Mondragon Unibertsitatea

ERASOKO SEGURTASUNA UNIBERTSITATE MIKRO-KREDENTZIALA (ONLINE)

GAIA	Informatika, Telekomunikazio Sistemak eta Sistema Txertatuak
ECTS/ORDUAK	3 ECTS
EGUTEGIA	2027/01/11 - 2027/02/26
HIZKUNTZA	Gaztelania
MODALITATEA	Online

Informazio gehiago eta izen-ematea

HELBURUAK

- Segurtasun iraingarriaren eta pentesting-aren printzipioak, irismena eta etika ulertzea.
- Sistema, aplikazio eta sareetan kalteberatasunak identifikatzea eta ustiatzea, teknika eta tresna espezifikoen bidez.
- Cloud inguruneetan errekonozimenduko, ustiapeneko, pibotingeko, iheseko eta erasoko teknikak aztertzea eta aplikatzea.
- Red Teaming metodologiak ezagutzea eta praktikatzea, zibereraso aurreratuen aurrean antolakuntza-erresilientzia ebaluatzeko.
- Aurkikuntzak dokumentatzeko eta sartze-testen txostenak egiteko gaitasuna garatzea.

PROGRAMA

- **Eraso-segurtasunerako sarrera.** Modulu honek segurtasun erasokorraren oinarriak sartzen ditu, eta erakundeen segurtasunaren hobekuntzan sartze-proben garrantzia nabarmentzen du. Funtsezko kontzeptuak jorratzen dira, hala nola hacking etika, eraso-jardueren irismena eta pentesting eta hacking arteko aldea. Ikasteko itxaropenak eta horiek mundu errealean duten aplikazioa ere ezartzen dira.

- **Gizarte Ingeniaritza eta HUMINT.** Ingeniaritza sozialeko eta informazio-bilketako teknikak erabiltzen ditu giza iturrien bidez (HUMINT). Moduluak erasotzaileek portaerak nola manipulatzen dituzten eta giza ahultasunak nola ustiatzen dituzten estaltzen du, informazio konfidentzialerako sarbidea lortzeko, eraso mota horiek gauzatzeko tresna komunak arakatzeaz gain.

- **Aintzatespen-faseak.** Modulu honek eraso iraingarri baten hasierako etapak aztertzen ditu, informazioa biltzeko tekniken bidez. OSINT, Maltego, The Harvester eta Nmap tresnak erabiltzen dira

ahulguneak identifikatzeko eta sareak mapatzeko. Erabilgarritasun aurreratuak ere sartzen dira, hala nola WhatWeb, Nikto eta Gobuster, web-teknologiak aztertzeko eta kalteberatasunak esploratzeko.

- **Kalteberatasunak eta ustiapena.** Sistemetako eta aplikazioetako kalteberatasunak identifikatu eta ustiatzera bideratzen da. OWASP Top 10aren azterketa xehatua barne hartzen du, baita ahulezia horiek web segurtasunari nola eragiten dioten ere. Gainera, Metasploitable2-rekin praktikak egiten dira, Metasploit erabiliz, ingurune kontrolatu batean ustiapen-teknikak aplikatzeko.

- **Pibotinga eta albo-mugimenduak.** Sare konprometitu baten barruan sarbidea zabaltzeko teknikak aztertzen ditu. Pivoting-estrategiak eztabaidatzen dira, albotik mugitzeko eta azpiegituraren barruan beste sistema batzuetara sartzeko. Moduluan, mugimendu horiek modu diskretuan eta eraginkorrean errazteko tresnak erabiltzen dira.

- **Ihes-teknikak.** Firewall-ak saihesteko metodo aurreratuak eta arrotzak detektatzeko sistemak (IDS) aztertzen ditu. Ofusikazio-teknikak, tunelen eta proxieen erabilera eta erasotzaileek sare korporatiboetako segurtasun-hesiak nola gainditzen dituzten estaltzen dira. Ezagutza hori funtsezkoa da segurtasun-kontrol tradizionalak nola saihesten diren ulertzeko.

- **Cloud azpiegituraren aurkako erasoak.** Ingurune horiek zer diren, erasoak eta kalteberatasunak, ingurune horien arrisku bakarren ulermena eta ingurune horiek ustiatzeko erabiltzen diren teknikak eta tresnak aztertzen ditu.

- **Teaming sarea eta metodologiak.** Red Teaming kontzeptua sartzen du, benetako erasoak simulatzeko eta erakunde bat mehatxu aurreratuen aurrean prestatzeko ikuspegi koordinatua. Blue Teaming bidezko desberdintasunak eta ariketa praktikoen plangintza lantzen dira, aurkikuntzen dokumentazioa eta ikasitakoa barne.

Multzo honetako jarduera praktikoetan ingeniaritza sozialeko ariketak, OSINT txostenak edo makina kaltebera baten intrusio-test bat sartzen dira.

IRAKASLEAK

Beleña De Lamor, Joel

EGUTEGIA

2027/01/11 - 2027/02/26

-

http://193.146.78.145:8080/Plone/eu/ikastaroa/erasoko-segurtasuna