

```
root@hacklab:~/parte-01/lezione-08
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 08

Social Engineering

Il fattore umano, con uno sguardo alle minacce potenziate dall'IA.

docente **Vincenzo Calabro** fase Fattore umano: Social Engineering

```
root@hacklab:~/lezione-08/agenda $
```

LEZIONE 08 / AGENDA

In questa lezione

// PERCORSO

- > Principi di persuasione e pretexting
- > Vettori di phishing
- > Progettazione e metriche di campagna
- > Minacce basate su IA (deepfake, BEC)
- > Difese tecniche e umane

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

```
root@hacklab:~/lezione-08/obiettivi $
```

LEZIONE 08 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – i principi psicologici dell'inganno
- > Applicare – campagne di phishing autorizzate
- > Analizzare – deepfake e voice cloning
- > Valutare – contromisure tecniche e umane
- > Creare – un piano di campagna e di formazione

```
root@hacklab:~/lezione-08/inquadramento $
```

LEZIONE 08 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

L'anello umano è spesso il più fragile: pretexting, phishing e manipolazione sfruttano fiducia e urgenza. La lezione tratta tecniche, limiti etici e difese organizzative, con regole d'ingaggio rigorose.

// PERCHE' CONTA

Il fattore umano, con uno sguardo alle minacce potenziate dall'IA.

```
root@hacklab:~/lezione-08/mappa-insieme $
```

LEZIONE 08 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

01 Principi di persuasione e pretexting

02 Canali del social engineering

03 Metriche di una campagna

04 IA come minaccia: deepfake e BEC

05 Difese tecniche e umane

APPROFONDIMENTI

06 Varianti mirate di phishing

07 A/B testing etico delle campagne

08 Voice cloning e frodi BEC

09 Autenticazione e-mail e sandbox

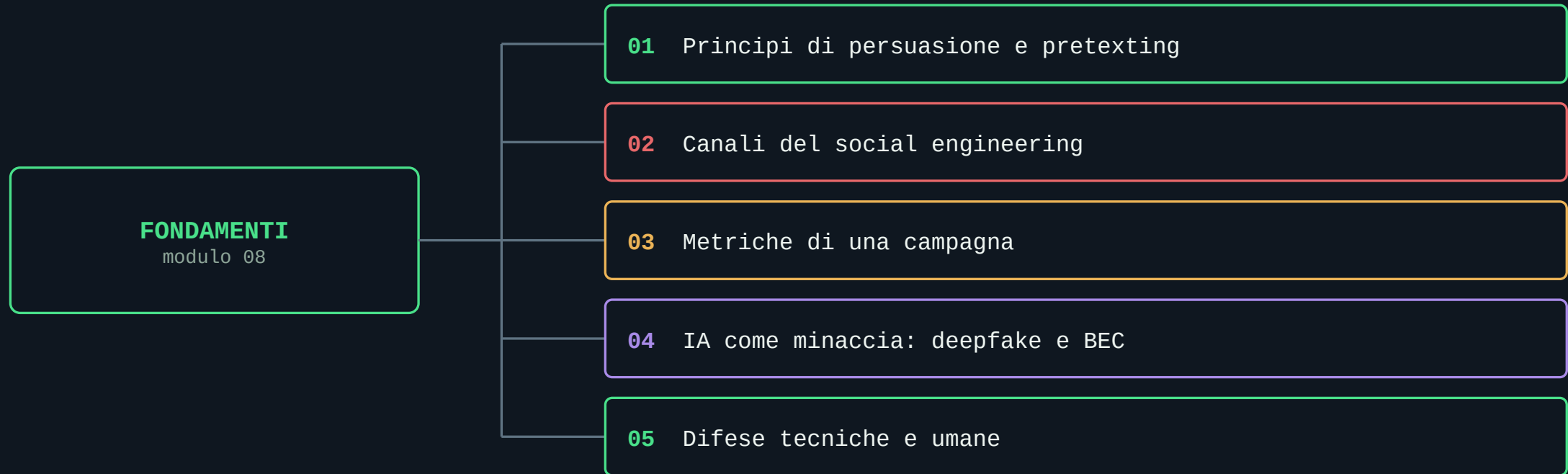
10 Cultura di segnalazione e verifica

```
root@hacklab:~/lezione-08/mappa-1 $
```

LEZIONE 08 / MAPPA // FONDAMENTI

Mappa dei concetti – Fondamenti

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



```
root@hacklab:~/lezione-08/concetto-1 $
```

LEZIONE 08 / CONCETTO 1/10

[Difesa]

Principi di persuasione e pretexting

// SPIEGAZIONE

Il social engineering sfrutta leve psicologiche descritte da Cialdini: autorità, urgenza, reciprocità, riprova sociale. Il pretexting costruisce uno scenario credibile, un ruolo e un motivo, che abbassa le difese della vittima e giustifica la richiesta.

// ESEMPIO

> Falso tecnico IT che 'deve risolvere un guasto urgente' per farsi dare le credenziali.

```
root@hacklab:~/lezione-08/concetto-2 $
```

LEZIONE 08 / CONCETTO 2/10

[Attacco/tecnica]

Canali del social engineering

// SPIEGAZIONE

L'inganno viaggia su molti canali: phishing via e-mail di massa, spear phishing mirato, vishing al telefono, smishing via SMS, baiting con supporti infetti, tailgating fisico. Ogni canale cambia contesto ma non la leva: la fiducia.

// ESEMPIO

> Una chiavetta USB 'smarrita' nel parcheggio che, inserita, esegue un payload (baiting).

```
root@hacklab:~/lezione-08/concetto-3 $
```

LEZIONE 08 / CONCETTO 3/10

[Norme & metodo]

Metriche di una campagna

// SPIEGAZIONE

Un test di phishing si misura: tasso di click, di inserimento credenziali (submission) e, soprattutto, di segnalazione. Il report-rate indica la salute della cultura di sicurezza meglio del solo click-rate e orienta la formazione.

// ESEMPIO

> Click-rate 30% ma report-rate 5%: molti abboccano e pochissimi segnalano.

```
root@hacklab:~/lezione-08/concetto-4 $
```

LEZIONE 08 / CONCETTO 4/10

[IA]

IA come minaccia: deepfake e BEC

// SPIEGAZIONE

L'IA alza la posta: voice cloning e deepfake rendono credibili vishing e truffe del CEO, mentre modelli senza freni producono e-mail di phishing impeccabili su scala. Sono trattati come minacce da conoscere per difendersi, non strumenti da usare.

// ESEMPIO

> Voce clonata del CEO che ordina un bonifico urgente (frode BEC assistita da IA).

```
root@hacklab:~/lezione-08/concetto-5 $
```

LEZIONE 08 / CONCETTO 5/10

[Difesa]

Difese tecniche e umane

// SPIEGAZIONE

Contro il phishing servono entrambe le linee: controlli tecnici come SPF, DKIM e DMARC che autenticano il mittente e riducono lo spoofing, e la formazione delle persone, che restano l'ultimo filtro quando un messaggio passa i controlli.

// ESEMPIO

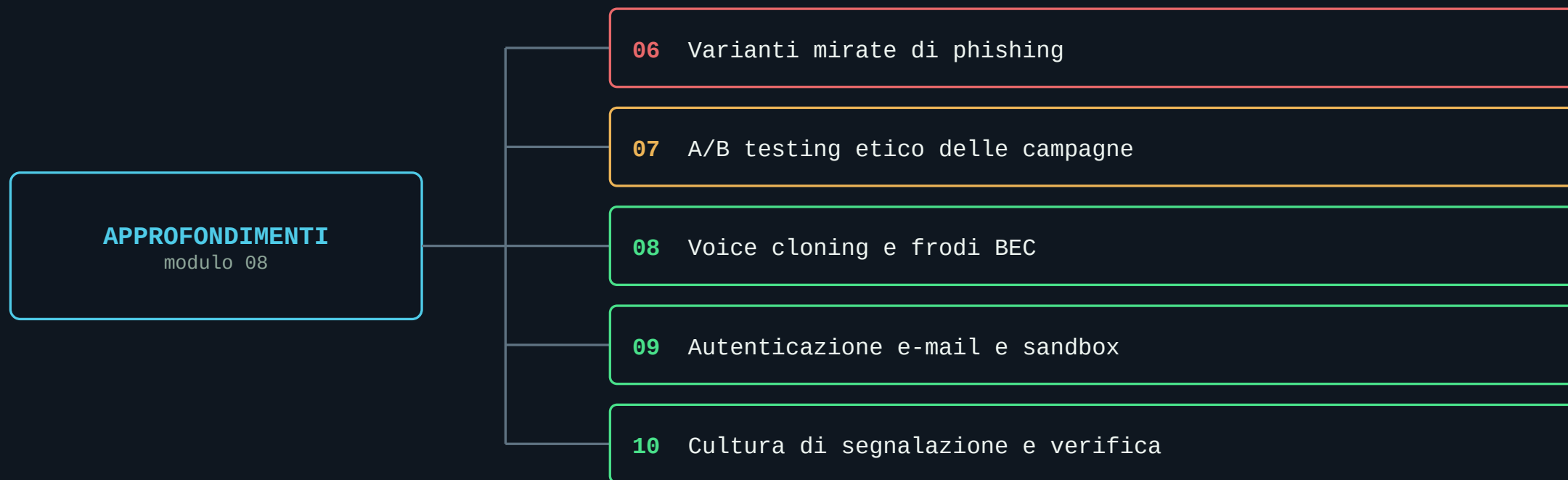
> DMARC in 'reject' blocca le e-mail che spacciano il dominio aziendale.

```
root@hacklab:~/lezione-08/mappa-2 $
```

LEZIONE 08 / MAPPA // APPROFONDIMENTI

Mappa dei concetti – Approfondimenti

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



```
root@hacklab:~/lezione-08/concetto-6 $
```

LEZIONE 08 / CONCETTO 6/10

[Attacco/tecnica]

Varianti mirate di phishing

// SPIEGAZIONE

Piu il bersaglio e specifico, piu l'attacco e curato: lo spear phishing personalizza il messaggio, il whaling punta ai dirigenti, vishing e smishing spostano l'inganno su voce e SMS dove si abbassa la diffidenza. La ricognizione OSINT li rende credibili.

// ESEMPIO

> E-mail al CFO che cita un progetto reale trovato su LinkedIn (whaling).

```
root@hacklab:~/lezione-08/concetto-7 $
```

LEZIONE 08 / CONCETTO 7/10

[Norme & metodo]

A/B testing etico delle campagne

// SPIEGAZIONE

Si possono confrontare due esche per capire cosa funziona, ma in modo etico: senza umiliare le persone, con obiettivo formativo e dati aggregati. La metrica che conta davvero è quanti segnalano, non quanti sbagliano.

// ESEMPIO

> Due oggetti e-mail a confronto per misurare quale genera più segnalazioni.

```
root@hacklab:~/lezione-08/concetto-8 $
```

LEZIONE 08 / CONCETTO 8/10

[Difesa]

Voice cloning e frodi BEC

// SPIEGAZIONE

Con pochi secondi di audio si clona una voce convincente; unita a una e-mail compromessa alimenta frodi del CEO difficili da smascherare in tempo reale. La difesa è procedurale: verifica fuori banda per ogni richiesta economica anomala.

// ESEMPIO

> Telefonata con voce clonata più e-mail: solo la richiamata al numero noto svela la frode.

```
root@hacklab:~/lezione-08/concetto-9 $
```

LEZIONE 08 / CONCETTO 9/10

[Difesa]

Autenticazione e-mail e sandbox

// SPIEGAZIONE

SPF dichiara i server autorizzati, DKIM firma il messaggio, DMARC dice cosa fare se i controlli falliscono: insieme riducono lo spoofing del dominio. Il sandboxing degli allegati fa detonare i file sospetti in ambiente isolato prima della consegna.

// ESEMPIO

> Un allegato sconosciuto viene eseguito in sandbox e bloccato prima di arrivare all'utente.

```
root@hacklab:~/lezione-08/concetto-10 $
```

LEZIONE 08 / CONCETTO 10/10

[Difesa]

Cultura di segnalazione e verifica

// SPIEGAZIONE

La difesa più resiliente e umana: persone che segnalano senza timore e verificano le richieste anomale su un canale diverso. Un pulsante 'segnala phishing' e la regola della verifica fuori banda valgono più di molti controlli tecnici.

// ESEMPIO

> Prima di pagare una fattura 'urgente' si richiama il fornitore al numero già in rubrica.

```
root@hacklab:~/lezione-08/strumenti $
```

LEZIONE 08 / STRUMENTI

Strumenti della lezione

// TOOLKIT

SET

Gophish

Evilginx

King Phisher

Zphisher

// 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-08/lab-1 $
```

LEZIONE 08 / LABORATORIO 1

Laboratorio 1

\$ Campagna di phishing simulata (Gophish)

// PROCEDURA

[1] Allestisci una campagna Gophish verso account di test e misura le metriche

[!] Verifica: Quali leve psicologiche rendono efficace un pretesto?

```
root@hacklab:~/lezione-08/lab-2 $
```

LEZIONE 08 / LABORATORIO 2

Laboratorio 2

\$ Riconoscere un deepfake (procedure di verifica)

// PROCEDURA

[1] Analizza un esempio di deepfake e definisci procedure di verifica (callback)

[!] Verifica: Come si mitiga una frode deepfake in azienda?

```
root@hacklab:~/lezione-08/caso-di-studio $
```

LEZIONE 08 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Frode deepfake di Arup (Hong Kong, 2024): circa 25 milioni di dollari trasferiti fraudolentemente.

// 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-08/etica $
```

LEZIONE 08 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Coinvolge persone reali: consenso dell'organizzazione, risultati anonimizzati, nessun intento lesivo.

```
root@hacklab:~/lezione-08/ricapitolazione $
```

LEZIONE 08 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > I principi psicologici dell'inganno
- > Campagne di phishing autorizzate
- > Deepfake e voice cloning
- > Contromisure tecniche e umane
- > Un piano di campagna e di formazione

```
root@hacklab:~/lezione-08/verifica $
```

LEZIONE 08 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Quali leve psicologiche rendono efficace un pretesto?
- ? Come si mitiga una frode deepfake in azienda?
- ? Perché i risultati individuali vanno anonimizzati?

// VALUTAZIONE

Progetto di campagna (pretesto, metriche, piano formativo).

// LETTURE

Hadnagy, Social Engineering; linee guida DMARC/SPF/DKIM.

lezione 08 completata

\$ next

Social Engineering

[!] 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

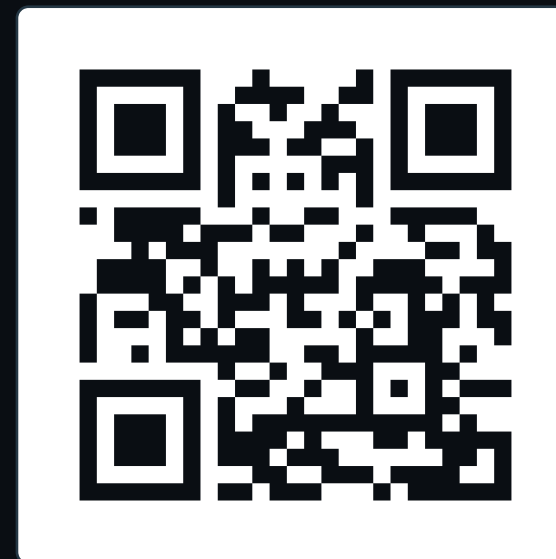


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.