Attachment I - CLIN 00005 - Current NETL Cybersecurity Definitions

Current NETL Cybersecurity Definitions

Risk and Vulnerability Assessment Knowledge Areas

Knowledge Areas include, but are not limited to:

- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, v3 (ITIL))
- Knowledge of system and application security threats and vulnerabilities
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)
- Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)
- Knowledge of network access, identity and access management (e.g., public key infrastructure, PKI)
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- Skill in assessing the robustness of security systems and designs
- Skill in the use of social engineering techniques
- Skill in applying host/network access controls (e.g., access control list)
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Skill in using network analysis tools to identify vulnerabilities
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
- Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (i.e., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure)
- Maintaining knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing

Cyber Hunt

Knowledge Areas include, but are not limited to:

- Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])
- Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)
- Knowledge of incident categories, incident responses, and timelines for responses
- Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
- Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
- Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.
- Conducts advanced analysis of collection and open-source data to ensure target continuity, profile targets and their activities, and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
- Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Incident Response

- Knowledge Areas include, but are not limited to:
    - Knowledge of incident categories, incident responses, and timelines for responses
    - Knowledge of incident response and handling methodologies
    - Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies

Penetration Testing

Knowledge Areas include but are not limited to:

- Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit, etc.)
- Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data

Information Assurance

Knowledge Areas include but are not limited to:

- Knowledge of binding directives, industry standards, regulations, and key frameworks (NIST, ISO, etc.) that govern information systems and their security controls
- Knowledge of information system integrity, availability, authentication, confidentiality, and nonrepudiation
- Knowledge of business risk management, risk mitigation, risk evaluation/assessment, and risk acceptance
- Knowledge of governing federal and internationals laws regarding release and security of information