INFORMAČNÝ LIST PREDMETU

Vysoká škola: Univerzita Komenského v Bratislave

Fakulta: Fakulta managementu

Kód predmetu:	**Názov predmetu:**
FM.KIS/280ME/21	Kybernetická bezpečnosť a etický hacking

Druh, rozsah a metóda vzdelávacích činností:
Forma výučby: prednáška / seminár
Odporúčaný rozsah výučby (v hodinách):
Týždenný: **Za obdobie štúdia:** 16s / 16s
Metóda štúdia: kombinovaná

Počet kreditov: 6

Odporúčaný semester/trimester štúdia: 4.

Stupeň štúdia: II.

Podmieňujúce predmety:

Podmienky na absolvovanie predmetu:
Online prezentácia na vybranú tému. Študent odprezentuje svoju seninárnu prácu vytvorenú v MS Power point alebo iný prezentačný nastroj - online cez MS Teams alebo inú dohodnutú platformu. (40% celkového hodnotenia)
Študent vypracuje seminárnu prácu v MS Word na vybranú tému po dohode s vyučujúcim. (60% celkového hodnotenia)
Termíny odovzdávania seminárnych prác budú stanovené počas online výučby po dohode so študentami.
Váha priebežného / záverečného hodnotenia: 40/60

Výsledky vzdelávania:
Cieľom predmetu je objasniť zložitosť a rozsah problému zabezpečenia systémov pre spracovanie údajov a poskytovanie informácií s dôrazom na úlohu manažéra v procese budovania a prevádzkovania takýchto systémov. Po úspešnom absolvovaní budú študenti ovládať základy IT bezpečnosti a budú schopní testovať bezpečnosť IS / IKT a vo firme, uplatňovať princípy IS / IT a informačnej bezpečnosti vo svojej manažérskej činnosti na pozíciách v rámci IT i mimo IT a pôsobiť v oblasti systému riadenia informačnej bezpečnosti vo firme v rôznych fázach vývoja životného cyklu informačného systému vo všetkých manažérskych pozíciách.

Stručná osnova predmetu:
1 seminár:
Úvod do etického hackingu, Základne pojmy - Minulosť, prítomnosť a budúcnosť v oblasti počítačovej bezpečnosti, Legislatíva
2 seminár:
OWASP, Kali Linux, Penetračné testovanie, Bezpečnosť
webových stránok, Zakladné hackerské techniky, Zraniteľnosti na hardvérovej úrovni,
3 seminár:
Personálna bezpečnosť, Trendy v manažmente bezpečnosti, Sociálne inžinierstvo, OWASP - Open Web Application Security Project
4 seminár:
Demonštrácia monitorovania sietí, Praktická ukážka penetračného testu IT bezpečnosti servera, Prezentácia študentov na vybranú tému

Odporúčaná literatúra:

[1.] Engebretson P.: The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series), 2011, ISBN-13: 978-1597496551 [2.] Scambray J., Liu V., Sima C. Hacking Exposed Web Applications, Third Edition, 2010, ISBN-13: 978-0071740647 [3.] Tipton, H F. -- Krause, M. Information security management [elektronický zdroj]: handbook. [S.l.]: Auerbach Publications, 2007. 978-1-4200-6045-4 [4.] Stallings, W.; Brown, L.: Computer Security, Principle and Practise, 2nd Edition, Prentice Hall, 2011, ISBN-10: 0132775069; [4.] Stallings, W.: "Cryptography and Network Security: Principles and Practice", 5th Edition. Prentice Hall, 2010, ISBN-10: 0-13-609704-9
[5.] OWASP. Category:OWASP -2021,Top Ten Project - OWASP. Dostupné na internete: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Jazyk, ktorého znalosť je potrebná na absolvovanie predmetu:

Poznámky:

Témy seminárnych prác:
Spôsoby ochrany pred Phishingom
Bezpečnosť WIFI sietí
Strana: 1Moderné vírusy
kryptografia
OWASP
Penetračné testovanie
Monitoring sietí
Techniky penetračného testovania
Rozdelenie a metodiky testovania
Zákon o ochrane osobných údajov
Spôsoby ochrany pred DdoS
Spôsoby ochrany pred Cross-site Scripting
Botnet

Hodnotenie predmetov

Celkový počet hodnotených študentov: 4

A	ABS	B	C	D	E	FX	M
50,0	0,0	25,0	25,0	0,0	0,0	0,0	0,0

Vyučujúci: Mgr. Vincent Karovič, PhD.

Dátum poslednej zmeny: 13.02.2022

Schválil: