JROTC Cyber Curriculum Map Years 1-4

Year 4 180 Total Class Hours	Fundamental JROTC Leadership Training kicks off the final year. The course also allows the students to learn the offensive side of cybersecurity while delving into advanced cybersecurity topics. Students explore specialized areas, such as forensics, compliance, reverse engineering, and SCADA. Students learn ethical hacking, beginning with the legal aspects of the topic and progressing through planning and scoping, performing vulnerability scanning and penetration testing, and analyzing and reporting the results. This year also focuses heavily on wireless communication and includes an introduction to the C++ programming language. The course covers topics relevant to CompTIA's PenTest+ exam and provides an extended capstone to allow students to focus on a select topic of interest. At the conclusion of the course, students can utilize their training in the government, industry, or academic sectors.		
36 hours	JROTC Leadership Education Training ● Leadership (select topics) ● Personal growth (select topics) ● Team building (select topics) ● Citizenship and government ● Service Learning		
7 hours	Compliance ● Understand the frameworks, standards, processes, and tools available to comply with information security laws and regulations. ● Apply these concepts to real-world scenarios.	F.CSF.t08 F.CSF.t09 F.CSF.t13 F.ISC.t15 F.CSF.t16 F.CSF.t17 F.ISC.t17	PenTest+ 1.1
7 hours	Planning and Scoping ● Planning for engagement ● Legal concepts ● Types of assessments ● Scoping ● Compliance-based assessments	F.CSF.t12 F.ISC.t15	PenTest+ 1.2 1.3
11 hours	Information Gathering and Vulnerability Identification ● Information gathering techniques ● Vulnerability scans ● Planning the exploit ● Specialized systems	F.ISC.t04 F.ISC.t06 F.ISC.t13 F.ISC.t14	PenTest+ 2.1 2.2 2.3 2.4
40 hours	Attacks and Exploits ● Social engineering attacks ● Network-based attacks ● Wireless/RF attacks (extended unit to align with 38 week training) ● Application-based attacks ● Local host attacks ● Physical security attacks ● Post-exploitation	F.ISC.t14 F.ISC.t15 F.ISC.t16	PenTest+ 3.1 3.2 3.3 3.4 3.5 3.6 3.7

JROTC Cyber Curriculum Map Years 1-4

5 hours	Penetration Testing Tools • Nmap • Tools by use case • Tool output analysis • Basic scripting	F.CSF.o03 F.ISC.t06 F.ISC.t13	PenTest+ 5.3
7 hours	Forensics • Follow data acquisition and storage guidelines. • Use open-source digital forensics tools to create disk images, recover deleted files, and extract hidden information. • Understand metadata and how it is stored and can be utilized in digital forensics.	F.ISC.t02 F.ISC.t07 F.CSF.t02 F.CSF.t05 F.CSF.t14 F.CSF.t15 F.ISC.t08 F.ISC.t09 F.ISC.t12 F.ISC.t15	PenTest+
7 hours	Reporting and Communication • Report writing • Post-engagement • Mitigation strategies • Communication importance		PenTest+ 4.1 4.2 4.3 4.4
7 hours	SCADA • Recognize the components of a SCADA system. • Investigate vulnerabilities associated with the component.	F.ISC.t04 F.CSF.t07 F.ISC.t16 F.ISC.t17	PenTest+ 3.5
15 hours	• Programming (C++)		PenTest+ 5.1
7 hours	Reverse Engineering • Explore the legal issues associated with reverse engineering. • Practice using open-source reverse engineering software to conduct file analysis.	F.CSF.t02 F.ISC.t08 F.ISC.t07 F.ISC.t12 F.CSF.t14 F.ISC.t16	PenTest+ 5.2
11 hours	Principles • Define the principles of cybersecurity • Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.	F.CSP.o01 F.CSP.o02 F.CSP.o03 F.CSP.o04 F.CSP.o05 F.CSP.t01a F.CSP.t01b F.CSP.t01c F.CSP.t01d	

JROTC Cyber Curriculum Map Years 1-4

	• Analyze common security failures and identify specific design principles that have been violated. • Given a specific scenario, identify the design principles involved or needed. • Understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.	F.CSP.t01e F.CSP.t01f F.CSP.t01g F.CSP.t01h F.CSP.t01i F.CSP.t01j F.CSP.t01k F.CSP.t01l F.CSP.t01m F.CSP.t01n F.CSP.t01o	
20 hours	JROTC Leader Education Training & Capstone project • Further exploration of topics of interest • Topics may include those related to forensics, compliance, reverse engineering, SCADA, or penetration testing		