

```
root@hacklab:~/parte-01/lezione-05
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 05

Password Attacks e Credential Access

Attacchi alle credenziali e relative difese.

docente **Vincenzo Calabro** fase Capacita trasversale: Credential Access

```
root@hacklab:~/lezione-05/agenda $
```

LEZIONE 05 / AGENDA

In questa lezione

// PERCORSO

- > Hashing, salting e formati
- > Attacchi a dizionario, brute force, mask
- > Cracking offline vs online
- > Credential access post-compromissione
- > Difese: MFA e policy

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

```
root@hacklab:~/lezione-05/obiettivi $
```

LEZIONE 05 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – meccanismi di hashing e autenticazione
- > Applicare – cracking online e offline in lab
- > Analizzare – robustezza di policy e formati di hash
- > Valutare – l'efficacia dell'MFA
- > Creare – raccomandazioni di hardening

```
root@hacklab:~/lezione-05/inquadramento $
```

LEZIONE 05 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Le credenziali restano la chiave piu ambita: capirne conservazione, hashing e debolezze e essenziale sia per attaccare sia per difendere. Vediamo cracking, spraying e furto di credenziali, e come le difese moderne cambiano l'equazione.

// PERCHE CONTA

Attacchi alle credenziali e relative difese.

```
root@hacklab:~/lezione-05/mappa-insieme $
```

LEZIONE 05 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Hashing, salting e stretching
- 02 Tecniche di cracking delle password
- 03 Attacchi offline e online
- 04 Furto di credenziali su Windows
- 05 MFA e policy secondo NIST 800-63B

APPROFONDIMENTI

- 06 Rainbow table e ruolo del salt
- 07 Spraying e credential stuffing
- 08 Dump SAM/LSASS e poisoning LLMNR
- 09 Wordlist mirate e analisi dei leak
- 10 Rilevare gli attacchi alle credenziali

```
root@hacklab:~/lezione-05/mappa-1 $
```

LEZIONE 05 / MAPPA // FONDAMENTI

Mappa dei concetti – Fondamenti

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



```
root@hacklab:~/lezione-05/concetto-1 $
```

LEZIONE 05 / CONCETTO 1/10

[Attacco/tecnica]

Hashing, salting e stretching

// SPIEGAZIONE

Le password non si conservano in chiaro ma come hash. Algoritmi veloci come MD5 o NTLM sono facili da attaccare in massa; il salt rende unico ogni hash e il key stretching (bcrypt, Argon2) lo rende lento da calcolare, ostacolando il cracking.

// ESEMPIO

> Argon2 e bcrypt impongono un costo per tentativo che rende il brute force molto più lento di MD5.

```
root@hacklab:~/lezione-05/concetto-2 $
```

LEZIONE 05 / CONCETTO 2/10

[Attacco/tecnica]

Tecniche di cracking delle password

// SPIEGAZIONE

Il cracking offline prova password contro un hash: per dizionario con liste di parole, per regole e mask con varianti e schemi comuni, o per brute force puro. Le rainbow table precalcolano hash per invertire rapidamente quelli non salati.

// ESEMPIO

```
$ hashcat -m 1000 -a 0 ntlm.txt rockyou.txt -r best64.rule
```

```
root@hacklab:~/lezione-05/concetto-3 $
```

LEZIONE 05 / CONCETTO 3/10

[Attacco/tecnica]

Attacchi offline e online

// SPIEGAZIONE

Gli attacchi offline lavorano su hash rubati senza limiti di tentativi; quelli online colpiscono i servizi e si scontrano con lockout e rate limiting. Il password spraying prova poche password su molti account, il credential stuffing riusa credenziali trapelate altrove.

// ESEMPIO

> Una sola password 'Autunno2025!' provata su mille account elude i lockout per utente.

```
root@hacklab:~/lezione-05/concetto-4 $
```

LEZIONE 05 / CONCETTO 4/10

[Attacco/tecnica]

Furto di credenziali su Windows

// SPIEGAZIONE

Su Windows le credenziali vivono nel database SAM e nel processo LSASS in memoria. Strumenti come Mimikatz le estraggono, mentre Responder avvelena le risposte di risoluzione nomi per catturare hash di autenticazione sulla rete locale.

// ESEMPIO

```
$ mimikatz: sekurlsa::logonpasswords
```

```
root@hacklab:~/lezione-05/concetto-5 $
```

LEZIONE 05 / CONCETTO 5/10

[Difesa]

MFA e policy secondo NIST 800-63B

// SPIEGAZIONE

La difesa migliore e non dipendere dalla sola password: l'MFA aggiunge un fattore indipendente. Le linee guida NIST SP 800-63B privilegiano lunghezza e controllo contro liste di password compromesse rispetto alla complessità forzata e ai cambi periodici.

// ESEMPIO

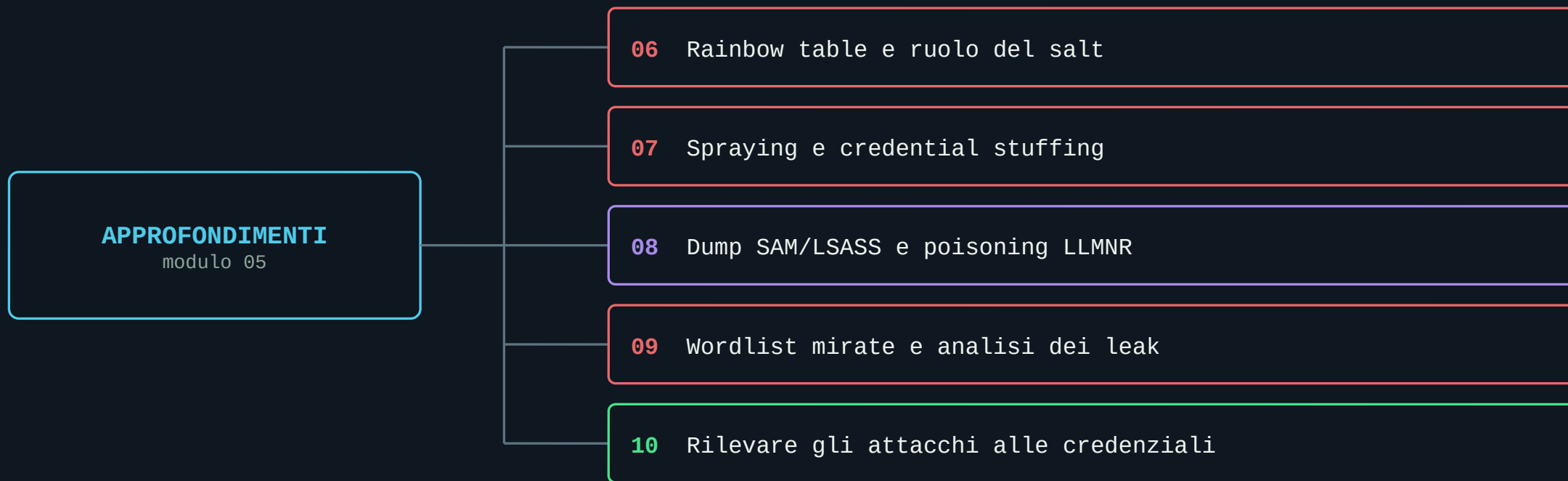
> Una passphrase lunga con MFA resiste a spraying e stuffing meglio di 'P@ss1!' cambiata ogni mese.

```
root@hacklab:~/lezione-05/mappa-2 $
```

LEZIONE 05 / MAPPA // APPROFONDIMENTI

Mappa dei concetti – Approfondimenti

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



```
root@hacklab:~/lezione-05/concetto-6 $
```

LEZIONE 05 / CONCETTO 6/10

[Attacco/tecnica]

Rainbow table e ruolo del salt

// SPIEGAZIONE

Le rainbow table barattano memoria per tempo, precalcolando catene di hash per invertirli in fretta. Un salt unico per utente rende inutile la tabella precalcolata, perché lo stesso testo produce hash diversi: per questo il salt è obbligatorio.

// ESEMPIO

> Due utenti con password 'estate' hanno hash diversi se il salt è unico per ciascuno.

```
root@hacklab:~/lezione-05/concetto-7 $
```

LEZIONE 05 / CONCETTO 7/10

[Attacco/tecnica]

Spraying e credential stuffing

// SPIEGAZIONE

Entrambi sfruttano la debolezza del riuso: lo spraying prova poche password diffuse su tanti account per non scattare i lockout; lo stuffing usa combinazioni utente/password già trapelate, efficaci perché le persone riusano le stesse credenziali.

// ESEMPIO

> Credenziali da un leak pubblico riusate con successo sul portale aziendale.

```
root@hacklab:~/lezione-05/concetto-8 $
```

LEZIONE 05 / CONCETTO 8/10

[IA]

Dump SAM/LSASS e poisoning LLMNR

// SPIEGAZIONE

Oltre a estrarre credenziali locali da SAM e LSASS, l'attaccante può avvelenare i protocolli di risoluzione nomi LLMNR e NBT-NS: quando un host cerca una risorsa inesistente risponde lui e cattura l'hash di autenticazione da crackare o rilanciare.

// ESEMPIO

```
$ responder -I eth0 (cattura NetNTLM da richieste LLMNR/NBT-NS)
```

```
root@hacklab:~/lezione-05/concetto-9 $
```

LEZIONE 05 / CONCETTO 9/10

[Attacco/tecnica]

Wordlist mirate e analisi dei leak

// SPIEGAZIONE

Le password riflettono la cultura del bersaglio: nomi locali, squadre, stagioni, pattern aziendali. Analizzare leak passati e costruire wordlist mirate aumenta molto il tasso di successo rispetto alle liste generiche.

// ESEMPIO

> Aggiungere il nome dell'azienda e l'anno corrente alle regole di mutazione della wordlist.

```
root@hacklab:~/lezione-05/concetto-10 $
```

LEZIONE 05 / CONCETTO 10/10

[Difesa]

Rilevare gli attacchi alle credenziali

// SPIEGAZIONE

Lato difensivo, spraying e stuffing lasciano tracce: picchi di login falliti su molti account, accessi da geografie improbabili, uso di credenziali note come compromesse. Correlare questi segnali nel SIEM permette di reagire prima della compromissione.

// ESEMPIO

> Alert su 'molti account, un tentativo ciascuno, dallo stesso IP', tipico dello spraying.

```
root@hacklab:~/lezione-05/strumenti $
```

LEZIONE 05 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Hashcat

John

Hydra

Medusa

Ncrack

Mimikatz

Responder

CeWL

Crunch

// 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-05/lab-1 $
```

LEZIONE 05 / LABORATORIO 1

Laboratorio 1

\$ Cracking offline (Hashcat con dizionario + regole)

// PROCEDURA

[1] Estrai e cracka hash con Hashcat (dizionario + regole)

[2] misurando i tempi

[!] Verifica: Perché il salt vanifica le rainbow tables?

```
root@hacklab:~/lezione-05/lab-2 $
```

LEZIONE 05 / LABORATORIO 2

Laboratorio 2

\$ Hardening (MFA/lockout; spraying rilevato)

// PROCEDURA

[1] Configura MFA/lockout e dimostra un password spraying rilevato

[!] Verifica: Perché l'MFA è decisiva?

```
root@hacklab:~/lezione-05/caso-di-studio $
```

LEZIONE 05 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Compromissione via credenziale debole senza MFA (collegamento al caso Colonial Pipeline).

// 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-05/etica $
```

LEZIONE 05 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Solo su dati di laboratorio o autorizzati; le credenziali reperite sono dati sensibili.

```
root@hacklab:~/lezione-05/ricapitolazione $
```

LEZIONE 05 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Meccanismi di hashing e autenticazione
- > Cracking online e offline in lab
- > Robustezza di policy e formati di hash
- > L'efficacia dell'MFA
- > Raccomandazioni di hardening

```
root@hacklab:~/lezione-05/verifica $
```

LEZIONE 05 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Perché il salt vanifica le rainbow tables?
- ? Quanto incide la lunghezza sull'entropia?
- ? Perché l'MFA è la difesa più efficace?

// VALUTAZIONE

Esercizio pratico di cracking + nota difensiva con policy.

// LETTURE

Doc. Hashcat/John; NIST SP 800-63B.

lezione 05 completata

\$ next

Password Attacks e Credential Access

[!] 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

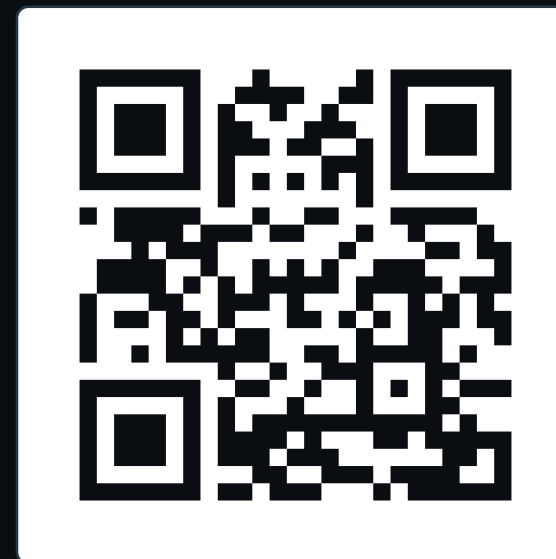


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.