Biomatika és Alkalmazott Mesterséges Intelligencia Intézet			Választható tárgy 2025-26-1			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tgy	lab
Kiberbiztonsági kihívások a gyakorlatban	NBVKK1HMLF	4	nappali heti	0	0	10
Tárgyfelelős: Dr. Bánáti-Baumann Anna			Beosztás: adjunktus			
Oktató(k): Kotcauer Péter						
Előtanulmányi feltételek:	-					
Számonkérés módja:	Évközi jegy					

A tananyag	
Oktatási cél:	A tantárgy célja a hallgatókat megismertetni a kiberbiztonsági fenyegetések módszereivel, illetve a támadások detektálását lehetővé tévő védelmi megoldásokkal. A Hack The Box (HTB) egy online platform, amely lehetővé teszi, hogy a kiberbiztonsággal foglalkozó szakemberek teszteljék a támadásokkal kapcsolatos képességeiket, valamint ötleteket és módszereket cseréljenek más, hasonló érdeklődésű tagokkal. Számos kihívást tartalmaz, amelyek folyamatosan frissülnek. Némelyikük valós forgatókönyveket szimulál, némelyikük pedig inkább a CTF (Capture the Flag) stílusú kihívások felé hajlik.
Tematika:	A kurzus során a hallgatóknak lehetőségük nyílik megismerkedni, gyakorlati tapasztalatot szerezni a kiberbiztonság különböző területeivel, a támadási technikákkal és ezek védelmi mechanizmusaival, továbbá elsajátítani az ezekhez szükséges alapismereteket interaktív feladatok és kihívásos versenyek megoldásán keresztül.

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	Linux, Windows alapismeretek - biztonsági és sérülékenységi megközelítésben
2.	Linux, Windows - beépített támadási technikák és eszközök
3.	Hálózati és Webes támadási technikák
4.	Hálózati és Webes támadások elleni védelmi technikák és eszközök
5.	Adatbázis alapismeretek - biztonsági és sérülékenységi megközelítésben
6.	Cyber Kill Chain folyamata és eszközei
7.	LPE (Local Privilege Escalation), privilégium szint emelés lokálisan 1.
8.	LPE (Local Privilege Escalation), privilégium szint emelés lokálisan 2
9.	Lateral movement - technikák és eszközök 1.
10.	Lateral movement - technikák és eszközök 2.
11.	Reverse engineering
12.	Malware elemzés - technikák és eszközök
13.	Forensics, Challenge bemutatók
14.	Detection Engineering, Challenge bemutatók
Félévközi követelmények	

Évközi jegy / aláírás megszerzésének feltételei:	Az órákon való részvétel legalább 50%-ban, továbbá a félév során 1 „machine” vagy „sherlock” feladatot” kell megoldani a HTB kihívásai közül, a megoldást pedig dokumentálni kell (writeup készítés).

Zárthelyi dolgozatok

Oktatási hét	Témakör
	-

Az *évközi jegy* kialakításának módszere (csak évközi jegyes tárgyak esetében töltendő ki)

Az érdemjegy kialakítása a féléves feladat beszámolója és dokumentációja alapján történik.

Pótlás módja

A ZH / évközi jegy / aláírás pótlásának módja:	**A Hallgató HKR-ben meghatározott módon a vizsgaidőszak első 10 munkanapjának valamelyikén egy alkalommal, egy előre megadott időpontban kísérletet tehet a javítására az aláíráspótlás díj ellenében.**

Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)

-

Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)

-

Az egyes érdemjegyek ponthatárai:

Elérhető eredmény	Érdemjegy
0-49%	Elégtelen (1)
50-61%	Elégséges (2)
62-73%	Közepes (3)
74-85%	Jó (4)
86-100%	Jeles (5)

Irodalom

Kötelező:	Az előadások anyaga
Ajánlott:	• Alan J White : Blue Team Field Manual (BTFM) , 2017 • Ben Clark: Red Team Field Manual (RTFM), 2014 • Tim Bryant: Purple Team Field Manual (PTFM), 2020 • Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Wiley, Indianapolis, 2014 • Dr. Allen Harper, Ryan Linn, Stephen Sims, Michael Baucom, Daniel Fernandez, Huáscar Tejeda, Moses Frost: Gray Hat Hacking: The Ethical Hacker's Handbook, 6th Edition, 2022
Egyéb segédletek:	-