

```
root@hacklab:~/parte-01/lezione-13
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 13

Reporting, comunicazione e remediation

Dal dato tecnico al report professionale e alla remediation.

docente **Vincenzo Calabro** fase Chiusura dell'ingaggio: Reporting e Remediation

```
root@hacklab:~/lezione-13/agenda $
```

LEZIONE 13 / AGENDA

In questa lezione

// PERCORSO

- > Struttura del report
- > Risk rating con CVSS
- > Priorità di remediation
- > Comunicazione tecnica e dirigenziale
- > Responsible disclosure

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

```
root@hacklab:~/lezione-13/obiettivi $
```

LEZIONE 13 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – struttura e scopo di un report
- > Applicare – il risk rating con CVSS
- > Analizzare – priorit  di remediation (impatto vs sforzo)
- > Valutare – comunicazione tecnica e dirigenziale
- > Creare – un report completo e un piano di remediation

```
root@hacklab:~/lezione-13/inquadramento $
```

LEZIONE 13 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Un test vale quanto il report che produce: tecnico per chi corregge, sintetico per chi decide. Vediamo come scrivere finding chiari, prioritizzati con CVSS e orientati alla remediation.

// PERCHE CONTA

Dal dato tecnico al report professionale e alla remediation.

```
root@hacklab:~/lezione-13/mappa-insieme $
```

LEZIONE 13 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Struttura del report
- 02 Prioritizzazione e retest
- 03 Comunicare a tecnici e board
- 04 Disclosure e tempistiche
- 05 IA nella stesura del report

APPROFONDIMENTI

- 06 Executive summary ed evidenze
- 07 Matrice impatto/sforzo e retest
- 08 Storytelling del rischio
- 09 Contratto e tempistiche di disclosure
- 10 Revisione umana obbligatoria

```
root@hacklab:~/lezione-13/flusso-1 $
```

LEZIONE 13 / FLUSSO // FONDAMENTI

Sequenza di fasi – Fondamenti

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



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-13/concetto-1 $
```

LEZIONE 13 / CONCETTO 1/10

[Norme & metodo]

Struttura del report

// SPIEGAZIONE

Un report efficace ha un executive summary per i decisori, poi scope, metodologia, findings con evidenze riproducibili e raccomandazioni. La struttura permette a lettori diversi di trovare subito ciò che li riguarda.

// ESEMPIO

> L'executive summary dice in dieci righe rischio, impatto e priorità, senza gergo tecnico.

```
root@hacklab:~/lezione-13/concetto-2 $
```

LEZIONE 13 / CONCETTO 2/10

[Difesa]

Prioritizzazione e retest

// SPIEGAZIONE

I finding si prioritizzano con CVSS per gravita ed EPSS per probabilita, e si ordinano con una matrice impatto/sforzo per guidare la remediation. Il retest verifica che le correzioni siano efficaci, non solo dichiarate.

// ESEMPIO

> Una vulnerabilita ad alto impatto e basso sforzo di fix e la prima da chiudere.

```
root@hacklab:~/lezione-13/concetto-3 $
```

LEZIONE 13 / CONCETTO 3/10

[Attacco/tecnica]

Comunicare a tecnici e board

// SPIEGAZIONE

Lo stesso finding va raccontato in due lingue: dettaglio tecnico per chi corregge, impatto di business e rischio per chi decide. Lo storytelling del rischio traduce la vulnerabilità in conseguenze comprensibili per il board.

// ESEMPIO

> 'RCE sul gestionale' diventa 'un attaccante può bloccare la fatturazione per giorni'.

```
root@hacklab:~/lezione-13/concetto-4 $
```

LEZIONE 13 / CONCETTO 4/10

[Norme & metodo]

Disclosure e tempistiche

// SPIEGAZIONE

La divulgazione responsabile bilancia il diritto a sapere con il tempo per correggere: si concordano finestre e si evita di pubblicare dettagli sfruttabili prima della patch. Gli aspetti contrattuali regolano riservatezza e responsabilit .

// ESEMPIO

> Embargo concordato finche la patch non   distribuita, poi pubblicazione coordinata.

```
root@hacklab:~/lezione-13/concetto-5 $
```

LEZIONE 13 / CONCETTO 5/10

[Norme & metodo]

IA nella stesura del report

// SPIEGAZIONE

Per bozze, riformulazioni e sintesi l'IA fa guadagnare tempo, ma il report resta responsabilit  dell'autore: ogni dato, prova e raccomandazione va verificato. Un report sbagliato perche 'l'ha scritto l'IA' resta un errore professionale.

// ESEMPIO

> L'IA stende l'executive summary; l'autore ne controlla numeri, toni e accuratezza.

```
root@hacklab:~/lezione-13/flusso-2 $
```

LEZIONE 13 / FLUSSO // APPROFONDIMENTI

Sequenza di fasi – Approfondimenti

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



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-13/concetto-6 $
```

LEZIONE 13 / CONCETTO 6/10

[Attacco/tecnica]

Executive summary ed evidenze

// SPIEGAZIONE

Il sommario esecutivo deve reggere da solo, senza gergo; le evidenze a supporto devono essere riproducibili, con passi, richieste e risposte che chiunque possa ripercorrere. Senza riproducibilit  un finding   solo un'opinione.

// ESEMPIO

> Ogni finding include la richiesta esatta e la risposta che ne dimostra l'impatto.

```
root@hacklab:~/lezione-13/concetto-7 $
```

LEZIONE 13 / CONCETTO 7/10

[Difesa]

Matrice impatto/sforzo e retest

// SPIEGAZIONE

Ordinare i finding per impatto e sforzo di correzione rende il piano di rientro realistico e condiviso. Il retest finale, documentato, chiude il ciclo verificando che il rischio sia davvero ridotto.

// ESEMPIO

> Il quadrante 'alto impatto / basso sforzo' in cima alla lista delle priorit .

```
root@hacklab:~/lezione-13/concetto-8 $
```

LEZIONE 13 / CONCETTO 8/10

[Attacco/tecnica]

Storytelling del rischio

// SPIEGAZIONE

Numeri e CVSS non bastano a muovere decisioni: serve una narrazione del rischio ancorata al business, che spieghi cosa puo succedere e perche conviene agire. Gestire le aspettative evita sia il panico sia la sottovalutazione.

// ESEMPIO

> Collegare un finding al 'blocco del servizio clienti' piu che a un punteggio astratto.

```
root@hacklab:~/lezione-13/concetto-9 $
```

LEZIONE 13 / CONCETTO 9/10

[Norme & metodo]

Contratto e tempistiche di disclosure

// SPIEGAZIONE

Chi può vedere il report, per quanto resta riservato, come si gestisce una scoperta critica fuori scope: sono aspetti contrattuali da chiarire prima. Le tempistiche di disclosure vanno concordate, non improvvisate a posteriori.

// ESEMPIO

> Il contratto fissa a chi consegnare il report e per quanti mesi resta confidenziale.

```
root@hacklab:~/lezione-13/concetto-10 $
```

LEZIONE 13 / CONCETTO 10/10

[Norme & metodo]

Revisione umana obbligatoria

// SPIEGAZIONE

L'IA è un copilota di scrittura, non il firmatario: può inventare riferimenti, sbagliare numeri e appiattare il tono. La revisione umana è obbligatoria perché la responsabilità del contenuto resta interamente dell'autore.

// ESEMPIO

> Si verifica che l'IA non abbia 'arrotondato' una gravità o inventato una CVE.

```
root@hacklab:~/lezione-13/strumenti $
```

LEZIONE 13 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Modelli PTES/OWASP

CVSS calculator

Gestione findings

// 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-13/lab-1 $
```

LEZIONE 13 / LABORATORIO 1

Laboratorio 1

\$ Dal dato grezzo al report (CVSS + remediation)

// PROCEDURA

[1] Trasforma i risultati di un modulo in un report con findings prioritizzati per CVSS

[!] Verifica: Cosa rende una raccomandazione actionable?

```
root@hacklab:~/lezione-13/lab-2 $
```

LEZIONE 13 / LABORATORIO 2

Laboratorio 2

\$ Comunicazione al board (executive summary)

// PROCEDURA

[1] Sintetizza i risultati in un executive summary per un pubblico non tecnico

[!] Verifica: Come si traduce un rischio tecnico per il board?

```
root@hacklab:~/lezione-13/caso-di-studio $
```

LEZIONE 13 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Confronto tra un report efficace e uno inefficace sullo stesso finding, e impatto sulla remediation.

// 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-13/etica $
```

LEZIONE 13 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Il report contiene informazioni sensibili: va protetto, cifrato e condiviso solo con gli autorizzati.

```
root@hacklab:~/lezione-13/ricapitolazione $
```

LEZIONE 13 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Struttura e scopo di un report
- > Il risk rating con CVSS
- > Priorità di remediation (impatto vs sforzo)
- > Comunicazione tecnica e dirigenziale
- > Un report completo e un piano di remediation

```
root@hacklab:~/lezione-13/verifica $
```

LEZIONE 13 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Cosa rende una raccomandazione actionable?
- ? Come si traduce un rischio tecnico per il board?
- ? A cosa serve il retest nel ciclo di vita delle vulnerabilità?

// VALUTAZIONE

Report professionale con rubrica + esercizio di comunicazione.

// LETTURE

PTES e OWASP WSTG (reporting); specifiche CVSS.

lezione 13 completata

\$ next

Reporting, comunicazione e remediation

[!] 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

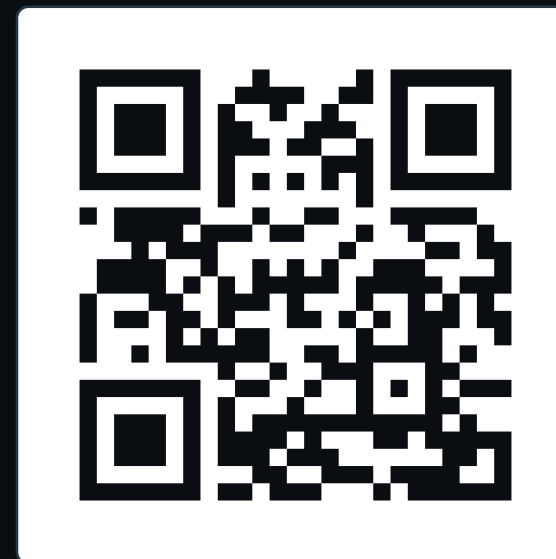


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.