



Fall 2018

Malware Analysis
Grading Rubrics for Final Project

Weight: 45%

Grading Rubric for Final Project: Final Report

Weight: 15%

Component	Sophisticated	Competent	Not Yet Complete
Teamwork (25 Points)	The team worked well together to achieve objectives. Each member contributed in a valuable way to the project. All project sources indicated a high level of mutual respect and collaboration.	The team worked well together most of the time, with only a few occurrences of communication breakdown or failure to collaborate when necessary.	The team did not collaborate or communicate well. Some members would work independently, without regard to objectives or priorities.
Contribution (25 Points)	All requirements and objectives are identified, evaluated and completed. The deliverables offered new information or approach to the topic under discussion. Likewise, the final report is based on stated criteria, analysis and constraints.	All requirements are identified and evaluated but some objectives are not completed. The deliverables offered some new information or approach to the topic under discussion. The final report is reasonable; further analysis of some of the alternatives or constraints may	Many requirements and objectives are not identified, evaluated and/or completed. The deliverables offered no new information or approach to the topic under discussion. Few malware features and considerations are analyzed and other factors were ignored or



Fall 2018

		have led to different findings and lessons learned.	incompletely analyzed.
Subject Knowledge (25 Points)	The deliverables demonstrated knowledge of the project requirements by integrating major and minor concepts into the response. The deliverables also demonstrated evidence of extensive research effort and a depth of thinking about the topic.	The deliverables demonstrated knowledge of the project requirements by integrating major concepts into the response. The deliverables also demonstrated evidence of limited research effort and/or initial of thinking about the topic.	The deliverables did not demonstrate knowledge of the project requirements, evidence of the research effort or depth of thinking about the topic.
Supporting Material (20 Points)	All relevant information was obtained and information sources were valid. Malware analysis considerations were well supported by the information.	Sufficient information was obtained and most sources were valid. Malware analysis considerations were mostly supported by the information.	Insufficient information was obtained and/or sources lack validity. Malware analysis considerations were not supported by the information collected.
Composition (5 Points)	The deliverables were well organized and clearly written. The underlying logic was clearly articulated and easy to follow. Words were chosen that precisely expressed the intended meaning and supported reader	The deliverables were organized and clearly written for the most part. In some areas the logic and/or flow of ideas were difficult to follow. Words were well chosen with some minor expectations. Diagrams were consistent with the text.	The deliverables lacked overall organization. The reader had to make considerable effort to understand the underlying logic and flow of ideas. Diagrams were absent or inconsistent with the text.



Fall 2018

	comprehension. Diagrams or analyses enhanced and clarified presentation of ideas. Sentences were grammatical and free from errors.	Sentences were mostly grammatical and/or only a few spelling errors were present but they did not hinder the reader.	Grammatical and spelling errors made it difficult for the reader to interpret the text in places.
--	------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

Grading Rubric for Final Project: Presentation

Weight: 5%

Component	Sophisticated	Competent	Not Yet Complete
Content and Creativity (40 Points)	The presentation contained an abundance of material which clearly related to the main topic. External research was used to justify arguments or solutions. The presentation of the material was original and presented in a creative way that held audience attention.	The presentation contained material to support the main arguments, but: 1) not all material clearly related to the main arguments; 2) limited external research was used to justify arguments or solutions; and/or 3) the presentation of the material was appropriate, but only somewhat held audience attention.	The audience had to make considerable effort to understand the underlying logical and flow of ideas. Major aspects of the analysis or recommendations were absent. No external research was used to justify arguments or solutions. The presentation lacked creativity and did not hold audience attention.
Coherence and Organization (30 Points)	The problem, argument and solution were clearly stated and examples were appropriate. The transitions and flow were easy to follow.	The problem, argument and solution were clearly stated, but: 1) not all examples were supportive illustrations; 2) the transitions and /or	The problem, argument, solution and examples were not clearly stated. The conclusion was unclear. The transitions and flow were not logical.



Fall 2018

	Slides were error-free and logically presented.	flow were some what difficult to follow; and/or 3) slides were error-free and logically presented.	Slides contained errors and a lack of logical progression.
Speaking Skills and Participation (30 Points)	Team members were poised and had clear articulation. Every team member spoke and participated at a very high and balanced level. Speakers demonstrated good volume, and eye contact. Enthusiasm and confidence was exuded. The presentation fit into the time allotment	Team members were mostly audible and/or fluent on the topic, but:1) not all team members spoke and/or participated in a high and balanced level; 2) speakers demonstrated fair volume and/or eye contact was broken with audience; 3) light discomfort with public speaking was exuded; and/or 4) the presentation slightly went over the time allotment.	Team members were often inaudible and/or hesitant and relied heavily on notes. Speakers made distracting gestures with little or no audience eye contact. A high level of discomfort with public speaking was exuded. The presentation went over the time allotment.

Grading Rubric for Final Project: Malware Demo

Weight: 5%

Component	Sophisticated	Competent	Not Yet Complete
Teamwork (30 Points)	The team worked well together to achieve objectives. Each member contributed in a valuable way to the project. All project sources indicated a high level of mutual respect and collaboration.	The team worked well together most of the time, with only a few occurrences of communication breakdown or failure to collaborate when necessary.	The team did not collaborate or communication well. Some members would work independently, without regard to objectives or priorities.



Fall 2018

Contribution (30 Points)	The demonstration offered new information or approach about the malware. The demonstration also showed strong effort was made in breaking new ground and building excitement about the malware analysis.	The demonstration offered some new information or approach about the malware. The demonstration also showed initial effort was made in building excitement about the malware analysis.	The demonstration was not complete and offered no new information or approach about the malware. The demonstration also showed that little effort was made in building excitement about the malware analysis.
Content and Creativity (40 Points)	The demonstration was imaginative and effective in conveying ideas to the audience.	The demonstration techniques used were effective in conveying main ideas, but a bit unimaginative.	The demonstration failed to capture the interest of the audience and/or is confusing in what was communicated.

Grading Rubric for Final Project: Project Assessment

Weight: 20%

Component	Sophisticated	Competent	Not Yet Complete
Network architecture of Virtual Lab (10 Points)	The virtual lab included very reliable network architecture to perform the malware analysis.	The virtual lab included reliable network architecture to perform the malware analysis.	The virtual lab included poor network architecture to perform the malware analysis.
Configuration of Virtual Lab (10 Points)	Configuration of all virtual machines, tools and devices have been fully completed and verified without any issues.	Configuration of all virtual machines, tools and devices have been partially completed and some issues may arise.	Configuration of all virtual machines, tools and devices have not been completed properly and multiple issues may arise. Some misconfigurations exist.



Fall 2018

Security (10 Points)	Security measures were properly selected and implemented throughout the project.	Security measures were properly selected and implemented most of the time for the project.	Security measures were not properly selected and implemented throughout the project. Or, some measures were taken leaving certain areas without protection.
Selection of tools (10 Points)	Dynamic and static analysis tools have been properly selected.	Dynamic and static analysis tools have been partially selected.	Dynamic and static analysis tools have not been properly selected.
Selection of malware samples (10 Points)	The group selected at least two malware samples.	The group only selected one malware sample.	The group did not select any malware sample.
Static Analysis (20 Points)	Proper guidelines were followed to complete the static analysis of malware samples.	Some guidelines were followed to complete the static analysis of malware samples.	Guidelines were not followed to complete the static analysis of malware samples.
Dynamic Analysis (20 Points)	Proper guidelines were followed to complete the dynamic analysis of malware samples.	Some guidelines were followed to complete the dynamic analysis of malware samples.	Guidelines were not followed to complete the dynamic analysis of malware samples.
Findings and Conclusions of Project (5 Points)	The project outcomes include very useful findings and conclusions.	The project outcomes include useful findings and conclusions.	The project outcomes do not include findings and conclusions.
Lessons Learned (5 Points)	The project provided realistic successes and potential improvements for the team.	The project provided some successes and potential improvements for the team.	The project did not provide successes and potential improvements for the team.