Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**Cyber-Security Capstone Project**
Corso di studio	Laurea Magistrale in Computer Science
Anno Accademico	2024/25
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	6 CFU
Settore Scientifico Disciplinare	ING-INF/05
Lingua di erogazione	Inglese
Anno di corso	Secondo
Periodo di erogazione	1^ semestre, le date esatte sono riportate nel manifesto/regolamento
Obbligo di frequenza	La frequenza è fortemente raccomandata
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/computer-science/computer-science

Docente/i

Nome e cognome	Vita Santa Barletta
Indirizzo mail	vita.barletta@uniba.it
Telefono	080-5443270
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Laboratorio SERLab, IV piano
Sede virtuale	Piattaforma E-learning - https://elearning.uniba.it/
Sito web del docente	https://serlab.di.uniba.it
Ricevimento	(da confermare) martedì dalle 15:00 alle 16:00 (previo appuntamento)

Syllabus

Obiettivi formativi	L'insegnamento di Cyber-Security Capstone Project si propone di fornire strumenti e tecniche per l'esecuzione di attività di offesa e difesa in campo cybersecurity. Ciò

	include lo sviluppo di un progetto che permetta di applicare tali strumenti in contesti IT, OT e IoT e che tenga in considerazione gli attuali modelli di AI alla base di tali sistemi.
Prerequisiti	Lo studente deve avere familiarità con almeno un linguaggio di programmazione e con le strutture dati fondamentali, metodologie di sviluppo software.
Contenuti di insegnamento (Programma)	**Security Information and Event Management** - Ciclo di vita della sicurezza - Strumenti e tecniche **Security Orchestration Automation and Response** - Contesto di applicazione - Strumenti e tecniche **API Security** - Vulnerabilità - Gestione del rischio - Identificazione delle minacce **Adversarial Threat Landscape for Artificial-Intelligence Systems** - Pattern di attacco - Tattiche - Tecniche di mitigazione - Strumenti ed esempi pratici **Caso di studio** - Introduzione caso di studio - Esempi e best practices - Progettazione caso di studio
Testi di riferimento	• Omar Santos, Joseph Muniz, Stefano De Crescenzo, “CCNA Cyber Ops SECFND 210-250”, Cisco Systems; Har/Psc edizione (3 aprile 2017) Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.
Note ai testi di riferimento	I testi di riferimento sono integrati con slide, dispense del docente e altro materiale didattico messi a disposizione degli studenti sulla piattaforma di e-learning usata dal CdS.

Organizzazione della didattica

Ore			
Totali	Didattica frontale	Pratica (laboratorio, progetto, esercitazione, altro)	Studio individuale
150 ore	24 ore	15 + 50 ore di laboratorio ed esercitazioni guidate	61 ore
CFU/ETCS			
6 CFU	3 CFU	1 + 2P CFU	

Metodi didattici	
	Lezioni frontali con l'ausilio di slide che riportano esempi per illustrare gli argomenti trattati. Esercitazioni pratiche sull'utilizzo dei vari principi e tecniche presentate a lezione attraverso esercizi da svolgere singolarmente. Un progetto da svolgere preferibilmente in gruppo utilizzando strumenti e tecniche approfondite a lezione. Utilizzo della piattaforma di e-learning del Dipartimento di Informatica per la distribuzione del materiale e per le interazioni tra docenti e studenti durante e dopo il corso.

Risultati di apprendimento previsti	
Conoscenza e capacità di comprensione	• Il principale risultato di apprendimento atteso è la conoscenza relativa a processi, metodi e tecniche per l'analisi e la modellazione di minacce cyber e relative mitigazioni. • Lo studente acquisisce tale conoscenza sia attraverso le lezioni frontali e la partecipazione a seminari tematici erogati durante il corso, sia attraverso esercitazioni che gli consente di mettere in pratica e verificare quanto appreso, acquisendo così consapevolezza della capacità di comprensione e di come migliorare l'applicazione delle tecniche apprese.
Conoscenza e capacità di comprensione applicate	• Per consentire allo studente di applicare le conoscenze per l'identificazione e la gestione delle vulnerabilità, si svolgono in aula sia esercitazioni individuali che collettive. • Allo studente è richiesto di sviluppare un progetto, nel quale è necessario applicare alcune delle tecniche presentate in aula, dopo aver selezionato quelle più appropriate per il caso specifico. Questo progetto contribuisce alla valutazione finale dello studente e quindi al voto finale d'esame.
Competenze trasversali	**Autonomia di giudizio** • Acquisire una significativa autonomia nel valutare i pericoli inerenti alle minacce cyber di sistemi informatici. • Acquisire la capacità di lavorare in team per la gestione delle minacce cyber. Le esercitazioni che si svolgono durante il corso contribuiscono al raggiungimento di tali competenze grazie anche alla discussione di tali scelte con il docente. • L'autonomia di giudizio è parte della valutazione finale dello studente e tiene conto delle discussioni avvenute durante le lezioni, delle esercitazioni e della presentazione del progetto. **Abilità comunicative** • Illustrare in modo chiaro ed efficace le conoscenze apprese, presentare casi applicativi ed esempi illustrativi. • La presentazione e discussione del progetto sviluppato in gruppo è parte della prova orale d'esame e consente allo studente di mostrare le proprie abilità comunicative. **Capacità di apprendere in modo autonomo** • Per stimolare la capacità di apprendere in modo autonomo, allo studente è richiesto di approfondire specifici argomenti oppure è invitato a partecipare

	a seminari tenuti da altri docenti, interni o in visita al dipartimento, sui quali lo studente deve poi presentare durante le lezioni, e riportare in sede d'esame.

Valutazione	
Modalità di verifica dell'apprendimento	La verifica dei risultati formativi raggiunti avviene durante l'esame finale, che prevede: • Un colloquio orale in cui si presenta e si discute il progetto sviluppato in gruppo e si verificano le competenze acquisite durante il corso e le capacità espositive dello studente. Per gli studenti frequentanti sono previste le seguenti facilitazioni: • Bonus punteggio a valere sulla valutazione del progetto per gli studenti che svolgono positivamente le esercitazioni sul progetto/caso di studio.
Criteri di valutazione	**Conoscenza e capacità di comprensione** • Lo studente dovrà essere in grado di effettuare opportune scelte per individuare, elaborare e organizzare informazioni appropriate per soluzioni di problemi connessi alle minacce di sicurezza informatica. **Conoscenza e capacità di comprensione applicate** • Si valuta la presentazione del progetto per verificare le competenze acquisite dallo studente e la sua capacità di sintesi nonché la chiarezza di esposizione, la capacità di fare confronti significativi tra metodologie, tecniche e tecnologie diverse adottate e riportare un proprio giudizio critico. **Autonomia di giudizio** • Lo studente dovrà essere in grado di applicare opportune soluzioni per la gestione dei problemi connessi alle minacce di sicurezza informatica. • Si valuta la presentazione del progetto per verificare le competenze acquisite dallo studente e la sua capacità di sintesi nonché la chiarezza di esposizione, la capacità di fare confronti significativi tra metodologie, tecniche e tecnologie diverse adottate e riportare un proprio giudizio critico. **Abilità comunicative** • Lo studente dovrà essere in grado di produrre una documentazione chiara e contenente le informazioni necessarie per le minacce di sicurezza e il contesto identificato. **Capacità di apprendere** • Lo studente dovrà essere in grado di applicare e tradurre autonomamente le tecniche apprese per la gestione delle minacce cyber e che integrino le normative vigenti sulla cyber security.

Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	**Voto**	**Descrittori**
	< 18 insufficiente	Conoscenze frammentarie e superficiali dei contenuti, errori nell'applicare i concetti, descrizione carente.
	18 - 20	Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell'applicazione di concetti teorici.
	21 - 23	Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice.

	24 - 25	Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato.
	26 - 27	Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta.
	28 - 29	Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta.
	30 30 e lode	Conoscenze dei contenuti molto ampie, complete ed approfondite, capacità ben consolidata di applicare i contenuti, ottima capacità di analisi, di sintesi e di collegamenti interdisciplinari, padronanza di descrizione.

Altro

Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea
- https://www.uniba.it/it/ricerca/dipartimenti/informatica
- https://elearning.di.uniba.it/

I programmi degli insegnamenti sono disponibili qui:

- https://programmi.di.uniba.it/

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

Link al corso sulla piattaforma e-learning UNIBA:

- https://elearning.uniba.it/course/view.php?id=6531

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO | DIPARTIMENTO DI INFORMATICA

Main information on the course	
Course name	**Cyber-Security Capstone Project**
Degree	Computer Science (second level of Computer Science)
Academic year	2024/25
European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU)	6 CFU
Settore Scientifico Disciplinare	ING-INF 05
Course language	English
Course year	Second
Course period	First Semester - exact dates can be found in the didactic regulations
Course attendance requirement	None, but it is highly recommended to attend classes
Website of the Degree	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/computer-science/computer-science

Teacher(s)	
Name and Surname	Vita Santa Barletta
email	vita.barletta@uniba.it
phone	080-5443270
office	Department of Computer Science, Via Orabona 4, 70125 Bari. SERLab Laboratory, 4th floor
e-learning platform	E-learning Platform - https://elearning.uniba.it/
Teacher's homepage	https://serlab.di.uniba.it
Office hours	(To be confirmed) Tuesday15:00 - 16:00 (by appointment)

Syllabus	
Course goals	The Cyber-Security Capstone project course aims to provide tools and techniques for secure and performing offense and defense activities in the cybersecurity field. This includes developing a project to apply these tools in IT, OT and IoT contexts and taking into consideration the current AI models underlying these systems.
Prerequisites/requirements	Students must be familiar with at least one programming language and with fundamental data structures, software development methodologies.
Course program	**Security Information and Event Management** - Security Life Cycle - Tools and Techniques

	Security Orchestration Automation and Response - Application Context - Tools and Techniques **API Security** - Vulnerabilities - Risk Management - Threat identification **Adversarial Threat Landscape for Artificial-Intelligence Systems** - Attack Patterns - Tactics - Mitigation Techniques - Tools and practical examples **Case study** - Case Study Introduction - Example and best practices - Case study design
Books of reference	• Omar Santos, Joseph Muniz, Stefano De Crescenzo, "CCNA Cyber Ops SECFND 210-250", Cisco Systems; Har/Psc edizione (3 aprile 2017) Students can borrow these texts from the library. It is advisable to check availability through the University Library System (https://opac.uniba.it/easyweb/w8018/index.php?) and contact the library for lending.
Notes to the books	The reference texts are supplemented with slides, teacher's notes, and other teaching materials made available to students on the e-learning platform used by the degree program.

Organization of the didactic activities

Hours				
Total	Lectures	Practice sessions	Project work	Individual study
150 hours	24 hours	15 hours	50 hours	61 hours
CFU/ETCS				
6 CFU	3 CFU	1 CFU	2P CFU	

Teaching methods

- Lectures with the aid of slides illustrating the discussed topics with examples.
- Practical exercises on using the various principles and techniques presented during the lectures through individual exercises.
- A project, preferably to be carried out in a group, using Fortify SCA as Static Code Analysis tool.
- Use of the Department of Computer Science's e-learning platform for distributing materials and facilitating interactions between teachers and students during and after the course.

Expected learning outcomes	
Knowledge and understanding	• The main expected learning outcome is knowledge related to processes, methods and techniques for analyzing and modeling cyber threats and their mitigation. • Students acquire this knowledge through lectures and thematic seminars during the course and through practical exercises that allow them to practice and verify what they have learned, gaining awareness of their understanding and how to improve the application of learned techniques.
Applying knowledge and understanding	• To enable the student to apply knowledge for vulnerability identification and management, both individual and group exercises are conducted in the classroom. • The student is required to develop a project, in which they must apply some of the techniques presented in the classroom, after selecting those most appropriate for the specific case. This project contributes to the student's final evaluation and thus to the final exam grade.
Other skills	**Making judgements** • Gain significant autonomy in assessing the dangers inherent in information system vulnerabilities. • Acquire the ability to work in teams to manage cyber threats. The exercises conducted during the course contribute to achieving these skills, thanks also to the discussion of these choices with the teacher. • Autonomy of judgment is part of the final assessment of the student, taking into account the discussions held during lectures, exercises, and project presentation. **Communication** • Illustrate the results of exercises carried out independently or in a group with the aim of developing communication skills. • The presentation and discussion of the project developed in a group are part of the oral exam and allow the student to demonstrate their communication skills. **Learning skills** • Illustrate the results of exercises carried out independently or in a group with the aim of developing communication skills. • The presentation and discussion of the project developed in a group are part of the oral exam and allow the student to demonstrate their communication skills.

Assessment	
Assessment methods	The assessment of the achieved learning outcomes occurs during the final exam, which includes: • An oral interview presenting and discussing the group-developed project, verifying the knowledge acquired during the course and the student's presentation skills. For attending students, the following benefits are provided: • Score bonus for the project evaluation for students who positively complete the project/case study exercises.

Evaluation criteria

Knowledge and Understanding

- The student must be able to correctly apply decisions to identify, process, and organize appropriate information for solutions to problems related to cybersecurity threats.

Applied Knowledge and Understanding

- The project presentation is evaluated to verify the student's acquired skills, summarization ability, and clarity of presentation, as well as the ability to make significant comparisons between different methodologies, techniques, and technologies adopted and to provide their critical judgment.

Autonomy of Judgment

- The student must be able to apply appropriate solutions for cyber security threats.
- The project presentation is evaluated to verify the student's acquired skills, summarization ability, and clarity of presentation, as well as the ability to make significant comparisons between different methodologies, techniques, and technologies adopted and to provide their critical judgment.

Communication Skills

- The student must be able to produce clear documentation containing the necessary information for cyber security threats.

Learning Ability

- The student must be able to apply and translate the techniques learned to appropriately manage security in a specific context.

Measurements and final grade

Grade	Descriptors
< 18 insufficient	Fragmentary and superficial content knowledge, errors in applying concepts, poor description.
18-20	Sufficient but general content knowledge, simple description, uncertainties in applying theoretical concepts.
21-23	Appropriate but not deep content knowledge, ability to apply theoretical concepts, ability to present content simply.
24-25	Appropriate and broad content knowledge, fair ability to apply knowledge, ability to present content articulately.
26-27	Precise and complete content knowledge, good ability to apply knowledge, clear and correct description.
28-29	Broad, complete, and deep content knowledge, good content application, good analysis and synthesis ability, confident and correct description.
30 30 e lode	Very broad, complete, and deep content knowledge, well-established content application ability, excellent analysis, synthesis, and interdisciplinary connections, mastery of description.

Further information

Students are advised to rely exclusively on information/communications provided on the official websites of the Department of Computer Science or on social groups only if formed and administered exclusively by the lecturers of the related courses:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea
- https://www.uniba.it/it/ricerca/dipartimenti/informatica
- https://elearning.uniba.it/

The course programs are available here:

- https://elearning.uniba.it/

The information that all students should know is written in the Teaching Regulations and study posters available on the site:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea

Students are advised to be cautious of information and materials circulating on unofficial sites or social groups as they are often unreliable, incorrect, or incomplete. For any doubts, request a meeting with the instructor according to the office hour arrangements.

Link to the course on the e-learning platform of the University E-Learning Center:

- https://elearning.uniba.it/course/view.php?id=6531