🛡️ Dispense Master: Cyber Security & Ethical Hacking - Introduzione e Fondamenti

Introduzione al Corso e Struttura Didattica

1. 📖 Spiegazione Approfondita

Il corso è strutturato per formare professionisti operativi nel campo della sicurezza informatica, con un focus specifico sull'Ethical Hacking. L'obiettivo primario non è solo teorico, ma mira a fornire competenze tecniche avanzate per contrastare il crimine informatico (cybercrime) all'interno di contesti aziendali.

Il percorso didattico si articola in tre macro-unità (Unit) progressive:

- **Unit 1: Fondamenti di Ethical Hacking.** Questa fase è propedeutica e copre i prerequisiti teorici e tecnici essenziali. Gli argomenti trattati includono l'architettura delle reti, i sistemi operativi (con focus su Linux), la crittografia, il funzionamento dei firewall e gli elementi base di programmazione. È la "cassetta degli attrezzi" necessaria per operare.
- **Unit 2: Penetration Testing.** È il cuore operativo del corso. Si focalizza sulla simulazione di attacchi reali seguendo metodologie standardizzate. Gli studenti impareranno a identificare vulnerabilità, utilizzare strumenti di testing offensivo, applicare tecniche di hacking pratico e comprendere concetti moderni come l'Ingegneria Sociale e l'uso dell'Intelligenza Artificiale nel hacking.
- **Unit 3: Monitoraggio e Gestione degli Eventi (Blue Teaming).** Dopo aver imparato ad attaccare, si impara a difendere. Questa unità copre il monitoraggio degli eventi di sicurezza, la gestione degli incidenti in corso (Incident Response), l'adozione di best practices enterprise per la business continuity, la gestione di Windows Server e un'introduzione alla Malware Analysis.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** L'**Ethical Hacking** è la pratica di utilizzare competenze tecniche e strumenti di attacco con l'obiettivo legittimo di individuare e sanare vulnerabilità di sicurezza, prevenendo lo sfruttamento da parte di attori malevoli.
- **Contesto Reale:** Le aziende assumono Ethical Hacker non per "distruggere", ma per anticipare le mosse dei criminali, blindando le infrastrutture prima che avvenga un data breach.

Storia ed Evoluzione della Figura dell'Hacker

1. 📖 Spiegazione Approfondita

La percezione e il ruolo dell'hacker sono mutati drasticamente dagli anni '50 ad oggi.

- **Anni '50 e '60 (Le Origini - MIT):** Il termine nasce al MIT (Massachusetts Institute of Technology), specificamente nel *Tech Model Railroad Club* (TMRC). In origine, "hackerare" significava trovare soluzioni ingegnose e non convenzionali a problemi tecnici complessi (inizialmente legati al modellismo ferroviario, poi ai primi mainframe). Non aveva connotazione criminale, ma indicava pura curiosità intellettuale.

- **Anni '70 (Cultura Unix e ARPANET):** Con la nascita di Unix (Bell Labs) e ARPANET (precursore di Internet), gli hacker iniziano a esplorare le reti. In California nasce l'*Homebrew Computer Club* (con figure come Steve Jobs e Wozniak), dove l'hacking si fonde con la rivoluzione dei Personal Computer.
- **Anni '80 (Fenomeno Sociale e Criminalizzazione):** L'hacking entra nella cultura di massa, spesso con accezione negativa. Il caso emblematico è quello di **Kevin Mitnick**, noto per le intrusioni in grandi aziende ed enti governativi, che ha contribuito a cristallizzare l'immagine dell'hacker come criminale informatico nei media.
- **Anni 2000 e Oltre (Hacktivismo e Cyberwarfare):** Eventi come le rivelazioni di **Edward Snowden** (2013) sulla sorveglianza di massa (NSA) hanno spostato il dibattito su privacy e diritti civili. Oggi la figura si è professionalizzata: da "pirata" a "difensore" (White Hat), essenziale per la sicurezza nazionale e aziendale.

5. ⚠ Focus Esame

- **Trabocchetto:** Non confondere l'origine del termine con l'accezione odierna. L'hacking nasce come *problem solving creativo*, non come attività criminale.

Classificazione degli Hacker: I Colori (Hats)

1. 📖 Spiegazione Approfondita

Per classificare gli hacker si utilizza una matrice basata su due parametri fondamentali: **Autorizzazione** (permesso di agire) e **Fine** (intento dell'azione). Dall'incrocio di questi parametri derivano i tre "cappelli" principali:

- **White Hat (Ethical Hacker):**
  - *Autorizzazione:* SI (Esplicita e scritta).
  - *Fine:* Buono (Difensivo/Migliorativo).
  - *Ruolo:* Esperti di sicurezza assunti dalle aziende. Simulano attacchi (Penetration Test) seguendo regole d'ingaggio precise per scoprire falle e correggerle.
- **Grey Hat:**
  - *Autorizzazione:* NO.
  - *Fine:* Generalmente Buono (o Ambiguo).
  - *Ruolo:* Individuano vulnerabilità senza permesso, spesso per dimostrare abilità o per "fare del bene" non richiesto. Anche se non hanno intenti distruttivi, la loro azione è **illegale** perché viola i sistemi altrui senza consenso.
- **Black Hat (Criminal Hacker):**
  - *Autorizzazione:* NO.
  - *Fine:* Cattivo (Malevolo/Lucro).
  - *Ruolo:* Violano i sistemi per sottrarre dati, distribuire malware (es. Ransomware), distruggere servizi o chiedere riscatti. Spesso vendono i dati sottratti nel Dark Web.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Concetto Cruciale:** La discriminante legale principale non è l'intenzione, ma l'**autorizzazione**. Un Grey Hat che agisce "a fin di bene" commette comunque un reato (accesso abusivo).

Il Processo di Penetration Testing (Pentesting)

1. 📖 Spiegazione Approfondita

Il Penetration Testing è la simulazione autorizzata di un attacco informatico. Si articola in 5 fasi cicliche:

1. **Raccolta di Informazioni (Reconnaissance/Footprinting):** Fase passiva o attiva preliminare. Si raccolgono dati sul target (IP, domini, email dipendenti).
    - *Tool tipici:* `Whois`, `Nslookup`, OSINT framework.
2. **Scansione (Scanning):** Analisi tecnica per trovare porte aperte, servizi attivi e vulnerabilità note.
    - *Tool tipici:* `Nmap` (Network Mapper), `Nessus` (Vulnerability Scanner).
3. **Accesso (Gaining Access/Exploitation):** Tentativo di sfruttare le vulnerabilità trovate nella fase 2 per entrare nel sistema.
    - *Tool tipici:* `Metasploit Framework`.
4. **Mantenimento dell'Accesso (Maintaining Access/Persistence):** Installazione di backdoor o creazione di utenti per garantire l'accesso futuro anche se il sistema viene riavviato o la falla iniziale corretta.
5. **Analisi e Report (Reporting):** Stesura di un documento dettagliato per il cliente che elenca le vulnerabilità trovate, le prove di concetto (PoC) e le raccomandazioni per la mitigazione (Remediation).

4. 🔗 Cross-Connection Master

In ambito professionale, la fase di **Reporting** è spesso considerata la più importante. Un attacco tecnicamente eccellente è inutile se non viene comunicato chiaramente al management per giustificare gli investimenti in sicurezza.

I Triadi della Sicurezza: CIA vs DAD

1. 📖 Spiegazione Approfondita

La sicurezza informatica si basa su un modello di difesa (CIA) e un modello di attacco/fallimento (DAD). Sono speculari.

Il Triangolo C.I.A. (Obiettivi di Sicurezza):

1. **Confidenzialità (Confidentiality):** Garantire che i dati siano accessibili *solo* agli utenti autorizzati.
    - *Soluzioni:* Crittografia, Autenticazione (MFA), ACL (Access Control Lists).
2. **Integrità (Integrity):** Garantire che i dati non siano stati alterati o manomessi in modo non autorizzato.
    - *Soluzioni:* Hashing (es. SHA-256), Firma Digitale, Version Control.
3. **Disponibilità (Availability):** Garantire che i sistemi e i dati siano accessibili quando servono.
    - *Soluzioni:* Ridondanza, Backup, Protezione DDoS, Load Balancing.

Il Triangolo D.A.D. (Minacce Corrispettive):

1. **Divulgazione (Disclosure):** Opposto di Confidenzialità. Perdita di dati (Data Leak/Breach) verso soggetti non autorizzati.
2. **Alterazione (Alteration):** Opposto di Integrità. Modifica non autorizzata dei dati (es. cambiare l'IBAN in una transazione).

3. **Negazione (Denial):** Opposto di Disponibilità. Interruzione del servizio (es. attacco DoS, ransomware che cifra i file rendendoli inaccessibili).

5. ⚠ Focus Esame

- Memorizza le coppie opposte: Confidentiality <-> Disclosure; Integrity <-> Alteration; Availability <-> Denial/Destruction.

Riferimenti Legali (Codice Penale Italiano)

1. 📖 Spiegazione Approfondita

Ogni attività di testing senza autorizzazione scritta è un reato penale.

- **Art. 615-ter (Accesso abusivo a sistema informatico):** Punisce chi si introduce in un sistema protetto o vi rimane contro la volontà del titolare. Pena: reclusione fino a 3 anni (aggravata se commessa da operatore di sistema o pubblico ufficiale).
- **Art. 635-bis (Danneggiamento di informazioni e sistemi):** Punisce chi distrugge, deteriora, cancella o altera dati o programmi altrui.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Disclaimer:** La clausola di non responsabilità della scuola è netta. Gli strumenti appresi (Kali Linux, exploit) devono essere usati **esclusivamente** in ambienti di laboratorio controllati (virtualizzati) o su sistemi propri.

Virtualizzazione e Architettura del Laboratorio

1. 📖 Spiegazione Approfondita

La virtualizzazione permette di creare risorse virtuali (macchine, reti) a partire da un hardware fisico, ottimizzando le risorse e isolando gli ambienti.

Tipi di Hypervisor:

- **Tipo 1 (Bare-Metal):** L'hypervisor si installa direttamente sull'hardware (senza sistema operativo intermedio).
  - *Pro:* Prestazioni massime, sicurezza elevata.
  - *Esempi:* VMware ESXi, Microsoft Hyper-V (Server), KVM.
  - *Uso:* Data Center, Enterprise.
- **Tipo 2 (Hosted):** L'hypervisor è un programma installato sopra un sistema operativo "Host" (es. Windows 11 o macOS).
  - *Pro:* Facilità d'uso, ideale per laboratori personali.
  - *Contro:* Latenza maggiore (deve passare per l'OS Host).
  - *Esempi:* **Oracle VirtualBox** (usato nel corso), VMware Workstation.
- **Tipo 3 / Container (Docker):** Virtualizzazione leggera che condivide il Kernel dell'OS Host ma isola le librerie e le applicazioni. Non simula l'intero hardware ma solo l'ambiente di esecuzione.

Architettura del Laboratorio Virtuale: Useremo VirtualBox per creare un ambiente sicuro contenente:

1. **Kali Linux:** Macchina Attaccante.
2. **Metasploitable 2:** Macchina Target (intenzionalmente vulnerabile, basata su Linux).
3. **Windows 10 (Obsoleto):** Macchina Target (per simulare vulnerabilità su sistemi Microsoft non patchati).

2. 🛠 Sintassi & Configurazione Reti Virtuali

La configurazione della scheda di rete in VirtualBox è critica per il funzionamento del laboratorio e la sicurezza:

Modalità Rete	Visibilità VM <-> Host	Visibilità VM <-> Internet	Visibilità VM <-> Altre VM	Descrizione Tecnica
NAT	Limitata	SI (Outbound)	NO	La VM naviga usando l'IP dell'Host. È protetta dall'esterno (come dietro un router domestico).
Bridged (Scheda con Bridge)	SI	SI	SI	La VM ottiene un IP dalla stessa rete fisica dell'Host. È come se fosse un PC fisico sulla stessa LAN. **Pericoloso per macchine vulnerabili.**
Internal Network (Rete Interna)	NO	NO	SI	Le VM vedono solo le altre VM nella stessa rete interna. Totale isolamento dall'esterno e dall'Host.
Host-Only	SI	NO	SI	Rete privata tra Host e VM. Le VM non navigano su Internet.
NAT Network	Limitata	SI	SI	Simile al NAT, ma permette alle VM di vedersi tra loro. Ottimo per laboratori complessi.

5. ⚠ Focus Esame

- Perché usiamo sistemi operativi obsoleti (es. Win 10 non patchato) nel laboratorio? Perché i sistemi moderni correggono automaticamente le falle che dobbiamo studiare. L'apprendimento richiede vulnerabilità note ed sfruttabili.

Setup di Kali Linux e Primi Comandi

1. 📖 Spiegazione Approfondita

Kali Linux è una distribuzione basata su **Debian**, progettata specificamente per il Penetration Testing e la Digital Forensics. Viene fornita con centinaia di tool di sicurezza preinstallati.

Procedura di Installazione (VirtualBox):

1. Scaricare l'immagine pre-costruita per VirtualBox dal sito ufficiale (`kali.org`). È un file `.7z` o `.zip`.
2. Decomprimere il file (usando 7-Zip o WinRAR) per ottenere i file `.vbox` e `.vdi`.
3. Aggiungere la macchina in VirtualBox cliccando sul file `.vbox`.
4. Avviare la VM.
5. **Credenziali di Default:** Utente: `kali` / Password: `kali`.

2. 🛠 Sintassi & Comandi (Linux Basics)

Di seguito i comandi fondamentali da terminale (case-sensitive!):

- **Aggiornamento del sistema:**

  > `sudo apt update` (aggiorna la lista dei pacchetti) `sudo apt upgrade` (installa le nuove versioni)

- **Installazione software:**

  > `sudo apt install [nome_pacchetto]`

- **Navigazione e Gestione File:**

  > `ls` o `ls -la` (lista contenuto directory) `cd [percorso]` (cambia directory - 'change directory') `mv [vecchio] [nuovo]` (sposta o rinomina file) `rm [file]` (rimuove/cancella file)

- **Privilegi Amministrativi:**

  > `sudo [comando]` (esegue come SuperUser/Root)

- **Rete:**

  > `ip a` (mostra indirizzi IP e interfacce di rete - sostituisce il deprecato `ifconfig`)

5. ⚠ Focus Esame

- **Correzione OCR:** Nelle slide potrebbe apparire `dpkg -1`, il comando corretto è `dpkg -l` (list) per elencare i pacchetti installati.
- **Virtualizzazione:** Assicurarsi che "Intel VT-x" o "AMD-V" sia abilitato nel BIOS del PC fisico, altrimenti le VM (specialmente a 64-bit) non partiranno.