

Course Overview/Syllabus (QM Standards 1.2, 1.5, 1.6, 1.7, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4, 4.1, 4.4, 4.5, 4.6, 5.1, 5.3, 6.1, 6.2)

Course Overview (QM Standard 1.2)

Welcome to *Network Defense*!

This course examines the basics of Network Defense. During the semester we will take an in-depth look at the components that make up Network Defense, We will also take an in-depth look at the steps and technical tools used by network attackers and network defenders as well as case studies to illustrate the techniques used by both groups.

Pre-Requisites (QM Standard 1.6)

None

Minimum Technical Requirements and Skills (QM Standards 1.5 and 1.7)

Students will need to install virtualization software on their computers to complete this course. More specifically, students will download and install Kali Linux in the virtualization solution of their choice. Information on Kali Linux is available at <http://www.kali.org/> (including privacy and accessibility statements). For questions and troubleshooting, students should consult the Official Kali Linux Documentation, available at <http://www.kali.org/official-documentation/>

Students should also have a basic knowledge of Linux and basic Linux commands.

Instructor Information (QM Standards 1.8 and 5.3)

Please see Blackboard.

Alignment Map (QM Standards 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.4, 4.1, 4.4, 4.5, 5.1, 6.1, 6.2)

Course Objective	Module Learning Objectives	Module	Course Materials/Technology	Activity/Assignment/Assessment
Identify, defend, and manage threats against digital information.	Interpret common threats and best practices to defend against common threats. [M1S1, M1U1]	1	Online resources on Why Defend Networks (Threats)	M1S1: Self-assessment M1U1: Lab
Identify, defend, and manage threats against digital information.	Identify best practices and tools used to defend networks. [M2S1, M2A1, M2A2]	2	Online resources on Recon – Social Networks	M2S1: Self-assessment M2A1: Assignment M2A2: Lab
Identify, defend, and manage threats against digital information.	Identify best practices and tools used to defend networks. [M3S1, M3A1, M3U1, M3A2]	3	Online resources on Recon – Google Hacking and Deep Web Searching	M3S1: Self-assessment M3A1: Lab M3U1: Discussion M3A2: Lab
Identify, defend, and manage	Identify best practices and tools used to defend networks. [M4U1]	4	Online resources on Recon – Physical Surveillance and	M4S1: Self-assessment M4U1: Discussion

threats against digital information.	<p>Identify and explain the network attacks and proper defenses. [M4S1]</p> <p>Identify and react to network attacks. [M4A1]</p>		Log Analysis	M4A1: Lab
<p>Apply the principles of Network Defense to properly secure networks .</p> <p>Identify, defend, and manage threats against digital information.</p>	<p>Identify best practices and tools used to defend networks. [M5A1, M5A2, M5A3, M5A4]</p> <p>Identify and explain the network attacks and proper defenses. [M5S1, M5A1, M5A2, M5A3, M5A4]</p> <p>Identify and react to network attacks. [M5A2, M5A4]</p>	5	Online resources on Scan – War Driving and Scanning Tools	<p>M5S1: Self-assessment</p> <p>M5A1: Assignment</p> <p>M5A2: Lab</p> <p>M5A3: Assignment</p> <p>M5A4: Lab</p>
<p>Identify, defend, and manage threats against digital information.</p>	<p>Identify best practices and tools used to defend networks. [M6A1, M6A2, M6U1]</p> <p>Identify and explain the network attacks and proper defenses. [M6A1, M6U1]</p> <p>Identify and react</p>	6	Online resources on Explore – Authentication Security and Physical Security	<p>M6S1: Self-assessment</p> <p>M6A1: Assignment</p> <p>M6A2: Lab</p> <p>M6U1: Discussion</p>

	<p>to network attacks. [M6A2]</p> <p>Interpret common threats and best practices to defend against common threats. [M6S1, M6A2]</p>			
<p>Apply the principles of Network Defense to properly secure networks .</p> <p>Identify, defend, and manage threats against digital information.</p>	<p>Identify best practices and tools used to defend networks. [M7A1]</p> <p>Identify and explain the network attacks and proper defenses. [M7A1]</p> <p>Identify and react to network attacks. [M7A1]</p> <p>Interpret common threats and best practices to defend against common threats. [M7S1, M7A1]</p>	7	<p>Online resources on Exploit – Social Engineering</p>	<p>M7S1: Self-assessment</p> <p>M7A1: Lab</p>
<p>Apply the principles of Network Defense to properly secure networks .</p>	<p>Identify best practices and tools used to defend networks. [M8A1]</p> <p>Identify key figures, conferences, and concepts in hacker culture. [M8S1, M8A2]</p>	8	<p>Online resources on Hacker Culture and Metasploit</p>	<p>M8S1: Self-assessment</p> <p>M8A1: Lab</p> <p>M8A2: Assignment</p>

Identify, defend, and manage threats against digital information.	Identify and explain in the network attacks and proper defenses. [M8A1] Identify and react to network attacks. [M8A1] Interpret common threats and best practices to defend against common threats. [M8A1]			
--	---	--	--	--

Optional/Required Course Materials (QM Standard 4.6)

As noted elsewhere in this syllabus, students will need to install virtualization software on their computers to complete this course. More specifically, students will download and install Kali Linux in the virtualization solution of their choice. Information on Kali Linux is available at <http://www.kali.org/> (including privacy and accessibility statements). For questions and troubleshooting, students should consult the Official Kali Linux Documentation, available at <http://www.kali.org/official-documentation/>

Students should also have a basic knowledge of Linux and basic Linux commands.

Textbook Information (QM Standard 4.6)

No textbooks are required for this course.

Grading Policy (QM Standard 3.2)

Final number grades will be determined using this formula:

Points Earned/Points Possible x 100 = Final Number Grade

Final letter grades will be determined based on the following grading scale:

Percentage	Letter Grade

90 - 100%	A
80 – 89%	B
70 – 79%	C
60 – 69%	D
Below 60	F

Grading Criteria/Rubrics (QM Standard 3.3)

Points will be assigned for work submitted based on completeness and accuracy and/or adherence to assignment instructions. Please see individual assignment instructions.

Course Schedule (QM Standard 1.2)

Please see Blackboard.