), from https://dl.acm.org/doi/pdf/10.1145/3180465.3180467

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

Gupta, A., & Anand, A. (2017). *Ethical Hacking and Hacking Attacks "International.pdf. Academia* (4th ed., Vol. 6). International Journal Of Engineering And Computer Science. Retrieved February 7, 2022, from https://www.academia.edu/38177776/Ethical_Hacking_and_Hacking_Attacks_International_pdf

Holden, S. (2018, September 16). *Page*. Python Wiki. Retrieved February 12, 2022, from https://wiki.python.org/moin/

Jackson, A. (2020, July 14). *Python malware on the rise*. Cyborg Security. Retrieved February 4, 2022, from https://www.cyborgsecurity.com/cyborg_labs/python-malware-on-the-rise/

Khan, Mohd & Khan, Ihtiram Raza. (2017). Malware Detection and Analysis. 8. 1147-1149, from https://www.researchgate.net/profile/Ihtiram-Raza-Khan/publication/342491461_Malware_Detection_and_Analysis/links/5ef6d24745851550507530e2/Malware-Detection-and-Analysis.pdf

Kothari, V. (2021, May 27). *Internal working of python*. Internal working of Python. Retrieved February 12, 2022, from https://www.geeksforgeeks.org/internal-working-of-python/

Lyon, G. (2022). Nmap. Retrieved February 10, 2022, from https://nmap.org/ & https://insecure.org/fyodor/

Micro, T. (2022). *Hacking tools*. Definition of Hacking Tools. Retrieved February 8, 2022, from https://www.trendmicro.com/vinfo/us/security/definition/hacking-tools#:~:text=Hacking%20tools%20are%20programs%20that,have%20been%20designed%20to%20penetrate.

Miller, P., & Bryce, C. (2017). Python digital forensics cookbook : effective python recipes for digital investigations. Packt Publishing. Retrieved February 8, 2022, from https://uclibraryts.on.worldcat.org/search/detail/1007536293?queryString=malware%20created%20with%20python&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false.

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

Nolan, C. (2010, July 16). Inception. Retrieved February 10, 2022, from https://www.imdb.com/title/tt1375666/

O'Connor, T. (2012). *Violent Python: A cookbook for hackers, forensic analysts, penetration testers, and security engineers*. *BryteWave*. Elsevier Science. Retrieved 2021, from https://uclibraryts.on.worldcat.org/search/detail/900825104?queryString=Violent%20Python%20A%20Cookbook%20for%20Hackers%2C%20Forensic%20Analysts%2C%20Penetration%20Testers%20and%20Security%20Engineers%20by%20TJ%20O%27Connor&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false

Pauli, J. J. (2013). The basics of web hacking : tools and techniques to attack the web (Ser. The basics). Syngress, an imprint of Elsevier. Retrieved February 15, 2022, from https://uclibraryts.on.worldcat.org/search?queryString=The%20basics%20of%20web%20hacking%20%3A%20tools%20and%20techniques%20to%20attack%20the%20Web&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false

Penal Law, N. Y. S. L. (2022). *New York State law*. Article 156 - NY Penal Law. Retrieved February 10, 2022, from https://ypdcrime.com/penal.law/article156.php

Pramanick, S. (2022, February 11). *History of python*. History of Python. Retrieved February 7, 2022, from https://www.geeksforgeeks.org/history-of-python/

PurpleSec, -. (2021, August 6). *2021 Cyber Security Statistics Trends & Data*. 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends. Retrieved February 17, 2022, from https://purplesec.us/resources/cyber-security-statistics/

Rapid7, M. 2. (2022). *Metasploitable 2 exploitability guide*. Metasploitable 2 Exploitability Guide | Metasploit Documentation. Retrieved February 10, 2022, from https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide

Ripper, J. T. (2022). *John the ripper password cracker*. Openwall - John the Ripper password cracker. Retrieved February 10, 2022, from https://www.openwall.com/john/

Roohparvar, R. (2021, May 23). People - the weakest link in Cybersecurity. People – the Weakest Link in Cybersecurity. Retrieved February 7, 2022, from https://www.infoguardsecurity.com/people-the-weakest-link-in-cybersecurity/

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). *Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. EBSCOhost* (4th ed., Vol. 34), Journal of Management Information Systems. Retrieved February 8, 2022, from https://uclibraryts.on.worldcat.org/search?queryString=Exploring%20Emerging%20Hacker%20Assets%20and%20Key%20Hackers%20for%20Proactive%20Cyber%20Threat%20Intelligence&clusterResults=true&stickyFacetsChecked=true&groupVariantRecords=false

SBA, -. (2022). Stay safe from cybersecurity threats. Retrieved February 16, 2022, from https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

Sengupta, S. (2021, December 17). *【5 phases of ethical hacking】* What Are The Five Steps of Ethical Hacking? Retrieved February 10, 2022, from https://crashtest-security.com/five-steps-of-ethical-hacking/

Sharma, A. (2010). An Overview of Hacking. Trinity Journal of Management, IT & Media, 1(1), 11-14, from https://acspublisher.com/journals/tjmitm/archive-issues/2010-toc/an-overview-of-hacking/

S, M., H, M., & H, J. (2022). *BURP suite - application security testing software*. PortSwigger. Retrieved February 9, 2022, from https://portswigger.net/about & https://portswigger.net/burp & https://portswigger.net/burp/pro

Software Foundation, P. (2022). *Welcome to Python.org*. Python.org. Retrieved February 12, 2022, from https://www.python.org/ & https://www.python.org/doc/

Strowes, S. D. (2013, October 28). *Passively measuring TCP round-Trip Times - Volume 11, Issue 8*. Passively Measuring TCP Round-trip Times - ACM Queue. Retrieved February 10, 2022, from https://queue.acm.org/detail.cfm?id=2539132

Tech Target, T. T. (2009, June 15). *What is ubuntu? - definition from whatis.com*. SearchDataCenter - Definition - Ubuntu. Retrieved February 10, 2022, from https://searchdatacenter.techtarget.com/definition/Ubuntu

Tech, T. (2017, November 30). *Behind the data: Investigating metadata*. Investigating Visual Media - Behind the Data: Investigating Metadata. Retrieved February 10, 2022, from https://exposingtheinvisible.org/en/guides/behind-the-data-metadata-investigations/

Tenable, N. (2022, February 14). *Nessus product family*. Tenable® - Nessus. Retrieved February 10, 2022, from https://www.tenable.com/products/nessus

TrustedSec, T. (2019, September 27). *THE SOCIAL-ENGINEER TOOLKIT (SET)*. Open-Source Tools. Retrieved February 10, 2022, from https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/

Tsukerman, E. (2019). Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python. Packt Publishing Ltd, from https://books.google.com/books?hl=en&lr=&id=iFPADwAAQBAJ&oi=fnd&pg=PP1&dq=Machine+Learning+for+Cybersecurity+Cookbook:+Over+80+recipes+on+how+to+implement+machine+learning+algorithms+for+building+security+systems+using+Python&ots=Aiw9KSPzQ_&sig=Ic4O1Ke96INz1iwOhgUSoquiVoc#v=onepage&q=Machine%20Learning%20for%20Cybersecurity%20Cookbook%3A%20Over%2080%20recipes%20on%20how%20to%20implement%20machine%20learning%20algorithms%20for%20building%20security%20systems%20using%20Python&f=false

VMWare, V. (2022, January 27). *What is a virtual machine?: Vmware glossary*. VMware - What is a virtual machine? Retrieved February 6, 2022, from https://www.vmware.com/topics/glossary/content/virtual-machine.html

Williams, R., Samtani, S., Patton, M., Chen, H., & 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) Miami, FL, USA 2018 Nov. 9 - 2018 Nov. 11. (2018). 2018 ieee international conference on intelligence and security informatics (isi). In Incremental hacker forum exploit collection and classification for proactive cyber threat intelligence: an exploratory study (pp. 94–99). essay, IEEE, from https://doi.org/10.1109/ISI.2018.8587336 & https://www.researchgate.net/publication/329952002_Incremental_Hacker_Forum_Exploit_Collection_and_Classification_for_Proactive_Cyber_Threat_Intelligence_An_Exploratory_Study

Ying, F., & Zhang, Z. (2019). Data visualization analysis of big data recruitment positions in hangzhou based on python. Review of Computer Engineering Studies, 6(4), 81–86, from https://doi.org/10.18280/rces.060403