Óbudai Egyetem Neumann János Informatikai Kar			Biomatika Intézet	
Tantárgy neve és kódja: *Logelemzés NIXLO1KSLE* *Tantárgyfelelős: Dr. Póser Valéria* *Kiberbiztonsági szakmérnök/szakember SZT szak*			**Kreditérték:** *4* *Levelező tagozat 2017/18 tanév II. félév*	
Tantárgy oktató(i): Dr. Krasznay Csaba, Höltzl Péter				
Előtanulmányi feltételek: (kóddal)	-			
Heti óraszámok:	Előadás: 1	Tantermi gyak.: 0	Laborgyakorlat: 0,5	Konzultáció: 0
Számonkérés módja:	Évközi jegy			
A tananyag				
Oktatási cél: A tárgy célja, megismertetni a hallgatókkal a hálózati logelemzés elvi hátterét, eszközeit, a hálózati forgalom monitorozására és rögzítésére használható megoldásokat.				
Tematika: Megfelelőségi követelmények, belső szabályozás; Naplózó infrastruktúrák; A logok, mint bizonyítékok; Naplózó-, elemző-, gyűjtő rendszerek; Naplózás felhő rendszerekben.				

Féléves ütemezés:	
Oktatási hét (konzultáció)	Témakör
1.	EA: Bevezetés
2.	EA: Megfelelőségi követelmények
3.	EA: Naplózó infrastruktúrák tervezési kérdései
4.	EA: Belső szabályozás
5	EA: Alkalmazásfejlesztési megközelítés
6.	EA: A logok, mint bizonyítékok
7.	EA: Mi az a syslog? A syslog útja. Keletkezés. A keletkezés problémái. A továbbítás. Küldés (push) vagy Összegyűjtés (fetch).
8.	LAB: Protokollok. SIEM megoldások. Az üzenet továbbítás problémái. Üzenet formátumok.
9.	EA:. Cloud és logging. Strukturáltság vagy nem strukturáltság?
10.	LAB: Normalizáció. Data enrichment. Szűrés. Korreláció. Analitika. Alerting.
11.	EA: Tárolás. Formátumok. Mennyiségi problémák kezelése. Elasticsearch/Logstash.
12.	LAB: Archiválás. Megjelenítés/Dashboard-ok. Report generátorok.
13.	ZH
14.	Pótlás

Félévközi követelmények
Elméleti és/vagy gyakorlati feladatokat tartalmazó zárthelyi sikeres (legalább elégséges) megírása. Az előadások és laborgyakorlatok látogatása kötelező.

Zárthelyi dolgozatok	
Oktatási hét (konzultáció)	Témakör
13	ZH
14	Pótlás
1	Szöveg beírásához kattintson ide.

2019. 08. 07.

A *félévzáró érdemjegy* (é) kialakításának módszere

Az évközi jegy a ZH alapján kerül meghatározásra, melynek eredménye a következő táblázat alapján számítandó:

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

Pótlás módja

Az évközi jegy pótlásának módja: a vizsgaidőszak első 10 munkanapjának egyikére meghirdetett időpontban, egy alkalommal, ismétlő vizsga jelleggel.

Vizsga módja

Szöveg beírásához kattintson ide.

Vizsgajegy kialakítása

Szöveg beírásához kattintson ide.

Irodalom

Kötelező:

A Moodle rendszerben közzétett anyagok.

Ajánlott:

Egyéb segédletek:

Az előadások és laborgyakorlatok nem teljes anyaga és további segédletek a Moodle rendszerben