CCNA Cybersecurity Operations - Chapter 1, Cybersecurity and the Security Operations Center

Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 1.0 Introduction					
1.0.1 Welcome					
1.0.1.1 Chapter 1: Cybersecurity and the Security Operations Center			ITEA.1	IT 08-1	
1.0.1.2 Class Activity - Top Hacker Shows Us How It is Done				CCR.ELA-Literacy.RST.11-12.9.	
Section 1.1 The Danger				IT 08-1	
1.1.1 War Stories				IT 08-1	
1.1.1.1 Hijacked People	K0003, K0004, K0005	HS-ETS1-3.	ITEA.1	IT 08-1	
1.1.1.2 Ransomed Companies	K0003, K0004, K0005	HS-ETS1-3.	ITEA.1	IT 08-1	
1.1.1.3 Targeted Nations	K0003, K0004, K0005	HS-ETS1-3.	ITEA.1	IT 08-1	
1.1.1.4 Lab – Installing the CyberOps Workstation Virtual Machine	K0003, K0004, K0005	HS-ETS1-4.	ITEA.2	CCR.ELA-Literacy.RST.11-12.3.	
1.1.1.5 Lab – Cybersecurity Case Studies	K0003, K0004, K0005	HS-ETS1-4.	ITEA.3	CCR.ELA-Literacy.RST.11-12.3.	
1.1.2 Threat Actors					
1.1.2.1 Amateurs	K0003, K0004, K0005	HS-ETS1-1.	ITEA.2.	IT 08-1	secops(210-255) 1.8.b Threat actor
1.1.2.2 Hacktivists	K0003, K0004, K0005	HS-ETS1-1.	ITEA.2.	IT 08-1	secfnd(210-250) 6.2.a Denial of service secfnd(210-250) 6.2.b Distributed denial of service
1.1.2.3 Financial Gain	K0003, K0004, K0005	HS-ETS1-1.	ITEA.1.M ITEA.2.	IT 08-1	
1.1.2.4 Trade Secrets and Global Politics	K0003, K0004, K0005	HS-ETS1-1.	ITEA.2.	IT 08-1	
1.1.2.5 How Secure is the Internet of Things?	K0003, K0004, K0005	HS-ETS1-1.	ITEA.2.	IT 08-1	
1.1.2.6 Lab – Learning the Details of Attacks	K0003, K0004, K0005		ITEA.2.	CCR.ELA-Literacy.RST.11-12.3.	
1.1.3 Threat Impact					
1.1.3.1 PII and PHI	K0003, K0004, K0005	HS-ETS1-1.	ITEA.3.	IT 04	secops(210-255) 3.7.b HIPAA (Health Insurance Portability and Accountability Act) secfnd(210-250) 2.3.f PII secfnd(210-250) 2.3.g PHI
1.1.3.2 Lost Competitive Advantage	K0003, K0004, K0005	HS-ETS1-1.	ITEA.3.	IT 04	
1.1.3.3 Politics and National Security	K0003, K0004, K0005	HS-ETS1-1.	ITEA.3.	IT 04	
1.1.3.4 Lab – Visualizing the Black Hats	K0003, K0004, K0005		ITEA.3.	CCR.ELA-Literacy.RST.11-12.3.	
Section 1.2 Fighters in the War Against Cybercrime					
1.2.1 The Modern Security Operation Center					
1.2.1.1 Elements of a SOC	S0111, T0136, T0598	HS-ETS1-1.	ITEA.4.	IT 04	
1.2.1.2 People in the SOC	S0111, T0136, T0598	HS-ETS1-1.	ITEA.4.	IT 04	

1.2.1.3 Process in the SOC	S0111, T0136, T0598	HS-ETS1-1.	ITEA.4.	IT 04	
1.2.1.4 Technologies in the SOC	S0111, T0136, T0598	HS-ETS1-1.	ITEA.4.	IT 04	secfnd(210-250) 2.6.c SIEM and log collection
1.2.1.5 Enterprise and Managed Security	S0111, T0136, T0598	HS-ETS1-1.	ITEA.4.	IT 04	
1.2.1.6 Security vs. Availability	S0111, T0136, T0598	HS-ETS1-1.	ITEA.4.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 1.3.c Availability
1.2.1.7 Activity - Identify the SOC Terminology	S0111, T0136, T0598	HS-ETS1-4.	ITEA.4.	CCR.ELA-Literacy.RST.11-12.9.	
1.2.2 Becoming a Defender					
1.2.2.1 Certifications	A0154	HS-ETS1-1.	ITEA.1.	IT 02	
1.2.2.2 Further Education	A0154	HS-ETS1-1.	ITEA.1.	IT 02	
1.2.2.3 Sources of Career Information	A0154	HS-ETS1-1.	ITEA.1.	IT 02	
1.2.2.4 Getting Experience	A0154	HS-ETS1-1.	ITEA.1.	IT 02	
1.2.2.5 Lab – Becoming a Defender	A0154	HS-ETS1-4.	ITEA.1.	CCR.ELA-Literacy.RST.11-12.3.	
1.2.4.5 Packet Tracer - Network Representation	A0154	HS-ETS1-4.	ITEA.1.	CCR.ELA-Literacy.RST.11-12.9.	
Section 1.3 Summary					
1.3.1 Conclusion					
1.3.1.1 Chapter 1: Cybersecurity and the Security Operations Center					

CCNA Cybersecurity Operations - Chapter 2, Windows Operating System

Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 2.0 Introduction					
2.0.1 Welcome					
2.0.1.1 Chapter 2: Windows Operating System			ITEA.2.		
2.0.1.2 Class Activity - Identify Running Processes			ITEA.2.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
Section 2.1 Windows Overview					
2.1.1 Windows History					
2.1.1.1 Disk Operating System	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	
2.1.1.2 Windows Versions	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	
2.1.1.3 Windows GUI	S0267	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	
2.1.1.4 Operating System Vulnerabilities	K0077, K0167, S0158	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secops(210-255) 2.7.c Firewall secfnd(210-250) 4.1.g Services
2.1.2 Windows Architecture and Operations		HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	
2.1.2.1 Hardware Abstraction Layer	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	
2.1.2.2 User Mode and Kernel Mode	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	
2.1.2.3 Windows File Systems	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secops(210-255) 1.4a FAT32 secops(210-255) 1.4b NTFS secops(210-255) 1.4c Alternative Data Streams secops(210-255) 1.4d MACE secops(210-255) 1.4f Free Space secops(210-255) 1.5e MAC
2.1.2.4 Windows Boot Process	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secops(210-255) 1.4e EFI secops(210-255) 1.5c MBR
2.1.2.5 Windows Startup and Shutdown	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secfnd(210-250) 4.1.g Services secfnd(210-250) 4.1.d Windows Registry
2.1.2.6 Processes, Threads, and Services	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secfnd(210-250) 4.1.b Threads secfnd(210-250) 4.1.g Services
2.1.2.7 Memory Allocation and Handles	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secfnd(210-250) 4.1.c Memory allocation secfnd(210-250)4.1.a Processes secfnd(210-250) 4.1.g Services secfnd(210-250) 4.1.f Handles
2.1.2.8 The Windows Registry	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secfnd(210-250) 4.1.d Windows Registry

2.1.2.9 Activity - Identify the Window Registry Hives	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 4.1.d Windows Registry
2.1.2.10 Lab - Exploring Processes, Threads, Handles, and Windows Registry	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.7.	CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 4.1.b Threads secfnd(210-250) 4.1.a Processes secfnd(210-250) 4.1.b Threads secfnd(210-250) 4.1.d Windows Registry secfnd(210-250) 4.1.f Handles secfnd(210-250) 4.1.g Services
Section 2.2 Windows Administration					
2.2.1 Windows Configuration and Monitoring					
2.2.1.1 Run as Administrator	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	
2.2.1.2 Local Users and Domains	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	
2.2.1.3 CLI and PowerShell	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	
2.2.1.4 Windows Management Instrumentation	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 4.1.e WMI secfnd(210-250) 4.1.g Services
2.2.1.5 The net Command	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 4.1.g Services
2.2.1.6 Task Manager and Resource Monitor	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 1.2.b TCP secfnd(210-250) 4.1.a Processes secfnd(210-250) 4.1.b Threads secfnd(210-250) 4.1.f Handles secfnd(210-250) 4.1.g Services
2.2.1.7 Networking	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.d ICMP secfnd(210-250) 1.3.b DNS
2.2.1.8 Accessing Network Resources	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 4.1.g Services
2.2.1.9 Windows Server	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 4.1.g Services
2.2.1.10 Lab - Create User Accounts	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	

2.2.1.11 Lab - Using Windows PowerShell	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.9.	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.3.	
2.2.1.12 Lab - Windows Task Manager	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.9.	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.3.	
2.2.1.13 Lab - Monitor and Manage System Resources in Windows	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.9.	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.3.	
2.2.2 Windows Security					
2.2.2.1 The netstat Command	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secfnd(210-250) 1.2.b TCP
2.2.2.2 Event Viewer	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secfnd(210-250) 4.1.g Services secfnd(210-250) 4.4.a Windows security event logs
2.2.2.3 Windows Update Management	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	
2.2.2.4 Local Security Policy	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secops(210-255) 2.7.c Firewall
2.2.2.5 Windows Defender	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secops(210-255) 2.7.f Antivirus secfnd(210-250) 6.4.b Phishing
2.2.2.6 Windows Firewall	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1	secops(210-255) 2.7.c Firewall
2.2.2.7 Activity - Identify the Windows Command	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	
2.2.2.8 Activity - Identify the Windows Tool	K0224, K0608	HS-ETS1. HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST.11-12.4.	
Section 2.3 Summary					
2.3.1 Conclusion					
2.3.1.1 Chapter 2: Windows Operating System					

CCNA Cybersecurity Operations - Chapter 3, Linux Operating System					
Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 3.0 Introduction					
3.0.1 Welcome					
3.0.1.1 Chapter 3: Linux Operating System			ITEA.9.		
Section 3.1 Linux Overview					
3.1.1 Linux Basics					
3.1.1.1 What is Linux?	K0397, K0608	HS-ETS1.	ITEA.2. ITEA.9. ITEA.17.	IT-NET 1.4 IT 06	
3.1.1.2 The Value of Linux	K0397, K0608	HS-ETS1.	ITEA.9.	IT 06	
3.1.1.3 Linux in the SOC	K0397, K0608	HS-ETS1.	ITEA.9.	IT 06	secfnd(210-250) 2.6.c SIEM and log collection
3.1.1.4 Linux Tools	K0397, K0608	HS-ETS1.	ITEA.9.	IT 06	
3.1.2 Working in the Linux Shell					
3.1.2.1 The Linux Shell	K0397, K0608		ITEA.9.	IT 06	
3.1.2.2 Basic Commands	K0397, K0608	HS-ETS1.	ITEA.2. ITEA.9. ITEA.17.	IT-NET 1.4	
3.1.2.3 File and Directory Commands	K0397, K0608	HS-ETS1.	ITEA.2. ITEA.9. ITEA.17.	IT-NET 1.4	
3.1.2.4 Working with Text Files	K0397, K0608	HS-ETS1.	ITEA.2. ITEA.9. ITEA.17.	IT-NET 1.4	secfnd(210-250) 3.7.g SSH
3.1.2.5 The Importance of Text Files in Linux	K0397, K0608	HS-ETS1.	ITEA.2. ITEA.9. ITEA.17.	IT-NET 1.4	
3.1.2.6 Lab – Working with Text Files in the CLI	K0397, K0608	HS-ETS1.	ITEA.2. ITEA.9. ITEA.17.	IT-NET 1.4 CCR.ELA-Literacy.RST.11-12.3.	
3.1.2.7 Lab – Getting Familiar with the Linux Shell	K0397, K0608		ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	
3.1.3 Linux Servers and Clients					
3.1.3.1 An Introduction to Client-Server Communications	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.1.3.2 Servers, Services, and Their Ports	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.1.3.3 Clients	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.1.3.4 Lab - Linux Servers	K0397, K0608	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	
Section 3.2 Linux Administration					
3.2.1 Basic Server Administration					
3.2.1.1 Service Configuration Files	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.2.1.2 Hardening Devices	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.2.1.3 Monitoring Service Logs	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	secops(210-255) 1.2.d User interaction secfnd(210-250) 4.2.e Daemon

3.2.1.4 Lab – Locating Log Files	K0397, K0608	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	
3.2.2 The Linux File System					
3.2.2.1 The File System Types in Linux	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	secops(210-255) 1.5a EXT4 secops(210-255) 1.5b Journaling secops(210-255) 1.5c MBR secops(210-255) 1.5d Swap File System
3.2.2.2Linux Roles and File Permissions	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	secfnd(210-250) 4.2.c Permissions
3.2.2.3 Hard Links and Symbolic Links	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.2.2.4 Lab - Navigating the Linux Filesystem and Permission Settings	K0397, K0608	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	
Section 3.3 Linux Hosts					
3.3.1 Working with the Linux GUI					
3.3.1.1 X Window System	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.3.1.2 The Linux GUI	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.3.2 Working on a Linux Host					
3.3.2.1 Installing and Running Applications on a Linux Host	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.3.2.2 Keeping the System Up To Date	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.3.2.3 Processes and Forks	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	secfnd(210-250) 4.2.a Processes secfnd(210-250) 4.2.b Forks
3.3.2.4 Malware on a Linux Host	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	secops(210-255) 1.2.a Attack vector secfnd(210-250) 6.5.c Malware
3.3.2.5 Rootkit Check	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	secfnd(210-250) 6.5.d Rootkit
3.3.2.6 Piping Commands	K0397, K0608	HS-ETS1-1.	ITEA.9.	IT 06	
3.3.2.7 Video Demonstration - Applications, Rootkits, and Piping Commands	K0397, K0608	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7.	secfnd(210-250) 6.5.d Rootkit
Section 3.4 Summary					
3.4.1 Conclusion					
3.4.1.1 Linux Operating System					

CCNA Cybersecurity Operations - Chapter 4, Network Protocols and Services					
Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 4.0 Introduction					
4.0.1 Welcome					
4.0.1.1 Chapter 4: Network Protocols and Services					
Section 4.1 Network Protocols					
4.1.1 Network Communications Process					
4.1.1.1 Views of the Network	T0023, T0028, T0153, T0144	HS-ETS1-3.	ITEA.1.L.	IT-NET 3 CCR.ELA-Literacy.RST.11-12.7.	
4.1.1.2 Client-Server Communications	T0043, T0144, T0081	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	
4.1.1.3 A Typical Session: Student	T0043, T0144, T0081	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	
4.1.1.4 A Typical Session: Gamer	T0043, T0144, T0081	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	
4.1.1.5 A Typical Session: Surgeon	T0043, T0144, T0081	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	
4.1.1.6 Tracing the Path	T0043, T0144, T0081	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	
4.1.1.7 Lab - Tracing a Route	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST.11-12.3.	
4.1.2 Communications Protocol					
4.1.2.1 What are Protocols?	T0335 S0158 T0027	HS-ETS1-3.	ITEA.8.H, ITEA.17.L	IT-NET 3	
4.1.2.2 Network Protocol Suites	T0335 S0158 T0027	HS-ETS1-3.	ITEA.8.H, ITEA.17.L	IT-NET 3	secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP
4.1.2.3 The TCP/IP Protocol Suite	K0332, K0565	HS-ETS1-3.	ITEA.8.H, ITEA.17.L	IT-NET 3	secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP
4.1.2.4 Format, Size, and Timing		HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP
4.1.2.5 Unicast, Multicast, and Broadcast	K0061	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	
4.1.2.6 Reference Models		HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	secfnd(210-250) 1.1 Describe the function of the network layers as specified by the OSI and the TCP/IP network models secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP
4.1.2.7 Three Addresses		HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	secfnd(210-250) 1.1 Describe the function of the network layers as specified by the OSI and the TCP/IP network models
4.1.2.8 Encapsulation	T0214	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP secfnd(210-250) 5.3.g Encapsulation
4.1.2.9 Scenario: Sending and Receiving a Web Page		HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP
4.1.2.10 Lab - Introduction to Wireshark		HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3 CCR.ELA-Literacy.RST.11-12.3.	
Section 4.2 Ethernet and Internet Protocol (IP)					

4.2.1 Ethernet					
4.2.1.1 The Ethernet Protocol		HS-ETS1.	ITEA.9.I, ITEA.10.I	IT-NET 3	
4.2.1.2 The Ethernet Frame		HS-ETS1.	ITEA.9.I, ITEA.10.I	IT-NET 3	
4.2.1.3 MAC Address Format	S0094	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	
4.2.1.4 Activity - Ethernet Frame Field Names				CCR.ELA-Literacy.RST.11-12.9.	
4.2.2 IPv4					
4.2.2.1 IPv4 Encapsulation	K0058	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	secfnd(210-250) 5.3.g Encapsulation
4.2.2.2 IPv4 Characteristics	K0059	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP
4.2.2.3 Activity - IPv4 Characteristics	K0060	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	
4.2.2.4 The IPv4 Packet	K0061	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	
4.2.2.5 Video Demonstration - Sample IPv4 Headers in Wireshark	K0061	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0 CCR.ELA-Literacy.RST.11-12.7.	
4.2.3 IPv4 Addressing Basics					
4.2.3.1 IPv4 Address Notation	K0254	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	
4.2.3.2 IPv4 Host Address Structure	K0471	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	
4.2.3.3 IPv4 Subnet Mask and Network Address	K0471	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	
4.2.3.4 Subnetting Broadcast Domains	K0471	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	secfnd(210-250) 1.6 Describe IP subnets and communication within an IP subnet and between IP subnets
4.2.3.5 Video Demonstration - Network, Host, and Broadcast Addresses				CCR.ELA-Literacy.RST.11-12.7.	
4.2.4 Types of IPv4 Addresses					
4.2.4.1 IPv4 Address Classes and Default Subnet Masks	K0471	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	
4.2.4.2 Reserved Private Addresses	K0471	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	
4.2.5 The Default Gateway					
4.2.5.1 Host Forwarding Decision	K0011	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	
4.2.5.2 Default Gateway	K0011	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.3.c DHCP
4.2.5.3 Using the Default Gateway	K0011	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	
4.2.6 IPv6					
4.2.6.1 Need for IPv6	K0185	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	

4.2.6.2 IPv6 Size and Representation	K0186	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	
4.2.6.3 IPv6 Address Formatting	K0187	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	
4.2.6.4 IPv6 Prefix Length	K0188	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	
4.2.6.5 Activity - IPv6 Address Notation	K0185	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3 CCR.ELA-Literacy.WHST.11-12.9.	
4.2.6.6 Video Tutorial - Layer 2 and Layer 3 Addressing	K0185	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3 CCR.ELA-Literacy.WHST.11-12.7.	
Section 4.3 Connectivity Verification					
4.3.1 ICMP					
4.3.1.1 ICMPv4 Messages	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	secfnd(210-250) 1.2.d ICMP
4.3.1.2 ICMPv6 RS and RA Messages	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	secfnd(210-250) 1.2.d ICMP
4.3.2 Ping and Traceroute Utilities					
4.3.2.1 Ping - Testing the Local Stack	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	
4.3.2.2 Ping - Testing Connectivity to the Local LAN	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	
4.3.2.3 Ping - Testing Connectivity to Remote Host	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	
4.3.2.4 Traceroute - Testing the Path	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	
4.3.2.5 ICMP Packet Format	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	secops(210-255) 1.2.a Attack vector secfnd(210-250) 1.2.d ICMP
Section 4.4 Address Resolution Protocol					
4.4.1 MAC and IP					
4.4.1.1 Destination on Same Network		HS-ETS1.	ITEA.17.	IT-NET 3	secops(210-255) 2.2.a Ethernet frame
4.4.1.2 Destination on Remote Network		HS-ETS1.	ITEA.17.	IT-NET 3	secops(210-255) 2.2.a Ethernet frame
4.4.2 ARP					
4.4.2.1 Introduction to ARP		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.3.a ARP
4.4.2.2 ARP Functions		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.3.a ARP
4.4.2.3 Video - ARP Operation - ARP Request		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST.11-12.7.	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.3.a ARP
4.4.2.4 Video - ARP Operation - ARP Reply		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST.11-12.7.	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.3.a ARP
4.4.2.5 Video - ARP Role in Remote Communication		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST.11-12.7.	secfnd(210-250) 1.3.a ARP
4.4.2.6 Removing Entries from an ARP Table		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	secfnd(210-250) 1.3.a ARP
4.4.2.7 ARP Tables on Networking Devices		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	secfnd(210-250) 1.3.a ARP
4.4.2.8 Lab - Using Wireshark to Examine Ethernet Frames					secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.3.a ARP
4.4.3 ARP Issues					

4.4.3.1 ARP Broadcasts		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	secfnd(210-250) 1.3.a ARP
4.4.3.2 ARP Spoofing		HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	secfnd(210-250) 1.3.a ARP
Section 4.5 The Transport Layer					
4.5.1 Transport Layer Characteristics					
4.5.1.1 Transport Layer Protocol Role in Network Communication	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	secops(210-255) 1.4c Alternative Data Streams
4.5.1.2 Transport Layer Mechanisms	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
4.5.1.3 TCP Local and Remote Ports	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
4.5.1.4 Socket Pairs	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.2.a IP
4.5.1.5 TCP vs UDP	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
4.5.1.6 TCP and UDP Headers	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
4.5.1.7 Activity - TCP and UDP Characteristics	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.4.	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
4.5.2 Transport Layer Operation					
4.5.2.1 TCP Port Allocation	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	secfnd(210-250) 1.2.b TCP
4.5.2.2 A TCP Session Part I: Connection Establishment and Termination	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	secfnd(210-250) 1.2.b TCP
4.5.2.3 Video Demonstration - TCP 3-Way Handshake	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.7.	secfnd(210-250) 1.2.b TCP
4.5.2.4 Lab - Using Wireshark to Observe the TCP 3-Way Handshake	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 1.2.b TCP
4.5.2.5 Activity - TCP Connection Process	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 1.2.b TCP
4.5.2.6 A TCP Session Part II: Data Transfer	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	secfnd(210-250) 1.2.b TCP
4.5.2.7 Video Demonstration - Sequence Numbers and Acknowledgments	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.7.	secfnd(210-250) 1.2.b TCP
4.5.2.8 Video Demonstration - Data Loss and Retransmission	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.7.	secfnd(210-250) 1.2.b TCP
4.5.2.9 A UDP Session	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
4.5.2.10 Lab - Exploring Nmap	K0332	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST.11-12.8.	
Section 4.6 Network Services					
4.6.1 DHCP					
4.6.1.1 DHCP Overview	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.3.c DHCP
4.6.1.2 DHCPv4 Message Format	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.3.c DHCP
4.6.2 DNS					
4.6.2.1 DNS Overview	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.2.c UDP secfnd(210-250) 1.3.b DNS
4.6.2.2 The DNS Domain Hierarchy	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.3.b DNS
4.6.2.3 The DNS Lookup Process	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.3.b DNS

4.6.2.4 DNS Message Format	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.2.c UDP secfnd(210-250) 1.3.b DNS
4.6.2.5 Dynamic DNS	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.3.b DNS
4.6.2.6 The WHOIS Protocol	K0332	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 1.3.b DNS
4.6.2.7 Lab - Using Wireshark to Examine a UDP DNS Capture	K0221	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST.11-12.8.	secfnd(210-250) 1.2.c UDP secfnd(210-250) 1.3.b DNS
4.6.3 NAT					
4.6.3.1 NAT Overview	S0192		ITEA.9.		secfnd(210-250) 5.3.b NAT/PAT
4.6.3.2 NAT-Enabled Routers	S0192		ITEA.9.		secfnd(210-250) 5.3.b NAT/PAT
4.6.3.3 Port Address Translation	S0192		ITEA.9.		secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP secfnd(210-250) 5.3.b NAT/PAT
4.6.4 File Transfer and Sharing Services					
4.6.4.1 FTP and TFTP	K0452	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.4.2 SMB	K0452	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.4.3 Lab - Using Wireshark to Examine TCP and UDP Captures	K0452	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.b TCP secfnd(210-250) 1.2.c UDP
4.6.5 Email					
4.6.5.1 Email Overview	K0444	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.5.2 SMTP	K0444	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.5.3 POP3	K0444	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.5.4 IMAP	K0444	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.6 HTTP					
4.6.6.1 HTTP Overview	K0444	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.6.2 The HTTP URL	K0444	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.6.3 The HTTP Protocol	K0444	HS-ETS1.	ITEA.2	IT-NET 3	secfnd(210-250) 3.7.h SSL/TLS
4.6.6.4 HTTP Status Codes	K0444	HS-ETS1.	ITEA.2	IT-NET 3	
4.6.6.5 Lab - Using Wireshark to Examine HTTP and HTTPS Traffic	K0332	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST.11-12.8.	
Section 4.7 Summary					
4.7.1 Conclusion					
4.7.1.1 Chapter 4: Network Protocols and Services					

CCNA Cybersecurity Operations - Chapter 5, Network Infrastructure

Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 5.0 Introduction					
5.0.1 Welcome					
5.0.1.1 Chapter 5, Network Infrastructure					
Section 5.1 Network Communication Devices					
5.1.1 Network Devices					
5.1.1.1 End Devices	T0126, T0104, T0335, T0129	HS-ETS1-3.	ITEA.17.O.	IT-NET 3	
5.1.1.2 Video Tutorial - End Devices	T0126, T0104, T0335, T0129	HS-ETS1-3.	ITEA.17.O.	IT-NET 3 CCR.ELA-Literacy.RST.11-12.7.	
5.1.1.3 Routers			ITEA.9.		secfnd(210-250) 1.4.a Router
5.1.1.4 Activity - Match Layers			ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	
5.1.1.5 Router Operation	K0011	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.4.a Router secfnd(210-250) 1.6 Describe IP subnets and communication within an IP subnet and between IP subnets
5.1.1.6 Routing Information	K0011	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	secfnd(210-250) 1.4.a Router
5.1.1.7 Video Tutorial - Static and Dynamic Routing			ITEA.9.	CCR.ELA-Literacy.RST.11-12.7.	
5.1.1.8 Hubs, Bridges, LAN Switches	T0035	HS-PS3-3., HS-PS4-5.	ITEA.17.O	IT-NET 3	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.4.b Switch secfnd(210-250) 1.4.c Hub secfnd(210-250) 1.4.d Bridge
5.1.1.9 Switching Operation	T0035	HS-PS3-3., HS-PS4-5.	ITEA.17.O	IT-NET 3	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.4.b Switch
5.1.1.10 Video Tutorial - MAC Address Tables on Connected Switches			ITEA.9.	CCR.ELA-Literacy.RST.11-12.7.	secfnd(210-250) 1.4.b Switch
5.1.1.11 VLANs	K0443			IT-NET 3.7	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.4.a Router secfnd(210-250) 1.4.b Switch secfnd(210-250) 1.7 Describe the relationship between VLANs and data visibility
5.1.1.12 STP	K0011	HS-ETS1.	ITEA.2.	IT-NET 3	secfnd(210-250) 1.4.b Switch
5.1.1.13 Multilayer Switching	K0011	HS-ETS1.	ITEA.8.	IT-NET 1	secfnd(210-250) 1.4.a Router
5.1.2 Wireless Communications					
5.1.2.1 Video Tutorial - Wireless Communications	K0108, K0274		ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	
5.1.2.2 Protocols and Features	K0108, K0274	HS-ETS1-2.	ITEA.11.	IT-NET 3	secops(210-255) 2.2.a Ethernet frame secfnd(210-250) 1.4.e Wireless access point (WAP) secfnd(210-250) 3.9.d Protocol version
5.1.2.3 Wireless Network Operations	K0108, K0274	HS-ETS1-4.	ITEA.8.	IT-NET 3	secfnd(210-250) 1.4.a Router
5.1.2.4 The Client to AP Association Process	K0108, K0274	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.1.2.5 Activity - Order the Steps in the Client and AP Association	K0108, K0274	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
5.1.2.6 Wireless Devices - AP, LWAP, WLC	K0108, K0274	HS-ETS1-4.	ITEA.8.	IT-NET 3	secfnd(210-250) 1.4.a Router secfnd(210-250) 1.4.b Switch secfnd(210-250) 1.4.e Wireless access point (WAP) secfnd(210-250) 1.4.f Wireless LAN controller (WLC)
5.1.2.7 Activity - Identify the LAN Device	K0108, K0274	HS-ETS1-4.		CCR.ELA-Literacy.RST.11-12.9.	
Section 5.2 Network Security Infrastructure					
5.2.1 Security Devices					

5.2.1.1 Video Tutorial - Security Devices	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	
5.2.1.2 Firewalls	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.c Firewall
5.2.1.3 Firewall Type Descriptions	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.c Firewall secfnd(210-250) 1.4.a Router secfnd(210-250) 1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices secfnd(210-250) 1.9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation secfnd(210-250) 5.1.d Traditional stateful firewall
5.2.1.4 Packet Filtering Firewalls	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.c Firewall secfnd(210-250) 1.4.a Router secfnd(210-250) 1.9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation
5.2.1.5 Stateful Firewalls	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.c Firewall secfnd(210-250) 1.9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation secfnd(210-250) 5.1.d Traditional stateful firewall
5.2.1.6 Next-Generation Firewalls	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.c Firewall secfnd(210-250) 5.1.c Next-Gen firewall
5.2.1.7 Activity - Identify the Type of Firewall	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 2.7.c Firewall
5.2.1.8 Intrusion Prevention and Detection Devices	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.b IDS / IPS secfnd(210-250) 1.4.a Router secfnd(210-250) 4.3.a Host-based intrusion detection
5.2.1.9 Advantages and Disadvantages of IDS and IPS	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.b IDS / IPS
5.2.1.10 Types of IPS	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.b IDS / IPS secops(210-255) 2.7.c Firewall
5.2.1.11 Specialized Security Appliances	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 1.1 AMP Threat Grid secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secfnd(210-250) 1.5.c Cisco Advanced Malware Protection (AMP) secfnd(210-250) 1.5.d Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS) secfnd(210-250) 1.5.e Email Security Appliance (ESA) / Cisco Cloud Email Security (CES)
5.2.1.12 Activity - Compare IDS and IPS Characteristics	T0696, S0084, S0192	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 2.7.b IDS / IPS
5.2.2 Security Services					
5.2.2.1 Video Tutorial - Security Services	K0158	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	
5.2.2.2 Traffic Control with ACLs	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	secfnd(210-250) 1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices secfnd(210-250) 5.3.a Access control list
5.2.2.3 ACLs: Important Features	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	secfnd(210-250) 1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices secfnd(210-250) 5.3.a Access control list
5.2.2.4 Packet Tracer - ACL Demonstration	K0158	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 5.3.a Access control list
5.2.2.5 SNMP	K0452, K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.2.2.6 NetFlow	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow secfnd(210-250) 5.1.b NetFlow
5.2.2.7 Port Mirroring	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.2.2.8 Syslog Servers	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	secfnd(210-250) 4.4.b Unix-based syslog
5.2.2.9 NTP	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.2.2.10 AAA Servers	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.2.2.11 VPN	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	secfnd(210-250) 5.3.c Tunneling

5.2.2.12 Activity - Identify the Network Security Device or Service	K0158	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
Section 5.3 Network Representations					
5.3.1 Network Topology					
5.3.1.1 Overview of Network Components	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	secfnd(210-250) 1.4.a Router secfnd(210-250) 1.4.b Switch
5.3.1.2 Physical and Logical Topologies	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.3.1.3 WAN Topologies	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.3.1.4 LAN Topologies	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.3.1.5 The Three-Layer Network Design Model	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	
5.3.1.6 Video Tutorial - Three-Layer Network Design	K0179, K0486	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	
5.3.1.7 Common Security Architectures	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	secops(210-255) 2.7.c Firewall secfnd(210-250) 1.4.a Router
5.3.1.8 Activity - Identify the Network Topology	K0179, K0486	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
5.3.1.9 Activity - Identify Features of Network Design Layers	K0179, K0486	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
5.3.1.10 Packet Tracer - Identify Packet Flow	K0179, K0486	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
Section 5.4 Summary					
5.4.1 Conclusion					
5.4.1.1 Chapter 5, Network Infrastructure					

CCNA Cybersecurity Operations - Chapter 6, Principles of Network Security					
Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 6.0 Introduction					
6.0.1 Welcome					
6.0.1.1 Chapter 6, Principles of Network Security					
Section 6.1 Attackers and Their Tools					
6.1.1 Who is Attacking Our Network?					
6.1.1.1 Threat, Vulnerability, and Risk	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.a Assets secfnd(210-250) 2.2 Compare and contrast Risk, Threat, Vulnerability, Exploit secfnd(210-250) 6.1 Compare and contrast an attack surface and vulnerability secfnd(210-250) 6.8 Compare and contrast remote exploit and a local exploit
6.1.1.2 Hacker vs. Threat Actor	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 2.3.a Threat actor
6.1.1.3 Evolution of Threat Actors	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.1.1.4 Cybercriminals	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.1.1.5 Cybersecurity Tasks	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.1.1.6 Cyber Threat Indicators	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.1.1.7 Activity - What Color is my Hat?	K0005, K0049	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
6.1.2 Threat Actor Tools					
6.1.2.1 Introduction of Attack Tools	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 10	
6.1.2.2 Evolution of Security Tools	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.1.2.3 Categories of Attacks	K0005, K0049	HS-ETS1-3.	ITEA.8.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.1.2.4 Activity - Classify Hacking Tools	K0005, K0049	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
Section 6.2 Common Threats and Attacks					
6.2.1 Malware					
6.2.1.1 Types of Malware	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.5.c Malware
6.2.1.2 Viruses	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.5.c Malware
6.2.1.3 Trojan Horses	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.5.c Malware
6.2.1.4 Trojan Horse Classification	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.2.a Denial of service
6.2.1.5 Worms	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.2.a Denial of service
6.2.1.6 Worm Components	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.2.a Denial of service
6.2.1.7 Ransomware	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.4.a Social engineering secfnd(210-250) 6.5.c Malware
6.2.1.8 Other Malware	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.4.b Phishing secfnd(210-250) 6.5.c Malware

6.2.1.9 Common Malware Behaviors	K0480	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 2.7.c Firewall secops(210-255) 2.7.f Antivirus secfnd(210-250) 6.5.c Malware
6.2.1.10 Activity - Identify the Malware Type	K0480	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 6.5.c Malware
6.2.1.11 Lab - Anatomy of Malware	K0480	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 6.5.c Malware
6.2.2 Common Network Attacks					
6.2.2.1 Types of Network Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.5.c Malware
6.2.2.2 Reconnaissance Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secops(210-255) 4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.5.f Host profiling
6.2.2.3 Sample Reconnaissance Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.2.2.4 Access Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.2.2.5 Types of Access Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 1.3.c DHCP secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.2.c Man-in-the-middle secfnd(210-250) 6.4.a Social engineering
6.2.2.6 Social Engineering Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.4.b Phishing secfnd(210-250) 6.4.a Social engineering
6.2.2.7 Phishing Social Engineering Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.4.b Phishing secfnd(210-250) 6.4.a Social engineering
6.2.2.8 Strengthening the Weakest Link	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
6.2.2.9 Lab – Social Engineering	K0005	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.4.a Social engineering
6.2.2.10 Denial of Service Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.2.a Denial of service
6.2.2.11 DDoS Attacks	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor secfnd(210-250) 6.2.b Distributed denial of service secfnd(210-250) 6.5.b Command and control (C2) secfnd(210-250) 6.5.c Malware
6.2.2.12 Example DDoS Attack	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.2.b Distributed denial of service
6.2.2.13 Buffer Overflow Attack	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secfnd(210-250) 6.2.a Denial of service secfnd(210-250) 6.5.a Buffer overflows
6.2.2.14 Evasion Methods	K0005	HS-ETS1-3.	ITEA.8.	IT 08 1	secops(210-255) 2.7.c Firewall secfnd(210-250) 5.3.c Tunneling secfnd(210-250) 6.4.c Evasion methods secfnd(210-250) 6.5.d Rootkit secfnd(210-250) 6.6 Describe these evasion methods

6.2.2.15 Activity - Identify the Types of Network Attack	K0005	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
6.2.2.16 Activity - Components of a DDoS Attack	K0005	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.3.a Threat actor
Section 6.3 Summary					
6.3.1 Conclusion					
6.3.1.1 Chapter 6, Principles of Network Security					

CCNA Cybersecurity Operations - Chapter 7, Network Attacks: A Deeper Look

Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 7.0 Introduction					
7.0.1 Welcome					
7.0.1.1 Chapter 7, Network Attacks: A Deeper Look		HS-ETS1-1.	ITEA.9.		
7.0.1.2 Class Activity – What's Going On?		HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	
Section 7.1 Network Monitoring and Tools					
7.1.1 Introduction to Network Monitoring					
7.1.1.1 Network Security Topology		HS-ETS1-1.	ITEA.9.	IT 10	
7.1.1.2 Network Monitoring Methods	K0180	HS-ETS1-1.	ITEA.9.	IT 10	secops(210-255) 2.7.a NetFlow secfnd(210-250) 1.11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic
7.1.1.3 Network Taps	K0180	HS-ETS1-1.	ITEA.9.	IT 10	secops(210-255) 2.7.c Firewall secfnd(210-250) 1.11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic
7.1.1.4 Traffic Mirroring and SPAN	K0180	HS-ETS1-1.	ITEA.9.	IT 10	
7.1.2 Introduction to Network Monitoring Tools					
7.1.2.1 Network Security Monitoring Tools	K0180	HS-ETS1-1.	ITEA.9.	IT 10	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow secfnd(210-250) 2.6.c SIEM and log collection secfnd(210-250) 5.1.a TCP Dump
7.1.2.2 Network Protocol Analyzers	K0180	HS-ETS1-1.	ITEA.9.	IT 10	secops(210-255) 2.5 Extract files from a TCP stream when given a PCAP file and Wireshark secfnd(210-250) 5.1.a TCP Dump
7.1.2.3 NetFlow	K0180	HS-ETS1-1.	ITEA.9.	IT 10	secops(210-255) 2.7.a NetFlow secfnd(210-250) 5.1.b NetFlow
7.1.2.4 SIEM	K0180	HS-ETS1-1.	ITEA.9.	IT 10	secfnd(210-250) 2.6.c SIEM and log collection
7.1.2.5 SIEM Systems	K0180	HS-ETS1-1.	ITEA.9.	IT 10	secfnd(210-250) 2.6.c SIEM and log collection
7.1.2.6 Activity - Identify the Network Monitoring	K0180	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 2.6.c SIEM and log collection
7.1.2.7 Packet Tracer - Logging Network Activity	K0180	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 4.4.b Unix-based syslog
Section 7.2 Attacking the Foundation					
7.2.1 IP Vulnerabilities					
7.2.1.1 IPv4 and IPv6	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secops(210-255) 2.2.b IPv4 secops(210-255) 2.2.c IPv6 secfnd(210-250) 1.2.a IP
7.2.1.2 The IPv4 Packet Header	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 2.2.b IPv4 secops(210-255) 2.2.f ICMP secfnd(210-250) 1.2.a IP
7.2.1.3 The IPv6 Packet Header	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 2.2.c IPv6
7.2.1.4 IP Vulnerabilities	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secops(210-255) 2.2.b IPv4 secops(210-255) 2.2.c IPv6 secops(210-255) 2.2.f ICMP secfnd(210-250) 1.2.a IP secfnd(210-250) 1.2.d ICMP secfnd(210-250) 6.2.a Denial of service secfnd(210-250) 6.2.b Distributed denial of service secfnd(210-250) 6.2.c Man-in-the-middle
7.2.1.5 ICMP Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secops(210-255) 2.2.b IPv4 secops(210-255) 2.2.c IPv6 secops(210-255) 2.2.f ICMP
7.2.1.6 DoS Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secops(210-255) 2.2.f ICMP secfnd(210-250) 6.2.a Denial of service secfnd(210-250) 6.2.b Distributed denial of service
7.2.1.7 Amplification and Reflection Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secops(210-255) 2.2.f ICMP

7.2.1.8 DDoS Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 2.2.g HTTP secops(210-255) 4.7 Map DNS logs and HTTP logs together to find a threat actor secops(210-255) 4.8 Map DNS, HTTP, and threat intelligence data together secfnd(210-250) 6.2.a Denial of service secfnd(210-250) 6.2.b Distributed denial of service
7.2.1.9 Address Spoofing Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor
7.2.1.10 Activity - Identify the IP Vulnerability	K0005, K0009	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 1.2.a IP
7.2.2 TCP and UDP Vulnerabilities					
7.2.2.1 TCP	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secfnd(210-250) 1.2.b TCP
7.2.2.2 TCP Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secops(210-255) 2.2.d TCP
7.2.2.3 UDP and UDP Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 2.2.d TCP secops(210-255) 2.2.e UDP
Section 7.3 Attacking What We Do					
7.3.1 IP Services					
7.3.1.1 ARP Vulnerabilities	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secfnd(210-250) 1.3.a ARP
7.3.1.2 ARP Cache Poisoning	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secfnd(210-250) 1.3.a ARP
7.3.1.3 DNS Attacks	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secops(210-255) 4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains secfnd(210-250) 1.3.b DNS secfnd(210-250) 6.2.a Denial of service secfnd(210-250) 6.2.b Distributed denial of service secfnd(210-250) 6.5.c Malware
7.3.1.4 DNS Tunneling	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secfnd(210-250) 1.3.b DNS secfnd(210-250) 5.3.c Tunneling
7.3.1.5 DHCP	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains secfnd(210-250) 1.3.b DNS
7.3.1.6 Lab - Exploring DNS Traffic	K0005, K0009	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 1.3.b DNS
7.3.2 Enterprise Services					
7.3.2.1 HTTP and HTTPS	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor
7.3.2.2 Email	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor
7.3.2.3 Web-Exposed Databases	K0005, K0009	HS-ETS1-2.	ITEA.9.	IT 8	secops(210-255) 1.8.b Threat actor secfnd(210-250) 6.3 Describe these web application attacks
7.3.2.4 Lab - Attacking a MySQL Database	K0005, K0009	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	
7.3.2.5 Lab - Reading Server Logs	K0005, K0009	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 4.4.b Unix-based syslog
Section 7.4 Summary					
7.4.1 Conclusion					
7.4.1.1 Chapter 7, Network Attacks: A Deeper Look					

CCNA Cybersecurity Operations - Chapter 8, Protecting the Network

Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 8.0 Introduction					
8.0.1 Welcome					
8.0.1.1 Chapter 8: Protecting the Network	K0005, K0009	HS-ETS1-3.	ITEA.17.		
Section 8.1 Understanding Defense	K0005, K0009				
8.1.1 Defense-in-Depth	K0005, K0009				
8.1.1.1 Assets, Vulnerabilities, Threats	K0005, K0009	HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.a Assets
8.1.1.2 Identify Assets	K0005, K0009	HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.a Assets secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.7.a Asset management secfnd(210-250) 6.1 Compare and contrast an attack surface and vulnerability
8.1.1.3 Identify Vulnerabilities	K0005, K0009	HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.a Assets
8.1.1.4 Identify Threats	K0005, K0009	HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.a Assets secops(210-255) 2.7.c Firewall
8.1.1.5 Security Onion and Security Artichoke Approaches	K0005, K0009	HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.b Threat actor
8.1.2 Security Policies					
8.1.2.1 Business Policies	K0009, K0158	HS-ETS1-3.	ITEA.17.	IT 08 2	
8.1.2.2 Security Policy	K0009, K0158	HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.a Assets secops(210-255) 5.3 Define these activities as they relate to incident handling
8.1.2.3 BYOD Policies	K0009, K0158	HS-ETS1-3.	ITEA.17.	IT 08 2	
8.1.2.4 Regulatory and Standard Compliance	K0009, K0158	HS-ETS1-3.	ITEA.17.	IT 08 2	
Section 8.2 Access Control					
8.2.1 Access Control Concepts					
8.2.1.1 Communications Security: CIA		HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secops(210-255) 1.3.c Availability
8.2.1.2 Access Control Models		HS-ETS1-3.	ITEA.17.	IT 08 2	secfnd(210-250) 2.4.a Principle of least privilege secfnd(210-250) 2.5.a Discretionary access control secfnd(210-250) 2.5.b Mandatory access control secfnd(210-250) 2.5.c Nondiscretionary access control secfnd(210-250) 6.7 Define privilege escalation
8.2.1.3 Activity - Identify the Access Control Model		HS-ETS1-3.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
8.2.2 AAA Usage and Operations					
8.2.2.1 AAA Operation		HS-ETS1-3.	ITEA.17.	IT 08 2	
8.2.2.2 AAA Authentication		HS-ETS1-3.	ITEA.17.	IT 08 2	
8.2.2.3 AAA Accounting Logs		HS-ETS1-3.	ITEA.17.	IT 08 2	
8.2.2.4 Activity - Identify the Characteristic of AAA		HS-ETS1-3.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
Section 8.3 Threat Intelligence					
8.3.1 Information Sources					
8.3.1.1 Network Intelligence Communities		HS-ETS1-3.	ITEA.17.	IT 08 2	
8.3.1.2 Cisco Cybersecurity Reports		HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.b Threat actor
8.3.1.3 Security Blogs and Podcasts		HS-ETS1-3.	ITEA.17.	IT 08 2	
8.3.2 Threat Intelligence Services					
8.3.2.1 Cisco Talos		HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 2.7.c Firewall
8.3.2.2 FireEye		HS-ETS1-3.	ITEA.17.	IT 08 2	secfnd(210-250) 6.5.c Malware
8.3.2.3 Automated Indicator Sharing		HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains
8.3.2.4 Common Vulnerabilities and Exposures Database		HS-ETS1-3.	ITEA.17.	IT 08 2	
8.3.2.5 Threat Intelligence Communication Standards		HS-ETS1-3.	ITEA.17.	IT 08 2	secops(210-255) 1.8.a Assets secops(210-255) 1.8.b Threat actor
8.3.2.6 Activity - Identify the Threat Intelligence Information Source		HS-ETS1-3.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
Section 8.4 Summary					
8.4.1 Conclusion					
8.4.1.1 Chapter 8, Protecting the Network					secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secops(210-255) 1.3.c Availability

CCNA Cybersecurity Operations - Chapter 9, Cryptography and the Public Key Infrastructure					
Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 9.0 Introduction					
9.0.1 Welcome					
9.0.1.1 Chapter 9, Cryptography and the Public Key Infrastructure		HS-ETS1-4.	ITEA.8.		
9.0.1.2 Class Activity – Creating Codes		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	
9.1 Cryptography					
9.1.1 What is Cryptography?					
9.1.1.1 Securing Communications	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.1 AMP Threat Grid secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secops(210-255) 1.5.a Firewall secfnd(210-250) 1.5.b Cisco Intrusion Prevention System (IPS) secfnd(210-250) secfnd(210-250) 1.5.c Cisco Advanced Malware Protection (AMP) secfnd(210-250) 1.5.d Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS) secfnd(210-250) 1.5.e Email Security Appliance (ESA) / Cisco Cloud Email Security (CES) secfnd(210-250) 3.1 Describe the uses of a hash algorithm secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 3.6.a MD5
9.1.1.2 Cryptology	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.8 Describe how the success or failure of a cryptographic exchange impacts security investigation
9.1.1.3 Cryptography - Ciphers	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.8 Describe how the success or failure of a cryptographic exchange impacts security investigation
9.1.1.4 Cryptanalysis - Code Breaking	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.8 Describe how the success or failure of a cryptographic exchange impacts security investigation
9.1.1.5 Keys	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secfnd(210-250) 3.2 Describe the uses of encryption algorithms
9.1.1.6 Lab - Encrypting and Decrypting Data Using OpenSSL	K0403	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	
9.1.1.7 Lab - Encrypting and Decrypting Data Using a Hacker Tool	K0403	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	
9.1.1.8 Lab - Examining Telnet and SSH in Wireshark	K0403	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 3.7.g SSH
9.1.2 Integrity and Authenticity					
9.1.2.1 Cryptographic Hash Functions	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.b Integrity
9.1.2.2 Cryptographic Hash Operation	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.1 Describe the uses of a hash algorithm
9.1.2.3 MD5 and SHA	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.b Integrity secfnd(210-250) 3.1 Describe the uses of a hash algorithm 3.6.a MD5 3.6.b SHA-1 3.6.c SHA-256 3.6.d SHA-512
9.1.2.4 Hash Message Authentication Code	K0403	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.b Integrity secfnd(210-250) 3.1 Describe the uses of a hash algorithm secfnd(210-250) 3.6.a MD5
9.1.2.5 Lab – Hashing Things Out	K0403	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	
9.1.3 Confidentiality					
9.1.3.1 Encryption	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.a Confidentiality secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 5.3.e Encryption

9.1.3.2 Symmetric Encryption	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 5.3.e Encryption
9.1.3.3 Symmetric Encryption Algorithms	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 3.7.a DES 3.7.b 3DES 3.7.c AES 3.7.d AES256-CTR 3.7.e RSA 3.7.f DSA 3.7.g SSH secfnd(210-250) 5.3.e Encryption 3.7.h SSL/TLS secfnd(210-250) 3.7.h SSL/TLS
9.1.3.4 Asymmetric Encryption Algorithms	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 3.7.g SSH secfnd(210-250) 3.7.h SSL/TLS secfnd(210-250) 3.8 Describe how the success or failure of a cryptographic exchange impacts security investigation
9.1.3.5 Asymmetric Encryption - Confidentiality	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.a Confidentiality secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms
9.1.3.6 Asymmetric Encryption - Authentication	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms
9.1.3.7 Asymmetric Encryption - Integrity	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 5.3.e Encryption
9.1.3.8 Diffie-Hellman	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 3.7.g SSH
9.1.3.9 Activity - Classify the Encryption Algorithms	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 3.3 Compare and contrast symmetric and asymmetric encryption algorithms secfnd(210-250) 5.3.e Encryption
Section 9.2 Public Key Infrastructure					
9.2.1 Public Key Cryptography					

9.2.1.1 Using Digital Signatures	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.b Integrity secops(210-255) 3.8 Identify data elements that must be protected with regards to a specific standard (PCI-DSS) secfnd(210-250) 3.4 Describe the processes of digital signature creation and verification secfnd(210-250) 3.7.f DSA secfnd(210-250) 3.7.e RSA secfnd(210-250) 3.9.e PKCS
9.2.1.2 Digital Signatures for Code Signing	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.b Integrity secfnd(210-250) 3.4 Describe the processes of digital signature creation and verification
9.2.1.3 Digital Signatures for Digital Certificates	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secfnd(210-250) 3.4 Describe the processes of digital signature creation and verification
9.2.2 Authorities and the PKI Trust System					
9.2.2.1 Public Key Management	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.5 Describe the operation of a PKI
9.2.2.2 The Public Key Infrastructure	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.5 Describe the operation of a PKI
9.2.2.3 The PKI Authorities System	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.5 Describe the operation of a PKI
9.2.2.4 The PKI Trust System	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.5 Describe the operation of a PKI
9.2.2.5 Interoperability of Different PKI Vendors	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.5 Describe the operation of a PKI
9.2.2.6 Certificate Enrollment, Authentication, and Revocation	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.5 Describe the operation of a PKI secfnd(210-250) 3.9.b X.509 certificates
9.2.2.7 Lab – Certificate Authority Stores	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	secfnd(210-250) 3.5 Describe the operation of a PKI secfnd(210-250) 6.2.c Man-in-the-middle
9.2.3 Applications and Impacts of Cryptography					
9.2.3.1 PKI Applications	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 3.5 Describe the operation of a PKI secfnd(210-250) 3.7.h SSL/TLS
9.2.3.2 Encrypting Network Transactions	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 3.5 Describe the operation of a PKI secfnd(210-250) 3.7.h SSL/TLS secfnd(210-250) 3.9.a Cipher-suite secfnd(210-250) 3.9.c Key exchange secfnd(210-250) 5.3.e Encryption
9.2.3.3 Encryption and Security Monitoring	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	secfnd(210-250) 1.5.b Cisco Intrusion Prevention System (IPS) secfnd(210-250) 3.2 Describe the uses of encryption algorithms secfnd(210-250) 5.3.e Encryption
Section 9.3 Summary					
9.3.1 Conclusion					
9.3.1.1 Chapter 9, Cryptography and the Public Key Infrastructure					secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity

CCNA Cybersecurity Operations - Chapter 10, Endpoint Security and Analysis					
Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 10.0 Introduction					
10.0.1 Welcome					
10.0.1.1 Chapter 10, Endpoint Security and Analysis			ITEA.10.		
Section 10.1 Endpoint Protection					
10.1.1 Antimalware Protection					
10.1.1.1 Endpoint Threats	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 6.5.c Malware
10.1.1.2 Endpoint Security	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 6.5.c Malware
10.1.1.3 Host-Based Malware Protection	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 2.7.c Firewall secops(210-255) 2.7.f Antivirus secfnd(210-250) 2.6.a Network and host antivirus secfnd(210-250) 2.6.b Agentless and agent-based protections secfnd(210-250) 4.3.b Antimalware and antivirus secfnd(210-250) 4.3.c Host-based firewall secfnd(210-250) 6.5.c Malware
10.1.1.4 Network-Based Malware Protection	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.1 AMP Threat Grid secfnd(210-250) 1.5.c Cisco Advanced Malware Protection (AMP) secfnd(210-250) 1.5.d Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS) secfnd(210-250) 1.5.e Email Security Appliance (ESA) / Cisco Cloud Email Security (CES) secfnd(210-250) 6.5.c Malware
10.1.1.5 Cisco Advanced Malware Protection (AMP)	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.1 AMP Threat Grid secfnd(210-250) 1.5.c Cisco Advanced Malware Protection (AMP) secfnd(210-250) 6.5.c Malware
10.1.1.6 Activity - Identify Antimalware Terms and Concepts	K0480, S0079	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.1.2 Host-Based Intrusion Protection					
10.1.2.1 Host-Based Firewalls	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 4.3.c Host-based firewall
10.1.2.2 Host-Based Intrusion Detection	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.3.b Integrity secfnd(210-250) 4.3.a Host-based intrusion detection
10.1.2.3 HIDS Operation	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 2.3.e Sliding window anomaly detection secfnd(210-250) 6.5.c Malware
10.1.2.4 HIDS Products	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.1 AMP Threat Grid
10.1.2.5 Activity - Identify the Host-Based Intrusion Protection Terminology	K0480, S0079	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.1.3 Application Security					
10.1.3.1 Attack Surface	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 6.1 Compare and contrast an attack surface and vulnerability
10.1.3.2 Application Blacklisting and Whitelisting	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 4.3.d Application-level whitelisting/blacklisting secfnd(210-250) 6.1 Compare and contrast an attack surface and vulnerability
10.1.3.3 System-Based Sandboxing	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.1 Cuckoo Sandbox secfnd(210-250) 4.3.e Systems-based sandboxing (such as Chrome, Java, Adobe reader) secfnd(210-250) 6.5.c Malware
10.1.3.4 Video Demonstration - Using a Sandbox to Launch Malware	K0480, S0079	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.7.	secfnd(210-250) 6.5.c Malware
Section 10.2 Endpoint Vulnerability Assessment					
10.2.1 Network and Server Profiling					
10.2.1.1 Network Profiling	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 3.5 Identify these elements used for network profiling secfnd(210-250) 6.5.f Host profiling secfnd(210-250) 6.5.c Malware
10.2.1.2 Server Profiling	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 2.7.a NetFlow secops(210-255) 3.6 Identify these elements used for server profiling
10.2.1.3 Network Anomaly Detection	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 1.12 Identify potential data loss from provided traffic profiles secfnd(210-250) 2.3.e Sliding window anomaly detection
10.2.1.4 Network Vulnerability Testing	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.8.a Assets secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.2 Compare and contrast Risk, Threat, Vulnerability, Exploit secfnd(210-250) 2.4.d Risk assessment
10.2.1.5 Activity - Identify the Elements of Network Profiling	K0480, S0079	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.2.2 Common Vulnerability Scoring System (CVSS)	K0480, S0079				

10.2.2.1 CVSS Overview	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 2.4.b Risk scoring/risk weighting secfnd(210-250) 2.4.d Risk assessment
10.2.2.2 CVSS Metric Groups	K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.2.d User interaction secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity
10.2.2.3 CVSS Base Metric Group		HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.2.a Attack vector secops(210-255) 1.2.b Attack complexity secops(210-255) 1.2.c Privileges required secops(210-255) 1.2.d User interaction secops(210-255) 1.2.e Scope secops(210-255) 1.3.a Confidentiality secops(210-255) 1.8.b Threat actor secops(210-255) 1.3.b Integrity secops(210-255) 1.3.c Availability
10.2.2.4 The CVSS Process		HS-ETS1-4.	ITEA.10.	IT 08 2	
10.2.2.5 CVSS Reports		HS-ETS1-4.	ITEA.10.	IT 08 2	
10.2.2.6 Other Vulnerability Information Sources		HS-ETS1-4.	ITEA.10.	IT 08 2	
10.2.2.7 Activity - Identify CVSS Metrics		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.2.3 Compliance Frameworks					
10.2.3.1 Compliance Regulations		HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.8.b Threat actor secops(210-255) 3.0 Incident Response
10.2.3.2 Overview of Regulatory Standards		HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 3.7.a PCI secops(210-255) 3.7.b HIPAA (Health Insurance Portability and Accountability Act) secops(210-255) 3.7.c SOX secops(210-255) 3.8 Identify data elements that must be protected with regards to a specific standard (PCI-DSS)
10.2.3.3 Activity - Identify Regulatory Standards		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.2.4 Secure Device Management		HS-ETS1-4.			
10.2.4.1 Risk Management		HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.2 Compare and contrast Risk, Threat, Vulnerability, Exploit secfnd(210-250) 2.4.c Risk reduction secfnd(210-250) 2.4.d Risk assessment
10.2.4.2 Activity - Identify the Risk Response		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.2.4.3 Vulnerability Management		HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 2.7.e Vulnerability management
10.2.4.4 Asset Management		HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 1.8.a Assets secfnd(210-250) 2.7.a Asset management
10.2.4.5 Mobile Device Management		HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 2.7.c Mobile device management
10.2.4.6 Configuration Management		HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 2.7.b Configuration management secfnd(210-250) 6.1 Compare and contrast an attack surface and vulnerability
10.2.4.7 Enterprise Patch Management		HS-ETS1-4.	ITEA.10.	IT 08 2	secops(210-255) 3.7.b HIPAA (Health Insurance Portability and Accountability Act) secops(210-255) 3.7.c SOX secfnd(210-250) 2.7.d Patch management
10.2.4.8 Patch Management Techniques		HS-ETS1-4.	ITEA.10.	IT 08 2	secfnd(210-250) 2.6.b Agentless and agent-based protections secfnd(210-250) 2.7.d Patch management
10.2.4.9 Activity - Identify Device Management Activities		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.2.5 Information Security Management Systems					
10.2.5.1 Security Management Systems		HS-ETS1-4.	ITEA.10.	IT 08 2	
10.2.5.2 ISO-27001		HS-ETS1-4.	ITEA.10.	IT 08 2	
10.2.5.3 NIST Cybersecurity Framework		HS-ETS1-4.	ITEA.10.	IT 08 2	
10.2.5.4 Activity - Identify the Parts of ISO 27001 Activity Cycle		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
10.2.5.5 Activity - Identify the Stages in the NIST Cybersecurity Framework		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
Section 10.3 Summary					
10.3.1 Conclusion					
10.3.1.1 Chapter 10, Endpoint Security and Analysis					

CCNA Cybersecurity Operations - Chapter 11, Security Monitoring

Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 11.0 Introduction					
11.0.1 Welcome					
11.0.1.1 Chapter 11: Security Monitoring	A0097	HS-ETS1-2.	ITEA.10.	IT 10	
Section 11.1 Technologies and Protocols					
11.1.1 Monitoring Common Protocols					
11.1.1.1 Syslog and NTP	A0097	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 4.4.b Unix-based syslog secops(210-255) 5.5 Describe the function of these protocols in the context of security monitoring
11.1.1.2 NTP	A0097	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 4.4.b Unix-based syslog secops(210-255) 5.5 Describe the function of these protocols in the context of security monitoring
11.1.1.3 DNS	A0097	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 2.7.e Proxy logs secfnd(210-250) 1.3.b DNS secfnd(210-250) 5.5 Describe the function of these protocols in the context of security monitoring
11.1.1.4 HTTP and HTTPS	A0097	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 5.1.f Web content filtering secops(210-255) 5.5 Describe the function of these protocols in the context of security monitoring
11.1.1.5 Email Protocols	A0097	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 1.8.b Threat actor secops(210-255) 4.5 Describe the retrospective analysis method to find a malicious file, provided file analysis report secops(210-255) 4.8 Map DNS, HTTP, and threat intelligence data together secops(210-255) 5.5 Describe the function of these protocols in the context of security monitoring
11.1.1.6 ICMP	A0097	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 1.2.d ICMP
11.1.1.7 Activity - Identify the Monitored Protocol	A0097	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 5.5 Describe the function of these protocols in the context of security monitoring
11.1.2 Security Technologies					
11.1.2.1 ACLs	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 1.2.d ICMP secfnd(210-250) 1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices secfnd(210-250) 5.3.a Access control list
11.1.2.2 NAT and PAT	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow secfnd(210-250) 5.3.b NAT/PAT
11.1.2.3 Encryption, Encapsulation, and Tunneling	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 5.3.c Tunneling secfnd(210-250) 5.3.e Encryption secfnd(210-250) 5.3.g Encapsulation
11.1.2.4 Peer-to-Peer Networking and Tor	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 5.3.d TOR secfnd(210-250) 5.3.f P2P
11.1.2.5 Load Balancing	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 5.3.h Load balancing
11.1.2.6 Activity - Identify the Impact of the Technology on Security and Monitoring	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
Section 11.2 Log Files					
11.2.1 Types of Security Data					
11.2.1.1 Alert Data	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 2.6 Interpret common artifact elements from an event to identify an alert secfnd(210-250) 5.2.g Alert data
11.2.1.2 Session and Transaction Data	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 5.2.b Session data secfnd(210-250) 5.2.c Transaction data
11.2.1.3 Full Packet Captures	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 5.2.b Session data secfnd(210-250) 5.2.c Transaction data secfnd(210-250) 5.2.f Extracted content

11.2.1.4 Statistical Data	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow secops(210-255) 4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains secfnd(210-250) 2.3.e Sliding window anomaly detection secfnd(210-250) 5.2.d Statistical data
11.2.1.5 Activity - Identify Types of Network Monitoring Data	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
11.2.2 End Device Logs					
11.2.2.1 Host Logs	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 4.4.a Windows security event logs
11.2.2.2 Syslog	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 4.4.b Unix-based syslog
11.2.2.3 Server Logs	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 2.7.e Proxy logs secfnd(210-250) 4.4.b Unix-based syslog
11.2.2.4 Apache Webserver Access Logs	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 4.4.c Apache access logs
11.2.2.5 IIS Access Logs	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 4.4.d IIS access logs
11.2.2.6 SIEM and Log Collection	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 4.1 Describe the process of data normalization secfnd(210-250) 2.6.c SIEM and log collection
11.2.2.7 Activity - Identify Windows Event Message Severity	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
11.2.3 Network Logs					
11.2.3.1 Tcpdump	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 5.1.a TCP Dump
11.2.3.2 NetFlow	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow secfnd(210-250) 5.1.a TCP Dump secfnd(210-250) 5.1.b NetFlow secfnd(210-250) 5.2.a Full packet capture
11.2.3.3 Application Visibility and Control	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 2.7.d Network application control secfnd(210-250) 5.1.e Application visibility and control secfnd(210-250) 5.3.f P2P
11.2.3.4 Content Filter Logs	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secfnd(210-250) 1.5.d Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS) secfnd(210-250) 1.5.e Email Security Appliance (ESA) / Cisco Cloud Email Security (CES) secfnd(210-250) 4.4.b Unix-based syslog secfnd(210-250) 5.1.f Web content filtering secfnd(210-250) 5.1.g Email content filtering
11.2.3.5 Logging from Cisco Devices	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	
11.2.3.6 Proxy Logs	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 4.7 Map DNS logs and HTTP logs together to find a threat actor
11.2.3.7 NextGen IPS	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	secops(210-255) 1.1 AMP Threat Grid secops(210-255) 1.3 Describe these terms as they are defined in the CVSS 3.0 secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow secops(210-255) 2.9 Interpret a provided intrusion event and host profile to calculate the impact flag generated by Firepower Management Center (FMC) secops(210-255) 4.9 Identify a correlation rule to distinguish the most significant alert from a given set of events from multiple data sources using the firepower management console secfnd(210-250) 5.1.e Application visibility and control secfnd(210-250) 5.4 Describe these NextGen IPS event types
11.2.3.8 Activity - Identify the Security Technology from the Data Type Description	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
11.2.3.9 Activity - Identify the NextGen IPS Wvent Type	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
11.2.3.10 Packet Tracer - Explore a NetFlow Implementation	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow
11.2.3.11 Packet Tracer - Logging from Multiple Sources	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 2.3 Identify the elements from a NetFlow v5 record from a security event secops(210-255) 2.7.a NetFlow
Section 11.3 Summary					
11.3.1 Conclusion					
11.3.1.1 Lab - Setup a Multi-VM Environment	K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.3.	
11.3.1.2 Chapter 11, Security Monitoring					

CCNA Cybersecurity Operations - Chapter 12: Intrusion Data Analysis					
Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 12.0 Introduction					
12.0.1 Welcome					
12.0.1.1 Chapter 12: Intrusion Data Analysis	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	
Section 12.1 Evaluating Alerts					
12.1.1 Sources of Alerts					
12.1.1.1 Security Onion	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	
12.1.1.2 Detection Tools for Collecting Alert Data	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secfnd(210-250) 1.5.b Cisco Intrusion Prevention System (IPS) secfnd(210-250) 5.2.g Alert data
12.1.1.3 Analysis Tools	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secfnd(210-250) 5.2.a Full packet capture
12.1.1.4 Alert Generation	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secops(210-255) 2.4 Identify these key elements in an intrusion from a given PCAP file secops(210-255) 2.6 Interpret common artifact elements from an event to identify an alert
12.1.1.5 Rules and Alerts	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secfnd(210-250) 1.3.b DNS secfnd(210-250) 2.7.a Asset management
12.1.1.6 Snort Rule Structure	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secops(210-255) 2.6 Interpret common artifact elements from an event to identify an alert
12.1.1.7 Lab - Snort and Firewall Rules	S0079, S0252	HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 2.7.c Firewall
12.1.2 Overview of Alert Evaluation					
12.1.2.1 The Need for Alert Evaluation	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secops(210-255) 1.8.b Threat actor
12.1.2.2 Evaluating Alerts	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secops(210-255) 2.8.a False Positive secops(210-255) 2.8.b False Negative secops(210-255) 2.8.c True Positive secops(210-255) 2.8.d True Negative secops(210-255) 4.5 Describe the retrospective analysis method to find a malicious file, provided file analysis report
12.1.2.3 Deterministic Analysis and Probabilistic Analysis	S0079, S0252	HS-ETS1-3.	ITEA.10.	IT 10	secops(210-255) 1.8.b Threat actor secops(210-255) 4.10 Compare and contrast deterministic and probabilistic analysis secfnd(210-250) 2.2 Compare and contrast Risk, Threat, Vulnerability, Exploit
12.1.2.4 Activity - Identify Deterministic and Probabilistic Scenarios	S0079, S0252	HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 4.10 Compare and contrast deterministic and probabilistic analysis
12.1.2.5 Activity - Identify the Alert Classification	S0079, S0252	HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	
Section 12.2 Working with Network Security Data					
12.2.1 A Common Data Platform					
12.2.1.1 ELSA	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	
12.2.1.2 Data Reduction	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	
12.2.1.3 Data Normalization	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 4.1 Describe the process of data normalization
12.2.1.4 Data Archiving	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 3.7.a PCI secops(210-255) 3.8 Identify data elements that must be protected with regards to a specific standard (PCI-DSS)
12.2.1.5 Lab – Convert Data into a Universal Format	S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 4.1 Describe the process of data normalization secops(210-255) 4.2 Interpret common data values into a universal format

12.2.2 Investigating Network Data					
12.2.2.1 Working in Sguil	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	
12.2.2.2 Sguil Queries	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 2.6 Interpret common artifact elements from an event to identify an alert
12.2.2.3 Pivoting from Sguil	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 1.8.a Assets secfnd(210-250) 6.6.f Pivot
12.2.2.4 Event Handling in Sguil	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	
12.2.2.5 Working in ELSA	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	
12.2.2.6 Queries in ELSA	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 2.1 Regular Expressions
12.2.2.7 Investigating Process or API Calls	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 2.6 Interpret common artifact elements from an event to identify an alert
12.2.2.8 Investigating File Details	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	
12.2.2.9 Lab – Regular Expression Tutorial	S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 2.1 Regular Expressions
12.2.2.10 Lab - Extract an Executable from a PCAP	S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 2.4 Identify these key elements in an intrusion from a given PCAP file secops(210-255) 2.5 Extract files from a TCP stream when given a PCAP file and Wireshark
12.2.3 Enhancing the Work of the Cybersecurity Analyst					
12.2.3.1 Dashboards and Visualizations	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	
12.2.3.2 Workflow Management	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 2.3.b Runbook automation (RBA)
Section 12.3 Digital Forensics					
12.3.1 Evidence Handling and Attack Attribution					
12.3.1.1 Digital Forensics	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 1.2.e Scope secops(210-255) 1.8.b Threat actor secops(210-255) 3.7.b HIPAA (Health Insurance Portability and Accountability Act)
12.3.1.2 The Digital Forensics Process	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 5.2 Apply the NIST.SP800-61 r2 incident handling process to an event
12.3.1.3 Types of Evidence	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 1.6.a Best Evidence secops(210-255) 1.6.b Corroborative Evidence secops(210-255) 1.6.c Indirect Evidence
12.3.1.4 Evidence Collection Order	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 5.4.a Evidence collection order secops(210-255) 5.4.d Volatile data collection
12.3.1.5 Chain of Custody	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 5.4.d Volatile data collection secfnd(210-250) 2.3.c Chain of custody (evidentiary)
12.3.1.6 Data Integrity and Preservation	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 1.3.b Integrity secops(210-255) 5.4.b Data integrity secops(210-255) 5.4.c Data preservation
12.3.1.7 Attack Attribution	S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	secops(210-255) 1.8.b Threat actor secfnd(210-250) 2.7.a Asset management
12.3.1.8 Activity - Identify the Type of Evidence	S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 1.6.a Best Evidence secops(210-255) 1.6.b Corroborative Evidence secops(210-255) 1.6.c Indirect Evidence
12.3.1.9 Activity - Identify the Forensic Technique Terminology	S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.9.	
Section 12.4 Summary					

12.4.1 Conclusion					
12.4.1.1 Lab - Interpret HTTP and DNS Data to Isolate Threat Actor	S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 4.8 Map DNS, HTTP, and threat intelligence data together secfnd(210-250) 1.3.b DNS secfnd(210-250) 6.3 Describe these web application attacks
12.4.1.2 Lab - Isolate Compromised Host using 5-Tuple	S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	secops(210-255) 4.3 Describe 5-tuple correlation secops(210-255) 4.4 Describe the 5-tuple approach to isolate a compromised host in a grouped set of logs
12.4.1.3 Chapter 12: Intrusion Data Analysis	S0079, S0252	HS-ETS1-3.	ITEA.12.		

CCNA Cybersecurity Operations - Chapter 13, Incident Response and Handling

Page	NICE	NGSS	ITEA	DODEA	Exam Objectives
Section 13.0 Introduction					
13.0.1 Welcome					
13.0.1.1 Chapter 13, Incident Response and Handling	A0097	HS-ETS1-4.	ITEA.13.	IT 09	
Section 13.1 Incident Response Models					
13.1.1 The Cyber Kill Chain					
13.1.1.1 Steps of the Cyber Kill Chain	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 1.8.b Threat actor secops(210-255) 5.1 Classify intrusion events into these categories as defined by the Cyber Kill Chain Model
13.1.1.2 Reconnaissance	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 5.1.a Reconnaissance
13.1.1.3 Weaponization	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 1.8.a Assets secops(210-255) 5.1.b Weaponization
13.1.1.4 Delivery	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 5.1.c Delivery
13.1.1.5 Exploitation	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 5.1.d Exploitation
13.1.1.6 Installation	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 5.1.e Installation
13.1.1.7 Command and Control	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 5.1.f Command and control secfnd(210-250) 6.5.b Command and control (C2)
13.1.1.8 Actions on Objectives	A0097	HS-ETS1-4.	ITEA.13.	IT 09	secops(210-255) 5.1.g Action on objectives
13.1.1.9 Activity - Identify the Kill Chain Step	A0097	HS-ETS1-4.	ITEA.13.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 5.1 Classify intrusion events into these categories as defined by the Cyber Kill Chain Model
13.1.2 The Diamond Model of Intrusion					
13.1.2.1 Diamond Model Overview	A0097	HS-ETS1-4.	ITEA.17.	IT 09	
13.1.2.2 Pivoting Across the Diamond Model	A0097	HS-ETS1-4.	ITEA.17.	IT 09	
13.1.2.3 The Diamond Model and the Cyber Kill Chain	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 4.6 Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains secfnd(210-250) 2.3.d Reverse engineering secfnd(210-250) 6.6.f Pivot
13.1.2.4 Activity - Identify the Diamond Model Features	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
13.1.3 The VERIS Schema					
13.1.3.1 What is the VERIS Schema?	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 5.5 Apply the VERIS schema categories to a given incident
13.1.3.2 Create a VERIS Record	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 5.5 Apply the VERIS schema categories to a given incident
13.1.3.3 Top-Level and Second-Level Elements	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.2.e Scope secops(210-255) 1.8.a Assets secops(210-255) 1.8.b Threat actor secops(210-255) 5.5 Apply the VERIS schema categories to a given incident
13.1.3.4 The VERIS Community Database	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 5.5 Apply the VERIS schema categories to a given incident
13.1.3.5 Activity - Apply the VERIS Schema to an Incident	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	secops(210-255) 5.5 Apply the VERIS schema categories to a given incident
Section 13.2 Incident Handling					
13.2.1 CSIRTs					
13.2.1.1 CSIRT Overview	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secops(210-255) 1.3.c Availability secops(210-255) 1.8.a Assets secops(210-255) 3.4 Describe the goals of the given CSIRT
13.2.1.2 Types of CSIRTs	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 3.4 Describe the goals of the given CSIRT secops(210-255) 3.4.f Incident response providers (MSSP)
13.2.1.3 CERT	A0097	HS-ETS1-4.	ITEA.17.	IT 09	
13.2.1.4 Activity - Match the CSIRT with the CSIRT Goal	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
13.2.2 NIST 800-61r2					secops(210-255) 3.1 Describe the elements that should be included in an incident response plan as stated in NIST.SP800-61 r2
13.2.2.1 Establishing an Incident Response Capability	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 5.2 Apply the NIST.SP800-61 r2 incident handling process to an event

13.2.2.2 Incident Response Stakeholders	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 3.3 Map the organization stakeholders against the NIST IR categories (C2M2, NIST.SP800-61 r2) secops(210-255) 5.2 Apply the NIST.SP800-61 r2 incident handling process to an event
13.2.2.3 NIST Incident Response Life Cycle	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.8.a Assets secops(210-255) 3.2 Map elements to these steps of analysis based on the NIST.SP800-61 r2 secops(210-255) 5.3.c Containment
13.2.2.4 Preparation	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.8.a Assets secops(210-255) 3.2.a Preparation
13.2.2.5 Detection and Analysis	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.2.e Scope secops(210-255) 3.2.b Detection and analysis secops(210-255) 5.3.b Scoping
13.2.2.6 Containment, Eradication, and Recovery	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.8.a Assets secops(210-255) 3.2.c Containment, eradication, and recovery secops(210-255) 5.3 Define these activities as they relate to incident handling secfnd(210-250) 2.3.c Chain of custody (evidentiary)
13.2.2.7 Post-Incident Activities	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.8.a Assets secops(210-255) 3.2.d Post-incident analysis (lessons learned) secops(210-255) 5.3.e Lesson-based hardening
13.2.2.8 Incident Data Collection and Retention	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.2.a Attack vector secops(210-255) 3.0 Incident Response secops(210-255) 5.2 Apply the NIST.SP800-61 r2 incident handling process to an event
13.2.2.9 Reporting Requirements and Information Sharing	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 5.3.f Reporting
13.2.2.10 Activity - Identify the Incident Response Plan Elements	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
13.2.2.11 Activity - Identify the Incident Handling Term	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
13.2.2.12 Activity - Identify the Incident Handling Step	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
13.2.2.13 Lab - Incident Handling	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.3.	
Section 13.3 Summary					
13.3.1 Conclusion					
13.3.1.1 Class Activity - Before You Go	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	
13.3.1.2 Chapter 13, Incident Response and Handling	A0097	HS-ETS1-4.	ITEA.17.	IT 09	secops(210-255) 1.3.a Confidentiality secops(210-255) 1.3.b Integrity secops(210-255) 1.3.c Availability