

```
root@hacklab:~/parte-01/lezione-11
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 11

Cloud, Container e IoT Security

Superfici d'attacco emergenti: cloud, container e dispositivi connessi.

docente **Vincenzo Calabro** fase Superfici emergenti: Cloud, Container e IoT

```
root@hacklab:~/lezione-11/agenda $
```

LEZIONE 11 / AGENDA

In questa lezione

// PERCORSO

- > Responsabilit  condivisa
- > Misconfigurazioni cloud e IMDS/SSRF
- > Sicurezza di container e Kubernetes
- > Sicurezza IoT
- > Rilevamento e posture con IA

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

```
root@hacklab:~/lezione-11/obiettivi $
```

LEZIONE 11 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – superfici di cloud, container e IoT
- > Applicare – riconoscimento di misconfigurazioni
- > Analizzare – SSRF verso i metadata service
- > Valutare – contromisure e segmentazione
- > Creare – una relazione con priorit  di rischio

```
root@hacklab:~/lezione-11/inquadramento $
```

LEZIONE 11 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Il perimetro si è dissolto in cloud, container e dispositivi: cambiano modelli di responsabilità, superfici e strumenti. Vediamo misconfigurazioni tipiche, isolamento e come adattare il metodo offensivo a questi ambienti.

// PERCHÉ CONTA

Superfici d'attacco emergenti: cloud, container e dispositivi connessi.

```
root@hacklab:~/lezione-11/mappa-insieme $
```

LEZIONE 11 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Responsabilita condivisa nel cloud
- 02 Superfici d'attacco cloud
- 03 Sicurezza di container e Kubernetes
- 04 Sicurezza IoT
- 05 Casi reali e analisi di posture

APPROFONDIMENTI

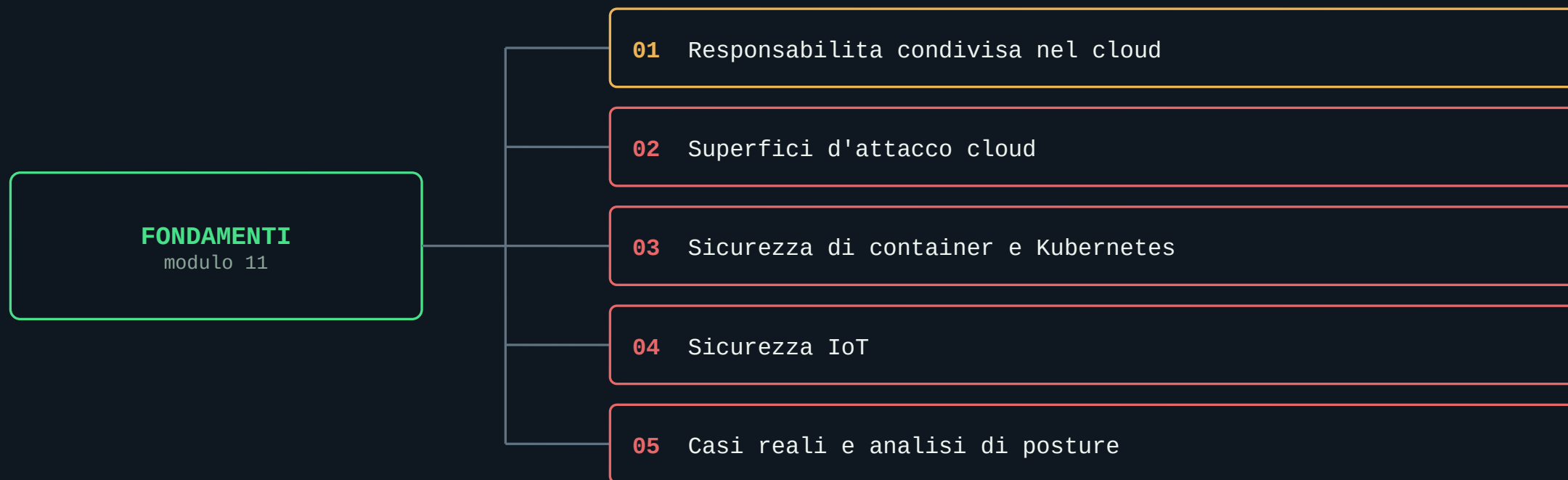
- 06 Storage, IAM e chiavi esposte
- 07 Container escape e segreti
- 08 RBAC e network policy in Kubernetes
- 09 Firmware, MQTT e update OTA
- 10 Capital One e Mirai a confronto

```
root@hacklab:~/lezione-11/mappa-1 $
```

LEZIONE 11 / MAPPA // FONDAMENTI

Mappa dei concetti – Fondamenti

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



```
root@hacklab:~/lezione-11/concetto-1 $
```

LEZIONE 11 / CONCETTO 1/10

[Norme & metodo]

Responsabilita condivisa nel cloud

// SPIEGAZIONE

Nel cloud la sicurezza e divisa: il provider protegge l'infrastruttura, il cliente configurazioni, dati e accessi. La maggior parte delle violazioni cloud nasce da errori del cliente, non del provider: tracciare quel confine orienta tutto il resto del lavoro.

// ESEMPIO

> Un bucket di storage lasciato pubblico e responsabilita del cliente, non del provider.

```
root@hacklab:~/lezione-11/concetto-2 $
```

LEZIONE 11 / CONCETTO 2/10

[Attacco/tecnica]

Superfici d'attacco cloud

// SPIEGAZIONE

Gli errori ricorrenti sono storage esposti, policy IAM troppo permissive, chiavi nel codice e logging assente. L'Instance Metadata Service, raggiunto via SSRF, può cedere credenziali temporanee all'attaccante.

// ESEMPIO

> Una SSRF che interroga l'IMDS recupera i token IAM della macchina.

```
root@hacklab:~/lezione-11/concetto-3 $
```

LEZIONE 11 / CONCETTO 3/10

[Attacco/tecnica]

Sicurezza di container e Kubernetes

// SPIEGAZIONE

Le immagini possono contenere vulnerabilità e segreti; un container escape porta dall'isolamento all'host. In Kubernetes contano RBAC, network policy e la protezione dell'API server, spesso bersaglio diretto degli attacchi.

// ESEMPIO

> Un container privilegiato o un segreto nell'immagine apre la strada all'escape verso il nodo.

```
root@hacklab:~/lezione-11/concetto-4 $
```

LEZIONE 11 / CONCETTO 4/10

[Attacco/tecnica]

Sicurezza IoT

// SPIEGAZIONE

I dispositivi IoT soffrono di credenziali di default, firmware non aggiornato e protocolli come MQTT spesso senza autenticazione. La scala e l'eterogeneità li rendono un bersaglio ideale per botnet e punti d'ingresso in rete.

// ESEMPIO

> Credenziali admin/admin di default su migliaia di telecamere esposte in Internet.

```
root@hacklab:~/lezione-11/concetto-5 $
```

LEZIONE 11 / CONCETTO 5/10

[Attacco/tecnica]

Casi reali e analisi di posture

// SPIEGAZIONE

Capital One nel 2019 nacque da una SSRF verso l'IMDS in cloud; Mirai arruolo dispositivi IoT con credenziali di default in una botnet devastante. L'IA aiuta oggi ad analizzare la posture e segnalare misconfigurazioni su larga scala.

// ESEMPIO

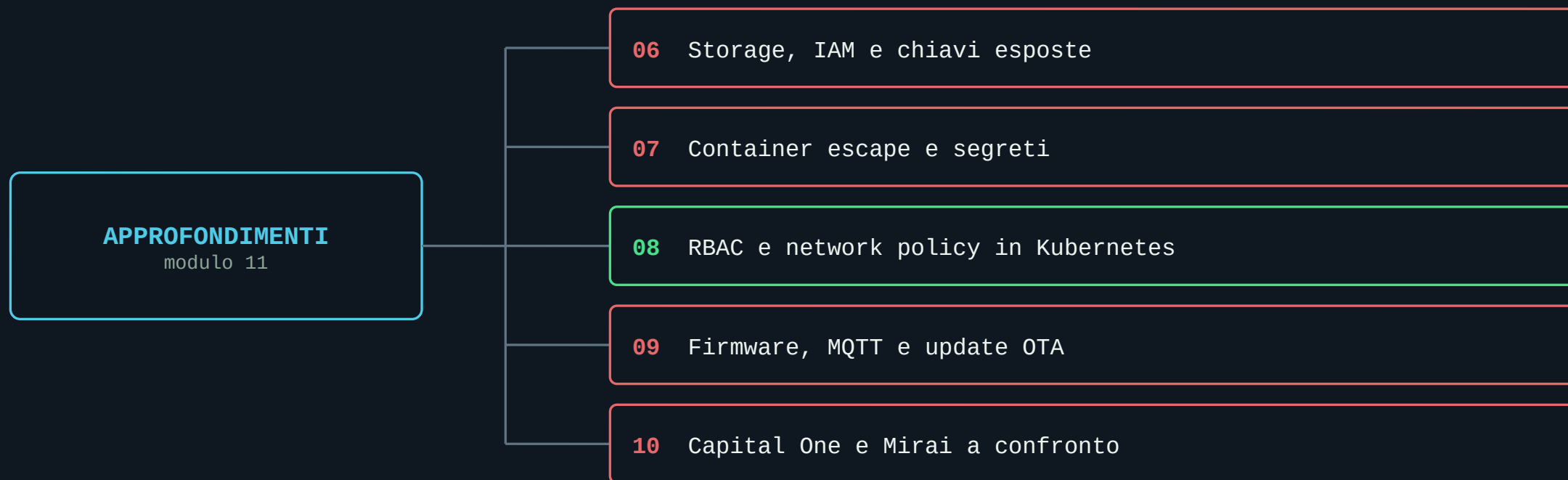
> Caso Capital One: SSRF piu IAM permissivo portano all'esfiltrazione di dati di milioni di clienti.

```
root@hacklab:~/lezione-11/mappa-2 $
```

LEZIONE 11 / MAPPA // APPROFONDIMENTI

Mappa dei concetti – Approfondimenti

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



```
root@hacklab:~/lezione-11/concetto-6 $
```

LEZIONE 11 / CONCETTO 6/10

[Attacco/tecnica]

Storage, IAM e chiavi esposte

// SPIEGAZIONE

Bucket pubblici, ruoli con permessi eccessivi e chiavi committate nei repository sono tra le cause più frequenti di breccia cloud. Il principio del minimo privilegio e la scansione dei segreti riducono drasticamente il rischio.

// ESEMPIO

> Una chiave AWS trovata in un repo pubblico concede accesso all'intero account.

```
root@hacklab:~/lezione-11/concetto-7 $
```

LEZIONE 11 / CONCETTO 7/10

[Attacco/tecnica]

Container escape e segreti

// SPIEGAZIONE

Container privilegiati, socket Docker montati e capability eccessive permettono di evadere verso l'host. I segreti incorporati nelle immagini restano negli strati anche se cancellati dopo: vanno gestiti fuori dall'immagine.

// ESEMPIO

```
$ docker history image (rivela un segreto rimasto in uno strato precedente)
```

```
root@hacklab:~/lezione-11/concetto-8 $
```

LEZIONE 11 / CONCETTO 8/10

[Difesa]

RBAC e network policy in Kubernetes

// SPIEGAZIONE

Un RBAC permissivo permette a un pod compromesso di controllare il cluster; senza network policy ogni pod parla con ogni altro. Minimo privilegio e segmentazione interna contengono un'eventuale compromissione.

// ESEMPIO

> Un service account con permessi cluster-admin trasforma un pod violato in controllo totale.

```
root@hacklab:~/lezione-11/concetto-9 $
```

LEZIONE 11 / CONCETTO 9/10

[Attacco/tecnica]

Firmware, MQTT e update OTA

// SPIEGAZIONE

Analizzare il firmware rivela credenziali e servizi nascosti; MQTT senza autenticazione espone i messaggi; un aggiornamento OTA non firmato permette di installare firmware malevolo. Se la catena di fiducia del firmware si rompe, cade tutta la sicurezza del dispositivo.

// ESEMPIO

> Estrarre il firmware e trovarvi una password hardcoded o un servizio di debug aperto.

```
root@hacklab:~/lezione-11/concetto-10 $
```

LEZIONE 11 / CONCETTO 10/10

[Attacco/tecnica]

Capital One e Mirai a confronto

// SPIEGAZIONE

Due lezioni opposte: Capital One mostra come un errore di configurazione cloud esfiltri dati sensibili; Mirai come dispositivi banali e mal protetti diventino un'arma di massa. Entrambi nascono da basi trascurate, non da exploit sofisticati.

// ESEMPIO

> Mirai scandiva Internet cercando credenziali di default per arruolare dispositivi.

```
root@hacklab:~/lezione-11/strumenti $
```

LEZIONE 11 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Nmap

Nuclei

Shodan

scanner IaC

CSPM

// 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-11/lab-1 $
```

LEZIONE 11 / LABORATORIO 1

Laboratorio 1

\$ Misconfigurazioni cloud (storage + SSRF->IMDS)

// PROCEDURA

[1] Individua uno storage mal configurato e simula una SSRF verso l'IMDS in lab

[!] Verifica: Perché l'IMDS è un bersaglio critico?

```
root@hacklab:~/lezione-11/lab-2 $
```

LEZIONE 11 / LABORATORIO 2

Laboratorio 2

\$ Hardening di un container (segreti, network policy)

// PROCEDURA

[1] Rileva segreti e privilegi eccessivi in un'immagine e applica una network policy

[!] Verifica: Come la segmentazione limita un container escape?

```
root@hacklab:~/lezione-11/caso-di-studio $
```

LEZIONE 11 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Capital One (2019): SSRF verso il metadata service AWS e WAF mal configurato.

// 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-11/etica $
```

LEZIONE 11 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Ambienti spesso multi-tenant: solo risorse di proprietà, nel rispetto delle policy del provider.

```
root@hacklab:~/lezione-11/ricapitolazione $
```

LEZIONE 11 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Superfici di cloud, container e IoT
- > Riconoscimento di misconfigurazioni
- > SSRF verso i metadata service
- > Contromisure e segmentazione
- > Una relazione con priorit  di rischio

```
root@hacklab:~/lezione-11/verifica $
```

LEZIONE 11 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Perché l'IMDS è un bersaglio critico in cloud?
- ? Come la segmentazione limita un container escape?
- ? Perché i test vanno limitati alle proprie risorse?

// VALUTAZIONE

Relazione su misconfigurazioni con priorità di rischio.

// LETTURE

OWASP Cloud-Native/Container Security; doc. provider (IMDS).

lezione 11 completata

\$ next

Cloud, Container e IoT Security

[!] 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

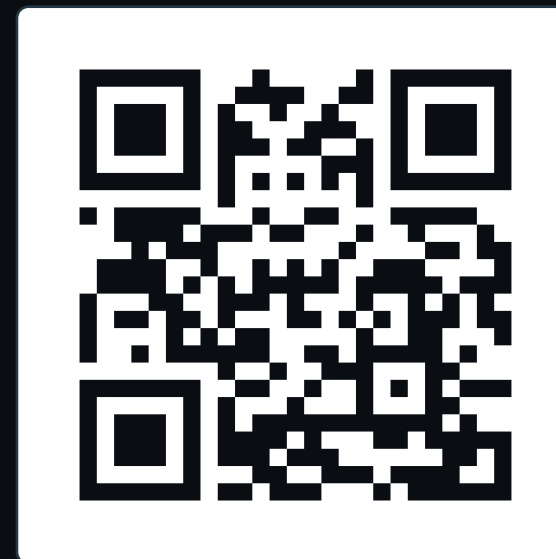


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.