

{EPITECH}

WINTER SCHOOL 2027

<PARIS - CYBER CAMP/>
FROM 4TH TO 15TH OF JANUARY

{ 2 WEEKS
1 PROJECT
4 CREDITS }



SYLLABUS

<ID 1: Recon & Web Attacks/>

- **Description** : Setup (Exegol, CTFd) followed by enumeration, port scanning, and service attacks, then coverage of major web vulnerabilities and exploitation tools.
- **Languages – Tech skills learnt** : Enumeration, port scanning, FTP/SMB/FreeRDP/MSSQL/WinRM attacks, SQL injection, XSS, LFI, file upload; ffuf, Burp Suite, sqlmap.

<ID 3: Password Cracking & Pivoting/>

- **Description** : Password cracking techniques across various file types, followed by pivoting methods to reach additional machines.
- **Languages – Tech skills learnt** : John the Ripper, Hashcat, rainbow tables, bruteforce, wordlist mutation, ZIP/Office/KeePass cracking; SSH port forwarding, proxychains, ligolo-ng.

<ID 2: Shells & Exfiltration/>

- **Description** : Shell types and stabilization (especially reverse shells), followed by data exfiltration techniques and alternative remote access methods.
- **Languages – Tech skills learnt** : Webshells, bind shells, reverse shells, pty stabilization, base64/wget/curl/nc exfiltration; psexec, evil-winrm, xfreerdp.

<ID 4: AD Enumeration & Poisoning/>

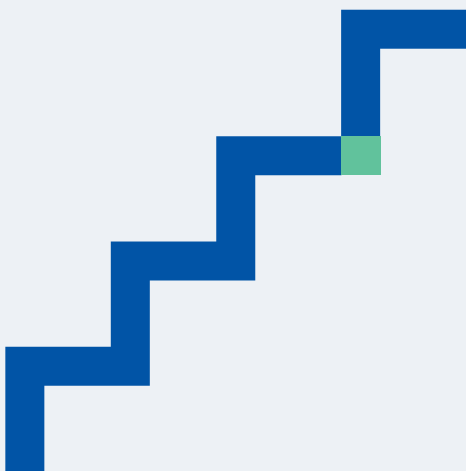
- **Description** : Active Directory enumeration and common AD weaknesses, followed by network poisoning and deeper permission-based enumeration.
- **Languages – Tech skills learnt** : BloodHound, nxc, password spraying, Kerbrute, Kerberoasting, Responder/Inveigh; GenericAll, GenericWrite, DCSync, WriteOwner, AddMember, ForceChangePassword.





APPLICATION DEADLINE

*Full package: November 15th 2026
Without accommodation: November 30th 2026*



<ID 5: Privilege Escalation/>

- **Description** : Linux privilege escalation to root, followed by Windows privilege escalation to SYSTEM using user rights abuse.
- **Languages – Tech skills learnt** : Sudo abuse, SUID, capabilities, cron, kernel exploits, LinPEAS, pspy; SeImpersonate, SeDebug, DLL injection.

<ID 6: Pass the Hash/Ticket & Kerberos Abuse/>

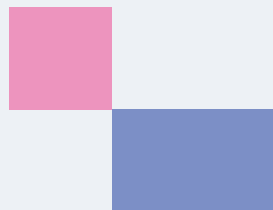
- **Description** : Pass the Hash/Ticket attacks and Kerberos fundamentals, followed by advanced Kerberos abuse with NTLM disabled.
- **Languages – Tech skills learnt** : PtH, PtT, psexec, Rubeus, getTGT, Mimikatz; Targeted Kerberoasting, Shadow Credentials, AS-REP Roasting.

<ID 7: Advanced AD Attacks & Review/>

- **Description** : Advanced AD attack techniques followed by a full review of the program's content.
- **Languages – Tech skills learnt** : Silver/Golden Ticket, delegation abuse, GMSA attacks.

<ID 8: Final Exam/>

- **Description** : Comprehensive exam covering all concepts from the program.
- **Languages – Tech skills learnt** : Cumulative assessment of Days 1–7.



WINTER SCHOOL 2027

<CYBER CAMP/>

Sharpen your cybersecurity skills and master the fundamentals of offensive security. Dive into an intensive two-week program covering reconnaissance, web application attacks, Active Directory exploitation, privilege escalation, password cracking, Kerberos abuse, and advanced post-exploitation techniques through hands-on labs and real-world scenarios.

Learn to use industry-standard tools while collaborating with international students. Immerse yourself in the French way of life with language classes and curated cultural tours in the heart of Paris.



WHAT'S INCLUDED

- French language courses
- Cultural activities
- Accommodation*
- Breakfast
- Welcome & farewell events

TUITION FEES

- Standard fee: €2,300
- EPITECH partner institutions: €2,000
- Program fee without accommodation : €1,500

GENERAL INFORMATION

Language of Instruction: English
Date: From 4th to 15th of January
Location: Paris
Credits: 4 Credits
Hours estimated : 70H
– 2 weeks – Monday to Friday 9h-18H



WANT TO KNOW MORE?

Visit and apply below



Find us online



PROGRAM LOCATION:

Epitech Paris
40 rue du Docteur Roux
75015 Paris

CONTACT:

international-relations@epitech.eu