Manassas Historic District Office
9401 Battle St.
Suite 202
Manassas, VA 20110
USA

Email: contact@csfi.us

# DoD Cyber Workforce Framework

## Cyberspace Operator

**Work Role ID:** 322 (NIST: N/A)
**Workforce Element:** Cyberspace Effects

### Role Overview:

Cyberspace Operators employ a diverse array of software tools for network navigation, tactical forensic analysis, surveillance, reconnaissance, and executing on-net operations to support offensive cyberspace missions as directed.

The Department of Defense (DoD) Cyber Workforce Framework (DCWF) categorizes this role under the 'Cyberspace Effects' workforce element, focusing on personnel who plan and execute cyberspace operations to project power in and through cyberspace.

**Comprehensive Mapping of the DCOE to DoD KSAT IDs (Core and Additional) for the Cyberspace Operator, Work Role ID: 322 (NIST: N/A) Workforce Element: Cyberspace Effects.**

# Core KSATs

## *Defensive Cyberspace Operations Engineer (DCOE) Certification*

### 22 (NIST ID: K0001)

**Knowledge of computer networking concepts and protocols, and network security methodologies.**

| | |
|---|---|
| **01** | **DCOE Mapping to Networking Concepts and Protocols:** |
| | Unit 1 explains cyberspace layers (persona, logical, physical) and DODIN architecture, covering IP addressing and physical networking (e.g., Ethernet). |
| **02** | **DCOE Mapping to Network Security Methodologies:** |
| | Focuses on **DCO-IDM** (internal defenses like firewalls, IDS/IPS) and **DCO-RA** (external threat responses), emphasizing active threat defense. |
| **03** | **DCOE Mapping to Labs:** |
| | Hands-on labs simulate network attacks (e.g., DDoS, penetration tests), focusing on detection, mitigation, and secure network configurations. |
| **04** | **DCOE Mapping to Threat Analysis:** |
| | Incorporates the cyber kill chain, detailing adversary tactics and defensive countermeasures for reconnaissance and lateral movement. |
| **05** | **DCOE Mapping to Tools and Techniques:** |
| | Utilizes VMs to analyze protocols, secure network traffic (e.g., HTTP/HTTPS), and deploy countermeasures against spoofing and breaches. |

This ensures technical mastery of networking and security methodologies through integrated theory and practical labs.

## 108 (NIST ID: K0002)

**Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).**

| | |
|---|---|
| **01** | **DCOE Mapping to Risk Management Framework (RMF)**: |
| | The course aligns with RMF processes, emphasizing **security assessment and authorization** under FISMA/NIST standards. |
| **02** | **DCOE Mapping to Risk Assessment Techniques**: |
| | Teaches identification, analysis, and prioritization of risks through real-world scenarios, addressing vulnerabilities and operational threats. |
| **03** | **DCOE Mapping to Mitigation Strategies**: |
| | Covers DCO-IDM and DCO-RA approaches for proactive mitigation, such as **threat hunting** and vulnerability patching. |
| **04** | **DCOE Mapping to Labs**: |
| | Labs simulate risk scenarios, enabling practical application of **vulnerability assessments, threat detection**, and protective strategies. |
| **05** | **DCOE Mapping to Active Defense**: |
| | Includes hands-on use of **IOCs** for early risk detection and mitigation, reinforcing proactive defense mechanisms. |

This ensures students gain actionable expertise in risk management through theory and applied practice.

## 1157 (NIST ID: K0003)

**Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyber Laws and Policies**: |
| | The course emphasizes **DoD Cyber Strategy**, including U.S. policies on **Defensive Cyberspace Operations (DCO)** and international frameworks such as **cyberspace as a warfighting domain**. |
| **02** | **DCOE Mapping to Ethical Considerations**: |
| | Explores the role of **Commander's Intent** in ethical decision-making during cyberspace operations, ensuring alignment with **legal and ethical standards**. |
| **03** | **DCOE Mapping to National Regulations**: |
| | Covers compliance frameworks like **FISMA/NIST RMF**, outlining requirements for cybersecurity operations within the **U.S. Government and DoD**. |
| **04** | **DCOE Mapping to International Norms**: |
| | Discusses **nation-state threats**, international cooperation, and the role of organizations like **NATO CCDCOE** in setting cybersecurity standards. |
| **05** | **DCOE Mapping to Case Studies**: |
| | Includes real-world scenarios (e.g., **Estonia DDoS attacks**, **Operation Glowing Symphony**) to demonstrate the practical application of legal and ethical principles in cybersecurity. |

This equips participants with a thorough understanding of cybersecurity's legal and ethical dimensions in national and international contexts.

## 1158 (NIST ID: K0004)

**Knowledge of cybersecurity principles.**

| | |
|---|---|
| **01** | **DCOE Mapping to Core Cybersecurity Principles**: |
| | The course introduces **confidentiality, integrity, and availability (CIA triad)** as foundational principles, integrated into both defensive and offensive cyberspace operations. |
| **02** | **DCOE Mapping to Defensive Cybersecurity Operations (DCO)**: |
| | Emphasizes **DCO-IDM** and **DCO-RA** as practical applications of cybersecurity principles, focusing on identifying, mitigating, and responding to threats. |
| **03** | **DCOE Mapping to Active Defense Techniques**: |
| | Includes **threat hunting** and use of **indicators of compromise (IOCs)** to proactively apply cybersecurity principles in operational environments. |
| **04** | **DCOE Mapping to Labs**: |
| | Hands-on labs provide experience in applying principles such as **segmentation, encryption**, and secure system configurations to protect critical networks. |
| **05** | **DCOE Mapping to Risk and Threat Analysis**: |
| | Integrates the cyber kill chain and adversary TTPs to reinforce the application of core principles in real-world scenarios. |

This ensures a deep understanding and operational application of cybersecurity principles in both defensive and offensive contexts.

### 1159 (NIST ID: K0005)

**Knowledge of cyber threats and vulnerabilities.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyber Threats**: |
| | Covers adversarial **TTPs** through the **cyber kill chain**, detailing reconnaissance, exploitation, and attack methods used by threat actors. |
| **02** | **DCOE Mapping to Vulnerability Analysis**: |
| | Includes instruction on identifying and mitigating **system vulnerabilities**, with a focus on real-world weaknesses in networks and software. |
| **03** | **DCOE Mapping to Defensive Cybersecurity Operations (DCO)**: |
| | Emphasizes **DCO-IDM** for internal threat detection and **DCO-RA** for external mitigation of advanced persistent threats (APTs) and DDoS attacks. |
| **04** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate scenarios involving **exploitation techniques**, such as lateral movement and privilege escalation, to develop defensive countermeasures. |
| **05** | **DCOE Mapping to Threat Hunting**: |
| | Focuses on analyzing **indicators of compromise (IOCs)** and leveraging threat intelligence to proactively detect and address vulnerabilities. |

This ensures a comprehensive understanding of modern cyber threats and vulnerabilities, paired with practical skills to mitigate them effectively.

## 6900 (NIST ID: K0006)

**Knowledge of specific operational impacts of cybersecurity lapses.**

| | |
|---|---|
| **01** | **DCOE Mapping to Operational Impact Analysis**: |
| | Explains consequences of lapses, such as **loss of data integrity**, system availability, and compromised mission objectives in **cyberspace operations**. |
| **02** | **DCOE Mapping to Case Studies**: |
| | Real-world scenarios, like **Operation Glowing Symphony** and **Estonian DDoS attacks**, demonstrate the cascading effects of cybersecurity breaches on national and operational levels. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate **cyberattack scenarios** to show how unaddressed vulnerabilities can lead to mission-critical failures and adversary exploitation. |
| **04** | **DCOE Mapping to Risk Mitigation**: |
| | Emphasizes **DCO-IDM** and **DCO-RA** for preventing and containing breaches, highlighting the operational cost of delayed or ineffective responses. |
| **05** | **DCOE Mapping to Proactive Measures**: |
| | Focuses on integrating **threat intelligence** and **early detection mechanisms** to minimize operational disruptions caused by cybersecurity lapses. |

This ensures students understand and mitigate the operational consequences of cybersecurity failures in mission-critical environments.

## 6935 (NIST ID: N/A)

**Knowledge of cloud computing service models: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).**

| | |
|---|---|
| **01** | **DCOE Mapping to Cloud Service Models**: |
| | Provides foundational knowledge of **SaaS, IaaS, and PaaS**, focusing on their architecture, use cases, and differences in cybersecurity challenges. |
| **02** | **DCOE Mapping to Threats in Cloud Environments**: |
| | Discusses specific risks, such as **data breaches, misconfigurations**, and shared responsibility vulnerabilities in cloud infrastructures. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate securing and defending **cloud-based systems**, emphasizing **access control, encryption**, and monitoring in SaaS, IaaS, and PaaS scenarios. |
| **04** | **DCOE Mapping to Mitigation Strategies**: |
| | Covers best practices for safeguarding cloud services, such as **identity management, securing APIs**, and implementing network segmentation. |
| **05** | **DCOE Mapping to Operational Integration**: |
| | Explains how cloud service models align with **mission objectives**, emphasizing their advantages and potential security trade-offs in operational contexts. |

This equips participants with a practical understanding of cloud service models and strategies for maintaining their security.

### 6938 (NIST ID: N/A)

**Knowledge of cloud computing deployment models in private, public, and hybrid environments, and the difference between on-premises and off-premises environments.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cloud Deployment Models**: |
| | Explains the characteristics, benefits, and security challenges of **private, public, and hybrid cloud environment** **s**in operational contexts. |
| **02** | **DCOE Mapping to On-Premises vs. Off-Premises**: |
| | Highlights the distinctions between **on-premises data centers** and **off-premises cloud services**, focusing on cost, control, and security implications. |
| **03** | **DCOE Mapping to Labs**: |
| | Provides hands-on practice in configuring and securing **hybrid environments**, emphasizing **data synchronization, access management**, and endpoint protection. |
| **04** | **DCOE Mapping to Security Risks**: |
| | Discusses risks specific to deployment models, such as **data sovereignty issues** in public clouds and **integration challenges** in hybrid setups. |
| **05** | **DCOE Mapping to Operational Strategies**: |
| | Demonstrates how to leverage deployment models to align with **mission requirements**, balancing scalability with operational security. |

This ensures a clear understanding of cloud deployment models and their integration into secure and effective operational strategies.

# Additional KSATs

### 4191 (NIST ID: N/A)

**Ability to apply tradecraft to minimize risk of detection, mitigate risk, and minimize creation of behavioral signature.**

| | |
|---|---|
| **01** | **DCOE Mapping to Operational Tradecraft**: |
| | Teaches methods to reduce detection, including **encryption techniques, stealthy lateral movement**, and avoiding predictable patterns in cyberspace operations. |
| **02** | **DCOE Mapping to Risk Mitigation**: |
| | Focuses on employing **dynamic IP configurations, obfuscation tools**, and techniques for reducing adversary visibility in network traffic. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate **low-profile operations**, emphasizing covert tactics such as **privilege escalation** and evasion of intrusion detection systems (IDS). |
| **04** | **DCOE Mapping to Behavioral Signature Reduction**: |
| | Covers advanced techniques to limit behavioral markers, including **script automation, anti-forensics tools**, and leveraging system-native processes. |
| **05** | **DCOE Mapping to Adversarial Emulation**: |
| | Reinforces tradecraft application by simulating adversary techniques (e.g., TTPs from known APTs), allowing students to refine stealth and detection-avoidance skills. |

This equips participants with practical abilities to operate covertly, reduce detection risks, and maintain mission secrecy in complex environments.

### 4199 (NIST ID: N/A)

**Ability to characterize a target admin/user’s technical abilities, habits, and skills.**

| | |
|---|---|
| **01** | **DCOE Mapping to Target Profiling**: |
| | Provides methods for analyzing **user behavior patterns**, technical proficiency, and typical workflows to infer skills and habits. |
| **02** | **DCOE Mapping to Reconnaissance Techniques**: |
| | Teaches techniques such as **log analysis, system interaction monitoring**, and passive network observation to profile targets effectively. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate scenarios for **monitoring admin activities**, identifying anomalous behaviors, and mapping skillsets based on interaction logs. |
| **04** | **DCOE Mapping to Threat Emulation**: |
| | Incorporates **TTP analysis** to predict potential responses or vulnerabilities based on a user’s technical proficiency and historical actions. |
| **05** | **DCOE Mapping to Operational Use**: |
| | Applies profiling insights to refine **targeted actions**, improve decision-making, and optimize cyber operations while minimizing risks. |

This ensures participants develop practical skills to evaluate and leverage insights into a target’s technical abilities for strategic operational advantage.

### 4204 (NIST ID: N/A)

**Ability to communicate operational plans and actions and provide feedback regarding OPSEC and tradecraft during mission pre-brief.**

| | |
|---|---|
| **01** | **DCOE Mapping to Operational Planning Communication**: |
| | Teaches structured methods for clearly presenting **mission objectives, roles, and action plans** in pre-brief scenarios. |
| **02** | **DCOE Mapping to OPSEC Feedback**: |
| | Emphasizes the evaluation of **operational security measures**, identifying weaknesses in tradecraft, and proposing mitigation strategies during planning stages. |
| **03** | **DCOE Mapping to Labs**: |
| | Includes exercises on **developing and delivering pre-briefs**, focusing on clarity, relevance, and ensuring alignment with mission goals and security protocols. |
| **04** | **DCOE Mapping to Tradecraft Refinement**: |
| | Covers feedback mechanisms to enhance **stealth, risk mitigation**, and alignment with mission tradecraft requirements. |
| **05** | **DCOE Mapping to Collaborative Coordination**: |
| | Reinforces the ability to engage with team members, providing **real-time feedback** on OPSEC and tradecraft while incorporating mission-specific considerations. |

This ensures proficiency in delivering effective pre-briefs, enhancing mission readiness, and maintaining robust operational security.

### 4213 (NIST ID: N/A)

**Ability to conduct open source research.**

| | |
|---|---|
| 01 | **DCOE Mapping to Open Source Research Techniques**: |
| | Teaches methods for leveraging **publicly available information (PAI)**, including search engines, social media platforms, and specialized databases. |
| 02 | **DCOE Mapping to Threat Intelligence Gathering**: |
| | Focuses on identifying **indicators of compromise (IOCs)** and analyzing adversary activity through open-source data. |
| 03 | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate research tasks, such as **identifying organizational vulnerabilities** and mapping adversarial infrastructures using open-source tools. |
| 04 | **DCOE Mapping to Analytical Skills**: |
| | Reinforces critical thinking to validate, contextualize, and correlate open-source data with operational intelligence requirements. |
| 05 | **DCOE Mapping to Ethical Considerations**: |
| | Covers guidelines for **compliance and legal frameworks** in the collection and use of open-source intelligence (OSINT). |

This ensures participants can effectively gather, analyze, and apply open-source data to support mission objectives.

### 4219 (NIST ID: N/A)

**Ability to construct a course of action using available exploitation tools and techniques.**

| | |
|---|---|
| 01 | **DCOE Mapping to Exploitation Planning**: |
| | Guides the creation of **target-specific courses of action (COAs)**, leveraging exploitation tools to achieve mission objectives. |
| 02 | **DCOE Mapping to Tool Utilization**: |
| | Focuses on deploying tools for **privilege escalation, lateral movement**, and data exfiltration while aligning with operational requirements. |
| 03 | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate constructing and executing **exploit-based COAs**, including **vulnerability exploitation** and system compromise scenarios. |
| 04 | **DCOE Mapping to Adaptive Techniques**: |
| | Emphasizes modifying tools and techniques to overcome **environment-specific defenses** and adapt to changing operational landscapes. |
| 05 | **DCOE Mapping to Ethical and Operational Oversight**: |
| | Covers compliance with **rules of engagement (ROE)** and ethical considerations while planning and executing exploitation strategies. |

This ensures participants gain the skills to design and implement effective exploitation plans using available tools and techniques.

### 4222 (NIST ID: N/A)

**Ability to continually research and develop new tools/techniques.**

| | |
|---|---|
| 01 | **DCOE Mapping to Research Methodologies**: |
| | Teaches systematic approaches for identifying emerging trends, vulnerabilities, and technological advancements to guide tool and technique development. |
| 02 | **DCOE Mapping to Tool Development**: |
| | Focuses on creating **custom scripts, payloads**, and tools tailored for specific operational requirements and evolving threats. |
| 03 | **DCOE Mapping to Labs**: |
| | Hands-on labs provide opportunities to **modify existing tools** and develop new ones for advanced tasks, such as **bypassing defenses or automating reconnaissance**. |
| 04 | **DCOE Mapping to Continuous Improvement**: |
| | Encourages iterative testing and refinement of techniques to enhance **efficiency, effectiveness, and stealth** in operations. |
| 05 | **DCOE Mapping to Innovation in Tradecraft**: |
| | Covers leveraging open-source frameworks and **collaborating with the community** to stay ahead of adversaries through innovative practices. |

This ensures participants are equipped to innovate and adapt tools and techniques to meet the dynamic challenges of cybersecurity operations.

### 4229 (NIST ID: N/A)

**Ability to create rules and filters (e.g., Berkeley Packet Filter, Regular Expression).**

| | |
|---|---|
| **01** | **DCOE Mapping to Filtering Fundamentals**: |
| | Teaches the creation of **packet filtering rules** using tools like **Berkeley Packet Filter (BPF)** for precise network traffic analysis and control. |
| **02** | **DCOE Mapping to Regular Expression (Regex) Development**: |
| | Covers crafting **regular expressions** to filter, match, and analyze logs or specific patterns in data for cybersecurity operations. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs provide practical experience in implementing **custom filters** for network traffic inspection, anomaly detection, and log parsing. |
| **04** | **DCOE Mapping to Threat Mitigation**: |
| | Explains the use of rules and filters to **block malicious traffic**, isolate specific threat patterns, and enhance defensive measures. |
| **05** | **DCOE Mapping to Automation**: |
| | Focuses on integrating rules and filters into **automated scripts and monitoring systems**, streamlining operational efficiency. |

This ensures participants can effectively create and deploy filtering rules and expressions to support cybersecurity objectives.

### 4243 (NIST ID: N/A)

**Ability to ensure collected data is transferred to the appropriate storage locations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Data Transfer Protocols**: |
| | Teaches secure methods for transferring data, such as **SFTP, SCP, and HTTPS**, ensuring confidentiality and integrity during transit. |
| **02** | **DCOE Mapping to Storage Solutions**: |
| | Covers the use of **centralized logging systems, cloud storage**, and local repositories to organize and secure collected data effectively. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate **data collection and transfer workflows**, focusing on maintaining operational efficiency and compliance with policies. |
| **04** | **DCOE Mapping to Error Mitigation**: |
| | Emphasizes methods to identify and resolve transfer issues, such as **network bottlenecks or permission errors**, to ensure seamless operations. |
| **05** | **DCOE Mapping to Compliance and Security**: |
| | Includes instruction on adhering to **data retention policies**, access controls, and encryption standards to protect sensitive information. |

This equips participants to manage secure and efficient data transfers aligned with operational and compliance requirements.

### 4244 (NIST ID: N/A)

**Ability to enumerate a network.**

| | |
|---|---|
| **01** | **DCOE Mapping to Network Enumeration Techniques**: |
| | Teaches methods for identifying **hosts, devices, services, and open ports** within a network using tools like **Nmap and Netstat**. |
| **02** | **DCOE Mapping to Active and Passive Enumeration**: |
| | Covers both **active scanning** for detailed insights and **passive observation** to minimize detection during enumeration activities. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate enumeration tasks, such as **mapping network topologies**, identifying vulnerabilities, and cataloging assets. |
| **04** | **DCOE Mapping to Threat Assessment**: |
| | Focuses on analyzing results to uncover **misconfigurations, exposed services**, and potential entry points for exploitation. |
| **05** | **DCOE Mapping to Operational Integration**: |
| | Demonstrates the role of enumeration in broader **cyber operations**, supporting both defensive hardening and offensive planning. |

This ensures participants can effectively enumerate networks to gain actionable insights while minimizing operational risk.

### 4248 (NIST ID: N/A)

**Ability to enumerate user permissions and privileges.**

| | |
|---|---|
| **01** | **DCOE Mapping to Privilege Enumeration Techniques**: |
| | Teaches the identification of **user roles, group memberships**, and associated permissions using tools like **PowerShell, Linux commands**, and AD utilities. |
| **02** | **DCOE Mapping to Access Control Analysis**: |
| | Focuses on evaluating **access control lists (ACLs)** and identifying potential **privilege escalation paths**. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate tasks such as **auditing user permissions**, detecting misconfigurations, and verifying least privilege principles. |
| **04** | **DCOE Mapping to Threat Mitigation**: |
| | Emphasizes remediation of overprivileged accounts and securing **critical systems** against unauthorized access. |
| **05** | **DCOE Mapping to Operational Relevance**: |
| | Demonstrates the integration of privilege enumeration in **post-exploitation scenarios** and **defensive assessments**. |

This ensures participants can accurately enumerate and assess user privileges to support security posture enhancement and operational planning.

### 4249 (NIST ID: N/A)

**Ability to evade or counter security products or host-based defenses.**

| | |
|---|---|
| **01** | **DCOE Mapping to Evasion Techniques**: |
| | Teaches methods to bypass **antivirus (AV), endpoint detection and response (EDR), and intrusion detection systems (IDS)** using obfuscation and stealthy payload delivery. |
| **02** | **DCOE Mapping to Countermeasure Avoidance**: |
| | Focuses on strategies to evade **firewalls, host-based monitoring**, and behavior-based analytics through **encryption, polymorphic malware**, and process injection. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate scenarios for testing and refining techniques to evade **host-based defenses**, including **bypassing application whitelisting**. |
| **04** | **DCOE Mapping to Adversary Emulation**: |
| | Reinforces evasion skills through **red team exercises** that replicate advanced persistent threat (APT) tactics. |
| **05** | **DCOE Mapping to Ethical and Operational Compliance**: |
| | Emphasizes **rules of engagement (ROE)** and ethical considerations to ensure proper use of evasion techniques in authorized scenarios. |

This ensures participants can effectively bypass security products in controlled environments, supporting both offensive and defensive mission objectives.

### 4261 (NIST ID: N/A)

**Ability to exploit vulnerabilities to gain additional access.**

| | |
|---|---|
| **01** | **DCOE Mapping to Exploitation Techniques**: |
| | Teaches methods for leveraging **buffer overflows, privilege escalation**, and misconfigurations to gain elevated access or move laterally. |
| **02** | **DCOE Mapping to Vulnerability Analysis**: |
| | Focuses on identifying exploitable weaknesses using tools like **Metasploit, Nessus**, and custom scripts to target specific vulnerabilities. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs provide practical experience in **exploiting common vulnerabilities** (e.g., CVEs) and gaining control over network assets. |
| **04** | **DCOE Mapping to Post-Exploitation**: |
| | Covers maintaining persistence, escalating privileges, and harvesting credentials after gaining access to the target. |
| **05** | **DCOE Mapping to Ethical Use and Oversight**: |
| | Stresses compliance with **rules of engagement (ROE)** and ensures exploitation aligns with authorized objectives in controlled environments. |

This ensures participants develop the skills to exploit vulnerabilities effectively and responsibly to support mission-critical operations.

### 4263 (NIST ID: N/A)

**Ability to extract credentials from hosts.**

| | |
|---|---|
| **01** | **DCOE Mapping to Credential Extraction Techniques:** |
| | Discusses methods for identifying and accessing stored credentials on target systems as part of post-exploitation tasks. |
| **02** | **DCOE Mapping to Labs:** |
| | Hands-on labs simulate scenarios involving the discovery of credential storage locations, such as files, memory, and configuration settings, and their extraction. |
| **03** | **DCOE Mapping to Post-Exploitation Activities:** |
| | Covers techniques for securely handling and leveraging extracted credentials to gain further access or escalate privileges within the operational environment. |
| **04** | **DCOE Mapping to Defensive Considerations:** |
| | Explores strategies for mitigating credential theft, including hardening systems and protecting sensitive information from unauthorized access. |
| **05** | **DCOE Mapping to Operational Relevance:** |
| | Demonstrates the role of credential extraction in broader cybersecurity operations, ensuring alignment with mission objectives and compliance. |

This ensures participants can effectively extract and utilize credentials while understanding their security implications.

### 4271 (NIST ID: N/A)

**Ability to identify capability gaps (e.g., insufficient tools, training, or infrastructure).**

| | |
|---|---|
| **01** | **DCOE Mapping to Capability Assessment**: |
| | Teaches methods for evaluating current **tools, infrastructure, and training** against mission requirements to identify deficiencies. |
| **02** | **DCOE Mapping to Operational Readiness**: |
| | Covers analysis of **mission needs and objectives** to highlight gaps in cybersecurity capabilities that could hinder performance. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate scenarios to test and evaluate **tools, infrastructure resilience**, and skill readiness, exposing areas needing improvement. |
| **04** | **DCOE Mapping to Strategic Planning**: |
| | Focuses on developing **actionable plans** to address gaps, including recommendations for acquiring new tools, enhancing training, or upgrading systems. |
| **05** | **DCOE Mapping to Continuous Improvement**: |
| | Reinforces the importance of iterative assessments to keep pace with evolving threats and operational demands. |

This ensures participants can systematically identify and address capability gaps, strengthening cybersecurity operations.

### 4276 (NIST ID: N/A)

**Ability to identify files containing information critical to operational objectives.**

| | |
|---|---|
| **01** | **DCOE Mapping to File Identification Techniques**: |
| | Teaches methods for locating and analyzing files using tools like **file system exploration**, metadata analysis, and keyword searches to identify critical data. |
| **02** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate the process of **searching file directories**, extracting metadata, and analyzing file content to determine relevance to mission objectives. |
| **03** | **DCOE Mapping to Operational Relevance**: |
| | Covers techniques to prioritize and secure identified files containing **sensitive or mission-critical information**during cybersecurity operations. |
| **04** | **DCOE Mapping to Threat Mitigation**: |
| | Focuses on preventing unauthorized access or leakage of critical files by implementing **file-level encryption and access control** strategies. |
| **05** | **DCOE Mapping to Data Categorization**: |
| | Reinforces understanding of file types, formats, and contexts to quickly recognize and safeguard **essential operational data**. |

This ensures participants are skilled in identifying and securing critical files within operational environments.

### 4278 (NIST ID: N/A)

**Ability to identify legal, policy, and technical limitations when conducting cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Legal and Policy Frameworks**: |
| | Explains national and international laws, **rules of engagement (ROE)**, and organizational policies governing cyberspace operations. |
| **02** | **DCOE Mapping to Technical Constraints**: |
| | Covers limitations such as **infrastructure capabilities, tool effectiveness**, and compatibility issues impacting operational execution. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs include exercises that integrate **legal and technical scenario-based constraints**, enabling participants to navigate operational boundaries. |
| **04** | **DCOE Mapping to Risk Management**: |
| | Focuses on balancing operational objectives with adherence to **legal, ethical, and technical guidelines**, mitigating potential risks. |
| **05** | **DCOE Mapping to Operational Decision-Making**: |
| | Reinforces evaluating limitations in real-time to adapt strategies while remaining compliant with **legal and technical requirements**. |

This ensures participants can identify and address constraints to execute cyberspace operations within defined boundaries.

### 4279 (NIST ID: N/A)

**Ability to identify logging capabilities on host.**

| | |
|---|---|
| **01** | **DCOE Mapping to Logging Configuration Analysis**: |
| | Teaches methods to locate and analyze **logging services** on hosts, such as **Windows Event Logs, syslog**, and application-specific logs. |
| **02** | **DCOE Mapping to Labs**: |
| | Hands-on labs focus on identifying logging capabilities, ensuring proper **log file locations, formats**, and configurations are understood and utilized. |
| **03** | **DCOE Mapping to Log Evaluation**: |
| | Covers techniques to verify the **accuracy, completeness, and reliability** of host-based logging systems for operational insights. |
| **04** | **DCOE Mapping to Operational Use**: |
| | Demonstrates the integration of logs into **incident detection, analysis, and forensic investigations**, emphasizing their role in host monitoring. |
| **05** | **DCOE Mapping to Enhancing Capabilities**: |
| | Explores best practices for **enabling and customizing logging configurations**, ensuring host systems generate actionable data. |

This ensures participants can identify, evaluate, and leverage host-based logging capabilities to support cybersecurity objectives.

### 4285 (NIST ID: N/A)

**Ability to identify what tools or Tactics, Techniques, and Procedures (TTPs) are applicable to a given situation.**

| | |
|---|---|
| **01** | **DCOE Mapping to TTP Analysis**: |
| | Teaches evaluation of operational scenarios to match **adversary tactics** with appropriate **defensive or offensive techniques**. |
| **02** | **DCOE Mapping to Tool Selection**: |
| | Covers selecting and deploying tools best suited for specific tasks, such as **vulnerability assessment, network reconnaissance**, or privilege escalation. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate operational environments, requiring participants to choose and apply **tools and TTPs** to achieve mission objectives. |
| **04** | **DCOE Mapping to Scenario-Based Planning**: |
| | Focuses on assessing **mission requirements and environmental factors** to align TTPs with desired outcomes. |
| **05** | **DCOE Mapping to Adaptation Skills**: |
| | Reinforces the ability to adjust **tools and TTPs** dynamically in response to changing conditions or adversary actions. |

This ensures participants can effectively evaluate and apply the most relevant tools and TTPs to meet situational requirements in cyberspace operations.

### 4292 (NIST ID: N/A)

**Ability to improve the performance of cyberspace operators by providing constructive (positive and negative) feedback.**

| | |
|---|---|
| **01** | **DCOE Mapping to Feedback Techniques**: |
| | Teaches methods for delivering actionable **positive reinforcement** and identifying areas for improvement using the **Plan-Brief-Execute-Debrief (PBED)** framework. |
| **02** | **DCOE Mapping to Performance Evaluation**: |
| | Integrates PBED principles by focusing on **post-execution debriefs** to assess operational tasks and provide feedback tailored to **individual and team skillsets**. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate operational scenarios, incorporating PBED by having participants **plan and brief missions**, execute tasks, and conduct debriefs with constructive feedback. |
| **04** | **DCOE Mapping to Team Development**: |
| | Reinforces PBED as a structured approach to fostering **collaboration, accountability**, and iterative improvement through targeted feedback. |
| **05** | **DCOE Mapping to Leadership Skills**: |
| | Highlights the role of **effective communication during debriefs**, ensuring feedback is productive, motivating, and aligned with mission objectives. |

This ensures participants can effectively apply the PBED model to provide feedback that drives performance improvements and cultivates a culture of excellence in cyberspace operations.

### 4293 (NIST ID: N/A)

**Ability to install/modify/uninstall tools on target systems in accordance with current policies and procedures.**

| | |
|---|---|
| **01** | **DCOE Mapping to Tool Deployment**: |
| | Covers secure methods for **installing, modifying, and uninstalling tools** on target systems, ensuring compliance with operational policies. |
| **02** | **DCOE Mapping to Procedural Adherence**: |
| | Focuses on aligning tool deployment activities with **rules of engagement (ROE)** and organizational procedures to maintain operational integrity. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate scenarios for **tool installation and removal**, emphasizing minimal disruption and stealth in operational environments. |
| **04** | **DCOE Mapping to Tool Customization**: |
| | Explains how to **modify tools** to adapt to mission-specific requirements while avoiding detection by host-based defenses. |
| **05** | **DCOE Mapping to Policy Compliance**: |
| | Reinforces the importance of **audit trails, documentation**, and adherence to established protocols to ensure accountability. |

By integrating these capabilities, participants gain practical skills to manage tools on target systems effectively and ethically within defined policies and procedures.

### 4293 (NIST ID: N/A)

**Ability to install/modify/uninstall tools on target systems in accordance with current policies and procedures.**

| | |
|---|---|
| **01** | **DCOE Mapping to Secure Tool Deployment**: |
| | Teaches methods for **installing, modifying, and uninstalling tools** while maintaining operational security and minimizing detection risks. |
| **02** | **DCOE Mapping to Policy Adherence**: |
| | Focuses on aligning actions with **rules of engagement (ROE), organizational policies**, and documented procedures to ensure compliance. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs provide practice in **stealthily deploying and removing tools** on target systems under realistic operational constraints. |
| **04** | **DCOE Mapping to Tool Customization**: |
| | Covers techniques for **modifying tools** to fit mission-specific requirements, including bypassing host-based defenses and optimizing functionality. |
| **05** | **DCOE Mapping to Operational Accountability**: |
| | Reinforces the need for **detailed documentation and reporting** of tool management activities to support auditability and mission transparency. |

This ensures participants develop the technical proficiency to manage tools on target systems effectively while adhering to policies and maintaining operational integrity.

### 4296 (NIST ID: N/A)

**Ability to interpret device configurations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Configuration Analysis**: |
| | Teaches methods for reviewing and understanding **device configurations**, including firewalls, routers, switches, and endpoint security systems. |
| **02** | **DCOE Mapping to Security Posture Assessment**: |
| | Focuses on identifying **misconfigurations, vulnerabilities**, and deviations from best practices that could impact operational security. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on labs provide experience in accessing, interpreting, and analyzing configurations for **network devices and operating systems**. |
| **04** | **DCOE Mapping to Operational Integration**: |
| | Demonstrates how to leverage configuration insights to support **threat mitigation, system hardening**, and troubleshooting. |
| **05** | **DCOE Mapping to Policy Alignment**: |
| | Covers techniques for ensuring configurations comply with **organizational policies** and industry standards. |

This ensures participants can effectively interpret and analyze device configurations to enhance security and operational efficiency.

### 4297 (NIST ID: N/A)

**Ability to interpret technical materials such as RFCs and technical manuals.**

| | |
|---|---|
| **01** | **DCOE Mapping to Technical Interpretation Skills**: |
| | Teaches methods to extract actionable information from **technical documents**, including protocol specifications and manuals for operational tools. |
| **02** | **DCOE Mapping to Practical Application**: |
| | Includes guidance on using information from manuals to configure systems and troubleshoot issues effectively during operations. |
| **03** | **DCOE Mapping to Labs**: |
| | Hands-on exercises emphasize interpreting **lab instructions, tool documentation**, and applying insights to configure and execute technical tasks accurately. |
| **04** | **DCOE Mapping to Operational Context**: |
| | Reinforces the ability to apply insights from technical materials in real-world scenarios, such as implementing tools or adhering to protocol requirements. |

This ensures participants can accurately understand and apply information from technical references critical to mission success. The content aligns strictly with practical application details outlined in the DCOE course materials.

### 4298 (NIST ID: N/A)

**Ability to maintain situational awareness of the target environment.**

| | |
|---|---|
| **01** | **DCOE Mapping to Network Traffic Analysis**: |
| | Participants analyze network activity to establish baselines and identify anomalies using tools like **Wireshark** and **tcpdump**. For example, a lab exercise involves capturing and analyzing network traffic to spot potential compromises. |
| **02** | **DCOE Mapping to IDS/IPS Deployment**: |
| | Hands-on labs include configuring and monitoring Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), enabling participants to track suspicious behaviors in real-time. |
| **03** | **DCOE Mapping to Threat Intelligence Integration**: |
| | Exercises involve correlating information from tools like Snort and Suricata alerts with network traffic to detect and analyze indicators of compromise (IOCs). |
| **04** | **DCOE Mapping to Hunting Operations**: |
| | Students are tasked with conducting **hunting missions**, proactively searching for malicious activity within a simulated network environment based on specific intelligence. |
| **05** | **DCOE Mapping to OSINT Integration**: |
| | A dedicated lab focuses on leveraging Open Source Intelligence (OSINT) for mapping the operational environment, adding external threat context to situational awareness. |

These activities ensure participants develop the skills to monitor, analyze, and respond effectively within a dynamic target environment.

### 4305 (NIST ID: N/A)

**Ability to model a simulated environment to conduct mission rehearsal and mitigate the risk of actions taken during operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to PBED Framework**: |
| | The **Plan-Brief-Execute-Debrief (PBED)** framework is central to modeling simulated environments. The **Plan** phase incorporates the ME3C-(PC)2 Model, which ensures mission objectives, environmental analysis, and potential contingencies are fully accounted for before simulation development. |
| **02** | **DCOE Mapping to Mission Planning**: |
| | The **Brief** phase ensures all operators understand their roles in the simulated environment. This includes walkthroughs of tools and techniques to be used, as well as identifying Go/No-Go criteria to mitigate risks during rehearsals. |
| **03** | **DCOE Mapping to Execution in Simulated Environments**: |
| | The **Execute** phase involves running the modeled environment to simulate adversarial actions and defensive responses, capturing logs for analysis. This provides real-time feedback on mission readiness and highlights operational gaps. |
| **04** | **DCOE Mapping to Debriefing and Risk Mitigation**: |
| | The **Debrief** phase is critical for evaluating the performance of the simulation. Logs and observations are reviewed to identify what went wrong, contributing factors, and root causes. This phase emphasizes developing lessons learned and instructional fixes to refine future simulations. |
| **05** | **DCOE Mapping to Labs**: |
| | Labs associated with PBED exercises guide participants through real-world tasks, such as using **Wireshark for network monitoring** or configuring systems to assess attack vectors within the simulation. |

This structured approach ensures that mission rehearsals are comprehensive, risks are mitigated, and operators are prepared for real-world scenarios.

### 4308 (NIST ID: N/A)

**Ability to operate automated systems to interact with the target environment.**

| | |
|---|---|
| **01** | **DCOE Mapping to Automated Interaction Tools**: |
| | Participants learn to use tools like **Metasploit** and **Armitage** for scanning and exploiting target environments, including scanning machines for open ports and selecting appropriate attack methods. |
| **02** | **DCOE Mapping to Automated Exploitation**: |
| | Labs focus on delivering **automated payloads** and interacting with compromised hosts by executing to confirm access and validate results. |
| **03** | **DCOE Mapping to Risk Mitigation**: |
| | Training emphasizes proper tool usage to prevent network disruption while maintaining operational security and ethical compliance. |
| **04** | **DCOE Mapping to Real-Time Monitoring**: |
| | Activities involve observing system-generated data in real-time, allowing operators to adjust actions dynamically based on live feedback. |
| **05** | **DCOE Mapping to Policy Adherence**: |
| | Operators are trained to follow rules of engagement and use automated tools responsibly during interactions with the target environment. |

This ensures participants can effectively operate automated systems to achieve mission objectives in the target environment while maintaining ethical and procedural integrity.

### 4324 (NIST ID: N/A)

**Ability to perform masquerade operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Masquerade Techniques**: |
| | Teaches methods for impersonating legitimate users or processes to evade detection, including **file name manipulation**, process injection, and credential spoofing. |
| **02** | **DCOE Mapping to Labs**: |
| | Hands-on labs simulate scenarios involving masquerade techniques, such as mimicking legitimate system processes or using **stolen credentials** to access restricted areas. |
| **03** | **DCOE Mapping to Detection Avoidance**: |
| | Focuses on leveraging stealth tactics to avoid detection by endpoint security tools, intrusion detection systems, or behavior-based analytics. |
| **04** | **DCOE Mapping to Operational Scenarios**: |
| | Demonstrates the application of masquerade operations during mission-critical tasks to maintain access and execute objectives without triggering alerts. |
| **05** | **DCOE Mapping to Ethical and Procedural Oversight**: |
| | Emphasizes adherence to **rules of engagement (ROE)** and operational policies to ensure ethical application of masquerade techniques. |

This prepares participants to execute effective masquerade operations while maintaining compliance with operational and ethical standards.

### 4325 (NIST ID: N/A)

**Ability to perform privilege escalation.**

| | |
|---|---|
| **01** | **DCOE Mapping to Escalation Techniques**: |
| | Covers methods to exploit misconfigurations and vulnerabilities for privilege escalation, such as using tools like Metasploit to elevate access from lower-privileged accounts to root or administrative levels. |
| **02** | **DCOE Mapping to Labs**: |
| | Labs include tasks where participants execute privilege escalation, such as:<br>• Using Metasploit to exploit a vulnerable service and confirm privilege escalation.<br>• Extracting and analyzing password hashes to access higher-privilege accounts. |
| **03** | **DCOE Mapping to Post-Escalation Actions**: |
| | Includes hands-on activities to secure elevated access, such as obtaining sensitive files (e.g., /etc/passwd) and maintaining persistence using techniques like service abuse and credential modification. |
| **04** | **DCOE Mapping to Threat Mitigation**: |
| | Participants analyze and identify steps to mitigate privilege escalation risks by applying patches, correcting misconfigurations, and strengthening access control policies. |
| **05** | **DCOE Mapping to Ethical Compliance**: |
| | Reinforces adherence to **rules of engagement (ROE)** while practicing escalation techniques in a controlled and ethical manner during operations. |

This ensures participants gain technical expertise in privilege escalation while maintaining operational integrity and compliance.

## 4327 (NIST ID: N/A)

**Ability to persist access to a target.**

| | |
|---|---|
| **01** | **DCOE Mapping to Persistence Techniques**: |
| | Explores methods such as **rootkits**, tunneling, and remote access to maintain a foothold in the target environment after initial access. |
| **02** | **DCOE Mapping to Command and Control (C2)**: |
| | Hands-on labs include scenarios for establishing C2 channels using tools like **Meterpreter** and maintaining connections via encrypted traffic, such as HTTPS shells, to bypass detection. |
| **03** | **DCOE Mapping to Rootkits Lab**: |
| | Participants execute the **Kernel Rootkit hands-on lab**, gaining experience in installing rootkits to hook into the operating system kernel and maintain persistence while evading detection. |
| **04** | **DCOE Mapping to Tunneling Techniques**: |
| | Labs involve using **HTTPTunnel** to send packets over HTTP connections, ensuring operational continuity even in restricted network environments. |
| **05** | **DCOE Mapping to Real-World Applications**: |
| | Emphasizes maintaining persistence across reboots or interruptions by deploying techniques like **service abuse** or fileless malware strategies. |

This equips participants with the skills to ensure access persistence in complex operational scenarios while leveraging advanced tools and methods.

### 4330 (NIST ID: N/A)

**Ability to plan, brief, execute, and debrief a mission.**

| | |
|---|---|
| **01** | **DCOE Mapping to Planning with PBED Framework**: |
| | The Plan-Brief-Execute-Debrief (PBED) framework begins with detailed planning, leveraging the ME3C-(PC)$^2$ model to address Mission, Environment, Enemy, Effects, Capabilities, Phasing, Contracts, and Contingencies. This phase ensures clarity in objectives and operational alignment. |
| **02** | **DCOE Mapping to Planning Labs**: |
| | Practical exercises involve using tools such as Nmap and Metasploit to gather intelligence, map target environments, and identify vulnerabilities. The planning phase ensures risk assessment and preparedness in simulated environments. |
| **03** | **DCOE Mapping to Briefing for Mission Execution**: |
| | Participants practice mission briefings, assigning roles and responsibilities while setting clear objectives. Briefings focus on establishing Go/No-Go criteria and aligning the team on operational priorities. |
| **04** | **DCOE Mapping to Execution Phase**: |
| | Labs guide participants through executing missions in controlled scenarios, including deploying payloads, monitoring operations, and maintaining comprehensive logs to capture actions and outcomes. |
| **05** | **DCOE Mapping to Debriefing Process**: |
| | Post-mission debriefs emphasize analyzing mission outcomes, identifying root causes of challenges, and developing instructional fixes. This phase reinforces actionable lessons learned for continuous improvement in future operations. |

This structured PBED approach ensures participants are proficient in conducting full-cycle mission planning, execution, and review to enhance operational effectiveness.

### 4334 (NIST ID: N/A)

**Ability to promote and enable organizational change.**

| | |
|---|---|
| **01** | **DCOE Mapping to Strategic Change Management**: |
| | Focuses on identifying areas within an organization that require transformation to adapt to emerging cyber threats and evolving operational needs. Emphasizes aligning change initiatives with overarching mission goals and objectives. |
| **02** | **DCOE Mapping to Collaborative Planning Labs**: |
| | Participants engage in hands-on labs simulating organizational shifts, such as integrating advanced tools or implementing new cybersecurity policies. These labs demonstrate how to address resistance and build support across teams. |
| **03** | **DCOE Mapping to Persistent Engagement**: |
| | Reinforces the concept of continual adaptation and innovation, enabling teams to remain proactive in addressing challenges through collaboration and information sharing. |
| **04** | **DCOE Mapping to Debrief and Feedback**: |
| | Post-mission debriefs include identifying barriers to change and devising strategies to overcome them. Instructional fixes and lessons learned are used to refine future change management initiatives. |
| **05** | **DCOE Mapping to Leadership Skills Development**: |
| | Includes training on effective communication, persuasion techniques, and leadership strategies to guide organizations through transformation while maintaining morale and operational effectiveness. |

This ensures participants are equipped to drive meaningful organizational change, fostering adaptability and resilience within mission-critical environments.

### 4335 (NIST ID: N/A)

**Ability to provide advice and guidance to various stakeholders regarding technical issues, capabilities, and approaches.**

| | |
|---|---|
| **01** | **DCOE Mapping to Stakeholder Communication**: |
| | Participants learn effective communication strategies for presenting technical concepts to non-technical audiences, ensuring clarity and actionable understanding during operations. |
| **02** | **DCOE Mapping to Scenario-Based Labs**: |
| | Labs focus on simulating interactions with diverse stakeholders, including briefing leadership on identified vulnerabilities and recommending remediation strategies using tools like OpenCTI for threat analysis. |
| **03** | **DCOE Mapping to Threat Intelligence Sharing**: |
| | Includes exercises on using platforms such as MISP and TAXII to demonstrate technical capabilities and share actionable insights tailored to stakeholder needs. |
| **04** | **DCOE Mapping to Multidisciplinary Collaboration**: |
| | Reinforces the importance of working across functional teams, ensuring technical advice aligns with organizational objectives and stakeholder priorities. |
| **05** | **DCOE Mapping to Policy and Compliance**: |
| | Participants practice advising stakeholders on aligning technical solutions with legal, ethical, and operational policies, emphasizing risk management and strategic planning. |

This ensures participants are equipped to effectively advise and guide stakeholders, bridging technical expertise and organizational decision-making.

### 4336 (NIST ID: N/A)

**Ability to provide feedback to developers if a tool requires continued development.**

| | |
|---|---|
| **01** | **DCOE Mapping to Tool Performance Evaluation**: |
| | Covers methods for assessing tool effectiveness by identifying functionality gaps, performance inefficiencies, or compatibility issues during operational testing. |
| **02** | **DCOE Mapping to Labs on Vulnerability Scanning Tools**: |
| | Participants use tools like **Nmap** and **Nikto** to identify weaknesses in existing configurations and report areas where the tools could be enhanced for improved detection and usability. |
| **03** | **DCOE Mapping to Root Cause Analysis**: |
| | Labs involve diagnosing tool malfunctions or limited outputs by reviewing system logs, tool configurations, and operational environments to provide actionable insights to developers. |
| **04** | **DCOE Mapping to Collaboration with Developers**: |
| | Exercises simulate scenarios where participants document findings and propose enhancements such as better user interfaces, streamlined workflows, or expanded database support for threat indicators. |
| **05** | **DCOE Mapping to Post-Mission Debriefing**: |
| | Incorporates the use of **Instructional Fixes** from the PBED framework to provide structured feedback to developers, ensuring tools are continually improved based on mission requirements. |

This approach equips participants to identify and communicate technical improvements for tools, fostering collaboration with development teams to enhance operational capabilities.

### 4340 (NIST ID: N/A)

**Ability to provide technical leadership within an organization.**

| | |
|---|---|
| **01** | **DCOE Mapping to Leadership in Mission Planning**: |
| | Focuses on using structured frameworks like the ME3C-(PC)$^2$ model to lead operational planning efforts, ensuring alignment with organizational goals and mission objectives. Leaders guide the integration of tactical and strategic priorities across teams. |
| **02** | **DCOE Mapping to Collaborative Exercises**: |
| | Hands-on labs emphasize leading collaborative sessions for cyber defense and offense, including managing cross-disciplinary teams during exercises such as network hardening, threat hunting, and simulated response to cyber incidents. |
| **03** | **DCOE Mapping to PBED Implementation**: |
| | Leaders are trained to implement the PBED (Plan, Brief, Execute, Debrief) cycle effectively, fostering team accountability and continuous improvement through structured feedback mechanisms. |
| **04** | **DCOE Mapping to Effective Communication**: |
| | Training includes techniques for articulating technical strategies to non-technical stakeholders and ensuring transparency in decision-making processes while maintaining operational security. |
| **05** | **DCOE Mapping to Organizational Innovation**: |
| | Encourages fostering a culture of persistent innovation and adaptation by identifying and integrating new technologies, methodologies, and tactics into organizational operations. |

This ensures participants are equipped to provide decisive and informed leadership, enabling their organizations to navigate complex technical challenges effectively.

## 4341 (NIST ID: N/A)

**Ability to read, write, modify, and execute compiled languages (e.g., C).**

| | |
|---|---|
| **01** | **DCOE Mapping to Code Analysis**: |
| | Training includes identifying and understanding compiled code structures, focusing on reverse engineering techniques used to analyze compiled binaries in cybersecurity operations. |
| **02** | **DCOE Mapping to Debugging Exercises**: |
| | Participants engage in labs where they analyze executable files, modify binary code, and observe the impact on system behavior. These exercises provide insight into how compiled languages function and their relevance to cyber operations. |
| **03** | **DCOE Mapping to Vulnerability Exploitation**: |
| | Labs include scenarios where participants manipulate executable code to exploit vulnerabilities, demonstrating the ability to modify and execute compiled programs in controlled environments. |
| **04** | **DCOE Mapping to Malware Examination**: |
| | Exercises focus on analyzing malicious executables, understanding their compiled structure, and modifying components to study potential countermeasures or defensive strategies. |
| **05** | **DCOE Mapping to Custom Tool Usage**: |
| | Participants practice using tools designed to decompile and modify binaries, applying these skills to cybersecurity tasks such as detecting tampered code or refining operational scripts. |

### 4342 (NIST ID: N/A)

**Ability to recognize and extract salient information from a large data set (e.g., critical information, anomalies).**

| | |
|---|---|
| **01** | **DCOE Mapping to Data Aggregation Techniques**: |
| | Participants learn to use tools such as **Maltego** and **ThreatMiner** for analyzing large datasets and identifying critical information. Maltego provides graphical link analysis to map relationships, while ThreatMiner aggregates data to detect potential threats and anomalies. |
| **02** | **DCOE Mapping to Labs for Data Analysis**: |
| | Labs involve using ThreatMiner to analyze malware hashes and extract relevant threat indicators, focusing on IP addresses, domain details, and file hashes. Participants also work with Maltego to identify connections and anomalies in structured datasets. |
| **03** | **DCOE Mapping to Anomaly Detection**: |
| | Exercises emphasize recognizing unusual patterns in network traffic or file behavior using tools like **Wireshark** and **Security Onion** to create baselines and detect deviations. |
| **04** | **DCOE Mapping to Practical Scenarios**: |
| | Labs include scenarios where participants extract and prioritize critical information from malware-related datasets or real-time network monitoring to identify actionable intelligence. |
| **05** | **DCOE Mapping to Reporting and Actionable Insights**: |
| | Training includes documenting findings in detailed reports that highlight extracted anomalies and critical data points for decision-making in operational environments. |

These hands-on exercises equip participants to efficiently process and analyze large datasets to extract valuable and actionable intelligence strictly using DCOE course materials.

### 4343 (NIST ID: N/A)

**Ability to recognize and report mistakes or poor tradecraft to appropriate leadership in accordance with Standard Operating Procedures (SOPs).**

| | |
|---|---|
| **01** | **DCOE Mapping to PBED Framework for Mistake Identification**: |
| | During the **Debrief phase** of the PBED process, participants are trained to document mission errors and poor tradecraft. Using structured approaches like identifying Debrief Focus Points (DFPs), they trace contributing factors to pinpoint root causes. This process fosters accountability and improvement. |
| **02** | **DCOE Mapping to Mission Logs**: |
| | Hands-on labs involve maintaining comprehensive logs during mission execution. These logs are critical for mission reconstruction and identifying deviations from SOPs, enabling operators to highlight tradecraft issues systematically. |
| **03** | **DCOE Mapping to Leadership Briefing Scenarios**: |
| | Labs include exercises where participants simulate presenting mission errors to leadership. This includes detailing what went wrong, why it occurred, and proposing actionable fixes based on SOPs. |
| **04** | **DCOE Mapping to Instructional Fixes**: |
| | Participants are tasked with developing Instructional Fixes and Lessons Learned during post-mission reviews, ensuring future missions avoid repeated mistakes. |
| **05** | **DCOE Mapping to Tradecraft Improvement**: |
| | Scenarios emphasize recognizing inadequate tactics or techniques, documenting them, and reporting these issues to leadership with clear, actionable recommendations for refinement. |

This structured training ensures operators can effectively identify and communicate mission errors, fostering a culture of continuous improvement and adherence to SOPs.

### 4344 (NIST ID: N/A)

**Ability to recognize and respond appropriately to Non-Standard Events.**

| | |
|---|---|
| **01** | **DCOE Mapping to Anomaly Detection Techniques**: |
| | Participants are trained to identify deviations from normal behavior in networks using tools like **Security Onion** and **Suricata**. Labs involve monitoring real-time events and alerts triggered by unexpected network activity. |
| **02** | **DCOE Mapping to Incident Response Labs**: |
| | Hands-on exercises guide participants through responding to non-standard events, such as identifying high-priority alerts generated during **intense Nmap scans** and investigating their root causes. |
| **03** | **DCOE Mapping to OSINT Integration**: |
| | Training includes gathering external data to contextualize non-standard events, ensuring a comprehensive understanding of their impact and mitigating risks effectively. |
| **04** | **DCOE Mapping to Reporting and Documentation**: |
| | Labs require participants to document anomalies, detailing their significance and proposed responses in structured reports, enhancing situational awareness and decision-making. |
| **05** | **DCOE Mapping to Proactive Measures**: |
| | Participants learn strategies to fortify networks against similar events, ensuring continuous monitoring and readiness for future anomalies. |

This structured training ensures participants can detect, analyze, and respond effectively to non-standard events while maintaining operational continuity.

### 4345 (NIST ID: N/A)

**Ability to redirect and tunnel through target systems.**

| | |
|---|---|
| **01** | **DCOE Mapping to HTTP Tunneling Techniques**: |
| | Labs include hands-on exercises with **HTTPTunnel**, where participants send packets through allowed protocols such as HTTP using GET and POST requests. This bypasses firewalls that restrict other types of traffic while maintaining stealth within the target environment. |
| **02** | **DCOE Mapping to DNS Tunneling**: |
| | Participants practice tunneling through DNS traffic using **dns2tcp**, configuring both server and client sides, and employing the SSH protocol to secure data transmission through DNS requests. |
| **03** | **DCOE Mapping to Remote Access Protocols**: |
| | Labs demonstrate the use of **Telnet** and **SSH** for remote command execution, including tunneling encrypted and unencrypted data between devices. Participants explore the advantages and risks of each protocol. |
| **04** | **DCOE Mapping to Covert Channels**: |
| | Additional lab exercises focus on establishing covert channels to redirect data and communication within compromised environments without detection by security systems. |
| **05** | **DCOE Mapping to Data Exfiltration through Tunneling**: |
| | Participants use tools like **tcpdump** and **Wireshark** to monitor and analyze tunneled traffic, enhancing their ability to detect, secure, and troubleshoot tunnel-based communications. |

This training equips participants with the technical skills needed to redirect and tunnel data through various protocols and systems effectively in operational scenarios.

### 4346 (NIST ID: N/A)

**Ability to remediate indicators of compromise (IOCs).**

| | |
|---|---|
| **01** | **DCOE Mapping to IOC Identification**: |
| | Participants analyze malware samples using tools such as PEStudio and VirusTotal to extract IOCs, including hashes, suspicious strings, and blacklisted functions. This data is critical for remediation efforts. |
| **02** | **DCOE Mapping to Incident Response Labs**: |
| | Labs include scenarios where participants identify and isolate compromised hosts, applying mitigation strategies such as blocking malicious IPs, removing malware, and restoring affected systems using clean backups. |
| **03** | **DCOE Mapping to Threat Sharing Platforms**: |
| | Training emphasizes the use of platforms like MISP and OpenIOC for documenting and sharing IOCs. Participants learn to operationalize shared intelligence to address threats effectively. |
| **04** | **DCOE Mapping to Post-Remediation Verification**: |
| | Labs require verifying that remediation efforts have fully neutralized threats, using tools like Wireshark to monitor network traffic for signs of residual or reoccurring compromise |
| **05** | **DCOE Mapping to Policy Adherence**: |
| | Participants practice documenting remediation actions and aligning efforts with organizational policies and Standard Operating Procedures (SOPs). |

These exercises provide practical skills for identifying and eliminating IOCs, ensuring comprehensive incident resolution and prevention of future occurrences.

### 4347 (NIST ID: N/A)

**Ability to research non-standards within a project.**

| | |
|---|---|
| **01** | **DCOE Mapping to Reconnaissance and Information Gathering**: |
| | Labs focus on gathering and analyzing information using tools like **Nmap** and **Metasploit** to identify unusual or unexpected configurations or practices within a target system. These tools help evaluate deviations from standard setups and processes. |
| **02** | **DCOE Mapping to OSINT Labs**: |
| | Participants conduct research using **Maltego** to map entities and uncover non-standard relationships or anomalies in data sources, enhancing their ability to detect and document irregularities Mapping to Network and Traffic Analysis**:<br>Exercises involve monitoring network traffic with **Wireshark** to identify anomalies that deviate from baseline behaviors, such as unexpected traffic patterns or configurations. |
| **03** | **DCOE Policy and Configuration Evaluation**: |
| | Labs guide participants to assess configurations against organizational policies and standards, highlighting non-compliance or deviations for further research and resolution. |
| **04** | **DCOE Mapping and Reporting**: |
| | Training emphasizes recording findings in structured reports to communicate non-standard elements effectively to stakeholders, ensuring alignment with project goals and organizational objectives. |

These labs develop the skills needed to identify, research, and address non-standard elements within a project context, focusing on thorough analysis and actionable insights.

### 4350 (NIST ID: N/A)

**Ability to retrieve historical operational and open-source data to analyze compatibility with approved capabilities.**

| | |
|---|---|
| **01** | **DCOE Mapping to Open-Source Intelligence (OSINT) Tools**: |
| | Participants use tools such as **Maltego** and **theHarvester** to gather historical data and analyze compatibility with operational objectives. For example, Maltego is used to perform entity-based searches and graphical link analysis for data aggregating to Packet Capture Analysis**:<br>Labs involve analyzing historical packet capture (pcap) files using **Wireshark** to detect anomalies and confirm the compatibility of network behaviors with approved security standards. |
| **02** | **DCOE Mapping Analysis**: |
| | Exercises include leveraging **ThreatMiner** to extract historical malware-related data, such as file hashes and threat actor associations, for evaluating operational relevance. |
| **03** | **DCOE Mapping to Doc and Reporting**: |
| | Training emphasizes documenting findings and providing actionable reports on compatibility assessments, ensuring alignment with organizational policies and mission needs. |

This training ensures participants can effectively analyze historical and open-source data to support decision-making and operational compatibility.

## 4359 (NIST ID: N/A)

**Ability to train other cyberspace operators.**

| | |
|---|---|
| **01** | **DCOE Mapping to Training Scenarios**: |
| | Participants practice creating and delivering simulated training exercises for other operators, covering key skills such as network defense, vulnerability exploitation, and incident response. |
| **02** | **DCOE Mapping to PBED Integration**: |
| | Incorporates the PBED (Plan, Brief, Execute, Debrief) framework to teach structured mission planning and execution processes, with an emphasis on iterative learning and skill enhancement through training cycles. |
| **03** | **DCOE Mapping to Leadership Labs**: |
| | Labs focus on leadership in instructional settings, guiding participants to mentor peers effectively by leading discussions and hands-on labs, such as network mapping, IDS deployment, and OSINT integration. |
| **04** | **DCOE Mapping to Curriculum Development**: |
| | Participants develop and refine training modules tailored to organizational needs, emphasizing realistic scenarios that align with mission goals and operational capabilities. |
| **05** | **DCOE Mapping to Collaborative Skills Building**: |
| | Training includes fostering collaboration through group labs and team-based problem-solving exercises, promoting a learning environment that enhances the capabilities of all operators. |

These elements ensure participants are equipped to provide effective training and mentorship, fostering a culture of continuous improvement in cyberspace operations.

### 4361 (NIST ID: N/A)

**Ability to troubleshoot technical problems.**

| | |
|---|---|
| **01** | **DCOE Mapping to Initial Configuration Labs**: |
| | Labs involve setting up virtual machines (VMs) with proper network configurations using commands like sudo ifconfig eth0 to resolve IP and connectivity issues. Participants troubleshoot common errors during initial setup and configuration Network Diagnostics**:<br>Hands-on activities include using tools like **Wireshark** and **tcpdump** to identify and resolve network communication problems, such as packet loss or misconfigured firewalls |
| **02** | **DCOE Mapping tmoval**: |
| | Participants identify system anomalies caused by rootkits using tools like **GMER**, then troubleshoot the impact of hidden processes or altered kernel data structures. Labs guide users through detection, verification, and resolution. |
| **03** | **DCOE Mapping** |
| | **DCOE Mapping to Security Onion Setup**: shooting tasks involve configuring and running **Security Onion** IDS/IPS systems, resolving installation errors, and verifying the functionality of monitoring systems for real-time alerting. |
| **04** | **DCOE Mapping to Metasploit Usage**: |
| | Labs with exploit execution in **Metasploit**, such as environment setup, payload misconfigurations, or database errors. Participants practice debugging these errors using msfdb and related commands. |

This structured approach equips participants with the skills to identify a range of technical issues, ensuring operational readiness and system reliability.

### 4367 (NIST ID: N/A)

**Ability to use core toolset (e.g., implants, remote access tools).**

| | |
|---|---|
| **01** | **DCOE Mapping to Remote Access Tools**: |
| | Participants engage in hands-on labs utilizing tools like **Metasploit** to deploy remote access payloads, including Meterpreter sessions. Tasks include setting up a listener and delivering payloads via vulnerabilities in Windows environments. |
| **02** | **DCOE Mapping to Implant Deployment**: |
| | Exercises cover deploying and maintaining persistent implants, including creating custom backdoors using tools such as **TheFatRat**. Labs emphasize payload compilation, execution, and session establishment on victim machines. |
| **03** | **DCOE Mapping to Command and Control (C2)**: |
| | Students practice maintaining C2 communications through encrypted channels and establishing persistent access using tools like HTTPTunnel and DNS tunneling methods. |
| **04** | **DCOE Mapping to Exploit Usage**: |
| | Training includes selecting and executing exploits tailored to vulnerabilities in target systems, demonstrating the practical application of tools for network penetration and exploitation. |
| **05** | **DCOE Mapping to Lab Scenarios**: |
| | Practical scenarios include configuring and utilizing the core toolset to gain and maintain control over target systems, focusing on stealth, operational persistence, and adherence to operational goals. |

This training ensures proficiency in deploying, managing, and utilizing core cyber tools effectively in mission-critical scenarios.

### 4369 (NIST ID: N/A)

**Ability to use dynamic analysis tools (e.g., Process Monitor, Process Explorer, and Registry Analysis).**

| | |
|---|---|
| **01** | **DCOE Mapping to Process Monitoring**: |
| | Participants learn to use **Process Monitor** to track system activities, including file system access, registry changes, and process behavior in real time. This helps identify anomalous or malicious activity. |
| **02** | **DCOE Mapping to Process Exploration**: |
| | Training includes using **Process Explorer** to inspect running processes, analyze their memory usage, and verify digital signatures to detect unauthorized or suspicious activities. |
| **03** | **DCOE Mapping to Registry Analysis**: |
| | Labs involve analyzing Windows registry keys to detect unauthorized modifications or persistence mechanisms, such as startup entries and configuration changes made by malware. |
| **04** | **DCOE Mapping to Malware Behavior Analysis**: |
| | Exercises focus on combining tools like Process Monitor and Process Explorer to dynamically analyze malware samples, capturing insights into their runtime behavior and system impact. |
| **05** | **DCOE Mapping to Post-Incident Forensics**: |
| | Participants practice documenting findings from dynamic analysis tools to support incident response and forensic investigations, ensuring detailed reporting for operational use. |

These labs and exercises provide hands-on experience in using dynamic analysis tools to detect, analyze, and respond to system-level activities and potential threats.

### 4370 (NIST ID: N/A)

**Ability to use enterprise tools to enumerate target information.**

| | |
|---|---|
| **01** | **DCOE Mapping to Reconnaissance Techniques:** |
| | Participants learn to use enterprise tools such as Nmap and Wireshark to identify network architecture, connected devices, and system vulnerabilities. This training focuses on mapping and understanding target environments to support operational planning. |
| **02** | **DCOE Mapping to Vulnerability Identification:** |
| | Hands-on labs teach students to identify weaknesses in systems and networks using enterprise enumeration tools, enabling proactive measures to secure critical cyber terrain. |
| **03** | **DCOE Mapping to Adversarial TTP Simulation:** |
| | Participants engage in exercises simulating adversarial reconnaissance phases, employing enumeration tools to replicate real-world threat scenarios and develop counterstrategies. |
| **04** | **DCOE Mapping to Incident Preparation:** |
| | Students practice integrating enumeration tools into their workflows to enhance threat detection and readiness, ensuring efficient responses to emerging risks. |
| **05** | **DCOE Mapping to Network Analysis:** |
| | Labs emphasize analyzing enumerated data to identify anomalous or suspicious activities within the target environment, fostering a comprehensive understanding of network behavior. |

These mappings highlight the practical application of enumeration tools within the DCOE training, equipping participants with essential skills for cybersecurity operations.

### 4378 (NIST ID: N/A)

**Ability to verify file integrity for both uploads and downloads.**

| | |
|---|---|
| **01** | **DCOE Mapping to Hash Verification:** |
| | Participants learn to use hash verification tools (e.g., SHA-256, MD5) to ensure that files retain their integrity during both uploads and downloads. Training includes calculating and comparing file hashes to detect any unauthorized modifications. |
| **02** | **DCOE Mapping to Secure Transfer Protocols:** |
| | Hands-on labs focus on implementing secure transfer protocols such as SFTP and HTTPS to maintain file integrity during data transmission. |
| **03** | **DCOE Mapping to File Integrity Monitoring:** |
| | Exercises involve configuring and using file integrity monitoring solutions to automatically validate files during uploads and downloads, ensuring compliance with security policies. |
| **04** | **DCOE Mapping to Incident Detection and Response:** |
| | Training incorporates scenarios where participants identify altered or corrupted files as part of incident response workflows, using file integrity verification as a key forensic method. |
| **05** | **DCOE Mapping to Digital Signature Utilization:** |
| | Participants practice using digital signatures to validate the authenticity and integrity of files, ensuring secure file exchange across organizational and operational environments. |

These mappings equip participants with the skills to verify and maintain file integrity as a core component of secure file management and data protection practices.

### 4379 (NIST ID: N/A)

**Ability to weaken a target to facilitate/enable future access.**

| | |
|---|---|
| **01** | **DCOE Mapping to Exploiting Vulnerabilities:** |
| | Participants engage in exercises that simulate the identification and exploitation of vulnerabilities in systems and networks, demonstrating how adversaries weaken targets to create future access opportunities. |
| **02** | **DCOE Mapping to Adversarial Tools and TTPs:** |
| | The course includes training on adversarial tactics, techniques, and procedures (TTPs) following the cyber kill chain, which encompasses weakening systems as a precursor to further exploitation. |
| **03** | **DCOE Mapping to Persistence Mechanisms:** |
| | Hands-on labs focus on understanding and replicating persistence techniques used by attackers, such as creating backdoors or altering configurations, to maintain access for subsequent operations. |
| **04** | **DCOE Mapping to Reconnaissance and Preparation:** |
| | Scenarios emphasize the importance of reconnaissance and preparation to weaken defenses, such as identifying and targeting weak points in an organization’s cyber infrastructure. |
| **05** | **DCOE Mapping to Malware Deployment:** |
| | Exercises include deploying controlled malware to observe its impact on target systems and to understand how adversaries weaken defenses to enable future exploitation. |

### 4380 (NIST ID: N/A)

**Ability to write and modify markup languages (e.g., HTML, XML).**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversarial Web Exploitation:** |
| | Participants engage in exercises that explore how adversaries manipulate web applications and markup languages to exploit vulnerabilities, fostering an understanding of HTML and XML modification. |
| **02** | **DCOE Mapping to Defensive Coding Practices:** |
| | Training includes scenarios that emphasize secure coding and markup validation to counter adversarial attempts to exploit improperly written HTML or XML files. |
| **03** | **DCOE Mapping to Threat Analysis:** |
| | Labs involve analyzing maliciously crafted markup language files (e.g., HTML phishing pages or XML injection payloads) to understand the attacker’s intent and methods. |
| **04** | **DCOE Mapping to Incident Response Documentation:** |
| | Participants learn to document findings using structured data in XML, highlighting the use of markup languages in operational workflows. |
| **05** | **DCOE Mapping to Operational Simulations:** |
| | Exercises simulate real-world scenarios where participants modify HTML or XML for tasks such as creating phishing simulations or identifying vulnerabilities in web applications. |

### 4381 (NIST ID: N/A)

**Ability to write and modify source code.**

| | |
|---|---|
| **01** | **DCOE Mapping to Offensive Coding Techniques:** |
| | Participants engage in exercises that involve writing and modifying source code to develop scripts or exploits for controlled offensive operations, simulating real-world adversarial tactics. |
| **02** | **DCOE Mapping to Defensive Coding Practices:** |
| | Training focuses on modifying source code to address vulnerabilities, implement security controls, and harden applications against known attack vectors. |
| **03** | **DCOE Mapping to Malware Analysis and Development:** |
| | Hands-on labs include crafting and analyzing basic malware or payloads, providing insight into how source code modifications impact operational behavior. |
| **04** | **DCOE Mapping to Automation and Tool Development:** |
| | Participants practice writing scripts and automating tasks using programming languages, enhancing operational efficiency and response capabilities. |
| **05** | **DCOE Mapping to Adversarial Simulations:** |
| | Scenarios emphasize modifying open-source tools or creating custom scripts to simulate adversarial behavior, supporting advanced threat emulation exercises. |

## 4391 (NIST ID: N/A)

**Knowledge of advanced redirection techniques.**

Based on the DCOE manual content:

| | |
|---|---|
| 01 | **DCOE Mapping to Tunneling and Covert Channels:** |
| | The manual describes tunneling techniques, such as using HTTP and DNS traffic to bypass network restrictions. These methods represent advanced redirection strategies to send traffic through allowed protocols while evading detection Reverse Shells:** Training includes setting up reverse shells using tools like Netcat and SQL injection, which redirect attacker-controlled communication back to their machines while avoiding detection on non-standard ports . |
| 02 | **DCOE Mapping to Redirection:** |
| | Participants practice using Metasploit and other tools to implement redirection techniques, such as backdoors and manipulated service configurations, to maintain stealth during operations. |

These mappings align with advanced redirection within the context of the DCOE training.

### 4393 (NIST ID: N/A)

**Knowledge of appropriate/inappropriate information to include in operational documentation.**

| | |
|---|---|
| **01** | **DCOE Mapping to Classified and Sensitive Information Handling:** |
| | The manual emphasizes that training materials and operational documents must only reach appropriate stakeholders, underscoring the importance of restricting sensitive information from broad dissemination. |
| **02** | **DCOE Mapping to Incident Reporting:** |
| | Participants are trained on the importance of including relevant technical details while avoiding unnecessary or inappropriate information that could compromise security in reports. |
| **03** | **DCOE Mapping to Documentation of Tools and Processes:** |
| | Scenarios highlight documenting operational actions (e.g., malware analysis and penetration testing) in a manner that conveys technical findings without exposing unnecessary or exploitable details. |

These mappings reflect the manual's guidance on appropriate documentation practices while maintaining operational security.

## 4395 (NIST ID: N/A)

**Knowledge of basic client software applications and their attack surfaces.**

| | |
|---|---|
| **01** | **DCOE Mapping to Application Exploitation:** |
| | The manual includes scenarios where participants analyze vulnerabilities in client-side applications, such as web browsers and document readers, to understand potential attack vectors. |
| **02** | **DCOE Mapping to SQL Injection Attacks:** |
| | Training highlights SQL injection as a method to exploit forms in web applications, emphasizing the significance of securing client-side interfaces. |
| **03** | **DCOE Mapping to Web Application Vulnerabilities:** |
| | The course covers cross-site scripting (XSS) and web shell exploitation, showcasing how attackers leverage client application weaknesses to infiltrate systems. |
| **04** | **DCOE Mapping to Wireless Threats:** |
| | Participants learn about vulnerabilities in wireless protocols and their exploitation via client-side configurations, such as WEP and WPA2 vulnerabilities. |
| **05** | **DCOE Mapping to Network-Based Client Attacks:** |
| | Training includes exploiting client-side software on victim machines using tools like Metasploit, illustrating practical methods to test and understand attack surfaces. |

## 4396 (NIST ID: N/A)

**Knowledge of basic cloud-based technologies and concepts.**

| | |
|---|---|
| **01** | **DCOE Mapping to Dynamic Evolution in Cyberspace:** |
| | The manual discusses the rise of cloud computing as part of the dynamic evolution in cyberspace technologies. It highlights how attackers and defenders adapt to evolving technologies like cloud platforms, emphasizing the need to understand their architecture and vulnerabilities. |
| **02** | **DCOE Mapping to Threat Detection in Cloud Environments:** |
| | Content includes methods for detecting malware and suspicious activity in hybrid environments that encompass on-premises and cloud infrastructures. This involves leveraging tools to monitor and secure data flow across these systems. |
| **03** | **DCOE Mapping to Network-Based Threat Scenarios:** |
| | The manual includes exercises on detecting and mitigating threats in distributed systems, which extend to cloud technologies used in large-scale cyber operations. |

### 4402 (NIST ID: N/A)

**Knowledge of basic redirection techniques (e.g., IP Tables, SSH Tunneling, netsh).**

The DCOE manual includes indirect references to basic redirection techniques:

| | |
|---|---|
| **01** | **DCOE Mapping to Tunneling Concepts:** |
| | The manual discusses tunneling methods such as DNS tunneling (Dns2tcp) and HTTP tunneling, which allow communication over restricted networks using permitted protocols like HTTP and DNS. |
| **02** | **DCOE Mapping to Secure Shell (SSH):** |
| | The training includes the use of SSH and RSA keys for secure remote access, providing an understanding of secure redirection techniques. |
| **03** | **DCOE Mapping to Protocol Manipulation:** |
| | Examples such as leveraging Telnet and SSH emphasize redirecting traffic to gain access to remote systems, highlighting the use of these tools to bypass traditional restrictions. |

These mappings highlight basic redirection methods addressed in the DCOE manual, relevant to the stated knowledge area.

### 4403 (NIST ID: N/A)

**Knowledge of basic server software applications and their attack surfaces.**

| | |
|---|---|
| **01** | **DCOE Mapping to Web Server Vulnerabilities:** |
| | The manual includes exercises where participants identify and exploit vulnerabilities in web servers, such as Apache and IIS, emphasizing their attack surfaces. |
| **02** | **DCOE Mapping to SQL Injection:** |
| | Training highlights SQL injection attacks on web applications running on server software, illustrating how attackers exploit backend server databases. |
| **03** | **DCOE Mapping to OWASP ZAP:** |
| | Participants utilize tools like OWASP ZAP to enumerate and test web applications, gaining insights into server vulnerabilities and security misconfigurations. |
| **04** | **DCOE Mapping to Configuration Weaknesses:** |
| | Labs demonstrate the impact of improper file/folder permissions and insecure server configurations, focusing on securing server application surfaces. |
| **05** | **DCOE Mapping to Threat Artifacts Analysis:** |
| | The manual details analyzing artifacts left by attackers on compromised servers, improving participants' understanding of server-side attack detection and mitigation. |

### 4404 (NIST ID: N/A)

**Knowledge of code injection and its employment in cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to SQL Injection Techniques:** |
| | The manual includes training on SQL injection attacks, detailing how adversaries manipulate backend systems using injected SQL commands. Participants practice exploiting vulnerabilities through user-input fields and observe how malicious code can bypass authentication mechanisms. |
| **02** | **DCOE Mapping to Cross-Site Scripting (XSS):** |
| | Participants learn about XSS attacks, which involve injecting malicious scripts into trusted web pages. The training covers identifying and mitigating these vulnerabilities in web applications. |
| **03** | **DCOE Mapping to Web Shell Exploitation:** |
| | The manual discusses the use of web shells for command injection and manipulation of targeted web servers. Participants simulate attacks to understand how adversaries employ web shells for deeper system access. |
| **04** | **DCOE Mapping to Command Injection:** |
| | Hands-on labs guide participants in creating and executing command injection scripts, such as PHP-based payloads, to demonstrate how attackers achieve unauthorized control over systems. |

These mappings demonstrate how the DCOE manual integrates training on code injection techniques within the context of offensive and defensive cyberspace operations.

### 4419 (NIST ID: N/A)

**Knowledge of credential sources and restrictions related to credential usage.**

| | |
|---|---|
| **01** | **DCOE Mapping to Password Cracking and Credential Gathering:** |
| | The DCOE manual includes exercises such as utilizing tools like John the Ripper to crack passwords from shadow and passwd files, demonstrating how credentials can be harvested from compromised systems. |
| **02** | **DCOE Mapping to Secure Handling of Credentials:** |
| | Training emphasizes the risks associated with exposed credentials during operations, such as saving or storing cracked passwords in unsecured files like "credentials.txt," highlighting restrictions and proper management of credential data. |
| **03** | **DCOE Mapping to Exploit Utilization:** |
| | Participants use harvested credentials to gain remote access to systems, demonstrating the operational impact of credential usage and associated restrictions when conducting penetration tests. |

These examples align with the DCOE manual's focus on using and managing credentials in cybersecurity operations.

### 4437 (NIST ID: N/A)

**Knowledge of device reboots, including when they occur and their impact on tool functionality.**

| | |
|---|---|
| **01** | **DCOE Mapping to Persistent Malware Functionality:** |
| | The manual discusses malware persistence techniques that ensure malicious tools remain active after a device reboot, illustrating the operational impact on tool functionality. |
| **02** | **DCOE Mapping to Driver and Service Reinstallation:** |
| | Scenarios in the manual cover how certain tools, such as rootkits, reload themselves or associated drivers after a system reboot, emphasizing the importance of understanding reboot behavior. |
| **03** | **DCOE Mapping to Network Configuration Revalidation:** |
| | Lab exercises highlight the need to verify network settings and tool functionality after rebooting devices, demonstrating how a reboot can reset configurations critical to operations. |

These mappings align with operational scenarios where understanding device reboots is critical to ensuring the resilience and functionality of tools.

### 4419 (NIST ID: N/A)

**Knowledge of evolving technologies.**

The DCOE manual includes references to evolving technologies in the context of cyberspace operations:

| | |
|---|---|
| **01** | **DCOE Mapping to Cyberspace Evolution:** |
| | The manual discusses the constant evolution of technologies that underpin cyberspace, such as web-based applications, cloud computing, and converging technologies. It highlights the need to adapt to technological advances and the resulting changes in tactics, techniques, and procedures for both attackers and defenders. |
| **02** | **DCOE Mapping to Operational Challenges:** |
| | Participants are introduced to the challenges presented by the dynamic nature of cyberspace technologies, including shifting terrain and unforeseen advancements that impact operational planning and execution. |
| **03** | **DCOE Mapping to Innovation in TTPs:** |
| | The manual emphasizes the continuous development and testing of new Tactics, Techniques, and Procedures (TTPs) to maintain an advantage in a rapidly evolving technological landscape. |

These mappings align with the manual's focus on addressing the impact of emerging technologies on cyberspace operations.

### 4444 (NIST ID: N/A)

**Knowledge of evolving technologies.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyberspace Dynamics:** |
| | The manual emphasizes the rapid evolution of technologies in the cyberspace domain, including the rise of cloud computing, mobile devices, and the increasing integration of IoT systems, all of which require constant adaptation to maintain operational effectiveness. |
| **02** | **DCOE Mapping to Threat Landscape Evolution:** |
| | Training incorporates scenarios where participants analyze the impact of emerging technologies on both adversarial and defensive capabilities, such as advanced malware targeting cloud-based environments. |
| **03** | **DCOE Mapping to Adaptation of TTPs:** |
| | Participants learn to adapt Tactics, Techniques, and Procedures (TTPs) in response to evolving technologies, ensuring that both offensive and defensive strategies remain relevant in rapidly changing environments. |
| **04** | **DCOE Mapping to Operational Resilience:** |
| | The manual includes discussions on maintaining operational resilience by integrating and leveraging new technologies, while mitigating associated risks introduced by their adoption. |

These mappings illustrate how the DCOE manual addresses the importance of understanding and adapting to evolving technologies in cyberspace operations.

### 4447 (NIST ID: N/A)

**Knowledge of factors that would suspend or abort an operation.**

| | |
|---|---|
| **01** | **DCOE Mapping to Go/No-Go Criteria:** |
| | The manual discusses the use of Go/No-Go criteria in planning cyberspace operations. These criteria define specific conditions under which tasks should be suspended or aborted, such as identifying active users on a target machine when a reboot is required. |
| **02** | **DCOE Mapping to Contingency Planning:** |
| | The planning process includes contingencies for potential mission hindrances, such as power outages or communication failures, which could necessitate suspending or aborting an operation. |
| **03** | **DCOE Mapping to Dynamic Execution Flexibility:** |
| | Participants are trained to adapt during the execution phase, following legal restrictions and operational goals, and to identify conditions where mission objectives cannot be met safely or effectively. |

These mappings reflect operational scenarios where aborting or suspending actions ensures mission success and adherence to planned protocols.

## 4463 (NIST ID: N/A)

**Knowledge of how computer programs are executed.**

| | |
|---|---|
| **01** | **DCOE Mapping to Process Execution and Management:** |
| | The manual includes labs where participants analyze how processes are executed on systems, such as running and hiding processes using tools like "fu.exe" in rootkit labs. This illustrates the behavior of programs during execution and their impact on system processes. |
| **02** | **DCOE Mapping to Malware Execution:** |
| | Exercises involve executing malware samples, observing their runtime behavior, and understanding how programs interact with system memory and resources. |
| **03** | **DCOE Mapping to Exploit Execution:** |
| | Participants use tools like Metasploit to execute payloads on target systems, demonstrating how programs are delivered and executed in cyberspace operations. |

These mappings focus on practical activities that enhance understanding of program execution within the context of operational scenarios in the DCOE training.

### 4464 (NIST ID: N/A)

**Knowledge of how host-based security products, logging, and malware may affect tool functionality.**

| | |
|---|---|
| **01** | **DCOE Mapping to Host-Based Intrusion Detection Systems (HIDS):** |
| | The manual provides insights into HIDS, which monitor specific devices for unauthorized logins and malware activity. This directly impacts how tools operate in environments with strict monitoring. |
| **02** | **DCOE Mapping to Malware and Tool Behavior Analysis:** |
| | Exercises include analyzing malware techniques, such as using rootkits and evasion tactics, which can conflict with host-based security products and affect operational tools. |
| **03** | **DCOE Mapping to Logging and Event Correlation:** |
| | Participants work with logging tools to monitor system and application logs, demonstrating how excessive logging or misconfigurations may hinder tool effectiveness or reveal tool usage. |

These mappings leverage the manual’s coverage of intrusion detection systems and malware interactions with host security mechanisms to reflect their impact on tool functionality.

### 4465 (NIST ID: N/A)

**Knowledge of how other actors may affect operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversary Influence:** |
| | The manual discusses how adversaries leverage the interconnected nature of cyberspace to conduct rapid and distributed attacks, including the use of botnets and crowd-sourced disruptions, which can significantly impact operational success. |
| **02** | **DCOE Mapping to Attribution Challenges:** |
| | Scenarios highlight the difficulty of attributing actions to specific actors due to the anonymity and rapid maneuverability in cyberspace, emphasizing how these factors influence operations. |
| **03** | **DCOE Mapping to Collaborative Operations:** |
| | The training includes the necessity of understanding multi-stakeholder dynamics in cyberspace, including the roles of nation-state actors, non-state actors, and private sector participants, which can directly affect operational decisions. |

These mappings reflect the manual's emphasis on understanding the influence of external actors in the planning and execution of cyberspace operations.

### 4482 (NIST ID: N/A)

**Knowledge of malware triage.**

| | |
|---|---|
| **01** | **DCOE Mapping to Malware Analysis:** |
| | The manual includes hands-on labs where students analyze malicious activities within controlled environments, providing foundational knowledge for identifying and categorizing malware. |
| **02** | **DCOE Mapping to Threat Detection:** |
| | The course emphasizes techniques for discovering, detecting, and mitigating threats, which can involve the preliminary examination of malware to assess its potential impact. |
| **03** | **DCOE Mapping to Active Defense and Hunting:** |
| | Active defense concepts in the manual encourage proactive measures like threat hunting and analysis, which may involve triaging malware to prioritize response actions. |

### 4486 (NIST ID: N/A)

**Knowledge of methods, strategies, and techniques of evading detection while conducting operations, such as noise, stealth, situational awareness, etc.**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversary TTPs:** |
| | The manual discusses adversary tactics, techniques, and procedures (TTPs), including the use of stealth and evasion strategies to avoid detection during operations. It highlights how adversaries maintain persistence and maneuver covertly in cyberspace. |
| **02** | **DCOE Mapping to Cyber Espionage:** |
| | Case studies and examples of espionage activities emphasize the importance of anonymity, limited attribution, and stealth in operations, which are relevant to evasion techniques. |
| **03** | **DCOE Mapping to Defensive Techniques:** |
| | Strategies for detecting and countering adversarial evasion techniques enhance situational awareness to uncover stealthy operations. |
| **04** | **DCOE Mapping to Persistent Engagement:** |
| | Persistent engagement includes methods to monitor and respond to adversary actions while understanding their use of noise and situational manipulation to evade detection. |

## 4487 (NIST ID: N/A)

**Knowledge of methods, tools, and procedures for collecting information, including accessing databases and file systems.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyber Threat Intelligence (CTI):** |
| | The manual emphasizes the collection and analysis of cyber threat intelligence, including methods to gather relevant information from various sources, which can involve accessing structured and unstructured data repositories |
| **02** | **DCOE Mapping to Offensive and Defensive Operations:** |
| | Scenarios in the course demonstrate tools and procedures used to retrieve data from compromised systems, including file systems and networked environments, as part of both offensive operations and incident response. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises involve using tools to analyze, extract, and manage data within controlled environments, providing students with an understanding of data collection techniques. |
| **04** | **DCOE Mapping to Reconnaissance Techniques:** |
| | The manual covers reconnaissance as a phase of the cyber kill chain, which includes methods for accessing databases and file systems to gather actionable intelligence. |

### 4488 (NIST ID: N/A)

**Knowledge of methods, tools, and procedures for exploiting target systems.**

| | |
|---|---|
| **01** | **DCOE Mapping to Offensive Cyber Operations:** |
| | The manual includes training on offensive techniques, focusing on exploiting vulnerabilities in target systems to achieve operational objectives. |
| **02** | **DCOE Mapping to Adversary TTPs:** |
| | Tools and methods used by adversaries to exploit systems are presented within the context of the cyber kill chain, providing an understanding of exploitation strategies. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical labs allow students to simulate exploitation scenarios in a controlled environment, using specific tools and procedures to compromise systems and analyze the outcomes. |
| **04** | **DCOE Mapping to Cyber Maneuver:** |
| | The course discusses maneuver tactics within cyberspace, including exploiting weaknesses to gain access and maintain persistence within target environments. |

### 4489 (NIST ID: N/A)

**Knowledge of methods, tools, and techniques used to determine the path to a target host/network (e.g., identify satellite hops).**

| | |
|---|---|
| **01** | **DCOE Mapping to Network Reconnaissance:** |
| | The manual covers reconnaissance techniques, including methods to map the network path to a target host. These techniques involve understanding routing paths, network topology, and intermediary nodes. |
| **02** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises in the course involve using network mapping tools (e.g., traceroute, network scanners) to identify routes, hops, and access points within a network environment. |
| **03** | **DCOE Mapping to Cyber Terrain Analysis:** |
| | Students learn to analyze key cyber terrain, which includes identifying critical nodes, potential chokepoints, and pathways leading to target systems or networks. |
| **04** | **DCOE Mapping to Persistent Engagement Strategies:** |
| | The manual emphasizes situational awareness and pathfinding to enable effective engagement with target hosts, including the identification of intermediary systems like proxies or satellite connections. |

### 4496 (NIST ID: N/A)

**Knowledge of models for examining cyber threats (e.g., cyber kill chain, MITRE ATT&CK).**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyber Kill Chain:** |
| | The manual extensively covers the cyber kill chain model, breaking down each phase (e.g., reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives) to provide a structured approach to analyzing and mitigating cyber threats. |
| **02** | **DCOE Mapping to Threat Actor TTPs:** |
| | Discussions focus on adversary tactics, techniques, and procedures (TTPs) within structured methodologies similar to those found in models like MITRE ATT&CK. |
| **03** | **DCOE Mapping to Hands-On Analysis:** |
| | Practical labs and scenarios involve applying the cyber kill chain to real-world cases, enabling students to use structured threat examination methods to identify and counter threats. |
| **04** | **Note on MITRE ATT&CK:** |
| | The MITRE ATT&CK framework is not explicitly mentioned in the manual but is conceptually aligned with its focus on TTPs and structured threat analysis. |

## 4498 (NIST ID: N/A)

**Knowledge of modes of communication used by a target, such as cable, fiber optic, satellite, microwave, VSAT, or combinations of these.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyber Terrain Analysis:** |
| | The manual covers the analysis of cyber terrain, including the identification and understanding of communication infrastructure components that may be used by a target. |
| **02** | **DCOE Mapping to Operational Environment:** |
| | Discussions on the operational environment include factors such as physical and logical layers, which encompass various communication modes like satellite links and fiber-optic networks. |
| **03** | **DCOE Mapping to Reconnaissance Techniques:** |
| | Scenarios involve reconnaissance to identify and map communication paths, which could include methods for detecting and analyzing different modes of communication. |
| **04** | **DCOE Mapping to Situational Awareness:** |
| | The manual emphasizes maintaining situational awareness of the technological infrastructure, including the use of mixed communication modes in adversary operations. |

### 4502 (NIST ID: N/A)

**Knowledge of open-source tactics that enable initial access (e.g., social engineering, phishing).**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversary TTPs:** |
| | The manual discusses tactics, techniques, and procedures (TTPs) used by adversaries, including social engineering and phishing, to gain initial access to systems. |
| **02** | **DCOE Mapping to Cyber Kill Chain:** |
| | Initial access methods like social engineering and phishing are covered within the reconnaissance and delivery phases of the cyber kill chain model. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Labs and scenarios provide practical exposure to detecting and mitigating tactics such as phishing, highlighting the methods adversaries use to exploit human vulnerabilities. |
| **04** | **DCOE Mapping to Threat Awareness:** |
| | Emphasis is placed on understanding open-source tools and techniques used by attackers to craft convincing social engineering campaigns or phishing attacks. |

### 4503 (NIST ID: N/A)

**Knowledge of operating system command shells, configuration data.**

| | |
|---|---|
| **01** | **DCOE Mapping to Hands-On Labs:** |
| | The manual includes practical labs where students interact with operating system command shells to execute commands, configure system settings, and troubleshoot issues. |
| **02** | **DCOE Mapping to System Hardening:** |
| | Training emphasizes using command-line interfaces (CLI) to secure and manage system configurations, including setting permissions and disabling unnecessary services. |
| **03** | **DCOE Mapping to Adversary TTPs:** |
| | The course explores how adversaries leverage command shells to manipulate configuration data and gain unauthorized access, enabling students to understand and counter these tactics. |
| **04** | **DCOE Mapping to Incident Response:** |
| | Scenarios involve analyzing and remediating compromised systems through the use of shell commands and configuration adjustments. |

### 4504 (NIST ID: N/A)

**Knowledge of methods, tools, and procedures for establishing and maintaining persistence on target systems.**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversary TTPs:** |
| | The manual explains tactics and techniques used by adversaries to maintain persistence on target systems, such as exploiting authentication mechanisms or creating backdoors. |
| **02** | **DCOE Mapping to Cyber Kill Chain:** |
| | Persistence is covered in the post-exploitation phase of the cyber kill chain, where adversaries ensure continued access to compromised systems. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical labs provide scenarios to explore how persistence is established, such as configuring autorun entries or modifying system processes for sustained access. |
| **04** | **DCOE Mapping to Incident Response:** |
| | Students learn to detect and remove adversarial persistence mechanisms during incident response scenarios, reinforcing an understanding of the methods used. |

### 4505 (NIST ID: N/A)

**Knowledge of physical and logical network segmentation.**

| | |
|---|---|
| **01** | **DCOE Mapping to Network Design Principles:** |
| | The manual discusses the importance of segmenting networks physically and logically to limit adversary movement and enhance system defense. |
| **02** | **DCOE Mapping to Cyber Terrain Analysis:** |
| | Training includes analyzing key cyber terrain, highlighting how segmentation creates boundaries that protect critical resources. |
| **03** | **DCOE Mapping to Defensive Techniques:** |
| | Scenarios emphasize applying segmentation techniques, such as VLANs, firewalls, and access control, to isolate sensitive systems from general traffic. |
| **04** | **DCOE Mapping to Hands-On Labs:** |
| | Labs explore configuring and verifying segmented networks to reinforce theoretical knowledge with practical application. |

### 4506 (NIST ID: N/A)

**Knowledge of tools and methods for collecting, analyzing, and archiving logs.**

| | |
|---|---|
| **01** | **DCOE Mapping to Threat Detection:** |
| | The manual emphasizes log collection and analysis as a critical component of threat detection and response, teaching students how to recognize anomalies and indicators of compromise. |
| **02** | **DCOE Mapping to SIEM Tools:** |
| | Scenarios include configuring and utilizing Security Information and Event Management (SIEM) systems to aggregate and analyze log data efficiently. |
| **03** | **DCOE Mapping to Incident Response:** |
| | Students practice using logs to trace incidents and reconstruct attack timelines during simulated exercises. |
| **04** | **DCOE Mapping to Forensics:** |
| | Training includes archiving and preserving log data for forensic analysis, ensuring chain of custody and data integrity for investigations. |

### 4507 (NIST ID: N/A)

**Knowledge of advanced persistent threats (APTs).**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversary Profiles:** |
| | The manual profiles APTs, highlighting their methodologies, objectives, and operational strategies to compromise high-value targets over extended periods. |
| **02** | **DCOE Mapping to Threat Intelligence:** |
| | Emphasis is placed on collecting and analyzing intelligence about APT activity to predict and mitigate their tactics. |
| **03** | **DCOE Mapping to Persistent Engagement:** |
| | Scenarios demonstrate how persistent engagement strategies can disrupt APT operations and prevent their objectives. |
| **04** | **DCOE Mapping to Incident Response:** |
| | Students explore detecting, responding to, and eradicating APT activity through hands-on scenarios that mirror real-world cases. |

### 4508 (NIST ID: N/A)

**Knowledge of methods for privilege escalation.**

| | |
|---|---|
| **01** | **DCOE Mapping to Offensive Techniques:** |
| | The manual covers privilege escalation methods used in offensive operations, such as exploiting vulnerabilities or misconfigurations to gain elevated access. |
| **02** | **DCOE Mapping to Adversary TTPs:** |
| | Training includes analyzing adversary techniques for escalating privileges during an attack, providing insights into their methodologies. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Students engage in controlled exercises to execute and detect privilege escalation techniques, reinforcing practical understanding. |
| **04** | **DCOE Mapping to Defensive Countermeasures:** |
| | Scenarios include mitigating privilege escalation risks through patch management, principle of least privilege, and monitoring for suspicious activity. |

### 4510 (NIST ID: N/A)

**Knowledge of password cracking techniques.**

| | |
|---|---|
| **01** | **DCOE Mapping to Offensive Cyber Operations:** |
| | The manual includes training on password cracking as part of offensive scenarios, teaching methods such as brute force and dictionary attacks to compromise credentials. |
| **02** | **DCOE Mapping to Adversary TTPs:** |
| | Discussions focus on how adversaries leverage password cracking techniques to bypass authentication mechanisms and gain unauthorized access. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Labs provide practical experience using tools like **John the Ripper** to perform controlled password cracking exercises and analyze their effectiveness. |
| **04** | **DCOE Mapping to Defensive Countermeasures:** |
| | Training emphasizes mitigating password cracking risks through strong password policies, multifactor authentication, and monitoring for repeated authentication attempts. |

This KSAT is addressed through theoretical discussions and practical applications using tools explicitly mentioned in the manual.

### 4519 (NIST ID: N/A)

**Knowledge of process migration.**

The concept of **process migration** is not explicitly covered in the DCOE manual. However, related topics in the manual may indirectly align with this KSAT:

|  |  |
|---|---|
| **01** | **DCOE Mapping to Adversary TTPs:** |
|  | Discussions on adversary tactics include maintaining persistence and maneuvering within systems, which can conceptually relate to techniques for moving processes across systems. |
| **02** | **DCOE Mapping to Cyber Maneuver:** |
|  | The manual highlights techniques for navigating and controlling systems within a network, which may include actions that facilitate moving or manipulating processes. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
|  | Practical exercises involve controlling system resources and maintaining access, potentially providing indirect insights into process manipulation techniques. |
| **04** | **DCOE Mapping to Defensive Measures:** |
|  | Scenarios include identifying and mitigating abnormal system behaviors that could indicate unauthorized process manipulation or migration. |

While the term "process migration" is not directly addressed, the manual's focus on adversary TTPs and system control provides foundational knowledge applicable to this concept.

## 4540 (NIST ID: N/A)

**Knowledge of system administration concepts for distributed or managed operating environments.**

| | |
|---|---|
| **01** | **DCOE Mapping to System Administration Fundamentals:** |
| | The manual discusses key system administration practices, including managing user accounts, permissions, and system updates in distributed operating environments. |
| **02** | **DCOE Mapping to Network and System Management:** |
| | Topics include monitoring and maintaining distributed systems, ensuring system availability, and implementing security measures across managed environments. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises involve configuring and managing distributed systems, with a focus on ensuring secure and efficient operations. |
| **04** | **DCOE Mapping to Incident Response:** |
| | Training includes scenarios where students identify and mitigate issues in distributed operating environments during incident response. |

This KSAT is supported by both theoretical discussions and practical applications related to system administration within distributed and managed operating environments.

### 4541 (NIST ID: N/A)

**Knowledge of system administration concepts for standalone operating systems.**

| | |
|---|---|
| **01** | **DCOE Mapping to System Administration Basics:** |
| | The manual covers foundational system administration tasks for standalone operating systems, such as user account management, file permissions, and system configuration. |
| **02** | **DCOE Mapping to Security Hardening:** |
| | Topics include securing standalone systems by implementing strong password policies, disabling unnecessary services, and applying system patches. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Labs involve configuring and troubleshooting standalone operating systems, providing practical skills for managing isolated systems securely. |
| **04** | **DCOE Mapping to Incident Management:** |
| | Scenarios include detecting and responding to security incidents on standalone systems, emphasizing root cause analysis and remediation. |

This KSAT is addressed through both theoretical and practical training focused on the administration of standalone operating systems.

### 4542 (NIST ID: N/A)

**Knowledge of system calls.**

| | |
|---|---|
| 01 | **DCOE Mapping to Operating System Fundamentals:** |
| | The manual explains how system calls serve as the interface between user applications and the operating system, enabling functions like file manipulation, process control, and memory management. |
| 02 | **DCOE Mapping to Adversary TTPs:** |
| | Discussions include how adversaries exploit system calls to perform malicious actions, such as privilege escalation or process injection. |
| 03 | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises involve analyzing and using system calls to understand their functionality and identify potential misuse in various scenarios. |
| 04 | **DCOE Mapping to Defensive Techniques:** |
| | Training emphasizes monitoring system calls to detect suspicious activity and mitigate potential threats. |

This KSAT is addressed through both theoretical instruction and practical exercises that highlight the role and significance of system calls in operating system security and functionality.

### 4552 (NIST ID: N/A)

**Knowledge of the components of an authentication system.**

| | |
|---|---|
| **01** | **DCOE Mapping to Authentication Basics:** |
| | The manual outlines key components of authentication systems, such as passwords, tokens, and protocols used to verify user identity. |
| **02** | **DCOE Mapping to Credential Management:** |
| | Topics include the importance of securely managing credentials to protect authentication systems from compromise. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Labs involve configuring authentication settings, demonstrating how to manage and secure access control mechanisms effectively. |
| **04** | **DCOE Mapping to Threat Mitigation:** |
| | Scenarios highlight adversary techniques targeting authentication systems, such as brute force attacks, and how to defend against them. |

This KSAT is addressed through a combination of theoretical explanations and practical exercises explicitly covered in the DCOE manual.

### 4553 (NIST ID: N/A)

**Knowledge of the concept of an advanced persistent threat (APT).**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversary Profiles:** |
| | The manual provides detailed profiles of APTs, including their objectives, persistence mechanisms, and long-term operational strategies to target high-value systems. |
| **02** | **DCOE Mapping to Threat Intelligence:** |
| | Discussions emphasize the role of cyber threat intelligence in identifying and analyzing APT activities, including their tactics, techniques, and procedures (TTPs). |
| **03** | **DCOE Mapping to Hands-On Scenarios:** |
| | Students engage in practical exercises to detect, analyze, and respond to simulated APT activities, reinforcing an understanding of their behaviors and methodologies. |
| **04** | **DCOE Mapping to Defensive Strategies:** |
| | The manual highlights strategies to counter APTs, such as enhancing network segmentation, monitoring for indicators of compromise (IOCs), and employing proactive defense mechanisms. |

This KSAT is thoroughly addressed with a focus on understanding APT operations and developing appropriate countermeasures.

### 4563 (NIST ID: N/A)

**Knowledge of the location and use of tool documentation.**

| | |
|---|---|
| **01** | **DCOE Mapping to Tool Familiarization:** |
| | The manual emphasizes understanding the documentation associated with cybersecurity tools used during training, including setup guides, user manuals, and reference materials. |
| **02** | **DCOE Mapping to Hands-On Labs:** |
| | Labs require students to reference tool documentation to configure, operate, and troubleshoot tools effectively, reinforcing the importance of leveraging available resources. |
| **03** | **DCOE Mapping to Operational Readiness:** |
| | Scenarios stress the value of tool documentation in real-world operations for ensuring proper usage and maximizing the tools' potential. |
| **04** | **DCOE Mapping to Problem-Solving Techniques:** |
| | Training includes using documentation as a resource for resolving technical challenges and understanding advanced tool features. |

This KSAT is explicitly addressed through practical exercises and scenarios that integrate the use of tool documentation as a critical component of effective operations.

### 4564 (NIST ID: N/A)

**Knowledge of the methods and procedures for communicating with tools/modules, including the use of listening posts.**

| | |
|---|---|
| **01** | **DCOE Mapping to Command-and-Control (C2):** |
| | The manual discusses the methods for establishing and maintaining communication between tools and modules, including the role of listening posts in command-and-control scenarios. |
| **02** | **DCOE Mapping to Adversary TTPs:** |
| | Training includes how adversaries use listening posts and communication techniques to control compromised systems and coordinate their operations. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises provide experience with configuring and monitoring communication channels between modules, emphasizing their role in offensive and defensive operations. |
| **04** | **DCOE Mapping to Cyber Operations Management:** |
| | Scenarios cover operational considerations for using listening posts, such as ensuring secure communications and monitoring for unauthorized access. |

This KSAT is addressed through practical applications and theoretical discussions of communication methods and tools within cyber operations.

### 4565 (NIST ID: N/A)

**Knowledge of the methods of persistence.**

| | |
|---|---|
| **01** | **DCOE Mapping to Adversary TTPs:** |
| | The manual discusses adversarial techniques for achieving persistence, such as creating backdoors, modifying system configurations, and leveraging startup scripts. |
| **02** | **DCOE Mapping to Cyber Kill Chain:** |
| | Persistence is covered in the post-exploitation phase, where adversaries implement techniques to maintain long-term access to compromised systems. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Labs include exercises in identifying and simulating persistence methods, such as registry modifications and scheduled tasks, to enhance practical understanding. |
| **04** | **DCOE Mapping to Defensive Strategies:** |
| | Training emphasizes detecting and mitigating persistence mechanisms through system monitoring, forensic analysis, and proactive security measures. |

This KSAT is addressed through detailed theoretical discussions and practical exercises focused on understanding, detecting, and countering persistence methods.

### 4567 (NIST ID: N/A)

**Knowledge of the Mission Improvement Process.**

| | |
|---|---|
| **01** | **DCOE Mapping to After-Action Reviews:** |
| | The manual includes discussions on the role of after-action reviews in identifying lessons learned from completed missions, which contribute to improving future operations. |
| **02** | **DCOE Mapping to Feedback Mechanisms:** |
| | Scenarios emphasize collecting and analyzing feedback from mission outcomes to refine strategies and processes for better performance. |
| **03** | **DCOE Mapping to Process Evaluation:** |
| | Training involves evaluating operational procedures during and after missions to identify inefficiencies and areas for enhancement. |
| **04** | **DCOE Mapping to Team Collaboration:** |
| | Exercises highlight the importance of team collaboration in reviewing mission results and implementing identified improvements. |

This KSAT is addressed through the manual’s focus on reviewing and refining operational processes to enhance mission outcomes.

### 4628 (NIST ID: N/A)

**Skill in enumerating a host (e.g., file systems, host metadata, host characteristics).**

| | |
|---|---|
| **01** | **DCOE Mapping to System Reconnaissance:** |
| | Training includes exercises focused on identifying and analyzing system-level attributes, such as file structures, configurations, and metadata, to support operational objectives. |
| **02** | **DCOE Mapping to Offensive Cyber Operations:** |
| | Scenarios provide hands-on experience in accessing and exploring host systems, emphasizing techniques to enumerate system details relevant to exploitation or data gathering. |
| **03** | **DCOE Mapping to Defensive Analysis:** |
| | Exercises cover identifying indicators of host enumeration attempts by adversaries, reinforcing defensive strategies to secure system characteristics. |
| **04** | **DCOE Mapping to Practical Tools:** |
| | Labs involve the use of tools to interact with and examine host systems, developing skills in extracting critical system information in controlled environments. |

This KSAT is addressed through targeted training and exercises that build the foundational skills required for host enumeration in both offensive and defensive contexts.

### 4674 (NIST ID: N/A)

**Skill in using network enumeration and analysis tools, both active and passive.**

| | |
|---|---|
| **01** | **DCOE Mapping to Network Reconnaissance:** |
| | Training includes scenarios where students perform network reconnaissance using both active and passive methods to identify network assets, topologies, and vulnerabilities. |
| **02** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises involve tools for network scanning, such as port scanners and traffic analyzers, to actively map networks or passively monitor traffic for insights. |
| **03** | **DCOE Mapping to Threat Hunting:** |
| | The training incorporates threat hunting activities that rely on network analysis to detect anomalies and identify potential threats. |
| **04** | **DCOE Mapping to Adversary TTPs:** |
| | Discussions highlight how adversaries employ enumeration tools to gather information about networks, providing students with an understanding of both offensive and defensive perspectives. |

This KSAT is addressed through targeted exercises and discussions, emphasizing the application of network enumeration and analysis tools in operational scenarios.

### 8017 (NIST ID: N/A)

**Task: As authorized, train cyberspace operators at one’s certification level or below.**

| | |
|---|---|
| **01** | **DCOE Mapping to Skill Proficiency Development:** |
| | The program emphasizes building operational and technical expertise through hands-on scenarios, enabling participants to reinforce their knowledge and guide others effectively. |
| **02** | **DCOE Mapping to Scenario-Based Exercises:** |
| | Participants engage in structured exercises that simulate real-world operations, which can serve as a framework for teaching and mentoring other operators. |
| **03** | **DCOE Mapping to Operational Tradecraft:** |
| | Training includes best practices and techniques in cyber operations, providing participants with the knowledge to instruct others in foundational and advanced tradecraft. |
| **04** | **DCOE Mapping to Leadership and Collaboration:** |
| | The program fosters collaboration and leadership skills, equipping participants to support and train team members in a mission-focused environment. |

This task aligns with the DCOE’s benefit of developing expertise and leadership, providing a strong foundation for training and mentoring others in cyberspace operations.

### 8020 (NIST ID: N/A)

**Task: Assess the technical health of the cyberspace operator work role.**

| | |
|---|---|
| **01** | **DCOE Mapping to Skills Assessment:** |
| | Training includes evaluations of participant performance during hands-on labs and scenarios, demonstrating methods to assess technical proficiency in cyberspace operations. |
| **02** | **DCOE Mapping to Force Readiness:** |
| | Scenarios emphasize the importance of maintaining readiness, providing insights into evaluating the capabilities and preparedness of operators in their roles. |
| **03** | **DCOE Mapping to Continuous Improvement:** |
| | The program integrates feedback loops through debriefs and performance reviews, which contribute to understanding and improving the technical health of operators. |
| **04** | **DCOE Mapping to Emerging Technology and Techniques:** |
| | Training on the latest tools and methodologies equips participants with the ability to gauge whether operators are keeping pace with evolving cyber threats and technologies. |

This task aligns with the DCOE's emphasis on operational readiness, performance evaluation, and continuous development within cyberspace roles.

### 8021 (NIST ID: N/A)

**Task: Assess, recommend, and evaluate remediation actions.**

| | |
|---|---|
| **01** | **DCOE Mapping to Incident Response:** |
| | Training includes scenarios where participants assess the impact of incidents, recommend mitigation strategies, and evaluate the effectiveness of remediation efforts. |
| **02** | **DCOE Mapping to Defensive Operations:** |
| | The program emphasizes identifying vulnerabilities and implementing countermeasures to secure systems, aligning with the task of recommending and evaluating remediation actions. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Exercises simulate real-world situations where participants must develop and test remediation strategies to resolve security threats and ensure system integrity. |
| **04** | **DCOE Mapping to Continuous Improvement:** |
| | Post-incident debriefs and evaluations encourage participants to analyze remediation actions, ensuring lessons learned are integrated into future responses. |

This task is supported by the DCOE's focus on incident response, defensive measures, and iterative evaluation of actions to improve cybersecurity posture.

### 8030 (NIST ID: N/A)

**Task: Conduct cyber activities to deny, degrade, disrupt, destroy, manipulate (D4M).**

| | |
|---|---|
| **01** | **DCOE Mapping to Offensive Cyber Operations:** |
| | The program includes scenarios where participants execute operations that align with D4M objectives, such as disrupting adversary networks or degrading their capabilities through targeted actions. |
| **02** | **DCOE Mapping to Cyber Effects:** |
| | Training emphasizes achieving operational effects through carefully planned and executed cyber activities, incorporating elements of denial and manipulation. |
| **03** | **DCOE Mapping to Adversary TTPs:** |
| | Participants learn to analyze and counter adversary tactics, gaining insights into how D4M strategies are applied and defended against in real-world scenarios. |
| **04** | **DCOE Mapping to Hands-On Labs:** |
| | Exercises involve simulated cyber operations where participants implement D4M actions, reinforcing technical and strategic execution skills. |

This task is well-represented in the DCOE’s focus on offensive operations and achieving mission objectives through tailored cyber effects.

### 8037 (NIST ID: N/A)

**Task: Conduct post-mission actions.**

| | |
|---|---|
| **01** | **DCOE Mapping to After-Action Reviews:** |
| | Training emphasizes conducting structured after-action reviews to evaluate mission outcomes, identify successes and failures, and document lessons learned. |
| **02** | **DCOE Mapping to Documentation and Reporting:** |
| | Participants practice compiling detailed reports on mission activities, including operational insights, key findings, and recommended follow-up actions. |
| **03** | **DCOE Mapping to Feedback Integration:** |
| | Scenarios highlight incorporating feedback from team members and stakeholders to improve future operations and refine processes. |
| **04** | **DCOE Mapping to Continuous Improvement:** |
| | The program fosters a culture of iterative improvement by using post-mission evaluations to enhance tradecraft and operational readiness. |

This task is supported through the DCOE's focus on structured debriefing, reporting, and the integration of lessons learned into future planning.

### 8039 (NIST ID: N/A)

**Task: Conduct pre-mission actions.**

| | |
|---|---|
| **01** | **DCOE Mapping to Mission Planning:** |
| | Training emphasizes defining mission objectives, identifying required resources, and assigning roles to prepare for successful execution. |
| **02** | **DCOE Mapping to Pre-Mission Briefings:** |
| | Participants practice delivering and receiving pre-mission briefings to ensure team alignment on objectives, operational details, and risk assessments. |
| **03** | **DCOE Mapping to Operational Preparation:** |
| | Scenarios include configuring tools, verifying system readiness, and rehearsing operational procedures to address mission-specific requirements. |
| **04** | **DCOE Mapping to Threat and Environment Analysis:** |
| | The program incorporates exercises to analyze the operational environment and potential adversary actions, providing essential context for pre-mission decision-making. |

This task is supported by the DCOE’s structured approach to mission preparation, ensuring participants are equipped to execute missions effectively.

### 8040 (NIST ID: N/A)

**Task: Conduct pre-operation research and prep.**

| | |
|---|---|
| **01** | **DCOE Mapping to Reconnaissance Activities:** |
| | Training includes performing reconnaissance to gather critical information about the operational environment, adversary capabilities, and potential vulnerabilities. |
| **02** | **DCOE Mapping to Intelligence Analysis:** |
| | Scenarios emphasize analyzing threat intelligence and contextual data to inform operational planning and decision-making. |
| **03** | **DCOE Mapping to Tool Configuration:** |
| | Participants engage in exercises to configure tools and systems, ensuring readiness for mission-specific requirements. |
| **04** | **DCOE Mapping to Operational Environment Preparation:** |
| | The program covers identifying and mitigating risks in the operational environment through thorough research and pre-deployment testing. |

This task aligns with the DCOE’s focus on preparation through reconnaissance, intelligence analysis, and tool readiness to enable effective operations.

## 8052 (NIST ID: N/A)

**Task: Create/normalize/document/evaluate TTPs in cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Operational Planning:** |
| | Training emphasizes developing and refining tactics, techniques, and procedures (TTPs) to support mission objectives and adapt to evolving threats. |
| **02** | **DCOE Mapping to Hands-On Exercises:** |
| | Scenarios involve applying and evaluating TTPs in simulated environments, enabling participants to assess their effectiveness and document improvements. |
| **03** | **DCOE Mapping to Standardization:** |
| | The program includes discussions on the importance of normalizing TTPs to ensure consistency and interoperability across teams and operations. |
| **04** | **DCOE Mapping to Lessons Learned:** |
| | Post-mission reviews focus on capturing lessons learned and updating TTPs based on mission outcomes and identified gaps. |

This task is addressed through the DCOE’s emphasis on developing, refining, and evaluating TTPs to enhance operational effectiveness.

### 8067 (NIST ID: N/A)

**Task: Develop and/or inform risk assessments.**

| | |
|---|---|
| **01** | **DCOE Mapping to Threat Analysis:** |
| | Training incorporates analyzing adversary tactics, techniques, and procedures (TTPs) to identify potential risks to systems and operations. |
| **02** | **DCOE Mapping to Mission Planning:** |
| | Scenarios emphasize identifying vulnerabilities and operational risks during mission planning to inform decision-making and mitigation strategies. |
| **03** | **DCOE Mapping to Incident Response:** |
| | Exercises include assessing risks associated with active threats and determining appropriate containment and remediation actions. |
| **04** | **DCOE Mapping to Continuous Improvement:** |
| | The program integrates feedback loops and lessons learned from operations to refine risk assessment processes and enhance organizational readiness. |

This task aligns with the DCOE’s focus on threat analysis, mission planning, and operational readiness to support informed risk assessment practices.

## 8071 (NIST ID: N/A)

**Task: Develop Operational Training Solutions.**

| | |
|---|---|
| **01** | **DCOE Mapping to Scenario Design:** |
| | Training includes designing and participating in realistic scenarios that replicate operational environments, providing a framework for creating effective training solutions. |
| **02** | **DCOE Mapping to Skills Development:** |
| | The program emphasizes skill-building exercises that can be adapted into training modules to address specific operational requirements. |
| **03** | **DCOE Mapping to Lessons Learned:** |
| | Participants review post-operation insights to refine and improve training content, ensuring alignment with evolving tactics and technologies. |
| **04** | **DCOE Mapping to Collaborative Exercises:** |
| | The DCOE promotes team-based exercises, offering a model for developing training solutions that enhance collaborative operational readiness. |

This task is supported by the DCOE’s focus on practical, scenario-based training and iterative improvement to develop effective operational training solutions.

### 8074 (NIST ID: N/A)

**Task: Develop risk assessments for non-standard events and ad hoc tradecraft.**

| | |
|---|---|
| **01** | **DCOE Mapping to Adaptive Threat Analysis:** |
| | Training emphasizes analyzing unconventional adversary tactics and techniques, providing the foundation for assessing risks in non-standard scenarios. |
| **02** | **DCOE Mapping to Scenario-Based Exercises:** |
| | Scenarios involve responding to unique and evolving operational conditions, enabling participants to evaluate risks associated with ad hoc tradecraft. |
| **03** | **DCOE Mapping to Operational Planning:** |
| | Exercises highlight identifying vulnerabilities and assessing risks during the planning phase, particularly in dynamic and unpredictable operational environments. |
| **04** | **DCOE Mapping to Continuous Improvement:** |
| | The program integrates lessons learned from atypical events into the risk assessment process, ensuring adaptability to future non-standard operations. |

This task aligns with the DCOE’s emphasis on flexible operational planning and dynamic threat analysis to develop robust risk assessments for unconventional scenarios.

### 8083 (NIST ID: N/A)

**Task: Employ collection TTPs in cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Reconnaissance Activities:** |
| | Training includes performing reconnaissance to gather critical information about target systems, networks, and adversary capabilities, employing tailored TTPs for effective collection. |
| **02** | **DCOE Mapping to Adversary TTPs:** |
| | Participants study adversary tactics, techniques, and procedures, learning to replicate and counter these methods in operational scenarios. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises simulate real-world collection activities, where participants use tools and techniques to extract valuable intelligence from operational environments. |
| **04** | **DCOE Mapping to Operational Planning:** |
| | Training emphasizes integrating collection TTPs into mission objectives, ensuring alignment with strategic goals and enhancing overall effectiveness. |

This task is supported by the DCOE’s focus on reconnaissance, intelligence gathering, and the operational application of collection TTPs.

### 8084 (NIST ID: N/A)

**Task: Employ credential access TTPs in cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Offensive Cyber Operations:** |
| | Training includes scenarios where participants execute credential access techniques, such as password cracking or exploiting credential stores, to achieve operational objectives. |
| **02** | **DCOE Mapping to Adversary TTPs:** |
| | Participants learn how adversaries use credential access tactics to gain unauthorized access, providing insights into employing similar techniques in controlled environments. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises involve tools and methods for obtaining credentials, such as analyzing authentication mechanisms and identifying vulnerabilities in access controls. |
| **04** | **DCOE Mapping to Defensive Awareness:** |
| | Scenarios also cover detecting and mitigating credential access attempts, ensuring participants understand both offensive and defensive implications of these techniques. |

This task is aligned with the DCOE's focus on operational application of credential access techniques and understanding their role in cyberspace operations.

### 8086 (NIST ID: N/A)

**Task: Employ discovery TTPs in cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Reconnaissance Techniques:** |
| | Training includes scenarios where participants perform discovery activities to identify network topologies, system configurations, and connected devices as part of operational planning. |
| **02** | **DCOE Mapping to Adversary TTPs:** |
| | Participants analyze how adversaries use discovery techniques to gather information, enabling the development of similar strategies for mission objectives. |
| **03** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises involve using tools to enumerate hosts, map network structures, and identify critical infrastructure, reinforcing discovery skills. |
| **04** | **DCOE Mapping to Defensive Practices:** |
| | Training also emphasizes recognizing and mitigating adversarial discovery attempts, providing participants with a comprehensive understanding of discovery TTPs. |

This task is supported by the DCOE’s focus on reconnaissance and operational discovery techniques in both offensive and defensive contexts.

### 8087 (NIST ID: N/A)

**Task: Employ exfiltration TTPs in cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyber Kill Chain - Exfiltration Phase:** |
| | The DCOE aligns with the **cyber kill chain**, particularly in the exfiltration phase, where participants learn techniques to move data from target systems while avoiding detection. |
| **02** | **DCOE Mapping to Offensive Operations:** |
| | Training scenarios include the planning and execution of exfiltration activities, emphasizing methods such as encrypted channels, covert protocols, or hidden storage mechanisms. |
| **03** | **DCOE Mapping to Adversary TTPs:** |
| | Participants study adversary exfiltration tactics to understand how data is exfiltrated in real-world operations and replicate these techniques in controlled environments. |
| **04** | **DCOE Mapping to Hands-On Labs:** |
| | Exercises involve using tools and techniques to transfer data securely and discreetly from target systems, reinforcing practical application of exfiltration TTPs. |
| **05** | **DCOE Mapping to Defensive Awareness:** |
| | Training highlights detection and mitigation strategies for exfiltration attempts, such as monitoring data flows and identifying anomalies. |

This task is effectively supported by the DCOE through its focus on the exfiltration phase of the cyber kill chain, practical applications, and defensive considerations.

### 8088 (NIST ID: N/A)

**Task: Employ lateral movement TTPs in cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Cyber Kill Chain - Lateral Movement Phase:** |
| | The training incorporates the **lateral movement phase** of the cyber kill chain, teaching participants techniques to traverse compromised networks and access additional systems. |
| **02** | **DCOE Mapping to Offensive Operations:** |
| | Scenarios involve leveraging credentials, exploiting trust relationships, and utilizing tools to move laterally within a network to achieve operational objectives. |
| **03** | **DCOE Mapping to Adversary TTPs:** |
| | Participants study how adversaries employ lateral movement techniques, providing insights into effective methods for use in cyberspace operations. |
| **04** | **DCOE Mapping to Hands-On Labs:** |
| | Labs simulate network environments where participants execute lateral movement using various tools and techniques, such as remote desktop protocols (RDP) or exploiting shared resources. |
| **05** | **DCOE Mapping to Defensive Practices:** |
| | Training includes recognizing and mitigating lateral movement attempts by adversaries, reinforcing a comprehensive understanding of these techniques. |

This task is well-supported by the DCOE’s focus on operational execution, adversary analysis, and practical application of lateral movement techniques.

### 8089 (NIST ID: N/A)

**Task: Employ TTPs in categories at one’s certification level or below.**

| | |
|---|---|
| **01** | **DCOE Mapping to Operational Readiness:** |
| | Training ensures participants develop proficiency in TTPs aligned with their certification level, providing a solid foundation for employing techniques effectively within their scope. |
| **02** | **DCOE Mapping to Hands-On Scenarios:** |
| | Practical exercises allow participants to apply TTPs in simulated environments, reinforcing their ability to execute these techniques confidently and accurately. |
| **03** | **DCOE Mapping to Knowledge Transfer:** |
| | Scenarios include opportunities to guide and mentor peers at lower certification levels, ensuring consistent understanding and application of TTPs. |
| **04** | **DCOE Mapping to Certification Alignment:** |
| | Training aligns operational tasks with certification competencies, ensuring that participants focus on techniques and procedures appropriate to their level of expertise. |

This task is supported by the DCOE’s structured training approach, emphasizing practical application and certification-aligned competency development.

### 8097 (NIST ID: N/A)

**Task: Evaluate cyberspace operator performance at one’s certification level or below.**

| | |
|---|---|
| **01** | **DCOE Mapping to Performance Assessment:** |
| | Training scenarios involve monitoring and assessing operator actions during exercises, providing a framework for evaluating performance against defined objectives and standards. |
| **02** | **DCOE Mapping to Certification Competencies:** |
| | The program emphasizes aligning tasks and evaluations with certification-level expectations, ensuring assessments are appropriate for the skill level being measured. |
| **03** | **DCOE Mapping to Feedback Mechanisms:** |
| | Participants learn to provide constructive feedback through post-exercise reviews and debriefs, fostering skill development and operational improvement. |
| **04** | **DCOE Mapping to Team Collaboration:** |
| | Training highlights evaluating team dynamics and individual contributions, ensuring operators perform effectively within a collaborative operational environment. |

This task aligns with the DCOE’s emphasis on structured evaluation, feedback, and alignment with certification competencies to enhance cyberspace operator performance.

## 8112 (NIST ID: N/A)

**Task: Identify targets of opportunity in order to influence operational planning.**

| | |
|---|---|
| **01** | **DCOE Mapping to Reconnaissance Activities:** |
| | Training emphasizes performing reconnaissance to identify potential targets of opportunity, including critical infrastructure, vulnerable systems, and key adversary assets. |
| **02** | **DCOE Mapping to Threat Analysis:** |
| | Scenarios involve analyzing adversary behaviors and identifying exploitable weaknesses that could serve as targets to advance operational goals. |
| **03** | **DCOE Mapping to Mission Planning:** |
| | Participants apply target identification to inform mission objectives, ensuring alignment between targets and strategic outcomes. |
| **04** | **DCOE Mapping to Adversary TTPs:** |
| | This task is supported by the DCOE’s focus on reconnaissance, analysis, and integration of identified targets into operational planning. |

Training includes understanding how adversaries identify and exploit opportunities, providing insights that participants can use in their own target identification processes.

**Task: Identify the appropriate operating authorities and guidance.**

| | |
|---|---|
| **01** | **DCOE Mapping to Rules of Engagement (ROE):** |
| | Scenarios emphasize understanding and applying Rules of Engagement (ROE) to ensure operations are conducted within authorized boundaries. |
| **02** | **DCOE Mapping to Mission Planning Frameworks:** |
| | Training integrates mission planning exercises that focus on identifying and adhering to operating authorities and guidance relevant to specific operational contexts. |
| **03** | **DCOE Mapping to Operational Scenarios:** |
| | Participants engage in scenarios where they analyze and align mission objectives with operational directives and permissions to maintain compliance. |
| **04** | **DCOE Mapping to Decision-Making Processes:** |
| | Exercises stress the importance of using ROE and operational guidance to make informed decisions during mission execution. |

This task aligns with the DCOE’s emphasis on applying ROE and operational guidelines in mission planning and execution scenarios.

### 8130 (NIST ID: N/A)

**Task: Maintain operational and technical situational awareness during operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Real-Time Scenario Execution:** |
| | Training scenarios require participants to actively monitor and adapt to dynamic changes within operational environments, interpreting results to make informed decisions. |
| **02** | **DCOE Mapping to Threat Awareness in CTI Labs:** |
| | Participants engage in Cyber Threat Intelligence (CTI) exercises, analyzing adversary activity and potential TTPs, maintaining awareness of evolving threats throughout operations. |
| **03** | **DCOE Mapping to Hands-On Lab Dynamics:** |
| | Labs involve dynamic, real-time interactions where participants must maintain situational awareness to understand system responses and assess operational impacts. |
| **04** | **DCOE Mapping to Decision-Making in Fluid Environments:** |
| | Exercises emphasize interpreting data and outcomes in real-time, ensuring alignment with mission objectives and the ability to adapt to unexpected developments. |

This task aligns with the DCOE's emphasis on maintaining situational awareness through hands-on, dynamic training scenarios and CTI-focused exercises.

### 8158 (NIST ID: N/A)

**Task: Produce strategy to inform commander's decision-making process.**

| | |
|---|---|
| **01** | **DCOE Mapping to Mission Planning:** |
| | The DCOE provides robust training in mission planning, enabling participants to craft strategies that align operational objectives with the commander's overall goals and priorities. |
| **02** | **DCOE Mapping to Adversary Awareness:** |
| | Exercises emphasize understanding Advanced Persistent Threats (APTs) and adversary TTPs, equipping participants with the knowledge to incorporate threat dynamics into strategic recommendations. |
| **03** | **DCOE Mapping to Real-Time Scenario Integration:** |
| | Training incorporates hands-on labs and dynamic scenarios that simulate adversary actions, helping participants develop strategies informed by realistic operational conditions. |
| **04** | **DCOE Mapping to Operational Recommendations:** |
| | Scenarios focus on creating actionable and clear recommendations, ensuring that strategies effectively communicate critical insights to support commander decision-making. |

This task aligns with the DCOE's emphasis on mission planning, adversary familiarity, and integrating operational insights to produce effective strategies for leadership.

### 8167 (NIST ID: N/A)

**Task: Provide input to mission debrief.**

| | |
|---|---|
| **01** | **DCOE Mapping to After-Action Reviews:** |
| | Training emphasizes conducting after-action reviews, where participants analyze mission outcomes and provide critical input on successes, challenges, and areas for improvement. |
| **02** | **DCOE Mapping to Hands-On Scenarios:** |
| | Scenarios simulate mission environments, requiring participants to assess performance, interpret results, and contribute insights during post-mission debriefs. |
| **03** | **DCOE Mapping to Threat Analysis Contributions:** |
| | Participants integrate observations about adversary TTPs and their impact on mission objectives, ensuring debriefs include actionable intelligence for future planning. |
| **04** | **DCOE Mapping to Continuous Improvement:** |
| | Training highlights the importance of input from all team members during debriefs to refine strategies, enhance operational readiness, and improve team collaboration. |

This task aligns with the DCOE’s focus on structured debriefing processes, emphasizing actionable insights and collaborative reflection to improve future operations.

### 8168 (NIST ID: N/A)

**Task: Provide input to operational policy.**

| | |
|---|---|
| **01** | **DCOE Mapping to Mission Planning Frameworks:** |
| | Training emphasizes structured mission planning, enabling participants to identify gaps or improvements that can inform operational policies. |
| **02** | **DCOE Mapping to Lessons Learned:** |
| | After-action reviews encourage participants to analyze mission outcomes and suggest changes to operational guidelines, ensuring policies remain adaptive to evolving challenges. |
| **03** | **DCOE Mapping to Threat Analysis:** |
| | Insights gained from studying adversary TTPs and operational scenarios provide a foundation for recommending policy updates that address current and emerging threats. |
| **04** | **DCOE Mapping to Scenario-Based Learning:** |
| | Hands-on scenarios help participants identify practical challenges and propose policy improvements to enhance effectiveness and readiness in real-world applications. |

This task is supported by the DCOE’s focus on integrating operational insights, lessons learned, and adversary analysis to inform and refine operational policies.

### 8169 (NIST ID: N/A)

**Task: Provide input to post-mission planning.**

| | |
|---|---|
| **01** | **DCOE Mapping to After-Action Reviews:** |
| | Training emphasizes structured after-action reviews, where participants analyze mission results and contribute recommendations for future planning and operations. |
| **02** | **DCOE Mapping to Lessons Learned Integration:** |
| | Participants identify successes, challenges, and gaps from completed missions, providing actionable insights to inform subsequent mission strategies. |
| **03** | **DCOE Mapping to Adversary TTP Analysis:** |
| | Training includes the analysis of adversary behaviors observed during missions, allowing participants to recommend adjustments to future plans to counter evolving threats. |
| **04** | **DCOE Mapping to Scenario-Based Feedback:** |
| | Scenarios foster the ability to reflect on operational dynamics and propose refinements to tools, techniques, or strategies for improved mission outcomes. |

This task aligns with the DCOE’s focus on continuous improvement and integration of mission insights to enhance future operational planning.

### 8170 (NIST ID: N/A)

**Task: Provide input to pre-mission planning.**

| | |
|---|---|
| **01** | **DCOE Mapping to Reconnaissance Activities:** |
| | Training emphasizes conducting reconnaissance to gather critical intelligence, enabling participants to provide valuable input during the mission planning phase. |
| **02** | **DCOE Mapping to Threat Analysis:** |
| | Participants analyze adversary TTPs and potential risks, contributing insights that shape objectives and strategies for pre-mission planning. |
| **03** | **DCOE Mapping to Operational Objectives:** |
| | Scenarios focus on aligning mission goals with operational realities, ensuring input supports achievable and effective planning. |
| **04** | **DCOE Mapping to Collaborative Planning:** |
| | Exercises promote team collaboration, encouraging participants to share knowledge and expertise during pre-mission strategy development. |

This task is supported by the DCOE’s emphasis on intelligence gathering, threat analysis, and collaborative preparation to inform effective mission planning.

### 8174 (NIST ID: N/A)

**Task: Provide oversight of operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to Mission Execution Monitoring:** |
| | Training scenarios require participants to monitor ongoing operations, ensuring alignment with mission objectives and adherence to operational guidelines. |
| **02** | **DCOE Mapping to Situational Awareness:** |
| | Exercises emphasize maintaining real-time awareness of technical and operational developments, equipping participants to oversee and adjust operations as necessary. |
| **03** | **DCOE Mapping to Team Coordination:** |
| | Scenarios highlight the importance of effective communication and coordination, enabling oversight of team activities and ensuring smooth execution of tasks. |
| **04** | **DCOE Mapping to Lessons Learned:** |
| | Post-mission debriefs incorporate oversight perspectives, allowing participants to evaluate operational performance and recommend improvements for future missions. |

This task aligns with the DCOE’s focus on monitoring, coordination, and continuous improvement to ensure effective oversight during cyber operations

### 8175 (NIST ID: N/A)

**Task: Provide quality control of operations and cyberspace operator products at one's certification level or below.**

| | |
|---|---|
| **01** | **DCOE Mapping to Mission Evaluation:** |
| | Training includes evaluating mission outputs and operational performance to ensure alignment with objectives and adherence to established standards. |
| **02** | **DCOE Mapping to Hands-On Scenario Assessments:** |
| | Scenarios involve reviewing the actions and products of operators during exercises, allowing participants to practice quality control techniques. |
| **03** | **DCOE Mapping to Certification Alignment:** |
| | Participants learn to assess tasks and outputs based on certification-level expectations, ensuring operators meet required competencies. |
| **04** | **DCOE Mapping to Lessons Learned and Feedback:** |
| | Post-mission debriefs focus on identifying discrepancies or areas for improvement in operator performance and operational outputs, reinforcing quality standards. |

This task is supported by the DCOE's emphasis on structured evaluation, performance feedback, and alignment with certification-level standards to maintain quality control.

### 8181 (NIST ID: N/A)

**Task: Recognize and respond to indicators of compromise (IOC).**

| | |
|---|---|
| **01** | **DCOE Mapping to Threat Detection:** |
| | Training emphasizes identifying IOCs through active monitoring and analysis of system behaviors, network traffic, and logs during operational scenarios. |
| **02** | **DCOE Mapping to Hands-On Labs:** |
| | Practical exercises involve using tools to detect IOCs, such as anomalous file changes, unusual network patterns, and unauthorized access attempts. |
| **03** | **DCOE Mapping to Incident Response:** |
| | Participants practice responding to detected IOCs by isolating affected systems, mitigating threats, and restoring normal operations. |
| **04** | **DCOE Mapping to Threat Intelligence Integration:** |
| | Scenarios integrate Cyber Threat Intelligence (CTI) activities to enhance participants' ability to correlate IOCs with adversary tactics and techniques. |

This task is supported by the DCOE's focus on proactive detection, analysis, and response to IOCs within dynamic operational environments.

### 8183 (NIST ID: N/A)

**Task: Recognize and respond to events that change risk.**

| | |
|---|---|
| 01 | **DCOE Mapping to Intrusion Detection Systems (IDS) Lab:** |
| | Participants use IDS tools in hands-on labs to detect and respond to anomalous events, such as unexpected traffic patterns or system behaviors, which indicate a shift in risk. |
| 02 | **DCOE Mapping to Threat Analysis:** |
| | Training emphasizes analyzing alerts and logs generated by IDS to assess how detected events alter the threat landscape and operational priorities. |
| 03 | **DCOE Mapping to Incident Response:** |
| | Scenarios focus on responding to risk changes identified through IDS alerts, including isolating affected systems, applying mitigations, and reassessing defensive strategies. |
| 04 | **DCOE Mapping to Adaptive Operations:** |
| | Participants engage in exercises requiring them to evaluate and adjust plans dynamically based on real-time data from IDS and other monitoring systems to ensure mission resilience. |

This task is supported by the DCOE’s hands-on IDS lab and its integration of dynamic risk response within operational contexts.

### 8184 (NIST ID: N/A)

**Task: Record and document activities during cyberspace operations.**

| | |
|---|---|
| **01** | **DCOE Mapping to After-Action Reports (AARs):** |
| | Training emphasizes capturing detailed insights from operations to produce comprehensive AARs, ensuring lessons learned are documented and actionable. |
| **02** | **DCOE Mapping to Lab-Based Note-Taking:** |
| | Participants practice documenting observations and outcomes during hands-on labs, focusing on system interactions, tool usage, and key insights for later analysis. |
| **03** | **DCOE Mapping to Deliverable Creation:** |
| | Scenarios highlight the importance of transforming operational records and notes into clear, structured deliverables, such as mission summaries and technical reports. |
| **04** | **DCOE Mapping to Strategic Feedback:** |
| | Documentation produced during operations is used to inform leadership and support continuous improvement, aligning with operational goals and enhancing future planning. |

This task aligns with the DCOE's focus on thorough documentation, actionable reporting, and the integration of lab-derived insights into structured deliverables.

### 8192 (NIST ID: N/A)

**Task: Steward the cyberspace operator work role.**

| | |
|---|---|
| **01** | **DCOE Mapping to Skill Development:** |
| | Training focuses on building foundational and advanced skills, enabling participants to take ownership of their professional growth and mentor others within their work role. |
| **02** | **DCOE Mapping to Scenario-Based Leadership:** |
| | Scenarios require participants to lead and coordinate activities during operations, fostering a sense of responsibility and stewardship for team performance. |
| **03** | **DCOE Mapping to Lessons Learned:** |
| | After-action reviews emphasize the importance of integrating operational insights into personal and team development, ensuring continuous improvement within the work role. |
| **04** | **DCOE Mapping to Certification Alignment:** |
| | Training aligns operational tasks with certification competencies, promoting accountability for maintaining and advancing the technical health of the work role. |

This task is supported by the DCOE's emphasis on leadership, skill refinement, and alignment with certification standards to ensure effective stewardship of the cyberspace operator role.

### 8197 (NIST ID: N/A)

**Task: Train cyberspace operators at their certified level or below.**

| | |
|---|---|
| **01** | **DCOE Mapping to Scenario-Based Training:** |
| | Participants engage in realistic operational scenarios that mirror training environments, providing a foundation to guide and mentor other operators effectively. |
| **02** | **DCOE Mapping to Hands-On Labs:** |
| | The program emphasizes practical, skill-based labs that participants can adapt into instructional modules for training operators at their certified level or below. |
| **03** | **DCOE Mapping to Operational Tradecraft:** |
| | Training includes discussions and demonstrations of best practices and techniques, equipping participants with the knowledge to instruct others in operational tasks. |
| **04** | **DCOE Mapping to Team Collaboration:** |
| | Exercises highlight collaborative problem-solving, enabling participants to develop leadership skills necessary for training and mentoring their peers. |

This task is supported by the DCOE’s focus on practical skill development, tradecraft, and teamwork, preparing participants to train operators effectively within their certification scope.

**Cyber Security Forum Initiative, Inc. (CSFI)**
9401 Battle Street, Suite 202 Manassas, VA 20110, USA
www.csfi.us
CAGE CODE 8L7W