

```
root@hacklab:~/parte-01/lezione-14
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 14

Capstone project

Esercitazione integrativa che chiude la traccia core, simulando un ingaggio reale dall'inizio alla fine.

docente **Vincenzo Calabro** fase Sintesi applicata: Capstone (red vs blue)

```
root@hacklab:~/lezione-14/agenda $
```

LEZIONE 14 / AGENDA

In questa lezione

// PERCORSO

- > Scelta del formato (CTF o red vs blue)
- > Ciclo completo end-to-end
- > Integrazione della componente IA
- > Ruoli red / blue / purple
- > Debrief e lezioni apprese

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

```
root@hacklab:~/lezione-14/obiettivi $
```

LEZIONE 14 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – come integrare le competenze del percorso
- > Applicare – un'operazione end-to-end
- > Analizzare e difendere – scenario red vs blue
- > Valutare – criticamente il proprio operato
- > Creare – il report finale e condurre il debrief

```
root@hacklab:~/lezione-14/inquadramento $
```

LEZIONE 14 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Il capstone integra tutto il percorso in un ingaggio completo, dallo scope al report finale. E la prova che metodo, tecnica ed etica funzionano insieme su un caso realistico.

// PERCHE CONTA

Esercitazione integrativa che chiude la traccia core, simulando un ingaggio reale dall'inizio alla fine.

```
root@hacklab:~/lezione-14/mappa-insieme $
```

LEZIONE 14 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Formati del capstone
- 02 Ciclo completo dell'ingaggio
- 03 Integrazione della componente IA
- 04 Ruoli e pianificazione
- 05 Debrief su kill chain e ATT&CK

APPROFONDIMENTI

- 06 Pianificazione dell'ingaggio
- 07 Gestione di tempo ed evidenze
- 08 Purple teaming e miglioramento
- 09 Mappatura su kill chain e ATT&CK
- 10 Analisi dei controlli mancanti

```
root@hacklab:~/lezione-14/flusso-1 $
```

LEZIONE 14 / 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-14/concetto-1 $
```

LEZIONE 14 / CONCETTO 1/10

[Attacco/tecnica]

Formati del capstone

// SPIEGAZIONE

Il progetto finale può prendere forma di CTF, jeopardy a sfide o attack-defense, o di esercizio red contro blue con sintesi purple. Ogni formato mette alla prova competenze diverse in condizioni realistiche e a tempo.

// ESEMPIO

> In attack-defense ogni squadra difende i propri servizi mentre attacca quelli altrui.

```
root@hacklab:~/lezione-14/concetto-2 $
```

LEZIONE 14 / CONCETTO 2/10

[Norme & metodo]

Ciclo completo dell'ingaggio

// SPIEGAZIONE

Il capstone integra l'intero percorso: ricognizione, exploitation, post-exploitation, forensics e reporting in un unico flusso coerente. E la prova che le fasi, studiate separatamente, funzionano insieme su un caso reale.

// ESEMPIO

> Da un sottodominio dimenticato fino al report con impatto e remediation.

```
root@hacklab:~/lezione-14/concetto-3 $
```

LEZIONE 14 / CONCETTO 3/10

[IA]

Integrazione della componente IA

// SPIEGAZIONE

Il progetto include l'uso consapevole dell'IA come assistente in ricognizione, analisi e stesura, documentandone apporto e verifiche. Dimostra non solo l'uso, ma il controllo critico sull'output del modello.

// ESEMPIO

> Si registra dove l'IA ha aiutato e come ogni suo suggerimento è stato verificato.

```
root@hacklab:~/lezione-14/concetto-4 $
```

LEZIONE 14 / CONCETTO 4/10

[Norme & metodo]

Ruoli e pianificazione

// SPIEGAZIONE

Prima di agire si pianifica: ruoli red, blue e purple, scope, Rules of Engagement e obiettivi misurabili. Una buona pianificazione e meta del risultato e distingue un esercizio serio da un'improvvisazione.

// ESEMPIO

> RoE e scope firmati prima dell'inizio, con finestre e contatti d'escalation definiti.

```
root@hacklab:~/lezione-14/concetto-5 $
```

LEZIONE 14 / CONCETTO 5/10

[Difesa]

Debrief su kill chain e ATT&CK

// SPIEGAZIONE

Il valore formativo sta nel debrief: ricostruire la kill chain, mappare le tecniche su MITRE ATT&CK e individuare dove la difesa ha funzionato o fallito. Trasforma l'esercizio in miglioramento concreto.

// ESEMPIO

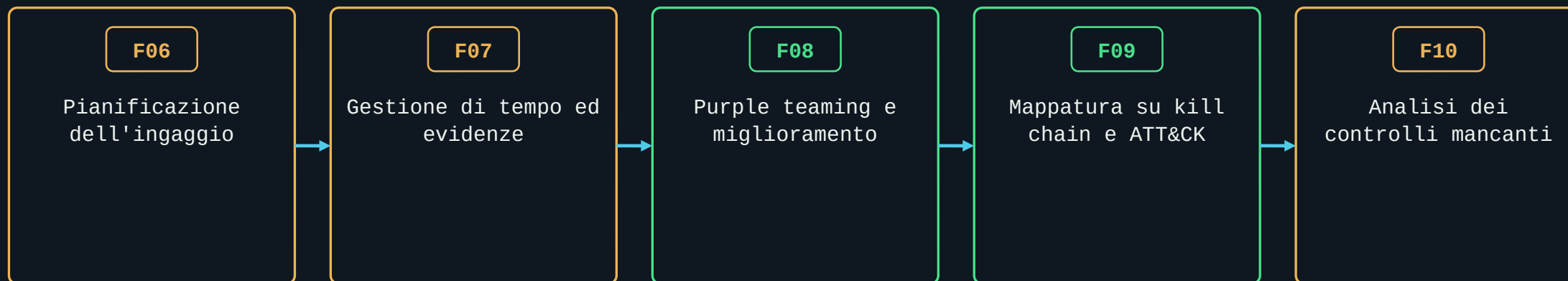
> Si evidenzia quale tecnica ATT&CK non è stata rilevata dal blue team e perché.

```
root@hacklab:~/lezione-14/flusso-2 $
```

LEZIONE 14 / 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-14/concetto-6 $
```

LEZIONE 14 / CONCETTO 6/10

[Norme & metodo]

Pianificazione dell'ingaggio

// SPIEGAZIONE

Definire obiettivi, perimetro, regole e tempi prima di iniziare evita deragliamenti e rischi legali. La pianificazione include anche la gestione delle evidenze e i criteri di successo concordati con il committente.

// ESEMPIO

> L'obiettivo 'dimostra accesso ai dati clienti' e piu utile di 'trova vulnerabilita'.

```
root@hacklab:~/lezione-14/concetto-7 $
```

LEZIONE 14 / CONCETTO 7/10

[Norme & metodo]

Gestione di tempo ed evidenze

// SPIEGAZIONE

In un ingaggio a tempo, prioritizzare e documentare man mano è decisivo: le evidenze raccolte in modo ordinato diventano il report. Rincorrere troppe piste disperde tempo e lascia buchi nella documentazione.

// ESEMPIO

> Screenshot e comandi salvati in tempo reale, pronti per il report finale.

```
root@hacklab:~/lezione-14/concetto-8 $
```

LEZIONE 14 / CONCETTO 8/10

[Difesa]

Purple teaming e miglioramento

// SPIEGAZIONE

Il purple team fa dialogare attacco e difesa: ogni tecnica provata diventa occasione per migliorare rilevamento e risposta. L'obiettivo non è 'vincere' ma rendere l'organizzazione più resiliente.

// ESEMPIO

> Dopo un attacco non rilevato, il blue crea subito la regola di detection mancante.

```
root@hacklab:~/lezione-14/concetto-9 $
```

LEZIONE 14 / CONCETTO 9/10

[Difesa]

Mappatura su kill chain e ATT&CK

// SPIEGAZIONE

Ricondurre ogni azione alle fasi della kill chain e alle tecniche ATT&CK offre un linguaggio comune e misurabile. Permette di vedere a colpo d'occhio copertura difensiva e punti ciechi.

// ESEMPIO

> Una matrice ATT&CK colorata mostra quali tecniche sono state rilevate e quali no.

```
root@hacklab:~/lezione-14/concetto-10 $
```

LEZIONE 14 / CONCETTO 10/10

[Norme & metodo]

Analisi dei controlli mancanti

// SPIEGAZIONE

Il capstone si chiude individuando i controlli assenti o inefficaci emersi durante l'esercizio, con raccomandazioni prioritizzate. E il ponte tra la simulazione e il piano di rafforzamento reale.

// ESEMPIO

> Mancanza di logging su un sistema critico: raccomandazione prioritaria nel report.

```
root@hacklab:~/lezione-14/strumenti $
```

LEZIONE 14 / STRUMENTI

Strumenti della lezione

// TOOLKIT

L'intera cassetta degli attrezzi

HTB / TryHackMe / laboratorio dedicato

// 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-14/lab-1 $
```

LEZIONE 14 / LABORATORIO 1

Laboratorio 1

\$ Operazione completa in laboratorio (red + blue + purple)

// PROCEDURA

[1] A squadre

[2] conduci l'ingaggio autorizzato end-to-end e produci il report finale

[!] Verifica: Quali controlli avrebbero interrotto la kill chain?

```
root@hacklab:~/lezione-14/caso-di-studio $
```

LEZIONE 14 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Ricostruzione guidata di un'intrusione reale complessa (es. SolarWinds) come modello per il debrief.

// 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-14/etica $
```

LEZIONE 14 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Solo ambiente isolato e autorizzato; competenze impiegate esclusivamente in contesti legali e deontologici.

```
root@hacklab:~/lezione-14/ricapitolazione $
```

LEZIONE 14 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Come integrare le competenze del percorso
- > Un'operazione end-to-end
- > Scenario red vs blue
- > Criticamente il proprio operato
- > Il report finale e condurre il debrief

```
root@hacklab:~/lezione-14/verifica $
```

LEZIONE 14 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Quali controlli avrebbero interrotto la kill chain?
- ? Dove l'IA ha dato il contributo maggiore, da entrambi i lati?
- ? Come si struttura un debrief efficace?

// VALUTAZIONE

Progetto capstone (operazione + report + debrief).

// LETTURE

Riepilogo dei materiali; The Hacker Playbook.

lezione 14 completata

\$ next

Capstone project

[!] 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

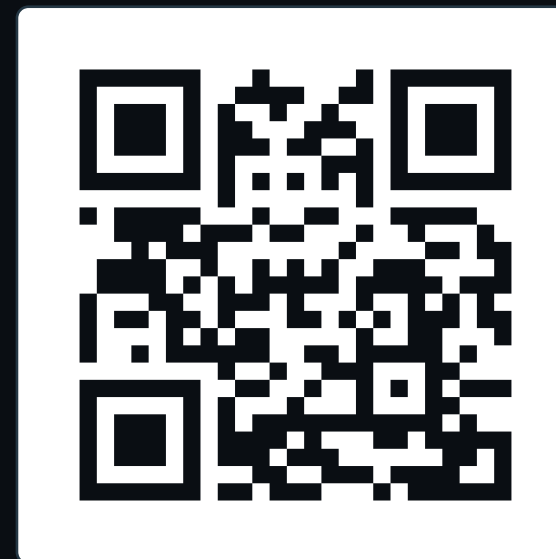


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.