USACyS, 170A WOAC Advanced Technical Block Resources

REQUIREMENT - Advanced cyber technical industry training seven (7) modules, two (2) iterations per module. The Period of Performance is 14 August 2023 – 03 May 2024.

TECHNICAL SALIENT CHARACTERISTICS – Each Module list a Learning Outcome or Terminal Learning Objective (TLO) and the Enabling Learning Objectives (ELOs); learning support activities associated to each Learning Outcome/TLO.

MODULE – WEB APPLICATIONS.

Learning Outcome/TLO: Given access to enterprise services, examine services and operations and develop posture of Defense-In-Depth.

- Evaluate the interoperability of Enterprise Services.
- Understand current threat techniques such as the OWASP Top 10 Web.
- Application Security Threats.
- Evaluate data flow between services.
- Evaluate advanced security methods.
- Evaluate authentication and authorization methods.
- Evaluate encryption methods such as cryptography, digital signatures, and hashing algorithms.
- Evaluate Defense-in-Depth methodology.
- Validate Enterprise Services data flow and operations.
- Understand defense validation of web application security testing with techniques such as fuzzing, SQL injection, Cross Site Request Forgery (CSRF), and Cross Site Scripting (XSS) attacks.
- Understand secure coding practices such as the software development lifecycle (SDLC) within enterprise applications.
- Ability to recommend advanced security measures and secure application practices.
- Ability to implement security measures in highly scalable domains.
- Integration of robust authentication and authorization methods.
- Integration of robust encryption methods.

MODULE – ICS/SCADA.

Learning Outcome/TLO: Examine the different Embedded Operating Systems and their corresponding infrastructures.

- Comprehend Industrial Control Systems / Supervisory Control and Data Acquisition (ICS/SCADA).
- Comprehend Military Communication Systems and Networks for tactical operations.
- Comprehend other embedded operating systems and Internet of Things (IoT) devices.
- Understand differences in security posture of ICS/SCADA environment and traditional enterprise services.
- Assess ICS/SCADA protocols and systems such as Modbus traffic, Human Machine Interface (HMI), Programmable logic controllers (PLC), and Remote Terminal Units (RTU).
- Understand logic with PLC/RTU programming.
- Understand building a network and host collection plans within ICS/SCADA environment with sensors and collection methodology.
- Understand analysis of ICS/SCADA environment and military communications system host and network artifacts.
- Assess Military Communication Systems and Networks for tactical operations.
- Assess other Embedded Operating Systems in cyberspace operations, as required.
- Understand ICS/SCADA regulations and regulatory compliance with organizations such as NERC CIP, NIST, AGA12, API, ISA/IEC 62443, and CIDX/ACC.

MODULE – ADVANCED WINDOWS SCRIPTING (POWERSHELL).

Learning Outcome/TLO: Microsoft Windows-based System with PowerShell, design PowerShell scripts to enable Cyberspace Operations.

- Integrate installation & security considerations, interpret advanced logic, operators, and techniques.
- Integrate advanced WMI, .NET, and WS-MAN concepts.
- Integrate advanced debugging techniques.
- Understand Interacting with Windows Registry and COM objects.
- Understand using windows scripting to interact with Active Directory objects, and Kerberos gold, and silver Tickets, domain, and forest machines.
- Understand PowerShell attacks with frameworks like PowerShell Empire and the stages of the penetration testing methodology from vulnerability scanning, information gathering and enumeration, privilege escalation, lateral movement, persistence, and finally covering tracks.
- Understand API calls and develop custom WMI Classes and Namespaces.
- Retrieve, alter, or create specific data from a group of systems using Windows scripting.
- Create PowerShell scripts and programs to solve complex problems.
- Repurpose complex scripts.

MODULE – ADVANCED UNIX SCRIPTING (PYTHON).

Learning Outcome/TLO: Given a Unix/Linux environment with python 3.8 or greater installed, the student will design Python scripts to enable Cyberspace Operations.

- Integrate installation & security considerations, interpret advanced logic, operators, and techniques.
- Understand code reuse and the potential security risks.
- Understand and implement advanced exception handling.
- Integrate API calls (web based / OS based).
- Understand threading and the limitations of GIL.
- Understand forks and forking.
- Understand and integrate pipes (anonymous pipes and named pipes).
- Integrate third party python libraries into scripts (i.e. Scapy, Requests, BeautifulSoup, Fabric, etc.).
- Understand network programming.
- Create python scripts and programs to solve complex problems.

MODULE – ADVANCED DIGITAL FORENSICS.

Learning Outcome/TLO: Given a disk image, memory image, and captured network traffic activity, the student will compose a written assessment of malicious activity.

- Understand different forensics tool suites such as FTK, Encase, Magnet Axiom, or Autopsy.
- Understand digital acquisition methods such as local and remote acquisitions with non-memory forensics for non-volatile memory artifacts.
- Understand digital acquisition methods such as local and remote acquisitions with memory forensics for volatile memory artifacts.
- Understand browser and email artifact analysis.
- Assess advanced volatile and non-volatile memory analysis with Linux and Windows Systems.
- Assess advance malware purposes, techniques, and construction.
- Assess mid-level malware changes to systems and networks.
- Comprehend advanced file and process signatures.
- Validate forensic evidence collection.
- Integrate knowledge of threat tactics, techniques, and procedures (TTP) into advanced memory analysis.
- Correlate multiple sources of data into a holistic timeline.
- Develop advanced file and process search capabilities.
- Present analysis of forensic conclusions in operator notes and executive reports.
- Understand anti-forensics techniques and tactics.
- Understand enterprise forensic analysis with enterprise platforms like Tanium, Endgame, Carbon Black, or Security Information and Event Management (SIEM) platforms.
- Perform active hunting of digital forensics artifacts with digital range to defeat read team tactics with purple/blue team tactics.

MODULE – ADVANCED PROTOCOL ANALYSIS.

Learning Outcome/TLO: Given complex network traffic, the student will discern between benign and malicious network activity within more than 75% of the network traffic.

- Identify advanced tunneling methods.
- Understand of advanced encryption methodologies and secure protocols.
- Understanding of intrusion detection \ prevention system signature development.
- Understand incorporating log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past.
- Develop advanced tunneling methods.
- Develop advanced intrusion detection \ prevention system signatures and heuristic
- analysis.
- Develop advanced encryption methodologies and secure protocols.
- Perform filtering and cutting of network traffic.
- Perform deep packet analysis and diagram network traffic with timeline analysis.
- Integrate knowledge of threat tactics, techniques, and procedures (TTP) into advanced network analysis.
- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations.
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation.
- Develop and modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation.
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping.

MODULE – ADVANCED HACKING METHODOLOGIES.

Learning Outcome/TLO: Given a native OS and a training range, the student will employ hacking methodologies to successfully breach highly restricted / well defended networks.

- Introduction to Hacking Methodologies that covers cryptography/VPN, network security monitoring applications like Wireshark, Binary Arithmetic Basics – Hex, Decimal, and Bitwise Operations
- Networking Introduction that covers OSI layer protocols like TCP/UDP or DNS, IP addresses (IPv4 and IPv6), basic understanding of routing, link layer protocols, firewall types, IDS/IPSs, network security monitoring packet filtering with tools like Wireshark
- Web Application Introduction – HTTP protocol basics, cookies, and sessions, tool overviews of web applications like Burp Suite.
- Penetration Testing Lifecycle
    - Engagement
    - Information Gathering
    - Foot printing/Scanning

    - Vulnerability Assessment
    - Exploitation
    - Reporting
- Programming basics with overviews of penetration testing command line scripting with languages such as C++, Python, Bash, PowerShell, and Windows Command line
    - PowerShell Cmdlets used like Get-ChildItem, Get-WMIObject, Get-Process, Get-Service, Invoke-Obfuscation, and Invoke-CradleCrafter
    - PowerShell frameworks like PowerShell Empire, PowerSploit, Posh-SecMod, Nishang, Psgetsystem
- Information Gathering process – Open-Source Intelligence with tools like Whois, Shodan, DNSdumpster, DNSEnum, DNSrecon, The Harvester, DNSMap, Maltego, Netcraft, Google Hacking, or Crunchbase
    - Understand resources to get DNS, domain, IP blocks for organizations.
- Foot printing/Scanning process – Mapping and scanning with tools like Hping, and FPing with basic/advanced Nmap scans like TCP connect, SYN, UDP, Idle, Xmas, ACK, Null, and NSE scripts.
    - Understand banner grabbing, active and passive OS fingerprinting.
    - Performing firewall/IDS evasion techniques with source ports, fragmentation, or timing methods.
- Enumeration process
    - Enumeration of NetBIOS, SMB, SNMP with tools like Dumpsec, Enum4Linux, RPCClient, Winfo, smbclient, mount, snmpwalk, snmpset, and Nmap scripts
- Sniffing with tools like Dsniff, Wireshark, TCPDump, WinDump
- Man-in-the-middle (MiTM) attacks with tools like Ettercap, Cain & Abel, Macof, arpspoof, Bettercap, and SSLStrip
- Vulnerability Assessment process – Using Vulnerability scanners like OpenVAS or Nessus.
    - Identifying weak passwords with tools like Ncrack, Medusa, EyeWitness, Mentalist, CeWL, John the Ripper, or Hydra
- Exploitation process with exploits like Eternal Blue, Shellshock, Heartbleed, remote and client-side exploitation.
- Post-exploitation process with techniques for maintaining access with tools like Mimikatz or Mimipenguin, privilege escalation, lateral movement, building backdoors, maintaining persistence, data exfiltration with tools like Iodine, and performing clean-up after penetration exploitation
- Web Application Attack process:
    - Fingerprinting web applications using tools like Netcat, OpenSSL, Dirbuster, SQLmap, or Httprint.
    - HTTP request examples like GET, POST, or HEAD
    - Cross-site-scripting (XSS) –
        - Understanding of XSS types like reflected, persistent, and DOM-based
        - XSS attacks with tools like BeEF.
    - Server query language (SQL) injections –
        - Understanding of in-band, error-based, and blind SQL injections.
        - Understanding statements like SELECT, UNION, or Boolean operators

        - Understanding of advanced SQL exploitation with xp_cmdshell or database manipulation.
    - Understanding of other web attacks like session hijacking, cross-site request forgery, directory traversal, and file inclusion vulnerabilities.
- System Attacks
    - Introduction into terms like Viruses, Trojans, backdoors, rootkits, botnets, adware/spyware, keyloggers, ransomware, and worms.
    - Password Attack introduction with tools like John the Ripper, Hashcat, OphCrack, or Hydra to perform dictionary or rainbow table attacks of LM/NT hashes and SAM files.
    - Buffer Overflow attacks with introduction of heap and stack operations
- Network Attacks
    - Authentication attacks with tools like Hydra to perform brute force and dictionary attacks
    - Windows shares with NetBIOS protocols, Admin and misconfigured shares.
    - Null sessions with tools like nbtstat, netview, nmblookup, enum4linux, winfo, and smbclient.
    - ARP poisoning attacks with tools like dsniff, arpspoof, or Cain & Abel
    - Metasploit/Meterpreter modules used for configuring network attacks with exploits, payloads, and basic script configuration.
- Windows and Linux Architecture introduction which covers Assembly language, registers, process memory, and stack operations like POP, PUSH, and NOPs.
    - Understanding of security implementations like ASLR (Address Space Layout Randomization), DEP (Data Execution Prevention), Stack Canaries, SafeSEH, and ROP chains.
    - Assemblers, Debuggers, and Compilers like Microsoft Visual C ++ and debuggers like Immunity Debugger, IDA Pro, GDB, WinDBG, and OllyDBG
- Buffer Overflows
    - Understanding of vulnerable functions like strcpy/strncpy
    - Understanding of fuzzing and static code review for finding buffer overflows
    - Building buffer overflows with understanding offsets and using tools like pattern create, pattern offset, and mona to overwrite stack pointers.
- Shellcode
    - Introduction to local and remote shellcode
    - Building basic and advanced shellcode with tools like msfvenom to avoid terminators, Nulls, and security implementations.
- Cryptography and Password cracking
    - Discussion of Public Key Infrastructure, PGP, and misconfigurations in implementation of cryptography systems.
- Malware
    - Malware techniques with process hiding, hooking, obfuscation, packing, polymorphism and metamorphism.
    - Examination of malware types like key loggers, Trojans, viruses, or worms.
- Social Engineering process with tools like Social Engineering Toolkit (SET) to perform Phishing, Spear Phishing, and Whale Phishing.

- Wireless Attacks – Understanding of wireless standards like WEP, WPA, WPA2, WPS, and WPA3
    - Understanding of Wireless attacks like initialization vector flaws, birthday paradox, rogue access points, evil-twin attack, and war driving
    - Display knowledge in the operation of wireless tools like inSSIDer, Kismet, aircrack-ng, airodump-ng, oclHashCat, CloudCracker, Pyrit, and Eaphammer
- Ruby Fundamentals
    - Introduction to the data types, arrays, ranges and hashes, variables, declarations and how is it used as an interpreter.
    - Understanding of Ruby methods, blocks, aliases, classes, modules and handling exceptions
    - Understanding of exploitation methodology with Ruby
- Understanding of maintaining in-depth notes and screenshots for penetration reports.