

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

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 01

Information Gathering e OSINT

Prima fase operativa del penetration test: raccolta di informazioni e mappatura della superficie d'attacco.

docente **Vincenzo Calabro** fase Fase 1 del pentest: Reconnaissance (Cyber Kill Chain)

```
root@hacklab:~/lezione-01/agenda $
```

LEZIONE 01 / AGENDA

In questa lezione

// PERCORSO

- > Ricognizione passiva vs attiva
- > Footprinting di dominio, DNS, sottodomini
- > OSINT su persone, e-mail, repository
- > Dispositivi esposti (Shodan/Censys)
- > OSINT assistito dall'IA e verifica

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

```
root@hacklab:~/lezione-01/obiettivi $
```

LEZIONE 01 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – ricognizione passiva vs attiva
- > Applicare – footprinting di dominio/DNS e OSINT
- > Analizzare – superficie d'attacco e impronta digitale
- > Valutare – rischi di esposizione e confini di privacy
- > Creare – un profilo di reconnaissance verificabile

```
root@hacklab:~/lezione-01/inquadramento $
```

LEZIONE 01 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Ogni ingaggio comincia raccogliendo informazioni: piu conosciamo il bersaglio, piu mirata e sicura sara l'azione. Vediamo come mappare superficie d'attacco e footprint con fonti aperte, distinguendo raccolta passiva e attiva e i relativi rischi di rilevamento.

// PERCHE CONTA

Prima fase operativa del penetration test: raccolta di informazioni e mappatura della superficie d'attacco.

```
root@hacklab:~/lezione-01/mappa-insieme $
```

LEZIONE 01 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Footprinting di dominio, DNS e ASN
- 02 OSINT su persone e repository
- 03 Metadati e dispositivi esposti
- 04 OSINT potenziato dall'IA
- 05 Privacy e GDPR nell'aggregazione

APPROFONDIMENTI

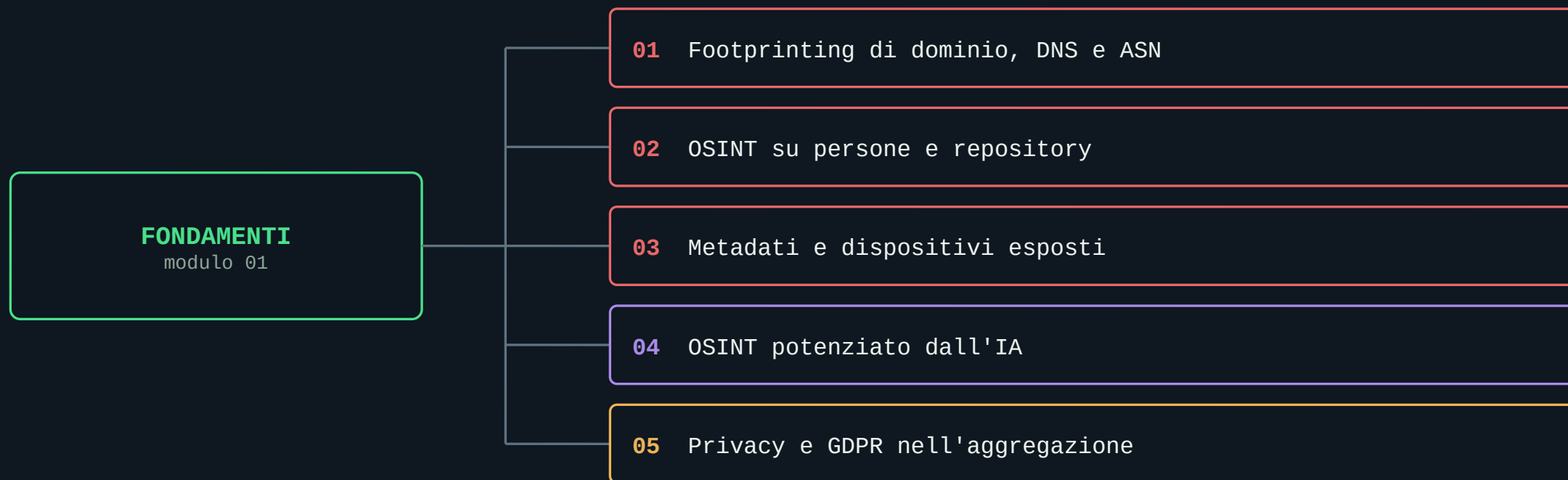
- 06 Certificate Transparency e sottodomini
- 07 Fingerprinting dello stack tecnologico
- 08 Geolocalizzazione e analisi metadati
- 09 Allucinazioni degli strumenti IA
- 10 Documentazione e tracciabilità

```
root@hacklab:~/lezione-01/mappa-1 $
```

LEZIONE 01 / MAPPA // FONDAMENTI

Mappa dei concetti – Fondamenti

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



```
root@hacklab:~/lezione-01/concetto-1 $
```

LEZIONE 01 / CONCETTO 1/10

[Attacco/tecnica]

Footprinting di dominio, DNS e ASN

// SPIEGAZIONE

La ricognizione passiva ricostruisce la presenza online del bersaglio partendo da DNS, sottodomini e numeri di sistema autonomo (ASN), senza inviare traffico sospetto. Mappare questi elementi delinea la superficie d'attacco esterna prima di qualsiasi interazione diretta.

// ESEMPIO

```
$ amass enum -passive -d esempio.it
```

```
root@hacklab:~/lezione-01/concetto-2 $
```

LEZIONE 01 / CONCETTO 2/10

[Attacco/tecnica]

OSINT su persone e repository

// SPIEGAZIONE

Fonti aperte come social, archivi pubblici e repository di codice rivelano e-mail, ruoli e talvolta segreti dimenticati. I Google dork usano operatori di ricerca mirati per trovare pagine e file esposti che non dovrebbero essere pubblici.

// ESEMPIO

```
$ site:esempio.it filetype:pdf (dork per documenti indicizzati)
```

```
root@hacklab:~/lezione-01/concetto-3 $
```

LEZIONE 01 / CONCETTO 3/10

[Attacco/tecnica]

Metadati e dispositivi esposti

// SPIEGAZIONE

I file pubblicati conservano metadati (EXIF nelle foto, autori e software nei documenti) che svelano informazioni interne; motori come Shodan e Censys indicizzano dispositivi e servizi raggiungibili da Internet, mostrando versioni e configurazioni esposte.

// ESEMPIO

```
$ shodan search 'org:"Esempio SpA" port:3389' (RDP esposti)
```

```
root@hacklab:~/lezione-01/concetto-4 $
```

LEZIONE 01 / CONCETTO 4/10

[IA]

OSINT potenziato dall'IA

// SPIEGAZIONE

L'IA aiuta a sintetizzare grandi volumi di dati OSINT e a correlare entita come persone, domini ed eventi piu in fretta. Resta indispensabile verificare ogni collegamento proposto, perche il modello puo inventare relazioni inesistenti.

// ESEMPIO

> Un LLM raggruppa profili come possibile stessa persona; l'analista conferma con prove indipendenti.

```
root@hacklab:~/lezione-01/concetto-5 $
```

LEZIONE 01 / CONCETTO 5/10

[Norme & metodo]

Privacy e GDPR nell'aggregazione

// SPIEGAZIONE

Anche dati singolarmente pubblici, se aggregati, creano profili personali soggetti al GDPR. La raccolta OSINT su persone deve avere base lecita, finalita definita e minimizzazione, evitando dossier che eccedono lo scopo dell'ingaggio.

// ESEMPIO

> Si raccolgono e-mail aziendali per il phishing test, non la vita privata dei dipendenti.

```
root@hacklab:~/lezione-01/mappa-2 $
```

LEZIONE 01 / MAPPA // APPROFONDIMENTI

Mappa dei concetti – Approfondimenti

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



```
root@hacklab:~/lezione-01/concetto-6 $
```

LEZIONE 01 / CONCETTO 6/10

[Attacco/tecnica]

Certificate Transparency e sottodomini

// SPIEGAZIONE

I log di Certificate Transparency registrano pubblicamente i certificati TLS emessi: consultarli rivela sottodomini, anche interni o di staging, che non compaiono altrove, ampliando la mappa della superficie d'attacco senza interrogare il bersaglio.

// ESEMPIO

```
$ curl 'https://crt.sh/?q=%25.esempio.it&output=json'
```

```
root@hacklab:~/lezione-01/concetto-7 $
```

LEZIONE 01 / CONCETTO 7/10

[Attacco/tecnica]

Fingerprinting dello stack tecnologico

// SPIEGAZIONE

Identificare CMS, framework, librerie e versioni in uso permette di prevedere vulnerabilità plausibili e mirare i test. Header HTTP, pattern di risorse e hash della favicon sono indizi che rivelano lo stack senza attacchi intrusivi.

// ESEMPIO

```
$ whatweb esempio.it
```

```
root@hacklab:~/lezione-01/concetto-8 $
```

LEZIONE 01 / CONCETTO 8/10

[Norme & metodo]

Geolocalizzazione e analisi metadati

// SPIEGAZIONE

Coordinate EXIF, fusi orari, lingue e riferimenti visivi nelle immagini permettono di localizzare persone o sedi. Incrociare questi segnali con mappe e fonti pubbliche e una tecnica OSINT potente e, proprio per questo, da usare con cautela etica.

// ESEMPIO

> L'EXIF GPS di una foto social rivela la sede di un ufficio non pubblicizzato.

```
root@hacklab:~/lezione-01/concetto-9 $
```

LEZIONE 01 / CONCETTO 9/10

[IA]

Allucinazioni degli strumenti IA

// SPIEGAZIONE

Gli strumenti basati su LLM possono produrre nomi, indirizzi o relazioni plausibili ma falsi. In OSINT questo è pericoloso perché un dato inventato può indirizzare male l'ingaggio o danneggiare una persona: ogni output va verificato su fonti primarie.

// ESEMPIO

> L'IA attribuisce un dominio al bersaglio, ma il whois mostra un intestatario diverso.

```
root@hacklab:~/lezione-01/concetto-10 $
```

LEZIONE 01 / CONCETTO 10/10

[Norme & metodo]

Documentazione e tracciabilità

// SPIEGAZIONE

Ogni informazione raccolta va annotata con fonte, data e metodo, così il risultato è riproducibile e difendibile. Una buona tracciabilità distingue un'analisi professionale da una raccolta di voci non verificabili.

// ESEMPIO

> Una tabella 'dato - fonte - URL - data - affidabilità' a corredo del report OSINT.

```
root@hacklab:~/lezione-01/strumenti $
```

LEZIONE 01 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Maltego

theHarvester

Recon-ng

SpiderFoot

Amass

Sublist3r

FOCA

Shodan

Censys

// 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-01/lab-1 $
```

LEZIONE 01 / LABORATORIO 1

Laboratorio 1

\$ Footprinting passivo (Amass, theHarvester, Maltego)

// PROCEDURA

[1] Enumera sottodomini (Amass)

[2] host/e-mail (theHarvester)

[3] grafo (Maltego)

[4] metadati (FOCA)

[!] Verifica: Cosa si raccoglie senza toccare il bersaglio?

```
root@hacklab:~/lezione-01/lab-2 $
```

LEZIONE 01 / LABORATORIO 2

Laboratorio 2

\$ Da OSINT a superficie d'attacco (sintesi LLM verificata)

// PROCEDURA

- [1]** Consolida i dati in un profilo e usa un LLM per la sintesi
- [2]** verificando ogni fonte

[!] Verifica: Come si valida un dato OSINT?

```
root@hacklab:~/lezione-01/caso-di-studio $
```

LEZIONE 01 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Violazione originata da informazioni pubbliche esposte: credenziali in repository, metadati, sottodomini dimenticati.

// 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-01/etica $
```

LEZIONE 01 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Fonti pubbliche ma GDPR sull'aggregazione; ricognizione attiva solo entro scope.

```
root@hacklab:~/lezione-01/ricapitolazione $
```

LEZIONE 01 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Ricognizione passiva vs attiva
- > Footprinting di dominio/DNS e OSINT
- > Superficie d'attacco e impronta digitale
- > Rischi di esposizione e confini di privacy
- > Un profilo di reconnaissance verificabile

```
root@hacklab:~/lezione-01/verifica $
```

LEZIONE 01 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Dove passa il confine tra OSINT e privacy?
- ? Come si valida un dato OSINT prima di usarlo?
- ? Cosa si raccoglie senza inviare traffico al bersaglio?

// VALUTAZIONE

Profilo di reconnaissance (copertura, accuratezza, metodo) + quiz.

// LETTURE

OSINT Framework; OWASP WSTG; Bazzell, OSINT Techniques.

lezione 01 completata

\$ next

Information Gathering e OSINT

[!] 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

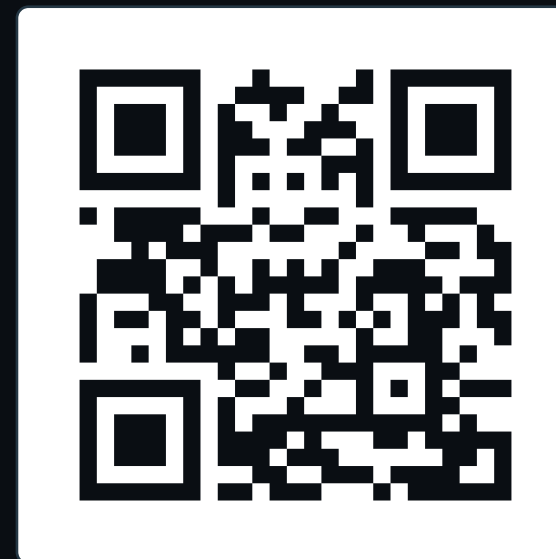


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.