

WEBINAR

SOFTWARE CYBER-SECURITY

Allo scopo di lavorare in maniera congiunta con il mondo accademico e definire dei progetti di formazione strutturati che possano garantire opportunità a tutte le aziende associate, è stato costituito un accordo di collaborazione tra ANIE ASSIFER e CINI (Consorzio Interuniversitario Nazionale per l'Informatica), principale punto di riferimento della ricerca accademica nazionale nei settori dell'Informatica e dell'Information Technology.

Il progetto di collaborazione prevede dei percorsi di formazione sulle nuove tecnologie in ambito ferroviario suddivisi in quattro aree tematiche (Computer Architectures, Design Methodologies, Machine Learning e Programming & Simulations).

Obiettivi

Il corso introduce tecniche di attacco a moderni sistemi software, discutendo i dettagli tecnici della loro attuazione, il loro potenziale impatto e i loro punti di forza e debolezza. Verranno presentati esempi pratici per ogni tipo di attacco. Successivamente, il corso si concentra sulle tecniche di mitigazione degli attacchi, fornendo una classificazione sistematica delle loro capacità, presentando dettagli implementativi e discutendo la loro disponibilità in sistemi operativi odierni.

Relatori

Prof. Alessandro Biondi

Scuola Superiore Sant'Anna di Pisa

Calendario

LEZIONE	DATA	ORARIO	ORE
1	4 novembre 2026	14:00 – 17:00	3
2	6 novembre 2026	14:00 – 17:00	3
3	11 novembre 2026	14:00 – 17:00	3
4	13 novembre 2026	14:00 – 17:00	3
5	18 novembre 2026	14:00 – 17:00	3
6	20 novembre 2026	14:00 – 17:00	3
7	25 novembre 2026	14:00 – 16:00	2
TOTALE ORE			20

Modalità e quota di iscrizione

1. Quota di partecipazione: Associato ANIE € 350,00+IVA
2. Pagamento: con carta di credito o con bonifico bancario.
Per pagamento con bonifico bancario inviare copia del pagamento a formazione@anieservizintegrati.it e amministrazione@anieservizintegrati.it
L'iscrizione si intende perfezionata con l'avvenuto pagamento.
3. Successivamente saranno inviate le modalità di partecipazione al webinar.

Programma

- Richiami di concetti di base di sistemi operativi, architetture dei calcolatori e compilatori.
- Tecniche di attacco per sfruttare vulnerabilità di memoria (stack/heap overflows, return-oriented programming).
- Introduzione agli shellcode.
- Attacchi basati su side channels.
- Tecniche di mitigazione di attacchi (executable space protection, canarini/cookies, stack rearrangement, address-space layout randomization, control-flow integrity).
- Supporto alle protezioni disponibile in sistemi operativi e compilatori.