

```
root@hacklab:~/parte-02/lezione-20
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE II

LEZIONE 20

Active Directory avanzato e identità cloud

Compromissione e difesa dell'identità on-premise e cloud.

docente **Vincenzo Calabro** fase Specializzazione avanzata: Active Directory e cloud

```
root@hacklab:~/lezione-20/agenda $
```

LEZIONE 20 / AGENDA

In questa lezione

// PERCORSO

- > Kerberos avanzato
- > AD Certificate Services
- > Identita ibrida e cloud
- > Attacchi ibridi
- > Difese dell'identita

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

```
root@hacklab:~/lezione-20/obiettivi $
```

LEZIONE 20 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – AD e identità ibrida/cloud
- > Applicare – tecniche avanzate su dominio e tenant
- > Analizzare – percorsi verso Domain/Global Admin
- > Valutare – le difese e la loro efficacia
- > Creare – un piano di hardening dell'identità

```
root@hacklab:~/lezione-20/inquadramento $
```

LEZIONE 20 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

L'identità e il nuovo perimetro: Active Directory e le identità cloud sono bersagli privilegiati. La lezione analizza percorsi di attacco, abusi di delega e difese su ambienti ibridi.

// PERCHÉ CONTA

Compromissione e difesa dell'identità on-premise e cloud.

```
root@hacklab:~/lezione-20/mappa-insieme $
```

LEZIONE 20 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Kerberos avanzato
- 02 AD CS e abuso di ACL
- 03 Identita cloud e attacchi ibridi
- 04 Difese di Active Directory
- 05 Persistenza e bonifica

APPROFONDIMENTI

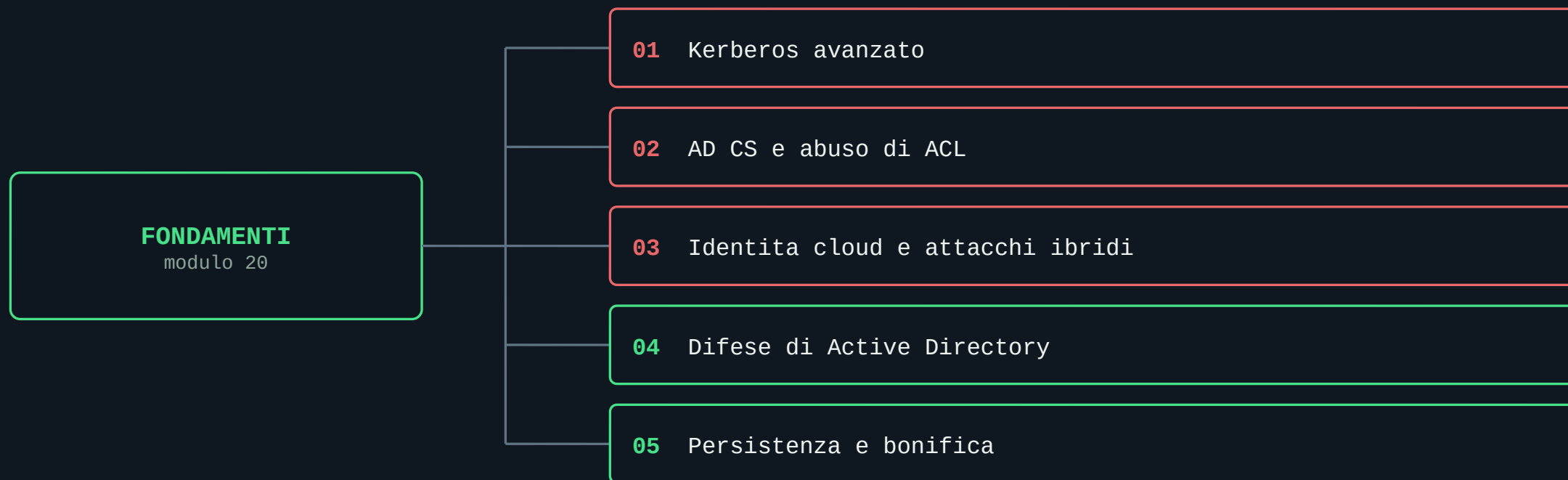
- 06 Golden ticket, silver ticket e delega
- 07 Percorsi ESC e ACL
- 08 Entra ID, federazione e token
- 09 Pass-the-PRT e consent phishing
- 10 Modello a tier e account protetti

```
root@hacklab:~/lezione-20/mappa-1 $
```

LEZIONE 20 / MAPPA // FONDAMENTI

Mappa dei concetti – Fondamenti

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



```
root@hacklab:~/lezione-20/concetto-1 $
```

LEZIONE 20 / CONCETTO 1/10

[Attacco/tecnica]

Kerberos avanzato

// SPIEGAZIONE

Kerberos autentica con ticket: chi compromette la chiave krbtgt forgia un golden ticket valido per tutto il dominio, con un ticket di servizio un silver ticket mirato. Le deleghe mal configurate permettono di impersonare altri utenti.

// ESEMPIO

> Un golden ticket, forgiato dall'hash di krbtgt, garantisce accesso persistente da Domain Admin.

```
root@hacklab:~/lezione-20/concetto-2 $
```

LEZIONE 20 / CONCETTO 2/10

[Attacco/tecnica]

AD CS e abuso di ACL

// SPIEGAZIONE

I servizi di certificati di Active Directory, se mal configurati, abilitano scalate note come ESC1-ESC8, fino a ottenere certificati per impersonare amministratori. Allo stesso modo, ACL permissive su oggetti del dominio creano percorsi di abuso.

// ESEMPIO

> Un template AD CS che lascia indicare l'utente (ESC1) permette di farsi un certificato da admin.

```
root@hacklab:~/lezione-20/concetto-3 $
```

LEZIONE 20 / CONCETTO 3/10

[Attacco/tecnica]

Identita cloud e attacchi ibridi

// SPIEGAZIONE

Con Entra ID l'identita si estende al cloud: il Primary Refresh Token puo essere rubato (pass-the-PRT) per impersonare l'utente, mentre il consent phishing induce a concedere permessi a un'app malevola. L'ambiente ibrido amplia la superficie.

// ESEMPIO

> Consent phishing: l'utente autorizza un'app OAuth che ottiene accesso persistente alla casella.

```
root@hacklab:~/lezione-20/concetto-4 $
```

LEZIONE 20 / CONCETTO 4/10

[Difesa]

Difese di Active Directory

// SPIEGAZIONE

La difesa si basa sulla separazione dei privilegi: modello a tier per isolare gli amministratori, LAPS per password locali uniche, PAW come postazioni dedicate e amministrative, gruppo Protected Users per irrobustire gli account critici.

// ESEMPIO

> Con LAPS ogni macchina ha una password admin locale diversa, bloccando il movimento laterale.

```
root@hacklab:~/lezione-20/concetto-5 $
```

LEZIONE 20 / CONCETTO 5/10

[Difesa]

Persistenza e bonifica

// SPIEGAZIONE

Un attaccante consolida l'accesso con ticket, certificati, backdoor su ACL o app OAuth nel cloud. La bonifica richiede di individuare e rimuovere ogni appiglio, a volte fino a ruotare krbtgt due volte: ripulire a meta lascia la porta aperta.

// ESEMPIO

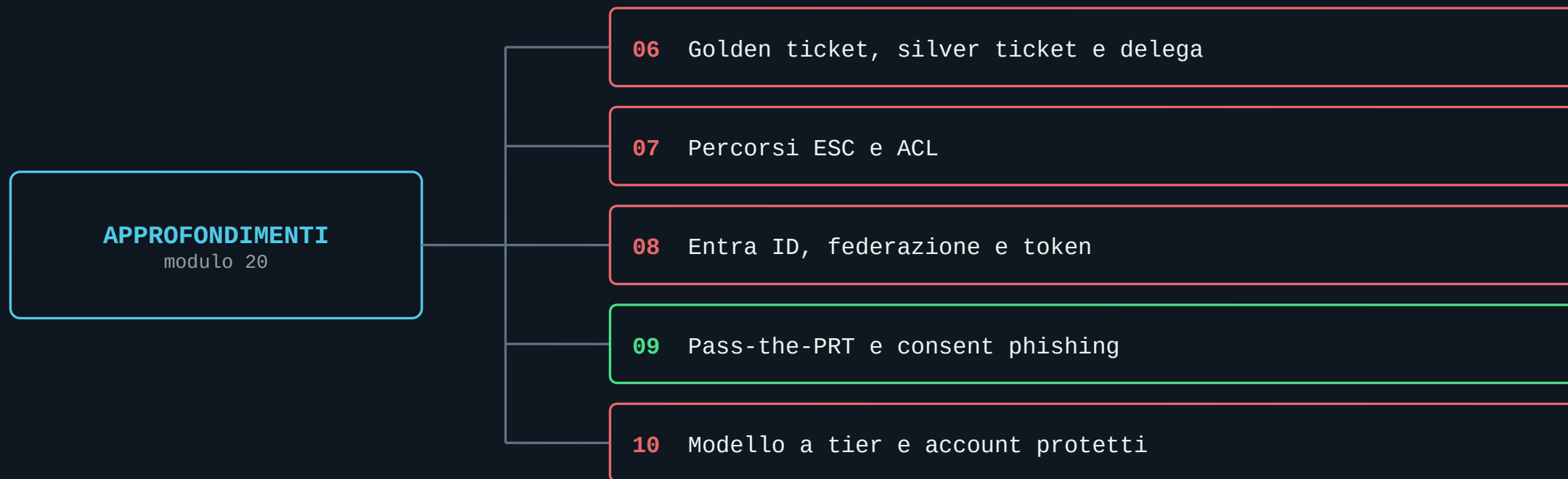
> Dopo una compromissione si ruota krbtgt due volte per invalidare i golden ticket.

```
root@hacklab:~/lezione-20/mappa-2 $
```

LEZIONE 20 / MAPPA // APPROFONDIMENTI

Mappa dei concetti – Approfondimenti

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



```
root@hacklab:~/lezione-20/concetto-6 $
```

LEZIONE 20 / CONCETTO 6/10

[Attacco/tecnica]

Golden ticket, silver ticket e delega

// SPIEGAZIONE

Il golden ticket falsifica il TGT dominando l'autenticazione, il silver ticket un singolo servizio; le deleghe non vincolate permettono a un server compromesso di riusare i ticket altrui. Sono abusi del cuore di Kerberos.

// ESEMPIO

> La delega non vincolata su un server consente di impersonare chi vi si autentica.

```
root@hacklab:~/lezione-20/concetto-7 $
```

LEZIONE 20 / CONCETTO 7/10

[Attacco/tecnica]

Percorsi ESC e ACL

// SPIEGAZIONE

Le scalate ESC sfruttano template di certificato e configurazioni AD CS troppo permissive; l'abuso di ACL usa diritti come WriteDACL o GenericAll per prendere il controllo di oggetti e account. BloodHound li evidenzia come cammini di attacco.

// ESEMPIO

> Il diritto GenericAll su un gruppo privilegiato permette di aggiungervisi da soli.

```
root@hacklab:~/lezione-20/concetto-8 $
```

LEZIONE 20 / CONCETTO 8/10

[Attacco/tecnica]

Entra ID, federazione e token

// SPIEGAZIONE

Nel cloud contano i token: access, refresh e PRT. La federazione tra on-premise e cloud, se mal protetta, permette di forgiare asserzioni e saltare l'autenticazione. Chi controlla i token e le chiavi di firma controlla l'identità, e vanno protetti di conseguenza.

// ESEMPIO

> Un attacco golden SAML forgia asserzioni valide impersonando qualsiasi utente federato.

```
root@hacklab:~/lezione-20/concetto-9 $
```

LEZIONE 20 / CONCETTO 9/10

[Difesa]

Pass-the-PRT e consent phishing

// SPIEGAZIONE

Il PRT è la chiave dell'identità su un dispositivo: rubarlo permette di autenticarsi come l'utente senza password né MFA. Il consent phishing non ruba credenziali ma ottiene permessi persistenti su un'app, difficili da notare.

// ESEMPIO

> Un'app malevola approvata dall'utente legge e-mail e file senza bisogno della password.

```
root@hacklab:~/lezione-20/concetto-10 $
```

LEZIONE 20 / CONCETTO 10/10

[Attacco/tecnica]

Modello a tier e account protetti

// SPIEGAZIONE

Separare gli amministratori per livelli (tier) impedisce che la compromissione di una workstation arrivi al dominio; PAW, LAPS e Protected Users riducono l'esposizione delle credenziali privilegiate. E l'architettura che spezza i percorsi di escalation.

// ESEMPIO

> Un admin di dominio non accede mai da una workstation utente, grazie al modello a tier.

```
root@hacklab:~/lezione-20/strumenti $
```

LEZIONE 20 / STRUMENTI

Strumenti della lezione

// TOOLKIT

BloodHound

SharpHound

Rubeus

Certify

Impacket

ROADtools

AADInternals

// 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-20/lab-1 $
```

LEZIONE 20 / LABORATORIO 1

Laboratorio 1

\$ Attacco AD CS (ESC1)

// PROCEDURA

[1] Sfrutta una misconfigurazione AD CS (ESC1) per ottenere privilegi

[!] Verifica: Perché i template certificati mal configurati sono critici?

```
root@hacklab:~/lezione-20/lab-2 $
```

LEZIONE 20 / LABORATORIO 2

Laboratorio 2

\$ Percorso ibrido verso il cloud

// PROCEDURA

[1] Traccia e sfrutta un percorso da AD on-prem verso il tenant cloud

[!] Verifica: Come si difende l'identita ibrida?

```
root@hacklab:~/lezione-20/caso-di-studio $
```

LEZIONE 20 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Compromissione di dominio reale tramite Kerberoasting / AD CS.

// 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-20/etica $
```

LEZIONE 20 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Solo domini/tenant di laboratorio o autorizzati; attenzione a persistenza e bonifica.

```
root@hacklab:~/lezione-20/ricapitolazione $
```

LEZIONE 20 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > AD e identità ibrida/cloud
- > Tecniche avanzate su dominio e tenant
- > Percorsi verso Domain/Global Admin
- > Le difese e la loro efficacia
- > Un piano di hardening dell'identità

```
root@hacklab:~/lezione-20/verifica $
```

LEZIONE 20 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Perché i template certificati mal configurati sono critici?
- ? Come si difende un'identità ibrida?
- ? Cos'è un golden ticket e come si rileva?

// VALUTAZIONE

Operazione AD/cloud documentata + piano di difesa.

// LETTURE

Doc. BloodHound; whitepaper AD CS (SpecterOps);
ATT&CK.

lezione 20 completata

\$ next

Active Directory avanzato e identità cloud

[!] 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

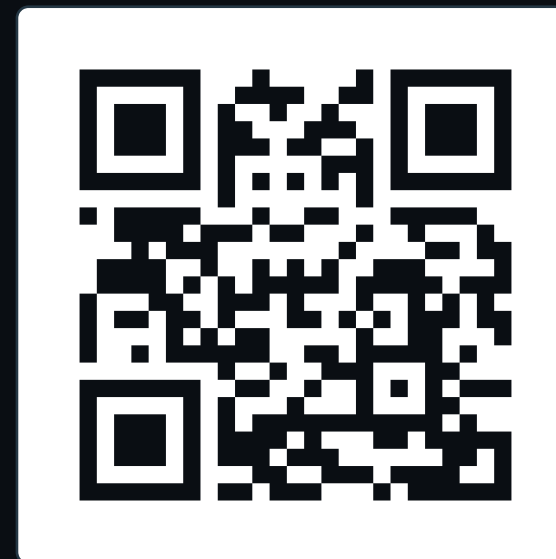


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.