Corso Ethical Hacker & Security Manager

SOMMARIO

MODULO SECURITY MANAGER PER LA CERTIFICAZIONE COMPTIA SECURITY+

UNIT 1 - THREATS, ATTACKS, AND VULNERABILITIES

MODULE 1 - COMPARE AND CONTRAST DIFFERENT TYPES OF SOCIAL ENGINEERING TECHNIQUES

- ✓ Phishing
- ✓ Smishing
- ✓ Vishing
- ✓ Spam
- ✓ Spam over instant messaging (SPIM)
- ✓ Spear phishing
- ✓ Dumpster diving
- ✓ Shoulder surfing
- ✓ Pharming
- ✓ Tailgating
- ✓ Eliciting information

- ✓ Whaling
- ✓ Prepending
- ✓ Identity fraud
- ✓ Invoice scams
- ✓ Credential harvesting
- ✓ Reconnaissance
- ✓ Hoax
- ✓ Impersonation
- ✓ Watering hole attack
- ✓ Typosquatting
- ✓ Pretexting
- ✓ Influence campaigns
  - Hybrid warfare
  - Social media
- ✓ Principles (reasons for effectiveness)
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

MODULE 2 - GIVEN A SCENARIO, ANALYZE POTENTIAL INDICATORS TO DETERMINE THE TYPE OF ATTACK

- ✓ Malware
  - Ransomware
  - Trojans
  - Worms
  - Potentially unwanted programs (PUPs)
  - Fileless virus
  - Command and control
  - Bots
  - Cryptomalware
  - Logic bombs
  - Spyware
  - Keyloggers
  - Remote access Trojan (RAT)
  - Rootkit
  - Backdoor
- ✓ Password attacks
  - Spraying
  - Dictionary
  - Brute force
    - Offline
    - Online
    - Rainbow table

- Plaintext/unencrypted

✓ Physical attacks
- Malicious Universal Serial Bus (USB) cable
- Malicious flash drive
- Card cloning
- Skimming

✓ Adversarial artificial intelligence (AI)
- Tainted training data for machine learning (ML)
- Security of machine learning algorithms

✓ Supply-chain attacks
✓ Cloud-based vs. on-premises attacks
✓ Cryptographic attacks
- Birthday
- Collision
- Downgrade

MODULE 3 - GIVEN A SCENARIO, ANALYZE POTENTIAL INDICATORS ASSOCIATED WITH APPLICATION ATTACKS

✓ Privilege escalation
✓ Cross-site scripting
✓ Injections
- Structured query language (SQL)
- Dynamic-link library (DLL)
- Lightweight Directory Access Protocol (LDAP)
- Extensible Markup Language (XML)

✓ Pointer/object dereference
✓ Directory traversal
✓ Buffer overflows
✓ Race conditions
- Time of check/time of use

✓ Error handling
✓ Improper input handling
✓ Replay attack
- Session replays

✓ Integer overflow
✓ Request forgeries
- Server-side
- Cross-site

✓ Application programming/interface (API) attacks
✓ Resource exhaustion
✓ Memory leak
✓ Secure Sockets Layer (SSL) stripping
✓ Driver manipulation
- Shimming
- Refactoring

✓ Pass the hash

MODULE 4 - GIVEN A SCENARIO, ANALYZE POTENTIAL INDICATORS ASSOCIATED WITH NETWORK ATTACKS

- ✓ Wireless
  - Evil twin
  - Rogue access point
  - Bluesnarfing
  - Bluejacking
  - Disassociation
  - Jamming
  - Radio frequency identification (RFID)
  - Near-field communication (NFC)
  - Initialization vector (IV)
- ✓ On-path attack (conosciuto anche come man-in-the-middle attack/ man-in-the-browser attack)
- ✓ Layer 2 attacks
  - Address Resolution / Protocol (ARP) poisoning
  - Media access control (MAC) flooding
  - MAC cloning
- ✓ Domain name system (DNS)
  - Domain hijacking
  - DNS poisoning
  - Uniform Resource Locator (URL) redirection
  - Domain reputation
- ✓ Distributed denial-of-service (DDoS)
  - Network
  - Application
  - Operational technology (OT)
- ✓ Malicious code or script execution
  - PowerShell
  - Python
  - Bash
  - Macros
  - Visual Basic for Applications (VBA)

MODULE 5 - EXPLAIN DIFFERENT THREAT ACTORS, VECTORS, AND INTELLIGENCE SOURCES

- ✓ Actors and threats
  - Advanced persistent threat (APT)
  - Insider threats
  - State actors
  - Hacktivists
  - Script kiddies
  - Criminal syndicates
  - Hackers
    - Authorized
    - Unauthorized
    - Semi-authorized

- Shadow IT
- Competitors

✓ Attributes of actors
- Internal/external
- Level of sophistication/capability
- Resources/funding
- Intent/motivation

✓ Vectors
- Direct access
- Wireless
- Email
- Supply chain
- Social media
- Removable media
- Cloud

✓ Threat intelligence sources
- Open-source intelligence (OSINT)
- Closed/proprietary
- Vulnerability databases
- Public/private information-sharing centers
- Dark web
- Indicators of compromise
- Automated Indicator Sharing (AIS)
  - Structured Threat Information eXpression (STIX) / Trusted Automated eXchange of Intelligence Information (TAXII)
- Predictive analysis
- Threat maps
- File/code repositories

✓ Research sources
- Vendor websites
- Vulnerability feeds
- Conferences
- Academic journals
- Request for comments (RFC)
- Local industry groups
- Social media
- Threat feeds
- Adversary tactics, techniques, and procedures (TTP)

MODULE 6 - EXPLAIN THE SECURITY CONCERNS ASSOCIATED WITH VARIOUS TYPES OF VULNERABILITIES

✓ Cloud-based vs. on-premises vulnerabilities

✓ Zero-day

✓ Weak configurations
- Open permissions
- Unsecure root accounts
- Errors

- Weak encryption
- Unsecure protocols
- Default settings
- Open ports and services

✓ Third-party risks
- Vendor management
  - System integration
  - Lack of vendor support
- Supply chain
- Outsourced code development
- Data storage

✓ Improper or weak patch management
- Firmware
- Operating system (OS)
- Applications

✓ Legacy platforms

✓ Impacts
- Data loss
- Data breaches
- Data exfiltration
- Identity theft
- Financial
- Reputation
- Availability loss

MODULE 7 - SUMMARIZE THE TECHNIQUES USED IN SECURITY ASSESSMENTS

✓ Threat hunting
- Intelligence fusion
- Threat feeds
- Advisories and bulletins
- Maneuver

✓ Vulnerability scans
- False positives
- False negatives
- Log reviews
- Credentialed vs. non-credentialed
- Intrusive vs. non-intrusive
- Application
- Web application
- Network
- Common Vulnerabilities and Exposures (CVE) / Common Vulnerability Scoring System (CVSS)
- Configuration review

✓ Syslog/Security information and event management (SIEM)
- Review reports
- Packet capture
- Data inputs

- User behavior analysis
- Sentiment analysis
- Security monitoring
- Log aggregation
- Log collectors

✓ Security orchestration, automation, and response (SOAR)

MODULE 8 - EXPLAIN THE TECHNIQUES USED IN PENETRATION TESTING

✓ Penetration testing
- Known environment
- Unknown environment
- Partially known environment
- Rules of engagement
- Lateral movement
- Privilege escalation
- Persistence
- Cleanup
- Bug bounty
- Pivoting

✓ Passive and active reconnaissance
- Drones
- War flying
- War driving
- Footprinting
- OSINT

✓ Exercise types
- Red-team
- Blue-team
- White-team
- Purple-team

UNIT 2 - ARCHITECTURE AND DESIGN

MODULE 1 - EXPLAIN THE IMPORTANCE OF SECURITY CONCEPTS IN AN ENTERPRISE ENVIRONMENT

✓ Configuration management
- Diagrams
- Baseline configuration
- Standard naming conventions
- Internet protocol (IP) schema

✓ Data sovereignty

✓ Data protection
- Data loss prevention (DLP)
- Masking
- Encryption

- At rest
- In transit/motion
- In processing
- Tokenization
- Rights management

✓ Geographical considerations
✓ Response and recovery controls
✓ Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection
✓ Hashing
✓ API considerations
✓ Site resiliency
- Hot site
- Cold site
- Warm site

✓ Deception and disruption
- Honeypots
- Honeyfiles
- Honeynets
- Fake telemetry
- DNS sinkhole

MODULE 2 - SUMMARIZE VIRTUALIZATION AND CLOUD COMPUTING CONCEPTS

✓ Cloud models
- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Anything as a service (XaaS)
- Public
- Community
- Private
- Hybrid

✓ Cloud service providers
✓ Managed service provider (MSP) / Managed Security Service Provider (MSSP)
✓ On-premises vs. off-premises
✓ Fog computing
✓ Edge computing
✓ Thin client
✓ Containers
✓ Microservices/API
✓ Infrastructure as code
- Software-defined networking (SDN)
- Software-defined visibility (SDV)

✓ Serverless architecture
✓ Services integration
✓ Resource policies

- ✓ Transit gateway
- ✓ Virtualization
  - Virtual machine (VM) sprawl avoidance
  - VM escape protection

MODULE 3 - SUMMARIZE SECURE APPLICATION DEVELOPMENT, DEPLOYMENT, AND AUTOMATION CONCEPTS

- ✓ Environment
  - Development
  - Test
  - Staging
  - Production
  - Quality assurance (QA)
- ✓ Provisioning and deprovisioning
- ✓ Integrity measurement
- ✓ Secure coding techniques
  - Normalization
  - Stored procedures
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and software development kits (SDKs)
  - Data exposure
- ✓ Open Web Application Security Project (OWASP)
- ✓ Software diversity
  - Compiler
  - Binary
- ✓ Automation/scripting
  - Automated courses of action
  - Continuous monitoring
  - Continuous validation
  - Continuous integration
  - Continuous delivery
  - Continuous deployment
- ✓ Elasticity
- ✓ Scalability
- ✓ Version control

MODULE 4 - SUMMARIZE AUTHENTICATION AND AUTHORIZATION DESIGN CONCEPTS.

- ✓ Authentication methods
  - Directory services
  - Federation
  - Attestation
  - Technologies

        - Time-based one-time password (TOTP)
        - HMAC-based one-time password (HOTP)
        - Short message service (SMS)
        - Token key
        - Static codes
        - Authentication applications
        - Push notifications
        - Phone call
    - Smart card authentication
- ✓ Biometrics
    - Fingerprint
    - Retina
    - Iris
    - Facial
    - Voice
    - Vein
    - Gait analysis
    - Efficacy rates
    - False acceptance
    - False rejection
    - Crossover error rate
- ✓ Multifactor authentication (MFA) factors and attributes
    - Factors
        - Something you know
        - Something you have
        - Something you are
    - Attributes
        - Somewhere you are
        - Something you can do
        - Something you exhibit
        - Someone you know
- ✓ Authentication, authorization, and accounting (AAA)
- ✓ Cloud vs. on-premises requirements

MODULE 5 - GIVEN A SCENARIO, IMPLEMENT CYBERSECURITY RESILIENCE

- ✓ Redundancy
    - Geographic dispersal
    - Disk
        - Redundant array of inexpensive disks (RAID) levels
        - Multipath
- ✓ Network
    - Load balancers
    - Network interface card (NIC) teaming
- ✓ Power
    - Uninterruptible power supply (UPS)

- Generator
- Dual supply
- Managed power distribution units (PDUs)

✓ Replication
- Storage area network
- VM

✓ On-premises vs. cloud

✓ Backup types
- Full
- Incremental
- Snapshot
- Differential
- Tape
- Disk
- Copy
- Network-attached storage (NAS)
- Storage area network
- Cloud
- Image
- Online vs. offline
- Offsite storage
  - Distance considerations

✓ Non-persistence
- Revert to known state
- Last known-good configuration
- Live boot media

✓ High availability
- Scalability

✓ Restoration order

✓ Diversity
- Technologies
- Vendors
- Crypto
- Controls

MODULE 6 - EXPLAIN THE SECURITY IMPLICATIONS OF EMBEDDED AND SPECIALIZED SYSTEMS

✓ Embedded systems
- Raspberry Pi
- Field-programmable gate array (FPGA)
- Arduino

✓ Supervisory control and data acquisition / (SCADA)/industrial control system (ICS)
- Facilities
- Industrial
- Manufacturing
- Energy
- Logistics

- ✓ Internet of Things (IoT)
  - Sensors
  - Smart devices
  - Wearables
  - Facility automation
  - Weak defaults
- ✓ Specialized
  - Medical systems
  - Vehicles
  - Aircraft
  - Smart meters
- ✓ Voice over IP (VoIP)
- ✓ Heating, ventilation, air conditioning (HVAC)
- ✓ Drones
- ✓ Multifunction printer (MFP)
- ✓ Real-time operating system (RTOS)
- ✓ Surveillance systems
- ✓ System on chip (SoC)
- ✓ Communication considerations
  - 5G
  - Narrow-band
  - Baseband radio
  - Subscriber identity module (SIM) cards
  - Zigbee
- ✓ Constraints
  - Power
  - Compute
  - Network
  - Crypto
  - Inability to patch
  - Authentication
  - Range
  - Cost
  - Implied trust

MODULE 7 - EXPLAIN THE IMPORTANCE OF PHYSICAL SECURITY CONTROLS

- ✓ Bollards/barricades
- ✓ Access control vestibules
- ✓ Badges
- ✓ Alarms
- ✓ Signage
- ✓ Cameras
  - Motion recognition
  - Object detection
- ✓ Closed-circuit television (CCTV)
- ✓ Industrial camouflage

- ✓ Personnel
  - Guards
  - Robot sentries
  - Reception
  - Two-person integrity/control
- ✓ Locks
  - Biometrics
  - Electronic
  - Physical
  - Cable locks
- ✓ USB data blocker
- ✓ Lighting
- ✓ Fencing
- ✓ Fire suppression
- ✓ Sensors
  - Motion detection
  - Noise detection
  - Proximity reader
  - Moisture detection
  - Cards
  - Temperature
- ✓ Drones
- ✓ Visitor logs
- ✓ Faraday cages
- ✓ Air gap
- ✓ Screened subnet (DMZ)
- ✓ Protected cable distribution
- ✓ Secure areas
  - Air gap
  - Vault
  - Safe
  - Hot aisle
  - Cold aisle
- ✓ Secure data destruction
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Third-party solutions

MODULE 8 - SUMMARIZE THE BASICS OF CRYPTOGRAPHIC CONCEPTS

- ✓ Digital signatures
- ✓ Key length
- ✓ Key stretching
- ✓ Salting
- ✓ Hashing

- ✓ Key exchange
- ✓ Elliptic-curve cryptography
- ✓ Perfect forward secrecy
- ✓ Quantum
  - Communications
  - Computing
- ✓ Post-quantum
- ✓ Ephemeral
- ✓ Modes of operation
  - Authenticated
  - Unauthenticated
  - Counter
- ✓ Blockchain
  - Public ledgers
- ✓ Cipher suites
  - Stream
  - Block
- ✓ Symmetric vs. asymmetric
- ✓ Lightweight cryptography
- ✓ Steganography
  - Audio
  - Video
  - Image
- ✓ Homomorphic encryption
- ✓ Common use cases
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation
- ✓ Limitations
  - Speed
  - Size
  - Weak keys
  - Time
  - Longevity
  - Predictability
  - Reuse
  - Entropy
  - Computational overheads
  - Resource vs. security constraints

UNIT 3 - IMPLEMENTATION

MODULE 1 - GIVEN A SCENARIO, IMPLEMENT SECURE PROTOCOLS

- ✓ Protocols
  - Domain Name System Security Extensions (DNSSEC)
  - SSH
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Real-time Transport / Protocol (SRTP)
  - Lightweight Directory Access Protocol Over SSL (LDAPS)
  - File Transfer Protocol, Secure (FTPS)
  - SSH File Transfer Protocol (SFTP)
  - Simple Network Management / Protocol, version 3 (SNMPv3)
  - Hypertext transfer protocol over SSL/TLS (HTTPS)
  - IPSec
    - Authentication header (AH)
    - Encapsulating Security Payloads (ESP)
    - Tunnel/transport
  - Post Office Protocol (POP)/Internet Message Access Protocol (IMAP)
- ✓ Use cases
  - Voice and video
  - Time synchronization
  - Email and web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services

MODULE 2 - GIVEN A SCENARIO, IMPLEMENT HOST OR APPLICATION SECURITY SOLUTIONS

- ✓ Endpoint protection
  - Antivirus
  - Anti-malware
  - Endpoint detection and response (EDR)
  - DLP
  - Next-generation firewall (NGFW)
  - Host-based intrusion prevention system (HIPS)
  - Host-based intrusion detection system (HIDS)
  - Host-based firewall
- ✓ Boot integrity
  - Boot security/Unified Extensible Firmware Interface (UEFI)
  - Measured boot
  - Boot attestation
- ✓ Database
  - Tokenization
  - Salting

- Hashing

✓ Application security
- Input validations
- Secure cookies
- Hypertext Transfer Protocol (HTTP) headers
- Code signing
- Allow list
- Block list/deny list
- Secure coding practices
- Static code analysis
  - Manual code review
- Dynamic code analysis
- Fuzzing

✓ Hardening
- Open ports and services
- Registry
- Disk encryption
- OS
- Patch management
  - Third-party updates
  - Auto-update

✓ Self-encrypting drive (SED)/full-disk encryption (FDE)
- Opal

✓ Hardware root of trust

✓ Trusted Platform Module (TPM)

✓ Sandboxing

MODULE 3 - GIVEN A SCENARIO, IMPLEMENT SECURE NETWORK DESIGNS

✓ Load balancing
- Active/active
- Active/passive
- Scheduling
- Virtual IP
- Persistence

✓ Network segmentation
- Virtual local area network (VLAN)
- Screened subnet (previously known as demilitarized zone)
- East-west traffic
- Extranet
- Intranet
- Zero Trust

✓ Virtual private network (VPN)
- Always-on
- Split tunnel vs. full tunnel
- Remote access vs. site-to-site
- IPSec
- SSL/TLS

- HTML5
- Layer 2 tunneling protocol (L2TP)

✓ DNS
✓ Network access control (NAC)
- Agent and agentless

✓ Out-of-band management
✓ Port security
- Broadcast storm prevention
- Bridge Protocol Data Unit (BPDU) guard
- Loop prevention
- Dynamic Host Configuration Protocol (DHCP) snooping
- Media access control (MAC) filtering

✓ Network appliances
- Jump servers
- Proxy servers
  - Forward
  - Reverse
- Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS)
  - Signature-based
  - Heuristic/behavior
  - Anomaly
  - Inline vs. passive
- HSM
- Sensors
- Collectors
- Aggregators
- Firewalls
  - Web application firewall (WAF)
  - NGFW
  - Stateful
  - Stateless
  - Unified threat management (UTM)
  - Network address translation (NAT) gateway
  - Content/URL filter
  - Open-source vs. proprietary
  - Hardware vs. software
  - Appliance vs. host-based vs. virtual
- Access control list (ACL)
- Route security
- Quality of service (QoS)
- Implications of IPv6
- Port spanning/port mirroring/Port taps
- Monitoring services
- File integrity monitors

MODULE 4 - GIVEN A SCENARIO, INSTALL AND CONFIGURE WIRELESS SECURITY SETTINGS

- ✓ Cryptographic protocols
  - WiFi Protected Access 2 (WPA2)
  - WiFi Protected Access 3 (WPA3)
  - Counter-mode/CBC-MAC Protocol (CCMP)
  - Simultaneous Authentication of Equals (SAE)
- ✓ Authentication protocols
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Authentication Protocol (PEAP)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1X
- ✓ Remote Authentication Dial-in User Service (RADIUS) Federation
- ✓ Methods
  - Pre-shared key (PSK) vs. Enterprise vs. Open
  - WiFi Protected Setup (WPS)
  - Captive portals
- ✓ Installation considerations
  - Site surveys
  - Heat maps
  - WiFi analyzers
  - Channel overlaps
  - Wireless access point (WAP) placement
  - Controller and access point security

MODULE 5 - GIVEN A SCENARIO, IMPLEMENT SECURE MOBILE SOLUTIONS.

- ✓ Connection methods and receivers
  - Cellular
  - WiFi
  - Bluetooth
  - NFC
  - Infrared
  - USB
  - Point-to-point
  - Point-to-multipoint
  - Global Positioning System (GPS)
  - RFID
- ✓ Mobile device management (MDM)
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notifications
  - Passwords and PINs
  - Biometrics

- Context-aware authentication
- Containerization
- Storage segmentation
- Full device encryption

✓ Mobile devices
- MicroSD hardware security module (HSM)
- MDM/Unified Endpoint Management (UEM)
- Mobile application management (MAM)
- SEAndroid

✓ Enforcement and monitoring of:
- Third-party application stores
- Rooting/jailbreaking
- Sideloading
- Custom firmware
- Carrier unlocking
- Firmware over-the-air (OTA) updates
- Camera use
- SMS/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS)
- External media
- USB On-The-Go (USB OTG)
- Recording microphone
- GPS tagging
- WiFi direct/ad hoc
- Tethering
- Hotspot
- Payment methods

✓ Deployment models
- Bring your own device (BYOD)
- Corporate-owned personally enabled (COPE)
- Choose your own device (CYOD)
- Corporate-owned
- Virtual desktop infrastructure (VDI)

MODULE 6 - GIVEN A SCENARIO, APPLY CYBERSECURITY SOLUTIONS TO THE CLOUD.

✓ Cloud security controls
- High availability across zones
- Resource policies
- Secrets management
- Integration and auditing
- Storage
  - Permissions
  - Encryption
  - Replication
  - High availability
- Network
  - Virtual networks
  - Public and private subnets

        - Segmentation
        - API inspection and integration
    - Compute
        - Security groups
        - Dynamic resource allocation
        - Instance awareness
        - Virtual private cloud (VPC) endpoint
        - Container security
- ✓ Solutions
    - CASB
    - Application security
    - Next-generation secure web gateway (SWG)
    - Firewall considerations in a cloud environment
        - Cost
        - Need for segmentation
        - Open Systems Interconnection (OSI) layers
- ✓ Cloud native controls vs. third-party solutions

MODULE 7 - GIVEN A SCENARIO, IMPLEMENT IDENTITY AND ACCOUNT MANAGEMENT CONTROLS

- ✓ Identity
    - Identity provider (IdP)
    - Attributes
    - Certificates
    - Tokens
    - SSH keys
    - Smart cards
- ✓ Account types
    - User account
    - Shared and generic accounts/credentials
    - Guest accounts
    - Service accounts
- ✓ Account policies
    - Password complexity
    - Password history
    - Password reuse
    - Network location
    - Geofencing
    - Geotagging
    - Geolocation
    - Time-based logins
    - Access policies
    - Account permissions
    - Account audits
    - Impossible travel time/risky login
    - Lockout
    - Disablement

MODULE 8 – GIVEN A SCENARIO, IMPLEMENT AUTHENTICATION AND AUTHORIZATION SOLUTIONS

- ✓ Authentication management
  - Password keys
  - Password vaults
  - TPM
  - HSM
  - Knowledge-based authentication
- ✓ Authentication/authorization
  - EAP
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
  - 802.1X
  - RADIUS
  - Single sign-on (SSO)
  - Security Assertion Markup Language (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - Kerberos
- ✓ Access control schemes
  - Attribute-based access control (ABAC)
  - Role-based access control
  - Rule-based access control
  - MAC
  - Discretionary access control (DAC)
  - Conditional access
  - Privileged access management
  - Filesystem permissions

MODULE 9 - GIVEN A SCENARIO, IMPLEMENT PUBLIC KEY INFRASTRUCTURE

- ✓ Public key infrastructure (PKI)
  - Key management
  - Certificate authority (CA)
  - Intermediate CA
  - Registration authority (RA)
  - Certificate revocation list (CRL)
  - Certificate attributes
  - Online Certificate Status Protocol (OCSP)
  - Certificate signing request (CSR)
  - CN
  - Subject alternative name
  - Expiration
- ✓ Types of certificates
  - Wildcard

- Subject alternative name
- Code signing
- Self-signed
- Machine/computer
- Email
- User
- Root
- Domain validation
- Extended validation

✓ Certificate formats
- Distinguished encoding rules (DER)
- Privacy enhanced mail (PEM)
- Personal information exchange (PFX)
- .cer
- P12
- P7B

✓ Concepts
- Online vs. offline CA
- Stapling
- Pinning
- Trust model
- Key escrow
- Certificate chaining

UNIT 4 - OPERATIONS AND INCIDENT RESPONSE

MODULE 1 - GIVEN A SCENARIO, USE THE APPROPRIATE TOOL TO ASSESS ORGANIZATIONAL SECURITY

✓ Network reconnaissance and discovery
- tracert/traceroute
- nslookup/dig
- ipconfig/ifconfig
- nmap
- ping/pathping
- hping
- netstat
- netcat
- IP scanners
- arp
- route
- curl
- theHarvester & similar
- sn1per & similar
- scanless & similar
- dnsenum & similar
- Nessus & similar
- Cuckoo & similar

- ✓ File manipulation
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger
- ✓ Shell and script environments
  - SSH
  - PowerShell
  - Python
  - OpenSSL
- ✓ Packet capture and replay
  - Tcpreplay
  - Tcpdump
  - Wireshark
- ✓ Forensics
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy
- ✓ Exploitation frameworks
- ✓ Password crackers
- ✓ Data sanitization

MODULE 2 - SUMMARIZE THE IMPORTANCE OF POLICIES, PROCESSES, AND PROCEDURES FOR INCIDENT RESPONSE

- ✓ Incident response plans
- ✓ Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- ✓ Exercises
  - Tabletop
  - Walkthroughs
  - Simulations
- ✓ Attack frameworks
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Cyber Kill Chain
- ✓ Stakeholder management
- ✓ Communication plan
- ✓ Disaster recovery plan

- ✓ Business continuity plan
- ✓ Continuity of operations planning (COOP)
- ✓ Incident response team
- ✓ Retention policies

MODULE 3 - GIVEN AN INCIDENT, UTILIZE APPROPRIATE DATA SOURCES TO SUPPORT AN INVESTIGATION

- ✓ Vulnerability scan output
- ✓ SIEM dashboards
  - Sensor
  - Sensitivity
  - Trends
  - Alerts
  - Correlation
- ✓ Log files
  - Network
  - System
  - Application
  - Security
  - Web
  - DNS
  - Authentication
  - Dump files
  - VoIP and call managers
  - Session Initiation Protocol (SIP) traffic
- ✓ Syslog/rsyslog/syslog-ng
- ✓ Journalctl
- ✓ NXLog
- ✓ Bandwidth monitors
- ✓ Metadata
  - Email
  - Mobile
  - Web
  - File
- ✓ Netflow/sFlow
  - Netflow
  - sFlow
  - IPFIX
- ✓ Protocol analyzer output

MODULE 4 - GIVEN AN INCIDENT, APPLY MITIGATION TECHNIQUES OR CONTROLS TO SECURE AN ENVIRONMENT

- ✓ Reconfigure endpoint security solutions
  - Application approved list
  - Application blocklist/deny list
  - Quarantine
- ✓ Configuration changes

- Firewall rules
- MDM
- DLP
- Content filter/URL filter
- Update or revoke certificates

✓ Isolation
✓ Containment
✓ Segmentation
✓ SOAR
- Runbooks
- Playbooks

MODULE 5 - EXPLAIN THE KEY ASPECTS OF DIGITAL FORENSICS

✓ Documentation/evidence
- Legal hold
- Video
- Admissibility
- Chain of custody
- Timelines of sequence of events
  - Time stamps
  - Time offset
- Tags
- Reports
- Event logs
- Interviews

✓ Acquisition
- Order of volatility
- Disk
- Random-access memory (RAM)
- Swap/pagefile
- OS
- Device
- Firmware
- Snapshot
- Cache
- Network
- Artifacts

✓ On-premises vs. cloud
- Right-to-audit clauses
- Regulatory/jurisdiction
- Data breach notification laws

✓ Integrity
- Hashing
- Checksums
- Provenance

- ✓ Preservation
- ✓ E-discovery
- ✓ Data recovery
- ✓ Non-repudiation
- ✓ Strategic intelligence / counterintelligence

UNIT 5 - GOVERNANCE, RISK, AND COMPLIANCE

MODULE 1 - COMPARE AND CONTRAST VARIOUS TYPES OF CONTROLS

- ✓ Category
  - Managerial
  - Operational
  - Technical
- ✓ Control type
  - Preventive
  - Detective
  - Corrective
  - Deterrent
  - Compensating
  - Physical

MODULE 2 - EXPLAIN THE IMPORTANCE OF APPLICABLE REGULATIONS, STANDARDS, OR FRAMEWORKS THAT IMPACT ORGANIZATIONAL SECURITY POSTURE

- ✓ Regulations, standards, and legislation
  - General Data Protection Regulation (GDPR)
  - National, territory, or state laws
  - Payment Card Industry Data Security Standard (PCI DSS)
- ✓ Key frameworks
  - Center for Internet Security (CIS)
  - National Institute of Standards and Technology (NIST) Risk
  - Management Framework (RMF)
  - Cybersecurity Framework (CSF)
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - Cloud security alliance
  - Cloud control matrix
  - Reference architecture
- ✓ Benchmarks /secure Configuration guides
  - Platform/vendor-specific guides
    - Web server
    - OS
    - Application server
    - Network infrastructure devices

MODULE 3 - EXPLAIN THE IMPORTANCE OF POLICIES TO ORGANIZATIONAL SECURITY

- ✓ Personnel
  - Acceptable use policy
  - Job rotation
  - Mandatory vacation
  - Separation of duties
  - Least privilege
  - Clean desk space
  - Background checks
  - Non-disclosure agreement (NDA)
  - Social media analysis
  - Onboarding
  - Offboarding
  - User training
    - Gamification
    - Capture the flag
    - Phishing campaigns
    - Phishing simulations
    - Computer-based training (CBT)
    - Role-based training
- ✓ Diversity of training techniques
- ✓ Third-party risk management
  - Vendors
  - Supply chain
  - Business partners
  - Service level agreement (SLA)
  - Memorandum of understanding (MOU)
  - Measurement systems analysis (MSA)
  - Business partnership agreement (BPA)
  - End of life (EOL)
  - End of service life (EOSL)
  - NDA
- ✓ Data
  - Classification
  - Governance
  - Retention
- ✓ Credential policies
  - Personnel
  - Third-party
  - Devices
  - Service accounts
  - Administrator/root accounts
- ✓ Organizational policies
  - Change management
  - Change control
  - Asset management

MODULE 4 - SUMMARIZE RISK MANAGEMENT PROCESSES AND CONCEPTS

- ✓ Risk types
  - External
  - Internal
  - Legacy systems
  - Multiparty
  - IP theft
  - Software compliance/licensing
- ✓ Risk management strategies
  - Acceptance
  - Avoidance
  - Transference
    - Cybersecurity insurance
  - Mitigation
- ✓ Risk analysis
  - Risk register
  - Risk matrix/heat map
  - Risk control assessment
  - Risk control self-assessment
  - Risk awareness
  - Inherent risk
  - Residual risk
  - Control risk
  - Risk appetite
  - Regulations that affect risk posture
  - Risk assessment types
    - Qualitative
    - Quantitative
  - Likelihood of occurrence
  - Impact
  - Asset value
  - Single-loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
- ✓ Disasters
  - Environmental
  - Person-made
  - Internal vs. external
- ✓ Business impact analysis
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Functional recovery plans
  - Single point of failure
  - Disaster recovery plan (DRP)
  - Mission essential functions

- Identification of critical systems
- Site risk assessment

MODULE 5 - EXPLAIN PRIVACY AND SENSITIVE DATA CONCEPTS IN RELATION TO SECURITY

- ✓ Organizational consequences of privacy and data breaches
  - Reputation damage
  - Identity theft
  - Fines
  - IP theft
- ✓ Notifications of breaches
  - Escalation
  - Public notifications and disclosures
- ✓ Data types
  - Classifications
    - Public
    - Private
    - Sensitive
    - Confidential
    - Critical
    - Proprietary
    - Personally identifiable information (PII)
    - Health information
    - Financial information
    - Government data
    - Customer data
- ✓ Privacy enhancing technologies
  - Data minimization
  - Data masking
  - Tokenization
  - Anonymization
  - Pseudo-anonymization
- ✓ Roles and responsibilities
  - Data owners
  - Data controller
  - Data processor
  - Data custodian/steward
  - Data protection officer (DPO)
- ✓ Information life cycle
- ✓ Impact assessment
- ✓ Terms of agreement
- ✓ Privacy notice

MODULO ETHICAL HACKER PER LA CERTIFICAZIONE COMPTIA PENTEST+

UNIT 1 – PLANNING AND SCOPING

MODULE 1 – COMPARE AND CONTRAST GOVERNANCE, RISK, AND COMPLIANCE CONCEPTS.

- Regulatory compliance considerations
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
- Location restrictions
  - Country limitations
  - Tool restrictions
  - Local laws
  - Local government requirements
  - Privacy requirements
- Legal concepts
  - Service-level agreement (SLA)
  - Confidentiality
  - Statement of work
  - Non-disclosure agreement (NDA)
  - Master service agreement
- Permission to attack

MODULE 2 – EXPLAIN THE IMPORTANCE OF SCOPING AND ORGANIZATIONAL/CUSTOMER REQUIREMENTS.

- Standards and methodologies
  - MITRE ATT&CK
  - Open Web Application Security Project (OWASP)
  - National Institute of Standards and Technology (NIST)
  - Open-source Security Testing Methodology Manual (OSSTMM)
  - Penetration Testing Execution Standard (PTES)
  - Information Systems Security Assessment Framework (ISSAF)
- Rules of engagement
  - Time of day
  - Types of allowed/disallowed tests
  - Other restrictions
- Environmental considerations
  - Network
  - Application
  - Cloud
- Target list/in-scope assets
  - Wireless networks
  - Internet Protocol (IP) ranges
  - Domains
  - Application programming interfaces (APIs)
  - Physical locations
  - Domain name system (DNS)

- External vs. internal targets
- First-party vs. third-party hosted

- Validate scope of engagement
  - Question the client/review contracts
  - Time management
  - Strategy
  - Unknown-environment vs. known-environment testing

MODULE 3 – GIVEN A SCENARIO, DEMONSTRATE AN ETHICAL HACKING MINDSET BY MAINTAINING PROFESSIONALISM AND INTEGRITY.

- Background checks of penetration testing team
- Adhere to specific scope of engagement
- Identify criminal activity
- Immediately report breaches/ criminal activity
- Limit the use of tools to a particular engagement
- Limit invasiveness based on scope
- Maintain confidentiality of data/information
- Risks to the professional
  - Fees/fines
  - Criminal charges

UNIT 2 – INFORMATION GATHERING AND VULNERABILITY SCANNING

MODULE 1 – GIVEN A SCENARIO, PERFORM PASSIVE RECONNAISSANCE.

- DNS lookups
- Identify technical contacts
- Administrator contacts
- Cloud vs. self-hosted
- Social media scraping
  - Key contacts/job responsibilities
  - Job listing/technology stack
- Cryptographic flaws
  - Secure Sockets Layer (SSL) certificates
  - Revocation
- Company reputation/security posture
- Data
- Password dumps
- File metadata
- Strategic search engine analysis/enumeration
  - Website archive/caching
  - Public source-code repositories
- Open-source intelligence (OSINT)
  - Tools
    - Shodan
    - Recon-ng
  - Sources
    - Common weakness enumeration (CWE)
    - Common vulnerabilities and exposures (CVE)

MODULE 2 – GIVEN A SCENARIO, PERFORM ACTIVE RECONNAISSANCE.

- Enumeration
  - Hosts
  - Services
  - Domains
  - Users
  - Uniform resource locators (URLs)
- Website reconnaissance
  - Crawling websites
  - Scraping websites
  - Manual inspection of web links
    - robots.txt
- Packet crafting
  - Scapy
- Defense detection
  - Load balancer detection
  - Web application firewall (WAF) detection
  - Antivirus
  - Firewall
- Tokens
  - Scoping
  - Issuing
  - Revocation
- Wardriving
- Network traffic
  - Capture API requests and responses
  - Sniffing
- Cloud asset discovery
- Third-party hosted services
- Detection avoidance

MODULE 3 – GIVEN A SCENARIO, ANALYZE THE RESULTS OF A RECONNAISSANCE EXERCISE.

- Fingerprinting
  - Operating systems (OSs)
  - Networks
  - Network devices
  - Software
- Analyze output from:
  - DNS lookups
  - Crawling websites
  - Network traffic
  - Address Resolution Protocol (ARP) traffic
  - Nmap scans
  - Web logs

MODULE 4 – GIVEN A SCENARIO, PERFORM VULNERABILITY SCANNING.

- Considerations of vulnerability scanning
  - Time to run scans
  - Protocols

  - Network topology
  - Bandwidth limitations
  - Query throttling
  - Fragile systems
  - Non-traditional assets
- Scan identified targets for vulnerabilities
- Set scan settings to avoid detection
- Scanning methods
  - Stealth scan
  - Transmission Control Protocol (TCP) connect scan
  - Credentialed vs. non-credentialed
- Nmap
  - Nmap Scripting Engine (NSE) scripts
  - Common options
    - A
    - sV
    - sT
    - Pn
    - O
    - sU
    - sS
    - T 1-5
    - script=vuln
    - p
- Vulnerability testing tools that facilitate automation

UNIT 3 – ATTACKS AND EXPLOITS

MODULE 1 – GIVEN A SCENARIO, RESEARCH ATTACK VECTORS AND PERFORM NETWORK ATTACKS.

- Stress testing for availability
- Exploit resources
  - Exploit database (DB)
  - Packet storm
- Attacks
  - ARP poisoning
  - Exploit chaining
  - Password attacks
    - Password spraying
    - Hash cracking
    - Brute force
    - Dictionary
  - On-path (previously known as man-in-the-middle)
  - Kerberoasting
  - DNS cache poisoning
  - Virtual local area network (VLAN) hopping
  - Network access control (NAC) bypass
  - Media access control (MAC) spoofing
  - Link-Local Multicast Name Resolution (LLMNR)/NetBIOS- Name Service (NBT-NS) poisoning

- New Technology LAN Manager (NTLM) relay attacks
- Tools
  - Metasploit
  - Netcat
  - Nmap

MODULE 2 – GIVEN A SCENARIO, RESEARCH ATTACK VECTORS AND PERFORM WIRELESS ATTACKS.

- Attack methods
  - Eavesdropping
  - Data modification
  - Data corruption
  - Relay attacks
  - Spoofing
  - Deauthentication
  - Jamming
  - Capture handshakes
  - On-path
- Attacks
  - Evil twin
  - Captive portal
  - Bluejacking
  - Bluesnarfing
  - Radio-frequency identification (RFID) cloning
  - Bluetooth Low Energy (BLE) attack
  - Amplification attacks [Near-field communication (NFC)]
  - WiFi protected setup (WPS) PIN attack
- Tools
  - Aircrack-ng suite
  - Amplified antenna

MODULE 3 – GIVEN A SCENARIO, RESEARCH ATTACK VECTORS AND PERFORM APPLICATION-BASED ATTACKS.

- OWASP Top 10
- Server-side request forgery
- Business logic flaws
- Injection attacks
  - Structured Query Language (SQL) injection
    - Blind SQL
    - Boolean SQL
    - Stacked queries
  - Command injection
  - Cross-site scripting
    - Persistent
    - Reflected
  - Lightweight Directory Access Protocol (LDAP) injection
- Application vulnerabilities
  - Race conditions
  - Lack of error handling

- Lack of code signing
- Insecure data transmission
- Session attacks
  - Session hijacking
  - Cross-site request forgery (CSRF)
  - Privilege escalation
  - Session replay
  - Session fixation
- API attacks
  - Restful
  - Extensible Markup Language- Remote Procedure Call (XML-RPC)
  - Soap
- Directory traversal
- Tools
  - Web proxies
    - OWASP Zed Attack Proxy (ZAP)
    - Burp Suite community edition
  - SQLmap
  - DirBuster
- Resources
  - Word lists

MODULE 4 – GIVEN A SCENARIO, RESEARCH ATTACK VECTORS AND PERFORM ATTACKS ON CLOUD TECHNOLOGIES.

- Attacks
  - Credential harvesting
  - Privilege escalation
  - Account takeover
  - Metadata service attack
  - Misconfigured cloud assets
    - Identity and access management (IAM)
    - Federation misconfigurations
    - Object storage
    - Containerization technologies
  - Resource exhaustion
  - Cloud malware injection attacks
  - Denial-of-service attacks
  - Side-channel attacks
  - Direct-to-origin attacks
- Tools
  - Software development kit (SDK)

MODULE 5 – EXPLAIN COMMON ATTACKS AND VULNERABILITIES AGAINST SPECIALIZED SYSTEMS.

- Mobile
  - Attacks
    - Reverse engineering
    - Sandbox analysis
    - Spamming

- Vulnerabilities
  - Insecure storage
  - Passcode vulnerabilities
  - Certificate pinning
  - Using known vulnerable components (i) Dependency vulnerabilities (ii) Patching fragmentation
  - Execution of activities using root
  - Over-reach of permissions
  - Biometrics integrations
  - Business logic vulnerabilities
- Tools
  - Burp Suite
  - Drozer
  - Mobile Security Framework (MobSF)
  - Postman
  - Ettercap
  - Frida
  - Objection
  - Android SDK tools
  - ApkX
  - APK Studio

- Internet of Things (IoT) devices
  - BLE attacks
  - Special considerations
    - Fragile environment
    - Availability concerns
    - Data corruption
    - Data exfiltration
  - Vulnerabilities
    - Insecure defaults
    - Cleartext communication
    - Hard-coded configurations
    - Outdated firmware/hardware
    - Data leakage
    - Use of insecure or outdated components
- Data storage system vulnerabilities
  - Misconfigurations—on-premises and cloud-based
    - Default/blank username/password
    - Network exposure
  - Lack of user input sanitization
  - Underlying software vulnerabilities
  - Error messages and debug handling
  - Injection vulnerabilities
    - Single quote method
- Management interface vulnerabilities
  - Intelligent platform management interface (IPMI)
- Vulnerabilities related to supervisory control and data acquisition (SCADA)/ Industrial Internet of Things (IIoT)/ industrial control system (ICS)
- Vulnerabilities related to virtual environments
  - Virtual machine (VM) escape

- Hypervisor vulnerabilities
- VM repository vulnerabilities
- Vulnerabilities related to containerized workloads

MODULE 6 – GIVEN A SCENARIO, PERFORM A SOCIAL ENGINEERING OR PHYSICAL ATTACK.

- Pretext for an approach
- Social engineering attacks
  - Email phishing
    - Whaling
    - Spear phishing
  - Vishing
  - Short message service (SMS) phishing
  - Universal Serial Bus (USB) drop key
  - Watering hole attack
- Physical attacks
  - Tailgating
  - Dumpster diving
  - Shoulder surfing
  - Badge cloning
- Impersonation
- Tools
  - Browser exploitation framework (BeEF)
  - Social engineering toolkit
  - Call spoofing tools
- Methods of influence
  - Authority
  - Scarcity
  - Social proof
  - Urgency
  - Likeness
  - Fear

MODULE 7 – GIVEN A SCENARIO, PERFORM POST-EXPLOITATION TECHNIQUES.

- Post-exploitation tools
  - Empire
  - Mimikatz
  - BloodHound
- Lateral movement
  - Pass the hash
- Network segmentation testing
- Privilege escalation
  - Horizontal
  - Vertical
- Upgrading a restrictive shell
- Creating a foothold/persistence
  - Trojan
  - Backdoor
    - Bind shell
    - Reverse shell
  - Daemons

- Scheduled tasks
- Detection avoidance
  - Living-off-the-land techniques/fileless malware
    - PsExec
    - Windows Management Instrumentation (WMI)
    - PowerShell (PS) remoting/Windows Remote Management (WinRM)
  - Data exfiltration
  - Covering your tracks
  - Steganography
  - Establishing a covert channel
- Enumeration
  - Users
  - Groups
  - Forests
  - Sensitive data
  - Unencrypted files

UNIT 4 – REPORTING AND COMMUNICATION

MODULE 1 – COMPARE AND CONTRAST IMPORTANT COMPONENTS OF WRITTEN REPORTS.

- Report audience
  - C-suite
  - Third-party stakeholders
  - Technical staff
  - Developers
- Report contents (** not in a particular order)
  - Executive summary
  - Scope details
  - Methodology
    - Attack narrative
  - Findings
    - Risk rating (reference framework)
    - Risk prioritization
    - Business impact analysis
  - Metrics and measures
  - Remediation
  - Conclusion
  - Appendix
- Storage time for report
- Secure distribution
- Note taking
  - Ongoing documentation during test
  - Screenshots
- Common themes/root causes
  - Vulnerabilities
  - Observations
  - Lack of best practices

MODULE 2 – GIVEN A SCENARIO, ANALYZE THE FINDINGS AND RECOMMEND THE APPROPRIATE REMEDIATION WITHIN A REPORT.

- Technical controls
  - System hardening
  - Sanitize user input/parameterize queries
  - Implemented multifactor authentication
  - Encrypt passwords
  - Process-level remediation
  - Patch management
  - Key rotation
  - Certificate management
  - Secrets management solution
  - Network segmentation
- Administrative controls
  - Role-based access control
  - Secure software development life cycle
  - Minimum password requirements
  - Policies and procedures
- Operational controls
  - Job rotation
  - Time-of-day restrictions
  - Mandatory vacations
  - User training
- Physical controls
  - Access control vestibule
  - Biometric controls
  - Video surveillance

MODULE 3 – EXPLAIN THE IMPORTANCE OF COMMUNICATION DURING THE PENETRATION TESTING PROCESS.

- Communication path
  - Primary contact
  - Technical contact
  - Emergency contact
- Communication triggers
  - Critical findings
  - Status reports
  - Indicators of prior compromise
- Reasons for communication
  - Situational awareness
  - De-escalation
  - Deconfliction
  - Identifying false positives
  - Criminal activity
- Goal reprioritization
- Presentation of findings

MODULE 4 – EXPLAIN POST-REPORT DELIVERY ACTIVITIES.

- Post-engagement cleanup

- Removing shells
- Removing tester-created credentials
- Removing tools

- Client acceptance
- Lessons learned
- Follow-up actions/retest
- Attestation of findings Data destruction process

UNIT 5 – EXPLAIN USE CASES OF THE FOLLOWING TOOLS DURING THE PHASES OF A PENETRATION TEST.

- Scanners
  - Nikto
  - Open vulnerability assessment scanner (Open VAS)
  - SQLmap
  - Nessus
  - Open Security Content Automation Protocol (SCAP)
  - Wapiti
  - WPScan
  - Brakeman
  - Scout Suite
- Credential testing tools
  - Hashcat
  - Medusa
  - Hydra
  - CeWL
  - John the Ripper
  - Cain
  - Mimikatz
  - Patator
  - DirBuster
- Debuggers
  - OllyDbg
  - Immunity Debugger
  - GNU Debugger (GDB)
  - WinDbg
  - Interactive Disassembler (IDA)
  - Covenant
  - SearchSploit
- OSINT
  - WHOIS
  - Nslookup
  - Fingerprinting Organization with Collected Archives (FOCA)
  - theHarvester
  - Shodan
  - Maltego
  - Recon-ng
  - Censys
- Wireless
  - Aircrack-ng suite
  - Kismet

    - Wifite2
    - Rogue access point
    - EAPHammer
    - mdk4
    - Spooftooph
    - Reaver
    - Wireless Geographic Logging Engine (WiGLE)
    - Fern
- Web application tools
    - OWASP ZAP
    - Burp Suite
    - Gobuster
    - w3af
- Social engineering tools
    - Social Engineering Toolkit (SET)
    - BeEF
- Remote access tools
    - Secure Shell (SSH)
    - Ncat
    - Netcat
    - ProxyChains
- Networking tools
    - Wireshark
    - Hping
- Misc.
    - SearchSploit
    - Responder
    - Impacket tools
    - Empire
    - Metasploit
    - mitm6
    - CrackMapExec
    - TruffleHog
    - Censys
- Steganography tools
    - Openstego
    - Steghide
    - Snow
    - Coagula
    - Sonic Visualiser
    - TinEye
- Cloud tools
    - Scout Suite
    - CloudBrute
    - Pacu
    - Cloud Custodian

LABORATORI PRATICI COMPTIA SECURITY PLUS

01: Exploring the Lab Environment

02: Scanning and Identifying Network Nodes

03: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools

04: Analyzing the Results of a Credentialed Vulnerability Scan

05: Installing, Using, and Blocking a Malware-based Backdoor

06: Performing Network Reconnaissance and Vulnerability Scanning

07: Managing the Life Cycle of a Certificate

08: Managing Certificates with OpenSSL

09: Auditing Passwords with a Password Cracking Utility

10: Managing Centralized Authentication

11: Managing Access Controls in Windows Server

12: Configuring a System for Auditing Policies

13: Managing Access Controls in Linux

14: Configuring Identity and Access Management Controls

15: Implementing a Secure Network Design

16: Configuring a Firewall

17: Configuring an Intrusion Detection System

18: Implementing Secure Network Addressing Services

19: Implementing a Virtual Private Network

20: Implementing a Secure SSH Server

21: Implementing Endpoint Protection

22: Securing the Network Infrastructure

23: Identifying Application Attack Indicators

24: Identifying a Browser Attack

25: Implementing PowerShell Security

26: Identifying Malicious Code

27: Identifying Application Attacks

28: Managing Data Sources for Incident Response

29: Configuring Mitigation Controls

30: Acquiring Digital Forensics Evidence

31: Backing Up and Restoring Data in Windows and Linux

32: Managing Incident Response, Mitigation and Recovery

- 25 ore totali di laboratori
- Per ogni laboratorio è fornito un tutorial scritto e illustrato su come svolgere il laboratorio passo dopo passo
- La piattaforma dei laboratori è in CLOUD

La durata di ogni singolo laboratorio varia tra i 20 ed i 60 minuti

LABORATORI PRATICI COMPTIA PENTEST PLUS

01: Exploring the Lab Environment

02: Exploring the Domain Tools: Nslookup, Dig, and Whois

03: Navigating Open-Source Intelligence Tools

04: Understanding Social Engineering Toolkit (SET)

05: Understanding Spear Phishing and Credentials Attack

06: Exploring OpenVAS

07: Using Web Scanners

08: Understanding Nmap Common Usage

09: Scanning a Vulnerable System

10: Understanding Scan Output

11: Navigating Steganography Tools

12: Demonstrating Enumeration Techniques

13: Exploring the Basics of Metasploit

14: Using VSFTP Manual and Metasploit

15: Monitoring with Aircrack-ng

16: Discovering IoT devices with Shodan

17: Using SQL Injection

18: Using Reverse and Bind Shells

19: Analyzing Exploit Code

20: Exploring Programming Shells

21: Applying PenTest Automation

22: Exploring Password Attacks with John the Ripper and Hydra

- 12 ore 30 minuti di laboratori
- Per ogni laboratorio è fornito un tutorial scritto e illustrato su come svolgere il laboratorio passo dopo passo
- La piattaforma dei laboratori è in CLOUD
- La durata di ogni singolo laboratorio varia tra i 30 ed i 60 minuti