

Óbudai Egyetem Neumann János Informatikai Kar		Kiberfizikai Rendszerek Intézet		
Tantárgy neve és kódja: Számítógép hálózatok és felhők biztonsága, NIXSH1KBNE Kreditérték: 5				
Üzemmérnök informatikus		Nappali tagozat 2020/21 tanév I. félév		
Tantárgy oktató(i): Dr. Bánáti Anna, Dr. Kail Eszter, Farkas Attila				
Előtanulmányi feltételek: (kóddal)		Hálózati technológiák I., NIXHT1KBNE		
Heti óraszámok: 4	Előadás: 2	Tantermi gyakorlat.:	Laborgyakorlat: 2	Konzultáció:
Számonkérés módja:	vizsga			
A tananyag				
Oktatási cél: Megismertetni a hallgatókat a hálózati infrastruktúrát alkotó eszközök, a forgalomirányítók, a kapcsolók, a különféle alkalmazások és a hozzáférés menedzselését, hitelesítését, az adatforgalom támogatását intéző szerverek biztonságot érintő megoldásaival. A hallgatók megismerkednek a hálózaton belülről, illetve kívülről eredő támadásokkal, és ezek elhárításával a hálózati eszközök segítségével. Foglalkozunk a kifejezetten a hálózatvédelmet szolgáló eszközökkel, a tűzfalakkal, a hálózati behatolás védelmi és sérülékenységet vizsgáló eszközökkel is. A hallgatók megismerkednek az Openstack privát felhő megoldás alapjaival és biztonsági koncepcióival a Keystone és a Neutron komponenseken keresztül.				
Tematika: Hálózatbiztonsági alapismeretek. Hardver tűzfalak alkalmazása. Virtuális magán hálózatok (VPN). Hálózatok behatolás védelmi eszközei. Forgalomirányítók biztonsági alapszolgáltatásai. Kapcsolók biztonsági beállításai. Forgalomirányítók és kapcsoló együttesével kialakítható szűrő és védelmi rendszerek. A hálózati eszközök központi felügyelete és ennek biztonsági vonzatai. Hálózatmenedzsment és ennek biztonsági vonzatai.				

Féléves ütemezés:	
Oktatási hét (konzultáció)	Témakör
1.	Hálózatbiztonsági alapismeretek
2.	A forgalomirányítók védelmi eszközei
3.	AAA – hitelesítés, jogosultság-kezelés, könyvelés
4.	Hozzáférési listák
5.	Forgalomirányítókön megvalósítható védelmi megoldások (ZPF)
6.	IDS, IPS
7.	Kapcsolók védelmi megoldásai, LAN-ok védelme
8.	A biztonságos kommunikáció alapjai (VPN) I.
9.	A biztonságos kommunikáció alapjai (IPSec, SSL)
10.	Dedikált tűzfalak
11.	Hálózatmenedzsment
12.	Openstack alapok
13.	Openstack Keystone komponens
14.	Felhő biztonsági modellek
Félévközi követelmények	
Két megírt, legalább 80%-ot elérő ZH (teszt), kiselőadás megtartása, Otthoni feladatok szimulációs környezetben történő megoldása (legalább 4 db)	

Zárthelyi dolgozatok	
Oktatási hét (konzultáció)	Témakör
7.	1. ZH
13.	2. ZH
14.	Pót ZH
A félévzáró érdemjegy (é) kialakításának módszere	
Az évközi jegy / aláírás kialakításának módja	
Pótlás módja	
Az utolsó gyakorlaton egy ZH pótolható	
Vizsga módja	
Labor és szóbeli vizsga átlaga	
Vizsgajegy kialakítása	
Az érdemjegy számítási módja: a zh eredménye	
Az egyes érdemjegyek ponthatárai:	
0% - 49%:	elégtelen (1)
50% - 62%:	elégséges (2)
63% - 74%:	közepes (3)
75% - 86%:	jó (4)
87% - 100%:	jeles (5)
Irodalom	
Kötelező:	
Az előadások prezentációi, és gyakorlati útmutatók.	
Ajánlott:	
Fundamentals of Network Security Companion Guide (Cisco Networking Academy Program) Cisco Systems, Cisco Networking Academy Program, ISBN: 1587131226 Fundamentals of Network Security Lab Companion and Workbook (Cisco Networking Academy Program) Cisco Systems, Inc., Cisco Networking Academy Program. ISBN: 1587131234 Matt Dorn, Preparing for the Certified OpenStack Administrator Exam, Packt Publishing, ISBN: 1787288412	
Egyéb segédletek:	