

```
root@hacklab:~/parte-02/lezione-22
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE II

LEZIONE 22

Physical Security e Red Team a perimetro completo

Sicurezza fisica e operazioni red team multi-vettore, dove il rischio legale e personale è massimo.

docente **Vincenzo Calabro** fase Specializzazione: sicurezza fisica e red team

```
root@hacklab:~/lezione-22/agenda $
```

LEZIONE 22 / AGENDA

In questa lezione

// PERCORSO

- > Controlli fisici e debolezze
- > Badge cloning e intrusione fisica
- > Drop di dispositivi
- > Catena fisica-logica
- > OPSEC, RoE e safety

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

```
root@hacklab:~/lezione-22/obiettivi $
```

LEZIONE 22 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – superfici fisiche e integrazione con le logiche
- > Applicare – intrusione fisica simulata in lab
- > Analizzare – operazioni red team multi-vettore
- > Valutare – OPSEC, rischi e contromisure
- > Creare – un piano operativo red team completo

```
root@hacklab:~/lezione-22/inquadramento $
```

LEZIONE 22 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Un avversario reale non si ferma al firewall: unisce vettore fisico e logico. La lezione tratta intrusione fisica, OPSEC e un'operazione red team end-to-end, con safety e regole d'ingaggio ferree.

// PERCHE CONTA

Sicurezza fisica e operazioni red team multi-vettore, dove il rischio legale e personale e massimo.

```
root@hacklab:~/lezione-22/mappa-insieme $
```

LEZIONE 22 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

01 Controlli di sicurezza fisica

02 Tecniche di intrusione fisica

03 Drop di dispositivi

04 Dalla fisica al logico

05 OPSEC, safety e autorizzazioni

APPROFONDIMENTI

06 Serrature, sorveglianza e barriere

07 Clonazione badge e lock picking

08 Implant e rogue device

09 Operazione red team end-to-end

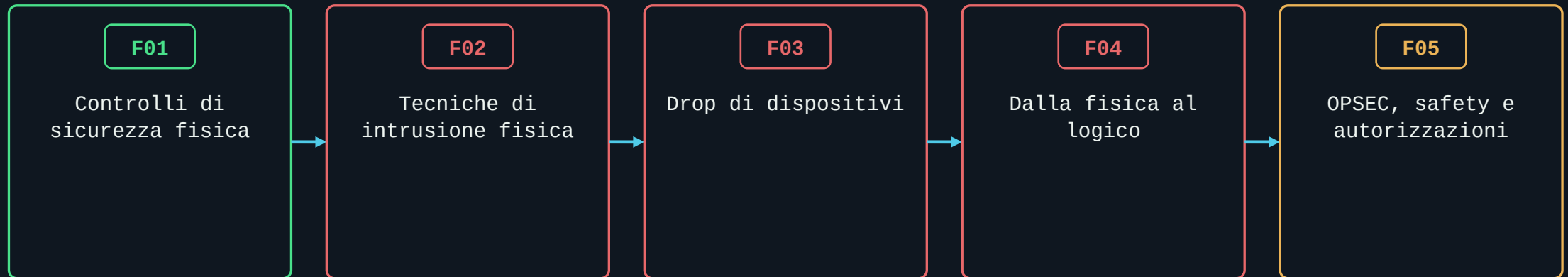
10 Autorizzazione e confronto col blue team

```
root@hacklab:~/lezione-22/flusso-1 $
```

LEZIONE 22 / 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-22/concetto-1 $
```

LEZIONE 22 / CONCETTO 1/10

[Difesa]

Controlli di sicurezza fisica

// SPIEGAZIONE

La sicurezza fisica e il primo perimetro: badge, serrature, videosorveglianza e barriere proteggono l'accesso. Un avversario reale le valuta come qualsiasi altra difesa, cercando l'anello debole tra tecnologia e procedure.

// ESEMPIO

> Una porta sul retro lasciata aperta per comodità vanifica i tornelli dell'ingresso principale.

```
root@hacklab:~/lezione-22/concetto-2 $
```

LEZIONE 22 / CONCETTO 2/10

[Attacco/tecnica]

Tecniche di intrusione fisica

// SPIEGAZIONE

L'ingresso non autorizzato combina tecnica e inganno: clonazione di badge RFID/NFC, lock picking, tailgating alle spalle di un dipendente, pretexting per farsi aprire. Spesso la via più semplice è la persona, non la serratura.

// ESEMPIO

> Un lettore nascosto clona il badge RFID di un dipendente a pochi centimetri.

```
root@hacklab:~/lezione-22/concetto-3 $
```

LEZIONE 22 / CONCETTO 3/10

[Attacco/tecnica]

Drop di dispositivi

// SPIEGAZIONE

Lasciare o installare dispositivi crea un ponte verso la rete interna: una Rubber Ducky che digita comandi come una tastiera, un implant di rete nascosto. Bastano pochi secondi di accesso fisico per piazzarli.

// ESEMPIO

> Una Rubber Ducky inserita in un PC sbloccato apre una reverse shell in pochi secondi.

```
root@hacklab:~/lezione-22/concetto-4 $
```

LEZIONE 22 / CONCETTO 4/10

[Attacco/tecnica]

Dalla fisica al logico

// SPIEGAZIONE

Un'operazione completa parte dall'accesso fisico e lo trasforma in accesso logico: entrare, collegare un implant, ottenere un punto d'appoggio in rete e proseguire come in un pentest interno. Fisico e logico sono un'unica catena.

// ESEMPIO

> Accesso a una sala riunioni, implant sulla presa di rete, poi movimento laterale interno.

```
root@hacklab:~/lezione-22/concetto-5 $
```

LEZIONE 22 / CONCETTO 5/10

[Norme & metodo]

OPSEC, safety e autorizzazioni

// SPIEGAZIONE

Il red team fisico richiede regole ferree: OPSEC per non farsi scoprire, RoE chiare, attenzione alla safety delle persone e una get-out-of-jail letter che autorizza l'operazione. Il confronto col blue team chiude il ciclo migliorativo.

// ESEMPIO

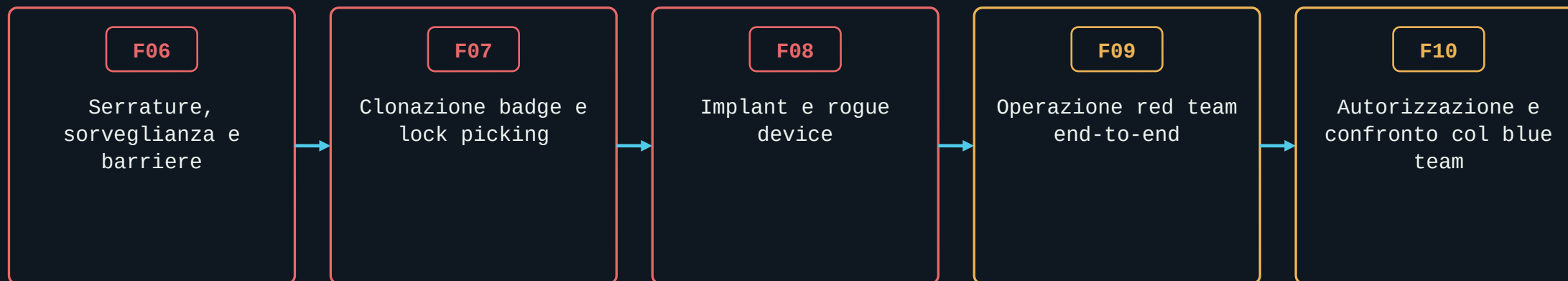
> La get-out-of-jail letter, firmata e al seguito, previene guai se si viene fermati.

```
root@hacklab:~/lezione-22/flusso-2 $
```

LEZIONE 22 / 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-22/concetto-6 $
```

LEZIONE 22 / CONCETTO 6/10

[Attacco/tecnica]

Serrature, sorveglianza e barriere

// SPIEGAZIONE

Ogni controllo fisico ha limiti noti: serrature apribili, telecamere con angoli ciechi, barriere aggirabili. Valutarli significa capire non solo se esistono, ma se sono davvero efficaci e monitorati nella pratica quotidiana.

// ESEMPIO

> Una telecamera che nessuno guarda in tempo reale documenta l'intrusione ma non la ferma.

```
root@hacklab:~/lezione-22/concetto-7 $
```

LEZIONE 22 / CONCETTO 7/10

[Attacco/tecnica]

Clonazione badge e lock picking

// SPIEGAZIONE

Molti badge usano tecnologie legacy facilmente clonabili a distanza ravvicinata; serrature comuni cedono al picking in tempi brevi. Badge cifrati e serrature di qualita, con controlli procedurali, alzano molto l'asticella.

// ESEMPIO

> Badge di vecchia generazione clonato da un dispositivo tascabile in corridoio.

```
root@hacklab:~/lezione-22/concetto-8 $
```

LEZIONE 22 / CONCETTO 8/10

[Attacco/tecnica]

Implant e rogue device

// SPIEGAZIONE

Dispositivi malevoli imitano periferiche innocue: una chiavetta che e una tastiera, un adattatore di rete che e un punto d'appoggio remoto. Il controllo delle porte e l'ispezione fisica periodica sono le contromisure principali.

// ESEMPIO

> Un rogue device dietro una stampante fornisce accesso remoto alla rete interna.

```
root@hacklab:~/lezione-22/concetto-9 $
```

LEZIONE 22 / CONCETTO 9/10

[Norme & metodo]

Operazione red team end-to-end

// SPIEGAZIONE

Un ingaggio completo unisce ricognizione, intrusione fisica, appoggio logico e obiettivi concordati, simulando un avversario reale su piu vettori. La pianificazione e la safety contano quanto la tecnica.

// ESEMPIO

> Obiettivo: raggiungere la sala server e dimostrare accesso ai dati partendo dall'esterno.

```
root@hacklab:~/lezione-22/concetto-10 $
```

LEZIONE 22 / CONCETTO 10/10

[Norme & metodo]

Autorizzazione e confronto col blue team

// SPIEGAZIONE

La get-out-of-jail letter rende lecita e tracciabile l'operazione, indicando contatti e limiti. Il debrief col blue team trasforma l'intrusione in apprendimento: cosa è stato notato, cosa no e come migliorare rilevamento e risposta.

// ESEMPIO

> Il blue team scopre di non avere alert sulle porte di rete nelle sale comuni.

```
root@hacklab:~/lezione-22/strumenti $
```

LEZIONE 22 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Proxmark3

Flipper Zero

Rubber Ducky

implant

OSINT

// 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-22/lab-1 $
```

LEZIONE 22 / LABORATORIO 1

Laboratorio 1

\$ RFID cloning controllato (badge di test)

// PROCEDURA

[1] Dimostra in laboratorio la clonazione di un badge RFID di test

[!] Verifica: Quali tecnologie di badge sono piu resistenti?

```
root@hacklab:~/lezione-22/lab-2 $
```

LEZIONE 22 / LABORATORIO 2

Laboratorio 2

\$ Piano red team multi-vettore (RoE + OPSEC)

// PROCEDURA

[1] Redigi un'operazione red team multi-vettore con RoE

[2] OPSEC e piano di safety

[!] Verifica: Perché la get-out-of-jail letter è indispensabile?

```
root@hacklab:~/lezione-22/caso-di-studio $
```

LEZIONE 22 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Ingaggio red team fisico autorizzato: lezioni su OPSEC e gestione del rischio.

// 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-22/etica $
```

LEZIONE 22 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Rischio legale e personale altissimo: solo con autorizzazione scritta, RoE dettagliate e lettera da esibire; mai improvvisare.

```
root@hacklab:~/lezione-22/ricapitolazione $
```

LEZIONE 22 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Superfici fisiche e integrazione con le logiche
- > Intrusione fisica simulata in lab
- > Operazioni red team multi-vettore
- > OPSEC, rischi e contromisure
- > Un piano operativo red team completo

```
root@hacklab:~/lezione-22/verifica $
```

LEZIONE 22 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Quali tecnologie di badge sono piu resistenti?
- ? Perche la get-out-of-jail letter e indispensabile?
- ? Come si integra il vettore fisico con quello logico?

// VALUTAZIONE

Piano operativo red team con rubrica (legalita e safety).

// LETTURE

Red Team Field Manual; materiali su physical red teaming.

lezione 22 completata

\$ next

Physical Security e Red Team a perimetro completo

[!] 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

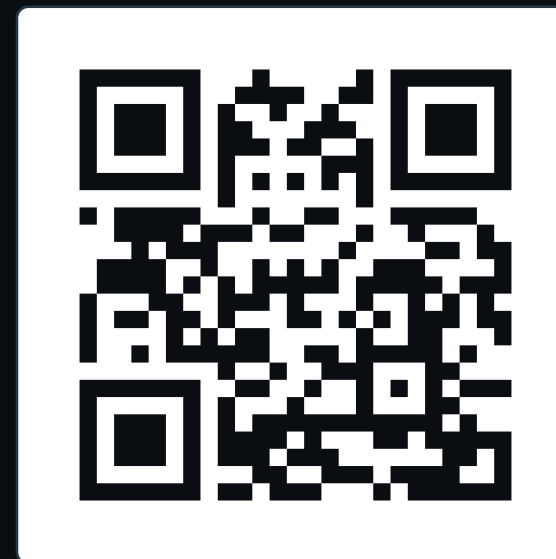


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.