

Biomatika és Alkalmazott Mesterséges Intelligencia Intézet			Mintatanterv szerinti 5. félév 2026-27-1			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tg	lab
Számítógép hálózatok és felhők biztonsága	NIXSH1KBNE	5	heti	2	0	2
Tárgyfelelős: Vörösné Dr. Bánáti-Baumann Anna			Beosztás: egyetemi adjunktus			
Oktató(k): Nemes Teréz						
Előtanulmányi feltételek:	NIXHT1KBNE	Informatikai biztonság				
Számonkérés módja:	vizsga					
A tananyag						
Oktatási cél:	A Számítógépes hálózatok és felhők biztonsága tantárgy célja, hogy a hallgatók átfogó és elmélyült ismereteket szerezzenek a hagyományos hálózati infrastruktúrákhoz, valamint a modern, felhőalapú környezetekhez kapcsolódó biztonsági kihívásokról és megoldásokról. A tantárgy az elméleti alapok és a gyakorlati alkalmazás együttes hangsúlyozásával felkészíti a hallgatókat biztonságos rendszerek tervezésére, üzemeltetésére és menedzselésére. A főbb témakörök közé tartozik a fenyegetések megelőzése, a biztonságos architektúrák kialakítása, a támadások észlelése és kezelése, valamint az iparági biztonsági szabványok és bevált gyakorlatok alkalmazása.					
Tematika:	A hallgatók a képzést a hálózatbiztonság alapelveinek, valamint a hálózati eszközök megerősítésének (hardening) megismerésével kezdik, beleértve a hitelesítés, jogosultságkezelés és elszámoltathatóság (AAA) kérdéskörét. A tantárgy részletesen tárgyalja a 2. rétegbeli fenyegetéseket, valamint azok elhárítási és megelőzési stratégiáit. Az oktatás kiterjed a hagyományos hozzáférés-vezérlési listákra (ACL) és a modern tűzfalakra (NGFW), továbbá a IDS/IPS rendszerekre is. A felhőszegmensben a hallgatók gyakorlati tapasztalatot szereznek az OpenStack használatában, különös tekintettel az azonosságkezelésre, a virtuális gépek izolációjára és a hálózati védelemre. A tantárgy foglalkozik a VPN-technológiákkal, valamint a titkosított forgalom ellenőrzésének kihívásaival is. A hallgatók megtanulják sebezhetőségvizsgálatok végrehajtását, fenyegetési intelligenciaforrások használatát, továbbá átfogó képet kapnak a naplózási gyakorlatokról, a monitorozási stratégiákról és a Security Operations Center (SOC) működéséről.					

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	EA: Hálózati támadási forgatókönyvek és védekezési stratégiák LA: Ismétlő laborgyakorlat I.
2.	EA: Hálózati és felhőbiztonsági alapelvek LA: Ismétlő laborgyakorlat II.
3.	EA: Eszközüvédelem, hardening és AAA Cisco eszközökön LA: Hardening és L2 védelem I.
4.	EA: Layer 2 támadások és Layer 2 védekezés LA: Hardening és L2 védelem II.
5.	EA: Detektálás hálózati szinten (IDS/IPS modellezve) és tűzfal alapok LA: IDS/IPS és ACL/ZPF gyakorlat I.
6.	EA: Forgalomszűrés IPv4/IPv6 és állapotartó Cisco megoldások LA: IDS/IPS és ACL/ZPF gyakorlat II.

7.	EA: OpenStack alapok és felhasználó kezelés LA: OpenStack labor I.
8.	EA: OpenStack virtuális gépek és hálózatok biztonsága LA: OpenStack labor II.
9.	EA: Peremvédelem és tűzfalgondolkodás Cisco környezetben LA: ASA és VPN gyakorlat I.
10.	EA: VPN technológiák és távoli elérés biztonsága LA: ASA és VPN gyakorlat II.
11.	EA: Naplózás, monitoring és visszakövethetőség LA: Zárthelyi gyakorlás
12.	EA: Rektori szünet LA: Rektori szünet
13.	EA: Projektbemutató I. LA: Zárthelyi dolgozat
14.	EA: Projektbemutató II. LA: Javító/Pótló zárthelyi dolgozat
Félévközi követelmények	
Évközi jegy / aláírás megszerzésének feltételei:	Az előadások és laborgyakorlatok látogatása kötelező. A vizsgára bocsátás feltétele aláírás megszerzése, amely a - Laborgyakorlatokon megtartott zárthelyi dolgozat legalább elégséges eredményű megírásával - A Projektfeladat legalább elégséges eredményű elkészítésével és bemutatásával érhető el. A zárthelyi dolgozaton és a projektfeladaton a megszerezhető pontok maximuma 100. Az elégségeshez, legalább 50 pont szükséges.
Zárthelyi dolgozatok	
Oktatási hét	Témakör
13	Gyakorlati zárthelyi dolgozat, projektbemutató
14	Pót gyakorlati zárthelyi dolgozat, projektbemutató
Az évközi jegy kialakításának módszere (csak évközi jegyes tárgyak esetében töltendő ki)	
-	
Pótlás módja	
A ZH / évközi jegy / aláírás pótlásának módja:	A 13. héten meg nem írt vagy elégtelen zárthelyi dolgozat pótlására a szorgalmi időszakban, a 14. héten van lehetőség. Aláírás pótlására akkor van szükség, ha a félév során, a laborgyakorlatokon megírt zárthelyi és Pót zárthelyi eredménye is elégtelen. A projektfeladat a 13. és 14 héten kerül bemutatásra előzetes beosztás alapján, aki azonban nem készíti el határidőre, annak a bemutató az aláíráspótló alkalmával kerül megszervezésre.
Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)	
Írásbeli beugró, majd szóbeli vizsga, melyben szerepelhet kérdés az előadás anyagából, valamint a laborokon elhangzott elméleti témájú anyagokból egyaránt.	
Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)	

A félévzáró érdemjegy az alábbi képlet szerint alakul:

Tárgyi eredmény = 0.25 * Zárthelyi dolgozat + 0.25 * Projekteredmény + 0.1 * Beugró eredmény + 0.4 * Szóbeli eredmény

Az egyes érdemjegyek ponthatárai:

Elért eredmény	Vizsgajegy
0%-49%	elégtelen (1)
50%-61%	elégséges (2)
62%-73%	közepes (3)
74%-85%	jó (4)
86%-100%	jeles (5)

Irodalom

Kötelező:	– Cisco Networking Academy tananyag – Andrew S. Tanenbaum: Számítógép Hálózatok – ötödik, bővített, átdolgozott kiadás Prentice Hall – Panem 2013. (ISBN 9789635455294 – Petrényi József: TCP/IP alapok I. kötet - http://mek.oszk.hu/08300/08374/
Ajánlott:	– IBM Redbooks: TCP/IP Tutorial and Technical Overview http://www.redbooks.ibm.com/redbooks.nsf/RedbookAbstracts/gg243376.html – Charles M. Kozierok: The TCP/IP Guide (On-line verzió) http://www.tcpipguide.com/free – Connected: An Internet Encyclopedia (On-line verzió) http://www.freesoft.org/CIE/ – Stephen A. Thomas: IP kapcsolás és útválasztás Kiskapu Kft. 2002. (ISBN 963-9301-41-8) – W. Richard Stevens: TCP/IP Illustrated, Volume 1 The Protocols Addison Wesley Longman, Inc. 1994 (ISBN 0-201-63346-9) – Eric A. Hall: Internet Core Protocols: The Definitive Guide O'Reilly & Associates, Inc. 2000 (ISBN 1-56592-572-6) – Petrényi József: TCP/IP alapok II. kötet http://mek.oszk.hu/08300/08374/
Egyéb segédletek:	Ld. Moodle rendszerben.