USAID
FROM THE AMERICAN PEOPLE

## Annex to the

# CERTIFICATE of COMPLETION

of the course

## Foundations of Computer and Network Security

within the 2022 Cybersecurity Summer Instructor Training Program

under the **USAID Cybersecurity for Critical Infrastructure in Ukraine Activity**

**11 July – 31 August 2022**

| Module | Hours |
|---|---|
| Remembering the networking basics<br>• Remembering the theory on OSI and TCP/IP models, IPv4 / IPv6, TCP / UDP, and Cybersecurity basics. | 2 |
| Remembering the information security basics<br>• Theory on cybersecurity threats/vulnerabilities/risks/controls.<br>Vulnerability management: Network / credentialed / agent-based scan, external / internal scan, cloud secure configuration checks, CVE/CVSS/CWE; Penetration testing (PTES, NIST SP 800-115, ISSAF); Auditing: manual/automated checks; CIS Controls / Internal Standards. | 4 |
| Physical network security<br>• Physical threats to modern networks and protection from them. | 2 |

| | |
|---|---|
| Switching security<br>• Attacks: ARP spoofing, CAM table overflow, STP abusing, Double VLAN tagging, abusing DTP, abusing VTP, bypassing 802.1X (MAB bypass, bridge-based attacks), discovering networks with CDP/LLDP, other methods of switch compromise (recovering passwords from backups, recovering passwords having direct access, delivering an infecting OS update package, brute-forcing passwords, exploiting switch vulnerabilities).<br>• Protection: port-security, root / BPDU / loop guard, DHCP Snooping, Dynamic ARP Inspection, protecting trunks and VTP, protecting 802.1X (profiling, EAP-TLS, 802.1xAE, MACsec + NEAT).<br>• L2 network design. | **4** |
| Routing security<br>• Attacks: ICMP redirection, IPv6 redirection attacking NDP, attacking RIPv1/RIPv2/OSPF, DNS spoofing and cache poisoning, LLMNR spoofing, WPAD spoofing, attacking VRRP/GLBP/HSRP, DHCP spoofing; ICMP exfiltration, IP headers fields exfiltration, DNS tunneling; DoS attacks like a smurf, DNS amplification, DHCP starvation, by attacking IPv6 NDP, IPv6 CGA flood, attacking DNS; other attacking vectors (password recovery online/from backups/having physical access, infecting OS update package, exploiting router vulnerabilities).<br>• Protection: DHCP Snooping, Dynamic ARP Inspection, port-security, IP source guard; protecting RIP/OSPF and VRRP/HSRP/GLBP protocols using strong authentication; IPv6 security (CGA, SEND, SAVI, IPv6 RA Guard, IPv6 Snooping, IPv6 Destination Guard, DHCPv6 Guard); DNSsec; Source IP Validation.<br>• L3 network design. | 4 |

| | |
|---|---|
| Remote access security<br>• VPN: RA/S2S, GRE/LT2P/PPTP, SSTP/MPPE/IPsec/TLS, L2/L3.<br>• Proxy: forward/reverse/transparent, anonymizers.<br>• Privacy: Tor/I2P, DoH/DoT.<br>• Remote access tools: telnet, SSH, RDP, others.<br>• ZTNA: Conditional Access, ZTVPN / Opportunistic encryption, ZTProxy.<br>• Remote Access Security: exploiting VPN concentrator/proxy vulnerabilities, enumerating users, brute-forcing accounts, and eavesdropping traffic by exploiting weak cryptography and configurations. | 4 |
| Transport layer security<br>• Attacks: SYN/UDP flood, Mitnick attack, opt-ack attack, footprinting of the network (using TCP Flags / UDP scans), fingerprinting of network services (using unique TCP parameters).<br>• Protection: stateful firewalls, SSL/TLS, QUIC, encrypted traffic inspection. | 2 |
| Wi-Fi security<br>• Wi-Fi basics.<br>• Attacks on Wi-Fi: eavesdropping, evil twin, evil free Wi-Fi sharing, jamming DoS, WPA-PSK cracking, WPS abusing, RADIUS replay attack, side-channel SSID leakage, war-driving, WPA2 attacks (KRACK, FragAttacks); other (password recovery online/from backups/having physical access, infecting OS update package, exploiting Wi-Fi router vulnerabilities).<br>• Wi-Fi security: SSID hiding, MAC filtering, WPA2/WPA3-Personal, WPA-Enterprise, AP power limiting, auditing for rogue Wi-Fi APs, WIDS/WIPS.<br>• Attacks and protection of Bluetooth. | 2 |
| Firewall, IDPS, Network Monitoring | 4 |

| | |
|---|---|
| • Packet filter/stateful/L7 firewalls, time-based firewalls; DMZ creation, VLANs network traffic protection, micro-segmentation; IDPS (network traffic analysis / log files monitoring / file integrity monitoring); Network monitoring (SNMPv3, NetFlow). | |
| Application layer security<br>• Attacks: software flaws and vulnerabilities (exploit, CVSS, CVE, zero-day), weaknesses (CWE, OWASP Top 10, weak default config, weak password, and account protection policies); password compromise (online/offline cracking, password leaks).<br>• Protection: HTTP security headers; Email (S/MIME, SPAM/Phishing filters, DNSBL/SURBL, SPF/DKIM/DMARC); FTPS (no anonymous logins, IP ACL / Time-based ACL, logging); DNSsec; SMB hardening; SNMP hardening; configuring things securely; Applications protection (application and its environment hardening, applying for brute-force protection, regular patching). | 4 |
| Host security<br>• Hardening an OS; preventing data leaks (DLP, USB/BT file transfers, HDD encryption); Zero-trust (CASB, ZTProxy, ZT-VPN, host compliance checks); Administrative protection measures. | 2 |

| | |
|---|---|
| Digital identity protection<br>• Authentication (password-based / passwordless), MFA (SMS, phone call, mobile app, biometry, digital tokens), SSO (NTLM, Kerberos, SAML, Certificate-based, RADIUS/TACACS+); UEBA; Administrative controls (phishing tests, awareness training, policies). | **2** |
| BCP & DRP<br>• BCP & DRP: backups (full/incremental/differential, on-site/off-site, hot/warm/cold backup, SSD/HDD/tape media), redundancy (RAID, additional network components, hot/warm/cold reserve); Administrative controls (edu users, recovery testing, BCP testing, policies). | 2 |
| Incidents Management<br>• Threat management: threat hunting, threat intelligence, threat modeling, IoC, unified kill chain, MITRE ATT&CK.<br>• Incident management: IRT/ERT/CSIRT; NIST SP 800-61 / SANS Incident Handler's Handbook / FIRST; SOC. Forensics basics; Administrative controls | 2 |
| Labs and Practices | 40 |
| Self-study | 90 |
| Tests | 10 |
| **Total** | **180** |

**Petro Matiaszek**

**Chief of Party, USAID Cybersecurity for Critical Infrastructure in Ukraine Activity**