INFORMAČNÝ LIST PREDMETU

Vysoká škola: Univerzita Konštantína Filozofa v Nitre

Fakulta: Fakulta prírodných vied a informatiky

Kód predmetu: KI/TCTF/26	**Názov predmetu:** Techniky CTF kybernetických hier

Druh, rozsah a metóda vzdelávacích činností:
Forma výučby: Seminár
Odporúčaný rozsah výučby (v hodinách):
Týždenný: 2 **Za obdobie štúdia:** 26
Metóda štúdia: prezenčná

Počet kreditov: 3

Odporúčaný semester/trimester štúdia: 6.

Stupeň štúdia: I.

Podmieňujúce predmety:

Podmienky na absolvovanie predmetu:
Aktívna účasť na seminároch. V priebehu semestra rieši študent sadu praktických individuálnych zadaní k jednotlivým témam (100%) a zúčastní sa záverečného CTF turnaja. Kredity nebudú udelené študentovi, ktorý získa v celkovom bodovom hodnotení menej ako 70 percent bodov.
Hodnotenie:
absolvoval = 100 % - 70 %, neabsolvoval = 69 % - 0 % .

Výsledky vzdelávania:
Znalosti absolventa predmetu
Po absolvovaní predmetu študent získa nasledujúce teoretické a aplikačné znalosti:
• princípy a typológiu Capture The Flag (CTF) súťaží a ich využitie v kybernetickej bezpečnosti,
• architektúru operačných systémov a sieťových služieb z pohľadu bezpečnosti,
• základné a pokročilé kryptografické algoritmy, klasické kódy a šifry a ich slabiny v kontexte CTF úloh,
• princípy steganografie a techniky ukrývania informácií v súboroch,
• typické zraniteľnosti webových aplikácií a mechanizmy ich zneužitia,
• princípy forenznej analýzy digitálnych dát a sieťovej komunikácie,
• základy reverzného inžinierstva a analýzy binárnych súborov,
• pamäťový model programov a mechanizmy vzniku binárnych zraniteľností,
• princípy OSINT (Open Source Intelligence) a možnosti získavania informácií z verejne dostupných zdrojov,
• obranné mechanizmy moderných systémov a spôsoby ich obchádzania v CTF prostredí,
• právne a etické rámce kybernetickej bezpečnosti, OSINT a bezpečnostného testovania.
Zručnosti absolventa predmetu
Po absolvovaní predmetu študent nadobudne nasledujúce odborné a praktické zručnosti:
• praktická práca v CTF a sandbox prostredí (Linux, VM, Docker),
• používanie bezpečnostných nástrojov na analýzu zraniteľností,
• riešenie kryptografických, steganografických, forenzných, webových, OSINT a binárnych CTF úloh,
• vyhľadávanie, korelácia a overovanie informácií z otvorených zdrojov (OSINT),
• dešifrovanie a analýza kódov a šifier, nájdenie skrytých informácií v súboroch,
• základná analýza sieťovej komunikácie a sieťových služieb,

• aplikácia techník reverzného inžinierstva a binary exploitation v kontrolovanom prostredí,
• tímová spolupráca pri riešení kybernetických incidentov,
• tvorba technickej dokumentácie a CTF write-upov,
• kritické myslenie pri hodnotení bezpečnostných rizík a dôveryhodnosti informácií,
• dodržiavanie etických a právnych princípov kybernetickej bezpečnosti a OSINT.

Výsledky vzdelávania

Po úspešnom absolvovaní predmetu študent:
• vysvetlí princípy a typy CTF hier a ich význam v oblasti kybernetickej bezpečnosti,
• identifikuje a analyzuje bežné zraniteľnosti softvéru, webových aplikácií a sieťových služieb,
• aplikuje OSINT techniky na získavanie a analýzu informácií z verejne dostupných zdrojov,
• aplikuje vhodné techniky na riešenie kryptografických, steganografických, forenzných a reverzno-inžinierskych úloh,
• demonštruje schopnosť exploitovať vybrané zraniteľnosti v kontrolovanom prostredí,
• dokáže dešifrovať a analyzovať kódy a šifry, identifikovať skryté informácie v súboroch,
• navrhne základné obranné opatrenia na minimalizáciu bezpečnostných rizík,
• pracuje efektívne v tíme pri riešení CTF úloh a súťaží,
• vypracuje odborný technický write-up dokumentujúci postup riešenia vrátane OSINT a steganografie,
• posúdi etické a právne aspekty bezpečnostného testovania a OSINT aktivít.

Stručná osnova predmetu:

1. Úvod do CTF hier a ich typológia
2. Prostredie a nástroje pre CTF (Linux, VM, Docker)
3. Kryptografia a klasické kódy a šifry v CTF
4. OSINT a analytické techniky pre získavanie informácií z verejných zdrojov
5. Webové zraniteľnosti
6. Forenzná analýza dát a steganografia
7. Reverzné inžinierstvo
8. Binary exploitation
9. Sieťové CTF úlohy
10. Záverečný CTF turnaj

Odporúčaná literatúra:

Jazyk, ktorého znalosť je potrebná na absolvovanie predmetu:
slovenský, anglický

Poznámky:

Hodnotenie predmetov
Celkový počet hodnotených študentov: 0

ABS	N
0.0	0.0

Vyučujúci: PaedDr. Peter Švec, Ph.D.,

Dátum poslednej zmeny: 12.01.2026

Schválil : prof. RNDr. Michal Munk, PhD. Dátum schválenia: 19.12.2025