USAF
OPERATIONAL TRAINING
COURSE

AIR FORCE SPACE COMMAND
CYBER WARFARE OPERATIONS TRAINING (CWO)
IOS-CWO 001 PDS CODE: INW

39TH INFORMATION OPERATIONS SQUADRON

June 2018

AIR FORCE SPACE COMMAND

USAF OPERATIONS TRAINING COURSE

INTRODUCTION

This formal training syllabus is a specialized publication authorized for issue by the Commander of the 39th Information Operations Squadron. This syllabus is directive in nature and prescribes the overall training strategy and approximate amount of instruction required for a student with entry prerequisites to attain course goals and graduate. Individuals tasked to implement this syllabus will ensure each student graduated possesses the knowledge, skills and proficiencies set forth in the course training standards. Within syllabus and other directive constraints, the amount and level of training devoted to mission elements, events, subjects or phases should be adjusted as required to meet individual student needs.

PIZOR.CHRISTOPHER.S.1095268079 Digitally signed by PIZOR.CHRISTOPHER.S.1095268079 Date: 2018.06.28 15:34:05 -05'00'

CHRISTOPHER S. PIZOR, GG-13, DAF
CWO Curriculum Lead

WATERS.ANGELA.MARIE.1242613275 Digitally signed by WATERS.ANGELA.MARIE.1242613275 Date: 2018.06.28 19:41:15 -05'00'

ANGELA M. WATERS, Lt Col, USAF
Commander, 39 IOS

RHONDA HUTSON, GS-13, DAF
AFSPC/A2/3/6TT

OPR: 39 IOS
OCR: 39 IOS/CCV
DISTRIBUTION:

Maxwell-Gunter AFB, Gunter Annex, 36114
CCAF/DECA
CCAF/CD

Peterson AFB, CO
AFSPC/A2/3/6TT

Lackland AFB, TX
24 AF/A3T

Hurlburt Field, FL 32544
39 IOS/CC

Table of Contents

Section 1 – Course Description & Admission Procedures

1.1 Course Title/Number. Air Force Cyber Warfare Operations Course (CWO) / IOS-CWO 001 PDS Code INW.

1.2 Course Entry Prerequisites and Student Selection Process.

1.2.1 This course is open to 17D Officers, 1B4 Enlisted, and other approved AFSCs (to include contractors and civilians) with assignment to a Cyber Mission Force Combat Mission Team, National Mission Team, Cyber Support Team, or Cyber Protection Team. Students must complete one of the following prior to enrollment:

a. Undergraduate Cyber Training (UCT) Initial Skills Training (17D Officer)
b. Cyber Warfare Operator Apprentice (CWO-A) Initial Skills Training (1B4 Enlisted)
c. Network Warfare Bridge Course (NWBC) Supplemental Skills Training (SST)
d. ANG Cyber Skills Validation Course (CSVC)
e. Other qualifying programs/training as determined by waiver authority (see 3.1).

1.2.2 Student Nomination

1.2.2.1 Unit Commanders nominate students meeting criteria outlined in paragraph 1.2.1 to the 39 IOS Registrar not later than 60 calendar days prior to the projected CWO class start date.

1.2.2.2 HQ AFSPC/A2/3/6TT, or delegated representative, will select students from nominations received based on prioritized operational requirements and space availability. HQ AFSPC/A2/3/6TT provides the final student roster to the 39 IOS Registrar no later than 45 days prior to the course start date.

1.2.2.3 Student Body. The 39 IOS and 39 IOS Det 1 have classrooms that support CWO instruction with capacities of 24, 25, 28, and 38. Maximum class size is dependent on the classroom.

1.3 Purpose and Graduate Status. The CWO course provides advanced Cyberspace Operations fundamentals training for students assigned to cyberspace operations units. Students learn cyberspace operations concepts and operational functions, employment of tactical offensive and defensive tactics. These include Windows and Linux operating system security fundamentals, networking concepts and security, malware analysis, incident handling, forensics, intermediate traffic analysis, offensive cyberspace operations, intelligence driven operations, tactical mission planning, and the plan/brief/execute/debrief (PBED) process.

1.4 Security Requirements. All students MUST possess Top Secret (TS) Sensitive Compartmented Information (SCI) clearances prior to enrollment at Hurlburt Field. Students enrolling at Joint Base San Antonio must have at least a SECRET clearance.

1.5 Location. Multiple Training Locations. 39 IOS Hurlburt Field and 39 IOS Detachment 1, Joint Base San Antonio.

1.6 Operational Risk Management/Safety. The academic challenges of this syllabus require a dedicated, daily Operational Risk Management (ORM) focus. Nothing in this syllabus requires safety to be compromised or is worth the cost of injuring a person. The safety focus is to instill risk management decision-making in the students and the development of safe, viable habit patterns. Safety is the responsibility all those assigned to support this syllabus.

1.7 Duration. 46 academic training days.

1.8 Number of In-Residence Training Hours: 374.25 hours

Table 1.1. Academic Training Inventory

Module	*Instructor-Led Subject*	*Instructor – Led Hours (Lecture, Demo, Briefing)*	*Self-Paced Hours*	*Student Performance Hours*	*Total Hours*
99	Administrative (Orientation, Graduation, Test Review)	15.25	0.0	0.0	15.25
29	Evaluation Preparation & Administration	6.0	17	31.0	54
1	Windows Operating System Foundations	10	0.0	24.5	34.5
2	Linux Operating System Foundations	8.0	0.0	15.5	23.5
3	Programming/Scripting Fundamentals	20.0	0.0	34.5	54.5
4	Networking and Protocols	4.5	0.0	0.0	4.5
5	SANS Advanced Digital Forensics and Incident Response & NetWars	19.0	0.0	55.5	74.5
6	Network Forensics	0.0	0.0	9.0	9.0
7	Forensics and Malware	13.0	0.0	25.0	38.0
8	Offensive Cyber Operations & Methodologies	8	0.0	41.0	49.0
9	Mission Analysis and PBED	12.5	0.0	5.0	17.5
Total		**116.25**	**17**	**241**	**374.25**

Section 2 – Course Training Standards / Graduation Requirements

2.1. Academic Training Standards (Cognitive and Performance). Academic competence is measured by cognitive and performance evaluations. The minimum passing score for an academic evaluation is 80%. The exception is the GIAC Certified Forensic Analyst (GCFA) certification exam. The commercial provider (GIAC) establishes the passing score.

2.2. Academic Evaluation Failure (Cognitive or Performance). If a student fails an academic evaluation (cognitive or performance) they will meet a training review panel (TRP) in

accordance with 39 IOS Standard Operating Procedure 36-01, *Instructor Responsibilities and Course Administration*. The Course Director chairs the TRP to determine internal/external factors as well any required remedial training. Students will be afforded one opportunity to retest per written or performance failure. If the student passes the re-test, they will be awarded the minimum passing score of 80%. If the student fails again, they will meet a TRP chaired by the 39 IOS Director of Operations (39 IOS/DO). Two test failures in the same block of instruction is grounds for elimination from the course.

2.2.1. GIAC Certified Forensic Analyst (GCFA) certification exam will not be retested during the in-residence course. Students will receive one retest voucher for use when the student returns to their unit. Dependent upon aptitude and performance, students not achieving a passing score may be allowed to continue with the course; however, will not graduate in-residence. Students must complete the GCFA certification examination within 90 days of the class graduation date in order to officially graduate the course. If the student is unable to achieve a passing score, the student will be academically eliminated from the course.

2.3. Corrective Action Options. Students experiencing difficulties with curriculum are provided additional instruction. This instruction may occur before/after class or outside of normal duty hours. Retesting discussed above (2.2) may also require time before or after normal duty hours depending on length of retest and classroom availability.

2.4. Graduation Criteria. CWO serves as part of initial qualification training (IQT) for units performing Combat Mission Team, National Mission Team, Cyber Support Team, and Cyber Protection Team missions for United States Cyber Command (USCYBERCOM). The knowledge and skills acquired have direct application to customer-driven master training task list items. For that purpose, all evaluations must be passed in order to successfully graduate CWO.

2.5. Elimination Procedures. If a student fails to meet the prescribed academic baselines established above, the 39 IOS/DO will recommend elimination actions to the 39 IOS Commander (39 IOS/CC) who will review actions on a case-by-case basis. For administrative elimination, the 39 IOS/CC may at any time initiate elimination proceedings when such action is warranted, in accordance with 39 IOS Standard Operating Procedure 36-01, *Instructor Responsibilities & Course Administration*.

2.6. End-of-Course (EOC) Report. The EOC report is documented on an AFSPC Form 4419, *Record of Training,* and/or AF 475, *Training Report*. The forms identify tasks covered during the training and details student proficiency ratings along with instructor comments. Student understanding is gauged through classroom participation, cognitive and performance evaluations. AF 475 are only provided to officers who have completed 8 weeks of training. Enlisted, civilians, and contractors will NOT receive an AF Form 475.

Section 3 – Waiver and Course Authority

3.1. Entry Prerequisites. The 39 IOS/CC is the waiver authority for prerequisites established in 1.2.1. Waiver requests will be evaluated on a case-by-case basis factoring in the member's previous training, education, and operational experience.

3.2. Training Completion/Events and Graduation. 39 IOS/CC is the waiver authority for training completion and training events. 39 IOS/CC evaluates training and event waivers on a case-by-case basis.

3.3. Course Execution Authority. The 39 IOS/DO is responsible for conducting the training specified under the authority/direction of this syllabus. The 39 IOS/DO may authorize deviations in the order of training subject to the availability of resources.

3.4. Elimination Authority. The 39 IOS/CC is the sole elimination authority for academic or administrative matters.

Section 4 – Course Resource Requirements

4.1. Instructional Staff. The instructor/student ratio for classroom informal lecture/demonstration is 1:38 (max classroom size). For student performance, the ratio is 1:8. Community College of the Air Force (CCAF) accredited courses must have at a minimum one CCAF qualified instructor in the classroom. This could drive a ratio of 2:38 if the primary instructor is in student status.

4.2. Facility Requirements. The CWO in-residence course is conducted in a secure facility. The 39 IOS provides a training environment for students throughout the course. Students are required to bring a laptop for homework and assignment research during the course. No personal or organizational laptops are authorized in the facility.

Section 5 – Academic Training Descriptions

CWO Modules

Module 99	**Instructor Led (Lecture, Demonstration)**	**Self Study**	**Performance**
Administrative Actions	**15.25**	**0.0**	**0.0**
Administrative (inprocessing and graduation activities to include: Course Director and Commander's Welcome, Local Orientation, Security, Safety, Network Accounts and Emergency Contact Information) Finally, this module incorporates time for Standards and Evaluation to review tests with students.			

Module 29	Cognitive Testing Hours	Self-Study (Test Prep)	Performance Testing Hours
Evaluation Preparation and Administration	**6.0**	**17**	**31.0**

Cognitive Testing:
- Pre Assessment (1 hr)
- Linux (1 hr)
- GCFA Certification (3 hr)
- Post Assessment (1 hr)

Performance Testing:
- NetWars (4 hrs)

Hybrid (Cognitive & Performance):
- Windows (2.5 hrs)
- Programming & Scripting (3 hrs)
- Malware Forensics (2.5 hrs)

- Student Academic Prep (Self Study) (17 hrs)

Retest Allotments:
- Linux (1hr)
- Windows (2.5 hrs)
- Programming & Scripting (3 hrs)
- Malware Forensics (2.5 hrs)
- NetWars (4 hrs)

Module 1	Instructor Led (Lecture, Demonstration)	Self Study	Performance
Windows Operating System Foundations	**10**	**0.0**	**24.5**

This module is for students to learn the principles and components of the various versions of the Microsoft Windows Operating Systems (OS). Note: Students will be using virtualization products during exercises and labs not only during the phase but also throughout the CWO course. These lessons are designed to introduce the students to attributes of different Windows kernel bases and explain the boot sequence of the system and the critical services and files involved. Additionally, standard Windows configuration files and the registry are discussed and manipulated to adjust system settings. The students are introduced to the Windows file system structures and key concepts of file types and attributes, and trained in depth on key directories and Windows shares on host and server architectures. Students will learn about Windows processes and services, and how to analyze them to identify anomalies. Students are introduced to Windows password hashes and network-based authentication. Students will be able to describe the security features of the different OS versions as well as the different log types and their functions. They will query local and remote event logs via the command line, graphical user interface (GUI), and PowerShell looking for specific security related event IDs. Students will be working with user and group accounts. Active Directory is introduced as well as Group Policy Objects, and how the two can be utilized to implement security measures in response to intrusion incidents. This module includes a heavy emphasis on hands-on skills where the students will be required to perform a variety tasks via the command line. Students will become familiar with various net commands used to manage services, connect to shared resources, and to manipulate network settings on the system. Students will use the command line to gather system and configuration information from local and remote systems and to analyze the data to create system baselines and determine anomalous activity. Students will perform hands-on labs manipulating registry key settings via the GUI and command line, as well

as search event logs and manipulate firewall settings. Students will be able to enumerate users and groups for both local and domain accounts, as well as create and push group policy to domain systems to increase security.

Module 2	**Instructor Led (Lecture, Demonstration)**	**Self Study**	**Performance**
Linux Operating System Foundations	**8.0**	**0.0**	**15.5**
This module focuses on the principles and components of the Linux OX. Students will understand the Linux boot process and essential skills for proper administration, usage, exploitation and defense of the Linux OS, and develop the skills needed to understand practical applications of Air Force cyber systems. The course will provide fundamentals of the average Linux Operation System boot process as it relates to the use of the Basic Input/Output System, the Master Boot Record, the Grand Unified Boot Loader and the Linux Kernel. Students will learn how the OS interacts with the hardware and the underlying processes in its environment. Students will learn multiple different Linux distributions, both Red Hat-based distributions (CentOS, Fedora, etc.) and debian-based distributions (Ubuntu, Kali Linux). Students will learn the basic file system layout and directory contents, essential commands for moving, creating, editing, and deleting files, file permissions and ownership and manipulation commands. Students will understand the operation and functionality of common Linux processes and their practical applications. The processes covered will include Samba, Apache, FTP, SFTP, SSH, and RDP, with particular focus will on the establishment of SSH, RDP, Samba, and SFTP connections. Students will be trained on the essentials of Linux OS-specific enhanced security features and system logging. Students will use the command line to gather system and configuration information on local and remote systems. They will analyze the data to create systems baselines and to identify anomalies. This module provides students with introduction to Linux OS-based firewalls and networking. This module is a combination of lecture, instructor-led demonstrations and student performance based labs.			

Module 3	**Instructor Led (Lecture, Demonstration)**	**Self Study**	**Performance**
Programming/Scripting Fundamentals	**20.0**	**0.0**	**34.5**
The purpose of this module is to introduce the students to the basics of programming. The students will be introduced to basic programming concepts ranging from variables and other data structures to basic program structure. These concepts are introduced in the C Programming language and then utilized to teach similar concepts and how they are applied using the Python scripting language through the interactive shell and integrated development environments. Language-specific syntax will be covered in lecture with hands on demonstrations and labs. Students will learn how to interpret the basic functionality of Python scripts and how to troubleshoot and/or modify existing scripts to meet specific criteria. Lastly, students will learn to use and write basic Windows PowerShell scripts to run commands on local and remote systems, combine commands and tools into more complex processes, create reusable tools and applications, and package those tools for others to use.			

Module 4	Instructor Led (Lecture, Demonstration)	Self Study	Performance
Networking and Protocols	**4.5**	**0.0**	**0.0**
The purpose of this module is for students to learn the principles and components of computer networking. This module focuses on student understanding of the seven layer OSI model, low level protocols, data encapsulation, network hardware, traffic classifications, and the common protocols used in the application, transport, network and datalink layers. Specific protocols and header interpretation will be reviewed for foundational understanding needed for later modules. This module introduces some of the advanced protocols utilized: RIP, OSPF, BGP, STP and EIGRP. Students will comprehend the basic concepts of routers, switches, firewall, proxies, and other networking hardware and software. This module introduces the concepts of network sniffers and sniffing. It will cover the basic concepts of what a sniffer is and how it works. This module will give students an in-depth analysis of internet protocols with a focus on traffic/packet analysis. Students will examine the information included in the headers, to include source and destination address, sizes, checksum, etc. Students will review common protocols (HTTP, DNS, FTP, telnet, SSH, etc.), what they look like at the packet level, how to distinguish different protocols, and how to differentiate and extract various file formats and rebuild them from network traffic.			

Module 5	Instructor Led (Lecture, Demonstration)	Self Study	Performance
SANS Advanced Digital Forensics and Incident Response & NetWars	**19.0**	**0.0**	**55.5**
NOTE: All courseware and associated materials are propriety to the civilian industry partner hosting the course onsite at the 39 IOS, currently The SANS Institute. This module includes FOR508: Advanced Digital Forensics and Incident Response, an in-depth incident response course that provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including advanced persistence threat (APT) adversaries, organized crime syndicates, and hacktivism. Constantly updated, the incident response course addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases. Students are trained to respond, detect, scope, and stop intrusions and data breaches. Students will be shown the importance of developing security intelligence in affecting the adversary's "kill chain." Students will also see demonstrations of live response techniques and tactics that can be applied on a single system and across the entire enterprise. This course addresses real Incident Response tactics to include preparation, identification and detecting all compromised systems, containment, eradication, and recovery. Students learn the importance of Cyber Threat Intelligence, remote incident response, and Windows Live Incident Response techniques and tools. The memory forensics portion is a critical component needed by incident response teams to detect advanced threats and can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware. This section will introduce some of the newest tools available and give students a solid foundation in core and advanced memory forensic skills. Students will learn advanced incident response techniques uncovered via timeline analysis. File system modified/access/creation/change times, log files, network data, registry data, and internet history files all contain time data that can be correlated into critical			

timeline analysis, which has become a critical incident response and forensics technique to solve complex cases. Students will learn the actions hackers might take to hide their actions and the skills to track what can be traced. Extensive hands-on exercises using the SIFT Workstation and numerous forensics tools will allow the students to perform live response techniques and tactics, including Volatile Data Collection, Comparison of Key Data Collected via Live Collection, Static Drive, and Memory Analysis Techniques, Live Memory Forensics, Memory Analysis Techniques, Advanced Memory Analysis with Volatility, Code Injection, Malware, and Rootkit Hunting in Memory. The last phase allows the students to apply the concepts from throughout the module in an Intrusion Forensic Challenge, which will have each incident response team analyzing multiple systems in an enterprise network. This module also includes SANS NetWars, a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world, in-depth skills they need to excel in their field. Students learn in a cyber range while working through various challenge levels, all hands-on, with a focus on mastering the skills information security professionals can use in their jobs every day. The exercise will progress in level of difficulty as the students learn new Cyber Warfare knowledge, skills, and abilities and culminates with a 4-hour hands-on practical test.

Module 6	**Instructor Led (Lecture, Demonstration)**	**Self Study**	**Performance**
Network Forensics	**0.0**	**0.0**	**9**
The purpose of this module is for students to learn the principles and components of network forensics. Students will learn what tools and resources are required to perform packet analysis as well as what types of intelligence can be obtained. Students will analyze packet capture files for signs of malicious traffic, and will carve various files that were transferred across the network. Students will leverage basic Linux traffic tools such as TCPDump and Ngrep to capture and analyze packets. Additionally, students will run through a deep-dive of Wireshark, where they will analyze a variety of network traffic and work through most of Wireshark's available functions.			

Module 7	**Instructor Led (Lecture, Demonstration)**	**Self Study**	**Performance**
Forensics and Malware	**13.0**	**0.0**	**25.0**
The purpose of this module is for students to learn the principles and components of network forensics. Students will learn what tools and resources are required to perform packet analysis as well as what types of intelligence can be obtained. Students will analyze packet capture files for signs of malicious traffic, and will carve various files that were transferred across the network. Students will leverage basic Linux traffic tools such as TCPDump and Ngrep to capture and analyze packets. Additionally, students will run through a deep-dive of Wireshark, where they will analyze a variety of network traffic and work through most of Wireshark's available functions.			

Module 8	**Instructor Led (Lecture, Demonstration)**	**Self Study**	**Performance**
Offensive Cyber Operations and Methodologies	**8.0**	**0.0**	**41.0**
This module will emphasize a disciplined and planned approach to the employment of offensive cyber operations capabilities against internet protocol (IP) networks. Students will walk through the entire attack methodology as outlined in AFTTP 3-1.CWO. This includes everything from footprinting and enumeration through the clean-up phase of an operation. Students will train on multiple techniques to conduct scanning and enumeration using nmap, hping3, as well as from the Windows and Linux command line without the use of a scanner. Kali and the Metasploit Framework will be used at a deeper level to uncover some of the more advanced functions available. Students will exercise methods for conducting client-side attacks as well as methods for bypassing host-based antivirus programs. There is a heavy focus on post-exploitation survey and follow-on actions to achieve the desired end state of the tasked mission. Multiple methods will be demonstrated and then exercised concerning how to maintain persistent access to a target system. Students will receive an in-depth lesson concerning tunneling focused on SSH tunneling and port-forwarding. Following the SSH tunneling exercises, approximately 50% of all training mission labs will be conducted using tunneling methods to obfuscate the true source IP. The students will be tasked to operate through the SSH tunnel against a target set of Windows and Linux machines that have a variety of vulnerabilities and misconfigurations. They will learn how to employ multiple methods of persistence, and how to clean up forensic artifacts that could be used to identify their activities. Students will be given a scenario and utilize the Plan, Brief, Execute, Debrief (PBED) process to complete an offensively focused operational exercise.			

Module 9	**Instructor Led (Lecture, Demonstration)**	**Self Study**	**Performance**
Mission Analysis and PBED	**12.5**	**0.0**	**5.0**
This module focuses on the nature of intelligence, PBED, Military Cyberspace Operations, and the Cyber Mission Force. Lessons focus on intelligence as a whole, and the specific intelligence disciplines Cyber Operators are most likely to encounter during operations. Specific members of the Intelligence Community are discussed and their pertinent resources accessed making students aware and appreciative of the Community's products and services. Concepts of operational and tactical-level Cyber Operations Planning are applied to develop a comprehensive Cyber Operations strategy to achieve Commander's objectives. Students are set up for success in further cyberspace warfare curriculum through introduction to the Cyber Mission Forces concept: the National Mission Team, the Combat Mission Team, and the Cyber Protection Team. Also, students will be exposed to the USCYBERCOM Cyber Lexicon to cultivate an environment using common communication of the profession. The concepts and processes taught in this module will be exercised in a realistic operations scenario during the Offensive Cyber Operations (OCO) Module, where they will be divided into teams where they will have to interpret orders and governing documentation to plan and execute OCO operations against a notional adversary to support the commander's objective. The teams will follow the PBED process as they conduct these operations with a goal of improving communication and execution of their operations.			

Abbreviations and Acronyms

AF	Air Force
AFSC	Air Force Specialty Code
AFSPC	Air Force Space Command
ANG	Air National Guard
APT	Advanced Persistent Threat
BGP	Border Gateway Protocol
CC	Commander
CCAF	Community College of the Air Force
CSVC	Cyber Skills Validation Course
CWO	Cyber Warfare Operations
CWO-A	Cyber Warfare Operator Apprentice
DNS	Domain Name Service
DO	Director of Operations
DoD	Department of Defense
EIGRP	Enhanced Interior Gateway Routing Protocol
EOC	End-of-Course
FTP	File Transfer Protocol
GCFA	GIAC Certified Forensics Analyst
GIAC	Global Information Assurance Certification
GUI	Graphic User Interface
HQ	Headquarters
HTTP	Hypertext Transfer Protocol
ID	Identifications
IOS	Information Operations Squadron
IP	Internet Protocol
IQT	Initial Qualification Training
NWBC	Network Warfare Bridge Course
OCO	Offensive Cyber Operations
ORM	Operation Risk Management
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PBED	Plan/Brief/Execute/Debrief
PDS	Personnel Data System
RDP	Remote Desktop Protocol
RIP	Routing Information Protocol
SANS	System Administration, Networking, and Security Institute
SCI	Sensitive Compartmented Information
SFTP	Secure File Transfer Protocol
SIFT	SANS Investigative Forensics Toolkit
SSH	Secure Shell
SST	Supplemental Skills Training
STP	Spanning Tree Protocol

TRP	Training Review Panel
TS	Top Secret
UCT	Undergraduate Cyber Training
USCYBERCOM	United States Cyber Command