Az „Informatikai biztonság” című tárgy tematikája

Korunk egyik mindannyiunkat érintő, igen érzékeny témája informatikai rendszereink biztonsága. Naponta hallhatunk rémisztő híreket biztonsági incidensekről, a sérülékenységeket kihasználó bűnözőkről és a kiberháborús fenyegetettségről.

Ám azzal együtt, hogy egyre több és súlyosabb támadással kell szembenéznünk, az informatikai biztonságról alkotott ismereteink is gyarapodnak, egyre kiterjedtebbek és rendszerezettebbek, és mára már nélkülözhetetlenek nem csak a szoftverfejlesztők és üzemeltetők, de a vállalatvezetők vagy alapszinten az egyszerű felhasználók számára is.

A kurzus célja egységes szemléletben áttekinteni, rendszerezni az alapvető informatikai biztonsági ismereteket, felhívni a figyelmet a veszélyekre, de bemutatni a védekezést és a bevált gyakorlatokat is, ezzel segítve a hallgatóságot, hogy modern biztonságcentrikus gondolkodásmódot alakítsanak ki magukban.

Az előadások tematikája lefedi a nemzetközi, gyártó és technológiafüggetlen CompTIA Security+ minősítővizsga témaköreit. A kurzushoz tartozó laborgyakorlatok pedig sérülékeny virtuális gépek és hálózatok közvetlen vizsgálatával bevezetést kívánnak nyújtani az etikus hackelés gyakorlatába bemutatva annak módszereit és eszközeit (Google Hacking, Kali Linux, Metaspoit, BeEF, stb.) Emellett a gyakorlatok segítséget kívánnak nyújtani a hallgatóknak az informatikai biztonsági témájú "Capture the flag (CTF)" versenyeken (például Hacktivity CTF, CSAW CTF, picoCTF) való részvételre, valamint a kurzus fórumot kíván biztosítani az aktuális biztonsági hírek, események, problémák és bármilyen információbiztonsággal kapcsolatos kérdés megvitatására.

A hallgatók részvétele a kurzuson egy előzetes teszt kitöltéséhez és egy etikai nyilatkozat aláírásához kötött, mely rögzíti, hogy a résztvevők a kurzuson szerzett ismereteket nem használják illegális célokra.

Előfeltételek: az IB103 Programozás alapjai, IB402 Operációs rendszerek és IB407 Számítógép hálózatok című kurzusok teljesítése.

Részletes tematika

1. Az informatikai biztonság alapfogalamai. Biztonsági célok (bizalmasság, integritás, rendelkezésre állás, hitelesítés, letagadhatatlanság), biztonság, kényelem, és funkcionalitás viszonya, használható biztonság, biztonsági alapelvek.

2. Biztonságmenedzsment, fenyegetések, sérülékenységek, kockázatok. Fenyegetések típusai. Biztonsági kontrollok típusai. Kockázatfelmérés módszerei, kockázatmenedzselés.

3. Támadók és támadások fajtái. Hackerek, motivációik, kiberbűnözés, deffenzív és offenzív védelem, etikus hackelés, sérülékenységvizsgálat és behatolástesztelés, a behatolástesztelés fázisai, eszközei.

4. Kriptográfiai és szteganográfiai alapfogalmak, nyilvános kulcsú infrastuktúra, tanúsítványok, hitelesítés, a legfontosabb kriptográfiai titkosító algoritmusok, hash függvények, szabványok és protokollok.

5. Hálózati biztonság, hálózati eszközök biztonsága, hálózati protokollok, port biztonság, tűzfalak, behatolás észlelő és megelőző rendszerek (IDS/IPS), távoli hozzáférés, VPN-ek. Hálózatok diagnosztikája és monitorozása. Szolgáltatásbénító támadások (DoS,DDoS), botnetek. Vezetéknélküli hálózatok biztonsága.

6. Hozzáférésvédelem és identitáskezelés. Hozzáférésvédelmi modellek. AAA (authentication, authorization, accounting – azonosítás, jogosultságkezelés, könyvelés). Azonosítási módszerek, autentikációs protokollok. Jelszavak, jelszavak erőssége, jelszótörési módszerek és eszközök. Biometrikus azonosítás.

7. Emberek megtévesztése (Social Engineering), támadási módszerek, személyiséglopás (Identity Theft), adathalászat (Phising) és változatai.

8. Operációs rendszer- és alkalmazásbiztonság. Szoftverek sérülékenységei és azok kihasználása, kártékony kódok (vírusok, férgek, trójaiak, spam), védekezés ellenük. Támadási stratégiák, jogosultság kiterjesztés.

9. Webalkalmazások biztonsága és védelme, OWASP TOP 10 fenyegetettségek és védekezés ellenük.

10. Fizikai biztonság. Épületek, helyiségek és eszközök védelme, beléptető, behatolás védelmi, tűzjelző és videó ellenőrző rendszerek. Zárak és zárnyitási technikák (Lockpicking).

11. Vészhelyreállítás (Disaster Recovery) és üzletmenet folytonossági terv (Business Continuity Plan). Biztonsági mentések.

12. Üzemeltetésbiztonság (Operation Security). Biztonsági szabályzatok, szabványok és útmutatások. Biztonságtudatosság és tréning a vállalatoknál. Az informatikai biztonság menedzselése, ellenőrzése, megfelelőség (Compliance) és biztonsági audit.

13. Az információbiztonság etikai és jogi kérdései. Személyes adatok védelme, vita a sérülékenységek teljes közzétételéről (Full Disclosure Debate). Számítógép kriminalisztika (Computer Forensics), támadások nyomainak rögzítése és elemzése.

Irodalom:

W. A. Conklin, G. White, D. Williams, R. Davis, Ch. Cothren: *CompTIA Security+ All-in-One Exam Guide (Exam SY0-301)*, 3rd Edition, McGraw-Hill Osborne Media, 2011.

D. Gibbson: *CompTIA Security+: Get Certified Get Ahead: SY0-301 Study Guide*, CreateSpace Independent Publishing Platform, 2011.

M. Walker: *CEH Certified Ethical Hacker All-in-One Exam Guide*, McGraw-Hill Osborne Media, 2011.

S. Harris: CISSP All-in-One Exam Guide, 4th Edition, McGraw-Hill Osborne Media, 2008.

R. E. Smith: Elementary Information Security, Jones & Bartlett Learning, 2011.

W. Stallings: Cryptography and Network Security, 4th ed., Prentice Hall, NJ, 2006.