

```
root@hacklab:~/parte-01/lezione-00
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 00

Fondamenti, etica, diritto e metodologie

Modulo propedeutico: lessico, perimetro giuridico-deontologico e metodo. Nessuna tecnica offensiva prima di autorizzazione e laboratorio isolato.

docente **Vincenzo Calabro** fase Fase trasversale: etica, diritto e metodo prima di ogni attivita

```
root@hacklab:~/lezione-00/agenda $
```

LEZIONE 00 / AGENDA

In questa lezione

// PERCORSO

- > Tassonomia dell'hacking e tipi di ingaggio
- > Metodologie: PTES, OWASP, MITRE, NIST
- > Quadro giuridico IT/UE e deontologia
- > Documenti d'ingaggio: autorizzazione, scope, RoE
- > Allestimento del laboratorio isolato

metodo obiettivi -> teoria -> strumenti -> laboratorio -> caso di studio -> etica -> verifica

```
root@hacklab:~/lezione-00/obiettivi $
```

LEZIONE 00 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – ethical hacking, tipi di ingaggio e metodologie
- > Applicare – redigere Rules of Engagement e definire lo scope
- > Analizzare – distinguere condotta lecita e illecito penale
- > Valutare – implicazioni etiche e responsible disclosure
- > Creare – allestire un laboratorio isolato

```
root@hacklab:~/lezione-00/inquadramento $
```

LEZIONE 00 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Prima di qualsiasi tecnica offensiva viene il metodo: chi siamo autorizzati a colpire, entro quali limiti e con quali responsabilità. Questa lezione fissa lessico, perimetro giuridico-deontologico e l'ambiente di laboratorio isolato su cui poggia tutto il corso.

// PERCHE' CONTA

Modulo propedeutico: lessico, perimetro giuridico-deontologico e metodo. Nessuna tecnica offensiva prima di autorizzazione e laboratorio isolato.

```
root@hacklab:~/lezione-00/mappa-insieme $
```

LEZIONE 00 / MAPPA // INSIEME

Mappa d'insieme del modulo

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA

FONDAMENTI

- 01 Tipi di hacker e team di sicurezza
- 02 Metodologie e framework di riferimento
- 03 Quadro giuridico italiano ed europeo
- 04 Responsible disclosure e bug bounty
- 05 Documenti d'ingaggio

APPROFONDIMENTI

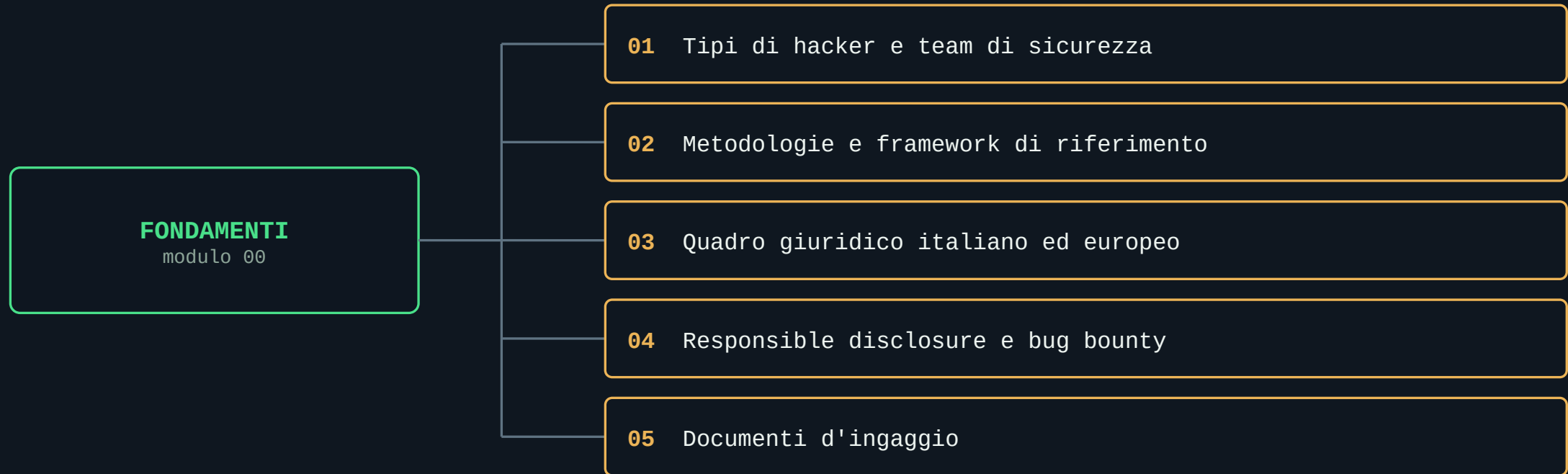
- 06 VA, penetration test e red team
- 07 Gestione e minimizzazione dei dati
- 08 Responsabilit  e comunicazione
- 09 Ruolo dell'IA nella sicurezza
- 10 Deontologia e conflitti d'interesse

```
root@hacklab:~/lezione-00/mappa-1 $
```

LEZIONE 00 / MAPPA // FONDAMENTI

Mappa dei concetti – Fondamenti

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA



```
root@hacklab:~/lezione-00/concetto-1 $
```

LEZIONE 00 / CONCETTO 1/10

[Norme & metodo]

Tipi di hacker e team di sicurezza

// SPIEGAZIONE

I 'cappelli' distinguono l'intento: il white hat opera solo su autorizzazione, il black hat viola la legge, il grey hat agisce in una zona ambigua. Nelle organizzazioni il red team attacca, il blue team difende e il purple team fa dialogare i due per migliorare i controlli.

// ESEMPIO

> In un ingaggio purple il red lancia una tecnica ATT&CK e il blue verifica se il SIEM la rileva.

```
root@hacklab:~/lezione-00/concetto-2 $
```

LEZIONE 00 / CONCETTO 2/10

[Norme & metodo]

Metodologie e framework di riferimento

// SPIEGAZIONE

Un test rigoroso segue una metodologia riconosciuta invece di procedere a caso: PTES descrive le fasi dell'ingaggio, OWASP WSTG guida i test web, NIST SP 800-115 e OSSTMM danno struttura, mentre MITRE ATT&CK/ATLAS e la Cyber Kill Chain mappano tattiche e tecniche dell'avversario.

// ESEMPIO

> Ogni finding viene etichettato con la tecnica ATT&CK corrispondente, es. T1566 Phishing.

```
root@hacklab:~/lezione-00/concetto-3 $
```

LEZIONE 00 / CONCETTO 3/10

[Norme & metodo]

Quadro giuridico italiano ed europeo

// SPIEGAZIONE

L'accesso abusivo a sistema informatico (art. 615-ter c.p.) e l'intercettazione illecita (617-quater) puniscono ciò che si fa senza autorizzazione; GDPR, NIS2 e AI Act impongono obblighi su dati e sicurezza, mentre la Convenzione di Budapest coordina la cooperazione internazionale.

// ESEMPIO

> Superare lo scope autorizzato può configurare accesso abusivo ex art. 615-ter c.p.

```
root@hacklab:~/lezione-00/concetto-4 $
```

LEZIONE 00 / CONCETTO 4/10

[Norme & metodo]

Responsible disclosure e bug bounty

// SPIEGAZIONE

La divulgazione responsabile prevede di segnalare una vulnerabilità al titolare e concordare i tempi di correzione prima di renderla pubblica. I programmi di bug bounty formalizzano questo patto definendo scope, ricompense e regole entro cui il ricercatore può operare lecitamente.

// ESEMPIO

> 90 giorni di embargo prima della pubblicazione, come nella prassi di molti CERT e vendor.

```
root@hacklab:~/lezione-00/concetto-5 $
```

LEZIONE 00 / CONCETTO 5/10

[Norme & metodo]

Documenti d'ingaggio

// SPIEGAZIONE

Prima di toccare un sistema servono documenti che rendano lecita e delimitata l'attività: l'autorizzazione scritta del titolare, lo scope che elenca bersagli e finestre, le Rules of Engagement che fissano cosa è permesso e l'NDA che protegge le informazioni raccolte.

// ESEMPIO

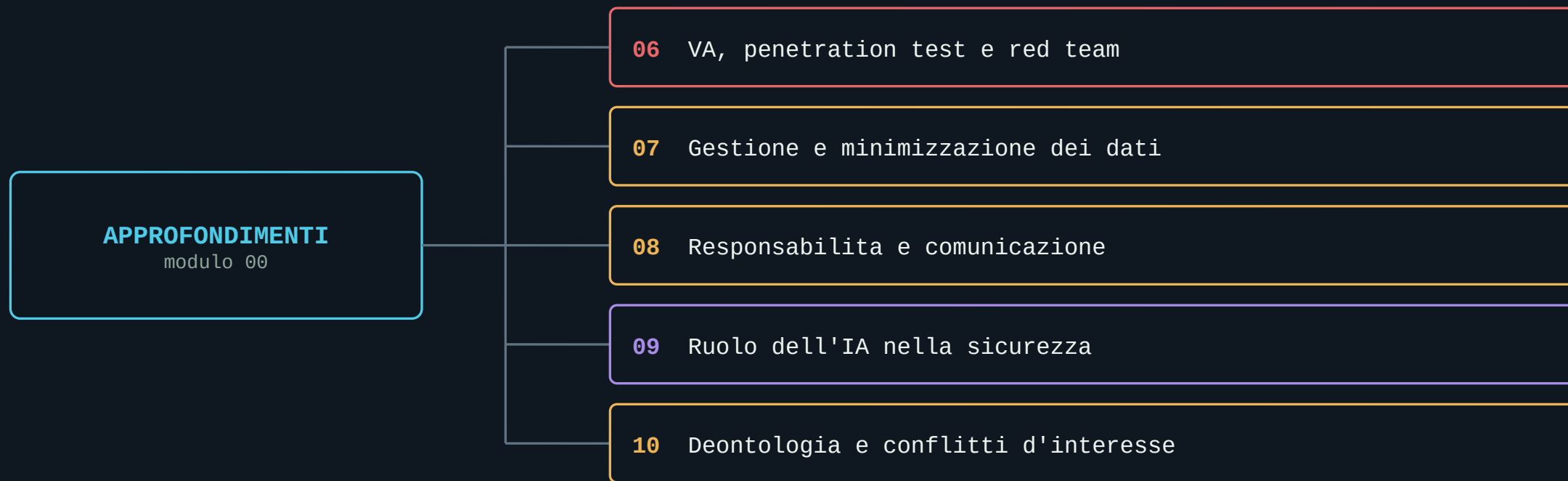
> Lo scope elenca gli IP in perimetro ed esclude esplicitamente i sistemi di produzione critici.

```
root@hacklab:~/lezione-00/mappa-2 $
```

LEZIONE 00 / MAPPA // APPROFONDIMENTI

Mappa dei concetti – Approfondimenti

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA



```
root@hacklab:~/lezione-00/concetto-6 $
```

LEZIONE 00 / CONCETTO 6/10

[Attacco/tecnica]

VA, penetration test e red team

// SPIEGAZIONE

Il vulnerability assessment elenca e classifica le debolezze senza sfruttarle; il penetration test le verifica ottenendo accesso entro lo scope; il red team assessment simula un avversario reale su obiettivi concordati, testando anche persone e processi oltre alla tecnologia.

// ESEMPIO

> 'Trova le vulnerabilita' (VA) contro 'dimostra l'impatto violando il dominio' (pentest).

```
root@hacklab:~/lezione-00/concetto-7 $
```

LEZIONE 00 / CONCETTO 7/10

[Norme & metodo]

Gestione e minimizzazione dei dati

// SPIEGAZIONE

Durante un test si raccolgono dati spesso sensibili: vanno trattati secondo il principio di minimizzazione, raccogliendo solo il necessario, proteggendoli con cifratura e cancellandoli a fine ingaggio secondo quanto concordato, nel rispetto del GDPR.

// ESEMPIO

> Le credenziali trovate si conservano cifrate e si distruggono alla consegna del report.

```
root@hacklab:~/lezione-00/concetto-8 $
```

LEZIONE 00 / CONCETTO 8/10

[Norme & metodo]

Responsabilità e comunicazione

// SPIEGAZIONE

Un ingaggio definisce chi autorizza, chi va informato e come escalare in caso di incidente o scoperta critica. Canali e contatti d'emergenza concordati evitano che un ritrovamento grave, come una compromissione preesistente, resti senza risposta.

// ESEMPIO

> Trovando segni di una breccia in corso si sospende e si attiva subito il contatto d'escalation.

```
root@hacklab:~/lezione-00/concetto-9 $
```

LEZIONE 00 / CONCETTO 9/10

[IA]

Ruolo dell'IA nella sicurezza

// SPIEGAZIONE

Usata bene, l'IA fa risparmiare tempo in ricognizione, analisi e stesura, senza però sostituire il giudizio: i suoi output vanno sempre verificati. In questo corso resta un assistente sotto controllo umano, mai un decisore autonomo su azioni che hanno impatto.

// ESEMPIO

> Un LLM riassume 200 sottodomini, ma l'analista conferma manualmente quelli in scope.

```
root@hacklab:~/lezione-00/concetto-10 $
```

LEZIONE 00 / CONCETTO 10/10

[Norme & metodo]

Deontologia e conflitti d'interesse

// SPIEGAZIONE

Oltre alla legge esiste un'etica professionale: riservatezza, onestà nei risultati, nessun uso improprio degli accessi e dichiarazione dei conflitti d'interesse. La competenza tecnica senza responsabilità deontologica non fa un buon professionista.

// ESEMPIO

> Non si testa un concorrente del cliente sfruttando informazioni apprese nell'ingaggio.

```
root@hacklab:~/lezione-00/strumenti $
```

LEZIONE 00 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Kali

Parrot

VirtualBox

Metasploitable

DVWA

Juice Shop

TryHackMe

HTB

// NOTA OPERATIVA

> Ogni strumento si usa in ambiente virtualizzato e isolato, solo su bersagli di proprietà o autorizzati. Output e artefatti vanno protetti e, a fine ingaggio, gestiti o distrutti.

```
root@hacklab:~/lezione-00/lab-1 $
```

LEZIONE 00 / LABORATORIO 1

Laboratorio 1

\$ Allestimento del laboratorio (VM + rete host-only)

// PROCEDURA

- [1] Crea le VM
- [2] isola la rete host-only
- [3] deploya Metasploitable
- [4] snapshot di ripristino

[!] Verifica: Perché la rete deve essere host-only?

```
root@hacklab:~/lezione-00/lab-2 $
```

LEZIONE 00 / LABORATORIO 2

Laboratorio 2

\$ Definizione dell'ingaggio (RoE su caso reale)

// PROCEDURA

[1] Compila scope

[2] finestre

[3] contatti

[4] escalation e regole sui dati su un modello RoE

[!] Verifica: Cosa rende un'autorizzazione giuridicamente valida?

```
root@hacklab:~/lezione-00/caso-di-studio $
```

LEZIONE 00 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Ingaggio autorizzato spinto oltre lo scope per definizione ambigua, con le relative conseguenze legali.

// ANALISI RICHIESTA

- > Ricostruisci la dinamica dei fatti con metodo e tracciabilità
- > Individua errori, cause radice e punti di decisione critici
- > Proponi contromisure, controlli e lezioni apprese

```
root@hacklab:~/lezione-00/etica $
```

LEZIONE 00 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Accesso senza autorizzazione scritta = art. 615-ter c.p. Solo bersagli di laboratorio o autorizzati.

```
root@hacklab:~/lezione-00/ricapitolazione $
```

LEZIONE 00 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Ethical hacking, tipi di ingaggio e metodologie
- > Redigere Rules of Engagement e definire lo scope
- > Distinguere condotta lecita e illecito penale
- > Implicazioni etiche e responsible disclosure
- > Allestire un laboratorio isolato

```
root@hacklab:~/lezione-00/verifica $
```

LEZIONE 00 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Quali articoli del Codice Penale delimitano l'attività?
- ? Cosa distingue uno scope ben definito da uno ambiguo?
- ? Perché il laboratorio deve essere isolato dalla produzione?

// VALUTAZIONE

Quiz su terminologia e normativa; documento di RoE valutato con rubrica.

// LETTURE

NIST SP 800-115; PTES; OWASP WSTG; Weidman.

lezione 00 completata

\$ next

Fondamenti, etica, diritto e metodologie

[!] Le competenze di questa lezione si impiegano esclusivamente in contesti legali, autorizzati e deontologicamente corretti, entro lo scope e con autorizzazione scritta.

root@hacklab:~# _

```
root@hacklab:~/contatti $
```

CONTATTI / RISORSE

Restiamo in contatto

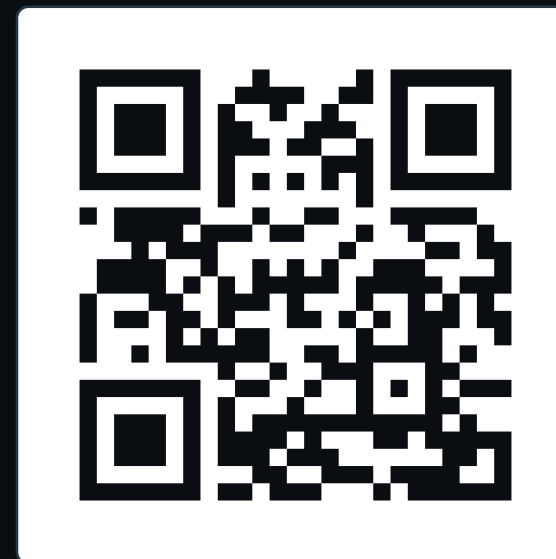


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.