Corso
Penetration Test e Hacking Etico
+ Laboratori Pratici CompTIA

IN-FORMAZIONE SRL - Via Riccardo Grazioli Lante, 9 - 00195 Roma
P.IVA 07252070722 - Tel. : 0687153208 - info@musaformazione.it

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 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