

**ITMS 458 RUBRIC****ITMS 458 Operating System Security**

Students may be scored on a scale of 1 to 5; scores of 2 and 4 may be interpolated.

<b>Program Educational Objectives</b>				
<b>Objective</b>	<b>Score ▶</b>	<b>5</b>	<b>3</b>	<b>1</b>
<i>Design and implement an enterprise security program using policy, technology, and awareness to implement appropriate controls and technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions</i>		The student is consistently able to implement appropriate operating system controls and technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions	The student is generally able to implement appropriate operating system controls and technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions	The student is unable to implement appropriate operating system controls and technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions
<b>Course student outcomes</b>				
Upon completion of this course the student should be able to do the following:				
<b>Outcome</b>	<b>Score ▶</b>	<b>5</b>	<b>3</b>	<b>1</b>
<i>Describe potential system attacks and the actors that might perform them</i>		The student is able to describe potential system attacks and the actors that might perform them accurately and in detail	The student is able to describe potential system attacks and the actors that might perform them with some omissions or inaccuracies	The student is unable to describe potential system attacks and the actors that might perform them
<i>Describe appropriate measures to be taken should a system compromise occur</i>		The student is able to describe appropriate measures to be taken should a system compromise occur accurately and in detail	The student is able to describe appropriate measures to be taken should a system compromise occur with some omissions or inaccuracies	The student is unable to describe appropriate measures to be taken should a system compromise occur
<i>Describe characteristics of malware and identify different malware</i>		The student is able to describe characteristics of malware and identify different malware accurately and in detail	The student is able to describe characteristics of malware and identify different malware with some omissions or inaccuracies	The student is unable to describe characteristics of malware and identify different malware
<i>Apply tools and techniques for identifying vulnerabilities</i>		The student has clearly demonstrated their ability to apply tools and techniques for identifying vulnerabilities	The student has adequately demonstrated their ability to apply tools and techniques for identifying vulnerabilities	The student is unable to apply tools and techniques for identifying vulnerabilities
<i>Describe, for a given OS, the steps necessary for hardening the OS with respect to various applications</i>		The student is able to describe, for a given OS, the steps necessary for hardening the OS with respect to various applications accurately and in detail	The student is able to describe, for a given OS, the steps necessary for hardening the OS with respect to various applications with some omissions or inaccuracies	The student is unable to describe, for a given OS, the steps necessary for hardening the OS with respect to various applications
<i>Securely install a given OS, remove or shut down un-necessary components and services, close unnecessary ports, and ensure that all patches and updates are applied</i>		The student has clearly demonstrated their ability to securely install a given OS, remove or shut down un-necessary components and services, close unnecessary ports, and ensure that all patches and updates are applied	The student has adequately demonstrated their ability to securely install a given OS, remove or shut down un-necessary components and services, close unnecessary ports, and ensure that all patches and updates are applied	The student is unable to securely install a given OS, remove or shut down un-necessary components and services, close unnecessary ports, and ensure that all patches and updates are applied
<i>Identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)</i>		The student is able to, accurately and in detail, identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)	The student is able to, with some omissions or inaccuracies, identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)	The student is unable to identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)
<i>Apply security principles and practices to maintain operations in the presence of risks and threats</i>		The student has clearly demonstrated their ability to apply security principles and practices to maintain operations in the presence of risks and threats	The student has demonstrated to some extent their ability to apply security principles and practices to maintain operations in the presence of risks and threats	The student is unable to demonstrate an ability to apply security principles and practices to maintain operations in the presence of risks and threats