Cybersecurity - National Initiative for Cybersecurity Education

Unit 1

Lessons 1-1	1-2	1-3	Identifer
		x	A0062 Monitor measures or indicators of system performance and availability.
		x	A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
		x	A0019 Produce technical documentation.
		x	A0021 Use and understand complex mathematical concepts (e.g., discrete math, boolean algebra)
		x	A0120 Share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.
		x	A0105 Tailor technical and planning information to a customer’s level of understanding.
	x		A0026 Analyze test data
	x		A0001 Identify systemic security issues based on the analysis of vulnerability and configuration data.
	x	x	A0025 Accurately define incidents, problems, and events
	x	x	A0040 Translate data and test results into evaluative conclusions
	x	x	A0070 Ability to apply critical reading/thinking skills.

Lessons			
1-1	**1-2**	**1-3**	Identifer
x			K0158 Know organizational information technology (it) user security policies (e.g., account creation, password rules, access control).
x			S0052 Use social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
x		x	A0085 Exercise judgment when policies are not well-defined.
x		x	A0092 Identify/describe target vulnerability.
x	x		A0042 Develop career path opportunities
x	x	x	A0074 Collaborate effectively with others.
x	x	x	A0106 Ability to think critically.
x	x	x	A0123 Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
x	x	x	A0155 Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
x	x	x	A0014 Communicate effectively when writing.
x	x	x	A0069 Ability to apply collaborative skills and strategies.

Cybersecurity - National Initiative for Cybersecurity Education

Unit 2

Lessons				Identifier
2-1	2-2	2-3	2-4	
			x	A0025 Accurately define incidents, problems, and events
		x		A0055 Operate common network tools (e.g., ping, traceroute, nslookup).
x		x	x	A0049 Apply secure system design tools, methods and techniques.
		x	x	A0048 Apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
		x	x	A0042 Develop career path opportunities
		x		A0041 Use data visualization tools
			x	A0040 Translate data and test results into evaluative conclusions
		x	x	A0035 Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
x		x	x	A0030 Collect, verify, and validate test data
		x	x	A0001 Identify systemic security issues based on the analysis of vulnerability and configuration data.
		x	x	A0026 Analyze test data

Lessons				
2-1	**2-2**	**2-3**	**2-4**	Identifier
	x		x	A0062 Monitor measures or indicators of system performance and availability.
			x	A0019 Produce technical documentation.
		x	x	A0015 Conduct vulnerability scans and recognize vulnerabilities in security systems.
			x	A0014 Communicate effectively when writing.
			x	A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
			x	A0012 Ask clarifying questions
			x	A0011 Answer questions in a clear and concise manner.
	x	x	x	A0010 Analyze malware.
		x	x	A0003 Determine the validity of technology trend data.
			x	A0027 Apply an organization's goals and objectives to develop and maintain architecture
x	x		x	A0093 Identify/describe techniques/methods for conducting technical exploitation of the target.
x			x	A0155 Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
		x	x	A0128 Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

Lessons				
2-1	**2-2**	**2-3**	**2-4**	Identifier
		x		A0126 Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
x			x	A0123 Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
x			x	A0120 Share meaningful insights about the context of an organization's threat environment that improve its risk management posture.
x	x	x	x	A0107 Think like threat actors.
x	x	x	x	A0106 Ability to think critically.
			x	A0105 Tailor technical and planning information to a customer's level of understanding.
		x		A0058 Execute os command line (e.g., ipconfig, netstat, dir, nbtstat).
			x	A0097 Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.
x				A0061 Design architectures and frameworks.
			x	A0092 Identify/describe target vulnerability.
			x	A0086 Expand network access by conducting target analysis and collection to identify targets of interest.
			x	A0085 Exercise judgment when policies are not well-defined.
x	x	x	x	A0083 Evaluate information for reliability, validity, and relevance.

Lessons				
2-1	**2-2**	**2-3**	**2-4**	Identifier
			x	A0074 Collaborate effectively with others.
			x	A0070 Ability to apply critical reading/thinking skills.
			x	A0069 Ability to apply collaborative skills and strategies.
			x	A0067 Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
			x	A0172 Set up a physical or logical sub-networks that separates an internal local area network (lan) from other untrusted networks.
	x		x	A0101 Recognize and mitigate cognitive biases which may affect analysis.

Cybersecurity - National Initiative for Cybersecurity Education

Unit 3

Lessons				
3-1	3-2	3-3	3-4	Identifer
	x	x		A0026 Analyze test data
		x	x	A0062 Monitor measures or indicators of system performance and availability.
		x	x	A0061 Design architectures and frameworks.
x	x	x	x	A0059 Operate the organization's lan/wan pathways.
x	x	x	x	A0058 Execute os command line (e.g., ipconfig, netstat, dir, nbtstat).
x	x	x	x	A0055 Operate common network tools (e.g., ping, traceroute, nslookup).
x	x	x	x	A0052 Operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
x	x	x	x	A0049 Apply secure system design tools, methods and techniques.
x	x	x	x	A0048 Apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
			x	A0041 Use data visualization tools
	x	x		A0040 Translate data and test results into evaluative conclusions

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
x	x	x	x	A0001 Identify systemic security issues based on the analysis of vulnerability and configuration data.
	x	x		A0030 Collect, verify, and validate test data
			x	A0069 Ability to apply collaborative skills and strategies.
	x			A0025 Accurately define incidents, problems, and events
		x	x	A0021 Use and understand complex mathematical concepts (e.g., discrete math, boolean algebra)
	x	x	x	A0019 Produce technical documentation.
x	x	x	x	A0015 Conduct vulnerability scans and recognize vulnerabilities in security systems.
			x	A0014 Communicate effectively when writing.
			x	A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
			x	A0012 Ask clarifying questions
			x	A0011 Answer questions in a clear and concise manner.
x	x	x	x	A0010 Analyze malware.
		x	x	A0003 Determine the validity of technology trend data.

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
	x		x	A0035 Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
x	x	x	x	A0097 Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.
	x			A0172 Set up a physical or logical sub-networks that separates an internal local area network (lan) from other untrusted networks.
x	x	x	x	A0159 Interpret the information collected by network tools (e.g. nslookup, ping, and traceroute).
		x	x	A0155 Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
x	x	x	x	A0128 Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
x	x	x	x	A0127 Ability to deploy continuous monitoring technologies and tools.
		x	x	A0126 Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
	x	x	x	A0124 Establish and maintain automated security control assessments
			x	A0113 Determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.
x	x	x	x	A0107 Think like threat actors.
x	x	x	x	A0106 Ability to think critically.
x	x	x	x	A0065 Monitor traffic flows across the network.

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
		x	x	A0101 Recognize and mitigate cognitive biases which may affect analysis.
			x	A0067 Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
x		x	x	A0096 Ability to interpret and understand complex and rapidly evolving concepts.
		x	x	A0093 Identify/describe techniques/methods for conducting technical exploitation of the target.
		x	x	A0092 Identify/describe target vulnerability.
		x	x	A0086 Expand network access by conducting target analysis and collection to identify targets of interest.
			x	A0085 Exercise judgment when policies are not well-defined.
x	x	x	x	A0084 Evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
x	x	x	x	A0083 Evaluate information for reliability, validity, and relevance.
		x	x	A0080 Develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
			x	A0074 Collaborate effectively with others.
			x	A0070 Ability to apply critical reading/thinking skills.
		x	x	K0158 Know organizational information technology (it) user security policies (e.g., account creation, password rules, access control).

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
			x	A0105

Tailor technical and planning information to a customer’s level of understanding.

Cybersecurity - National Initiative for Cybersecurity Education

Unit 4

Lessons 4-1	4-2	4-3	Identifer	
		x	A0027	Apply an organization's goals and objectives to develop and maintain architecture
x	x		A0001	Identify systemic security issues based on the analysis of vulnerability and configuration data.
x	x		A0062	Monitor measures or indicators of system performance and availability.
		x	A0061	Design architectures and frameworks.
x	x		A0059	Operate the organization's lan/wan pathways.
x	x		A0058	Execute os command line (e.g., ipconfig, netstat, dir, nbtstat).
x	x		A0055	Operate common network tools (e.g., ping, traceroute, nslookup).
x	x		A0052	Operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
		x	A0049	Apply secure system design tools, methods and techniques.
		x	A0048	Apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
x	x		A0043	Conduct forensic analyses in and for both windows and unix/linux environments.

Lessons 4-1	4-2	4-3	Identifer
x			A0042 Develop career path opportunities
x	x		A0067 Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
x	x		A0035 Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
x	x		A0069 Ability to apply collaborative skills and strategies.
	x		A0025 Accurately define incidents, problems, and events
x	x		A0021 Use and understand complex mathematical concepts (e.g., discrete math, boolean algebra)
	x		A0019 Produce technical documentation.
	x		A0015 Conduct vulnerability scans and recognize vulnerabilities in security systems.
	x		A0014 Communicate effectively when writing.
	x		A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
	x		A0012 Ask clarifying questions
	x		A0011 Answer questions in a clear and concise manner.
	x		A0010 Analyze malware.

Lessons 4-1	4-2	4-3	Identifer	
x		x	A0005	Decrypt digital data collections.
x		x	A0003	Determine the validity of technology trend data.
	x	x	A0041	Use data visualization tools
	x	x	A0101	Recognize and mitigate cognitive biases which may affect analysis.
	x		S0052	Use social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
	x	x	A0159	Interpret the information collected by network tools (e.g. nslookup, ping, and traceroute).
	x	x	A0155	Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
		x	A0128	Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
		x	A0127	Ability to deploy continuous monitoring technologies and tools.
	x	x	A0126	Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
		x	A0124	Establish and maintain automated security control assessments
	x		A0123	Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
	x	x	A0120	Share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.

Lessons			
4-1	**4-2**	**4-3**	Identifer
	x	x	A0113 Determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.
	x	x	A0107 Think like threat actors.
	x	x	A0065 Monitor traffic flows across the network.
		x	A0105 Tailor technical and planning information to a customer’s level of understanding.
	x		K0158 Know organizational information technology (it) user security policies (e.g., account creation, password rules, access control).
		x	A0097 Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.
		x	A0096 Ability to interpret and understand complex and rapidly evolving concepts.
	x	x	A0093 Identify/describe techniques/methods for conducting technical exploitation of the target.
	x	x	A0092 Identify/describe target vulnerability.
	x	x	A0086 Expand network access by conducting target analysis and collection to identify targets of interest.
		x	A0085 Exercise judgment when policies are not well-defined.
		x	A0084 Evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
x	x	x	A0083 Evaluate information for reliability, validity, and relevance.

Lessons			
4-1	**4-2**	**4-3**	Identifer
x		x	A0080 Develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
	x	x	A0074 Collaborate effectively with others.
	x	x	A0070 Ability to apply critical reading/thinking skills.
x	x	x	A0106 Ability to think critically.