RIT | Rochester Institute of Technology of Dubai

Department of Electrical Engineering and Computing

Computing Security

CSEC 202 Reverse Engineering Fundamentals

Spring 2024

Sections: 600, 601, and 602

Homework Assignment #1: Basic Static Analysis

"Us vs. the CAT"

Release Date: February 5, 2024

Due Date: February 19, 2024 – 11:59:59 p.m. (GST= GMT+4)

Instructor: Emad AbuKhousa (eakcad@rit.edu)

Homework Assignment #1: Basic Static Analysis

"Us vs. the CAT"

Objective:

Sharpen your skills in basic static analysis, a cornerstone of malware analysis. By examining a sample executable file without executing it, you will gain valuable insights into its structure, functionality, and potential suspicious characteristics. This hands-on experience will pave the way for your future mastery of assembly code analysis in later stages of the course.

Instructions:

1. **Initial Reconnaissance:** Employ a variety of safe and discussed tools to gather essential information about the provided executable. Consider file characteristics, embedded strings, imported libraries, PE headers, and other relevant details.

2. **Delving into Functionalities:** Based on your analysis, predict the executable's intended functionalities. Support your conclusions with concrete evidence gleaned from the tools you used, incorporating screenshots or relevant excerpts where appropriate.

3. **Is it malicious:** Analyze the executable's content, focusing on identifying potential suspicious indicators or characteristics that could suggest malicious intent. Explain your findings and provide evidence from the tools you used.

4. **Static Insights:** Ensure your analysis covers **all** the static analysis techniques discussed in class, demonstrating your understanding of each.

5. **Proposed Role of an Expert Witness Simulation**: As a cybersecurity expert witness in a Dubai courtroom, summarize the executable's presumed role or function based on your static analysis findings. Assume a role where you must explain to a judge the general functionality of the malware in layman's terms. Identify its primary behavior, whether it acts as ransomware, Trojan horse, virus, worm, backdoor, spyware, etc. Discuss whether the malware is capable of launching a ransomware attack independently, and if so, how it might execute such an attack. Your explanation should help the court understand the potential threats and the nature of the malware

6. **Comprehensive Report:** Compile a well-organized report documenting your entire investigative process. Clearly present your findings, insights, and supporting evidence, making it easy for instructors to follow your thought process and evaluate your work.

7. **Exploration (Bonus):** Using additional tools, other than those discussed in class, will be considered as bonus that helps you getting a full grade of this assignment.

8. **Attribution Exploration (Bonus):** Earn bonus points by identifying who's behind this malware. Utilize available references, Google searches, and research papers for your investigation. A particular report by MANDIANT might offer valuable insights into tracing the origins of this CAT and its associated variants.

Important Reminders:

1. **Safety First:** Always remember to employ safe and approved tools within controlled environments designed for static analysis. Never attempt to execute the executable or engage in any actions that could pose risks.

2. **Team Collaboration:** This assignment can be completed individually or collaboratively in a ~~group~~ **team** of up to three members. Once all team members have joined the ~~group~~ **team**, only one member needs to submit the assignment on behalf of the entire team

3. **Basic:** This assignment challenges your skills in basic static analysis, a crucial step in safely unraveling the secrets of malware. Think of this malware as a complex puzzle, guarded by hidden dangers. Your task is to use observation and analysis tools to understand its workings without ever activating its harmful potential. Remember: **Do not look into the code, do not run the cat**.

4. **Ethical Conduct:** Adhere to ethical hacking principles and refrain from using any tools or techniques that could harm systems or violate privacy.

5. **Academic Integrity:** Ensure your work is your own and properly cite any external resources used.

6. **It is versus the cat:** As you delve into the basic static analysis of malware, maintaining academic integrity is paramount. Feel free to use a wide array of tools and resources necessary to grasp the malware's functionality fully. You are allowed to use AI tools like Bard and ChatGPT for research purposes, to gather information, or to clarify concepts. However, these AI resources should not be used directly to generate your assignment text. This approach ensures that while leveraging advanced technologies for insights, the work you submit remains genuinely your own effort and understanding.

Rubric:

Homework Assignment #1 Rubric	
Criteria	**Pts**
1) Comprehensive Report: a. Craft a well-organized, step-by-step report detailing your entire analysis process. b. Include clear explanations for each step, accompanied by relevant screenshots. c. Discuss the result and purpose of each tool or command you employed, demonstrating your understanding. d. Format your report professionally in a standard Word document using consistent styles and headings. e. Include a cover page listing the assignment details, team members, their contributions, and this rubric for reference.	10%
2) Basic Static Analysis tasks: a. Indication of Packed or Obfuscated File [10 points] b. Hashing & Analysis using Online Antivirus Portals [10 points] c. Imported Libraries and APIs [10 points] d. Treasure Hunting and String Analysis of Executable [10 points] e. Discover Resources using Resource Hacker [5 points] **f.** Use Pestudio as a comprehensive tool [5 points]	50%
3) Explore and discuss the following, using supporting evidence, screenshots, and logical reasoning: a. Is the binary malicious or not, why? b. Is the binary local or remote, why? If it is remote, then what are the remote resources it interacts with? Why? c. Does the executable introduce any permanent change into the hosting operating system? What are the local resources the binary interacts with? d. If yes, then how?	20%
4) In Dubai Courts Room - Expert Witness Simulation a. **Clarity and Layman's Terms [2 points]:** Ensure the explanation of the malware's functionality and potential threats is accessible to non-experts. b. **Identification of Malware Type [2 points]:** Accurately identify the malware's primary behavior (virus, worm, ransomware, Trojan, etc.) and provide a rationale.	10%

c. **Independent Attack Capability [2 points]:** Discuss whether the malware can launch an attack on its own, particularly focusing on ransomware capabilities. d. **Execution Method of Attack [2 points]:** If applicable, describe how the malware could execute a ransomware attack, including its mechanisms. e. **Recommendation for Further Analysis [2 points]:** Advocate for additional investigation through advanced static and dynamic analysis. Define these methodologies to the court, explaining their importance for a deeper understanding of the malware's complexities, potential evasion techniques, and the full scope of its capabilities and threats	
5) **The report includes a list of reference that support your discussion and conclusion**. Example of these references are: a. Microsoft documentations b. Websites of used tools c. Research papers that discuss related malware. d. Websites that discuss malware e. Industry reports on malware trends and threat intelligence	10%
Total	100%
Exploration (Bonus): Using additional tools, other than those discussed in class.	10%
Attribution Exploration (Bonus): who's behind this malware?	5%

Note:

This assignment demands individual contributions from each team member. Collaboration and discussion are encouraged, but it is imperative that each member conducts their own analysis and significantly contributes to the final report, showcasing their personal comprehension. Individual efforts will be distinctly evaluated, reflecting in your final grade. Therefore, the final grades among team members may vary.

Good Luck with the GreenCat

جامعة روتشستر الأمريكية للتكنولوجيا في دبي
A Global American University in Dubai

Department of Electrical Engineering and Computing

Computing Security

CSEC 202 Reverse Engineering Fundamentals

Spring 2024

Sections: 600, 601, and 602

HOMEWORK 1 REPORT

Author(s):	**Instructor**
1. **2.** **3.**	**Emad AbuKhousa**

Date of Submission:

1. Comprehensive Report [10%]

Table of Content:

Introduction:

In this assignment, you've had the opportunity to dive into the world of basic static analysis. Static analysis involves dissecting and understanding an executable file without executing it. It's a crucial skill in the field of cybersecurity and low-level programming.

Please take a moment to reflect on your journey in this assignment:

- Basic Static Analysis: Explain what basic static analysis is and why it's important in the realm of cybersecurity and low-level programming. Share the key techniques you've used to analyze the provided executable.

- Skill Improvement: Describe the progress you've made in improving your skills related to basic static analysis throughout this assignment. Highlight any challenges you encountered and how you overcame them.

- Course Learning Outcomes (CLOs): Identify which Course Learning Outcomes (CLOs) are targeted by this homework. Specifically, discuss how the skills you've developed in static analysis align with the CLOs outlined for this course.

The rest of the report ….

2. Basic Static Analysis tasks [50%]

a) Indication of Packed or Obfuscated File [10 points]

In this scenario, a sophisticated malware was sent via a spear-phishing email to the CEO of a DSO-based company, culminating in a ransomware attack that was reported to the Dubai police. As a cybersecurity expert, you have been tasked by the incident response team to conduct a forensic analysis of the malware, with a court hearing set in two weeks. Your main goal is to perform a basic static analysis on the provided copy of the malware to uncover its characteristics and trace its origins, providing crucial insights for the upcoming legal proceedings.

1- **Identify File Type:** Utilize tools such as "file" on Unix or examining file properties on Windows to ascertain the file's type (e.g., executable, script, document).

2- **Determine File Fingerprint:** Employ hashing tools to generate MD5, SHA-1, and SHA-256 hashes, creating a unique fingerprint for the file.

3- **VirusTotal Analysis:** Upload the file or its hash to VirusTotal to investigate:
   a. The malware's creation date.
   b. The first appearance of this packed version on VirusTotal.
   c. The number of dynamically linked libraries and imported Windows functions, as seen in the detail tab.

4- **IDA Free Analysis:** Analyze the packed binary in IDA by viewing segments (View > Open subviews > Segments or Shift +F7) and noting:

   a. The total number of segments,
   b. their names, and
   c. the starting and ending memory addresses of each.

5- **Identify the Packing Tool:** Use PEid, Detect It Easy (on Linux), Exeinfo PE, or similar tools to confirm if the executable is packed and identify the packing tool used.

6- **Unpack the Binary:** Proceed to unpack the binary if it is indeed packed, preparing it for further analysis.

b) Hashing & Analysis using Online Antivirus Portals [10 points]

In phase two of your analysis on the "GreenCat" malware, begin with hashing techniques to check if it's recognized in security databases. Follow these steps, mirroring the process used for the packed file:

1- **Identify File Type:** Use "file" on Unix or check file properties on Windows to determine the file type (e.g., executable, script, document).

2- **Determine File Fingerprint:** Generate MD5, SHA-1, and SHA-256 hashes with hashing tools for a unique file identifier.

3- **VirusTotal Analysis:** Upload the file or its hash to VirusTotal, noting:
   a. The creation date of the malware.
   b. The debut of this unpacked version on VirusTotal.
   c. For the analysis, compare whether the count of dynamically linked libraries and imported Windows functions remains consistent between the packed and unpacked versions of the malware.

   Note: This comparison helps identify if the unpacking process reveals additional functionalities or hidden libraries that were not initially apparent in the packed version, providing insights into the malware's complexity and potential capabilities.

4- **IDA Free Analysis:** Open the unpacked binary in IDA to examine:
   a. The number of segments.
   b. Their names.
   c. The starting and ending memory addresses for each segment.
   d. Compare these findings to those from the packed file analysis to identify any changes or anomalies that unpacking might have revealed. This comparison can provide insights into how the packing process altered the binary's structure.

5- Use VirusTotal in order to check if the executable is a known malware.
   a. How many security vendors flagged the "GreenCat" malware as malicious according to the VirusTotal analysis?
   b. Can you list any two types of threats that "GreenCat" malware is identified as by different security vendors on VirusTotal?

c) Imported Libraries and APIs [10 points]

Objective: Utilize analysis tools such as IDA Free, Dependency Walker, VirusTotal, or Cuckoo's Static Analysis capabilities to examine the provided executable. Your goal is to compile a comprehensive list of all dynamically linked libraries (DLLs) and the APIs under each one.

Instructions:

A)

- **Tool Selection:** Choose from IDA Free, Dependency Walker, VirusTotal portal, or Cuckoo's Static Analysis capabilities for this task. Each tool offers unique insights into the executable's dependencies and API usage.
- **Analysis and Documentation:** Identify every imported (linked) library within the executable. For each DLL identified, list the APIs it provides access to. Focus on understanding the hierarchy and relationships between these libraries and functions.
- **Report Preparation:** Present your findings in a structured table format. Your table should clearly distinguish between the DLLs and the specific APIs they import. This structured approach will help elucidate the executable's external dependencies and potential functionalities.

#	Imported DLL	APIs
1	**urlmon.dll**	URLDownloadToFileA
2		
3		
4		
5		
6		

B) In our analysis of the malware's interactions with system libraries, we've come across the **URLDownloadToFileA** function within the **urlmon.dll** library. Can you explain the significance of this API in the context of malware activity?

Hint: For a deeper understanding, you might want to refer to the official documentation or reputable sources online that detail this function's behavior and usage.

d) Treasure Hunting and String Analysis of Executable [10 points]

Conduct a comprehensive strings analysis of the provided malware, employing tools and methodologies covered in class. Begin by using the "**strings**" tool or an equivalent method to unearth hard-coded data within the malware:

1- **Process and Service Manipulation Analysis:** Identify strings that suggest the malware has capabilities to alter or control system processes and services. Look for Windows API functions as clues.

2- **Networking Functionality:** Which strings show the malware's ability to connect to the internet?

3- **Command and Control Detection:** Find strings that resemble commands for controlling an infected computer. Hint: Search for command-line-like instructions such as opening a shell or listing directories.

4- **Error Handling and Debugging Messages:** Identify strings suggesting error handling and debugging features.

5- **File Manipulation:** Look for strings that hint at the malware creating, reading, or writing files. What are the potential purposes behind these actions?

6- **System and User Information Reconnaissance:** Discover strings used by the malware to collect information about the system or its users.

7- **Hardcoded Paths and Commands:** Can you identify strings that would enable the malware to access the command prompt directly? Hint: Search for strings typically used to interact with the Windows command line.

8- **DLL Interaction Analysis:** List the Dynamic Link Libraries identified from the malware strings. Why are these interactions significant? Hint: DLLs provide essential services, indicating the malware's capabilities.

9- **Custom User-Agent Strings:** Can you identify custom User-Agent strings used by the malware to mimic web browsers? Look for strings beginning with "Mozilla/". Hint: These resemble legitimate browser identifiers.

10- **Internet Communications**: Were any direct web addresses, URLs, or IP addresses found in the malware strings, indicating specific communication targets?

e) Discover Resources using Resource Hacker [5 points]

Using either the Windows version of Resource Hacker or by installing the Linux version and analyzing the malware, did you find any integrated resources within the provided executable file? Please describe any resources you discovered and provide insights into their significance.

To complete this task, you can choose one of the following methods:

1- Download Resource Hacker to your Windows host machine and upload the malware.
2- Install Resource Hacker (Wine) on your Linux machine following this link: https://snapcraft.io/install/resourcehacker/debian

f) Use Pestudio as a comprehensive tool [5 points]

Pestudio is a valuable tool for confirming findings obtained from other analysis methods. In this task, you have three options for using Pestudio:

1- **Option 1 (Windows VM):** Download and install Pestudio on your Windows virtual machine. Open the provided malware file using Pestudio and discuss the results you obtain. Analyze how these results align with the information revealed by the previous analysis tools.

2- **Option 2 (Linux VM with Wine):** Download and install Pestudio on your Linux virtual machine and use Wine as a Windows emulator to open the malware file (even if it doesn't function correctly). Once opened, discuss the findings and compare them with the results obtained from previous analysis tools.

3- **Option 3 (Windows Host Machine):** Alternatively, you can install Pestudio on your Windows host machine and upload the malware file without running it. This method is safe since it won't execute the malware. Analyze the results you obtain from Pestudio and determine if they are consistent with the information gathered from other tools. If the malware attempts to execute, rest assured that its command and control center is disabled.

3. Explore and discuss [20%]

Embrace the challenge "**Us vs. the CAT**" with a strategic and resourceful mindset to unravel the secrets of the malware you're up against. This mission is not just an assignment; it's a battleground where you're equipped with an arsenal of tools, resources, and collaborative networks. Your goal is to dissect, understand, and outsmart the malware, using every means at your disposal to reveal its mechanisms and intentions.

Resources at Your Disposal:

- **Utilize Provided References and Resources:** Start with the wealth of information already provided. These resources are your first line of defense in understanding the malware's complexities.
- **VirusTotal Report:** Dive deep into all aspects of the VirusTotal report. Don't just skim the surface; explore community comments and use the tabs extensively to gather a comprehensive view of the malware's signature.
- **Joe Sandbox Cloud Basic Report:** If the direct online report is inaccessible, don't hesitate to request it. The May 2022 findings can offer valuable insights into the malware's behavior and impact.
- **Cuckoo Sandbox Report:** If you encounter a "pending" status, cleverly search for the malware's hash directly. Sometimes the fastest route is not through the front door.
- **Mandiant Industry Report:** Leverage insights from one of the leaders in cybersecurity. The Mandiant report on this malware can provide critical analysis and context.
- **University of California (UCLA) Theses Research Paper**: Academic research can offer a unique perspective on the malware, perhaps highlighting theoretical underpinnings or previously unconsidered angles.
- **AI-Based Services (ChatGPT, Bard, etc.):** Use the power of language models to ask questions, clarify doubts, or explore new hypotheses. These AI companions can be invaluable allies.
- **Group Discussions:** Engage in discussions with peers, within your security groups, classmates, other classes, or even other universities. Collective intelligence is a powerful tool in understanding and combating cyber threats.
- **Original Work Only:** While collaboration and external resources are encouraged, the final report must be your own. Authenticity and integrity in your analysis are paramount.

Your Mission, Should You Choose to Accept It:

1- **Is the Binary Malicious?** Provide a reasoned argument, supported by evidence from your analyses and the resources above. What characteristics or behaviors tip the scale towards malicious intent?

2- **Local or Remote Binary?** Determine the nature of the binary's operations. If it's designed to interact with remote resources, identify those resources and discuss their relevance to the malware's functionality.

3- **Permanent Changes to the Hosting OS:** Investigate whether the executable is engineered to modify the system it infects permanently. Detail the specific local resources it interacts with and the nature of these interactions.

4- **Mechanisms of Change:** If the executable does introduce permanent changes, elucidate how it achieves this. The intricacies of its operations can shed light on its objectives and the threat level it poses.

4. In Dubai Courts Room - Expert Witness Simulation [10%]

a) Clarity and Layman's Terms [2 points]

As a Cybersecurity Expert taking the stand, how would you simplify the explanation of this malware's objectives and its associated risks for the judges in Dubai courts or any individual lacking a technical background, utilizing straightforward language and analogies?

b) Identification of Malware Type [2 points]

Based on your analysis, what type of malware have you identified (e.g., virus, worm, ransomware, Trojan, spyware, etc..)? Provide a clear justification for your classification.

c) Independent Ransomware Attack Capability [2 points]

The victim accuses the defendant, who sent this program to them via email, of being behind the cyberattack. They allege that the defendant encrypted all their important files and that they found a ransomware message on their device, which is a demand for payment in exchange for decrypting the files. The judge asks you, "***Is this program capable of doing that? Is this accusation correct?***" Your answer will determine the conviction or acquittal of the accused.

Does this malware have the ability to initiate a ransomware attack without any external commands or interactions? Support your answer with evidence from your analysis.

d) Execution Method of Attack [2 points]

If the malware does not directly encrypt data, how could it potentially be involved in a ransomware attack? Describe a hypothetical scenario where this might occur.

e) Recommendation for Further Analysis [2 points]

Why is it important to conduct further analysis on this malware? Highlight the benefits of employing both advance static and basic/advance dynamic analysis methods in this context.

5. The report includes a list of references [10%]

Incorporate References to Support Your Analysis

As you conclude your comprehensive analysis of the malware and prepare your final report, it's imperative to substantiate your discussions and conclusions with credible references.

6. Bonus Exploration: Additional Tool Usage [10%]

Detail any supplementary tools you employed in your analysis that were not covered during our course lectures.

7. Bonus Attribution Investigation [5%]

Identify the origins or responsible parties behind this malware.