

Képzési tematika

Átfogó informatikai alapképzés leendő rendszergazdáknak, hackereknek

A képzés célja:

- intenzív, gyakorlat orientált képzési módszerrel kialakítani a szakmai alapokat,
- valamint egy olyan gondolkodásmódot, problémamegoldási stratégiát ami az egyéni fejlődést helyezi előtérbe,
- mindezt egyszerre windows és linux környezetben, hogy az egész szakmára rálátást adjon.

Mottó: without basics everything is useless

A képzés négy alapvetően elméleti modulból és négy gyakorlati modulból áll, ami modulonként 15 alkalomra van bontva, így az iskolai szorgalmi időszakhoz illesztve két éven át tart. Ez alatt az időszak alatt megismerjük az internetet annak működésével, műszaki alapjaival, lehetőségeivel és veszélyeivel együtt, megismerjük az informatika történetét – de csak az érdekes részeket –, szerzünk tapasztalatokat a hardverek világában, megértjük mit csinál a számítógépünk és hogyan, miért kell nekünk helyi hálózat és az hogyan működik, hogyan 'lesz internet a gépen', és mit tegyünk ha 'nincs internet'. Megismerkedünk a szerverek világával is, és építünk magunknak egyet. Építünk saját hálózatot és összekötjük az internettel, majd igyekszünk megvédeni.

Lényegében a képzés végére a cél, hogy egy otthoni, kisvállalati rendszert képes legyen minden résztvevő önállóan vagy társai és/vagy az internetes források segítségével kialakítani és üzemeltetni. Függetlenül attól, hogy az a rendszer Windows vagy Linux alapú-e, ugyanis a képzés során folyamatosan, minden témát mindkét hazánkban elterjedt operációs rendszert használva körüljárunk, azaz mindent amit csinálunk meg fogunk tudni oldani mindkét operációs rendszer használatával.

Történik mindez egy, a megszokott iskolarendszerű képzésektől gyökeresen eltérő módszerrel, kötöttségek és feszítő elvárások nélkül, egy pedagógus és egy felnőttoktató által összeállított egyedi módszertan alapján, gamification elemekkel tűzdelt gyakorlatorientált formában. A képzés egyedülálló a tekintetben is, hogy végzett kiberbiztonsági szakértő tartja és egyszerre mindkét elterjedt operációs rendszer használatát el lehet sajátítani, gyakorlati környezetben.

Kiberbiztonsági alapismeretek – láss mielőtt futni készülsz

- kibertér, hacker, informatikai támadások szakaszai I.
- informatikai támadások szakaszai II. (hogyan csinálja a hacker)
- informatikai támadások jellegzetességei, támadási vektorok
- informatikai támadások elleni védekezés módszerei, védelmi intézkedések
- támadás megtörténtének felismerése, jogi háttér, aktuális kibertrendek

A bevezető modulban megismerjük a minket körülvevő világot egy olyan szemüvegen keresztül, ami sajnos ma még keveseknek adatik meg – a kiberbiztonsági szakértő (vagy ha úgy tetszik etikus hacker) szemével. Megismerjük az interneten zajló események egy olyan részét, amit az átlag internetező nem lát, és csak akkor szembesül a létezésével mikor támadás éri. De milyen támadás, miért, hogyan, miért pont én? Mit tehetek ellene, ki segít nekem, mire kell figyeljek? Az első modul ezekre a kérdésekre segít választ találni – választ találni, mert a képzés célja nem a kész válaszok átadása, hanem a gondolkodásmód kialakítása, amely segítségével a ma még ismeretlen kihívásoknak is meg fogunk tudni felelni.

Biztonságtudatos üzemeltetés – saját laborkörnyezet kialakítása

- virtualizáció fogalma, hypervisor, VM, cloud
- virtualizáció szerepe a modern IT-ban, virtuális hálózatok
- virtualizált laborkörnyezet kialakítása - Windows VM telepítése
- virtualizált laborkörnyezet kialakítása - linux VM telepítése

A bevezető modult követően elkezdjük felépíteni a saját játszótérünket, ahol biztonságosan, szabadon és stresszmentesen tanulhatjuk meg a dolgok működését. Hiszen mint minden technológiát, az informatikát is úgy lehet mélységében, alaposan megismerni, ha mi építjük fel magunknak, elkövetjük a saját hibáinkat, majd megjavítjuk azokat. Ehhez megépítjük a saját laborunkat, hálózattal, gépekkel a saját laptopunkon – és később összekötjük őket egyetlen hálózattá.

Biztonságtudatos üzemeltetés - hálózati alapok

- alapismeretek. Számítógép alapelemei, operációs rendszerek, informatika történet, Neumann-i elvek, érdekességek
- célja, kialakulása, hogyan működik az internet
- műszaki alapok: OSI és TCP/IP modell
- fizikai közegek, MAC cím (hexadecimális számr.), IP cím (bináris számr.), netmask
- címtartományok, tiltott címek, IP cím kiosztás, kiemelt címek egy hálózatban
- gateway, NAT, névfeloldás, DNS, TCP, UDP, portok, portscan
- hálózati hibakeresés alapjai

Készen van a saját laborunk, de mielőtt tudnánk, mire akarjuk használni, előtte meg kell ismernünk a világunkat átszövő 'világszöveget' (ahogy a modern nyelvújítók nevezni akarták az internetet) működését, ehhez beszélünk a számítógépek működéséről, azok kialakulásáról, az internet kifejlődéséről, elterjedéséről, felépítéséről – és annak műszaki megoldásairól, először csak általánosságban, majd egyre specifikusabban. Egészen addig, amíg elkezdjük megérteni, hogy mi is valójában az internet – hogy ne csak egy felhőként képzeljük el, hogy hogyan működik, és miért.

Hálózatépítés - hálózatok fizikai kiépítése

- ethernet hálózat, 802.11 szabvány, kábeles hálózatok
- vezeték nélküli hálózatok, wifi, bluetooth, stb.
- vezetékes hálózati eszközök, vezeték nélküli hálózati eszközök
- laborkörnyezet kialakítása, vezetékes és vezeték nélküli hálózat kiépítése
- MAC, IP, NAT, DNS, gateway, ping, stb. a gyakorlatban
- a virtuális laborkörnyezet összefűlése az elkészült fizikai hálózattal
- hálózati hibakeresés a gyakorlatban
- hálózat monitorozása

A negyedik modulban bepiszkoljuk a kezünket. Megbeszéljük, milyen lehetőségeink vannak rá, majd építünk egy hálózatot. Vagy többet. Vezetékest, vezeték nélkülit. Összekötjük a tantermet a világgal, a virtuális laborjainkat a többiekével, majd megnézzük mit építettünk. Aztán elrontjuk, majd megjavítjuk. Közben húzunk és szerelünk kábelt, konfigurálunk routert és vadászunk nyílt wifire, és végül megértjük, mit és miért csinál a hálózat. A mi hálózatunk.

Biztonságos üzemeltetés - operációs rendszer alapok

- operációs rendszerek általános felépítése, virtualizáció, konténerizáció
- szoftverek típusai, grafikus felület, karakteres felület, ablakkezelők, parancsértelmező, csomagkezelés
- felhasználók, felhasználói csoportok, felhasználókezelés, bejelentkezés általában
- felhasználókezelés, jogosultságkezelés windows és linux rendszerekben
- adattárolás alapjai, partíciók, fájlrendszerek, fájlok, kiterjesztések, könyvtárak kezelése
- alapvető fájlkezelő parancsok, létrehozás, másolás-mozgatás, törlés, tömörítés, keresés
- fájlokhoz kapcsolódó jogosultságok, unix-szerű jogosultságkezelés, jogosultságkezelés windowson
- hardverek elérése unix és windows rendszerek alatt, eszközfájlok, pszeudoeszközök

Van hálózatunk, tegyünk rá gépeket. Mire ide jutunk, már tudjuk – nekünk nem elég a készen kapható megoldás, mert ha tanulunk, megértjük, tudunk jobbat. Ebben a modulban megtanuljuk miért kell jelszót adni a Windows belépéshez, miért nem elég egy felhasználó, hova tűnnek a fájlok amiket töröltünk de mégsem, és hogyan működik valójában egy számítógép. Egy linuxos és egy Windows alapú is. Ekkorra már párszor újratelepítjük a saját laborkörnyezetünkben futó gépeket, mert rájövünk, hogy máshogy akarjuk, és ekkora már tudjuk is máshogy.

Hálózati kiszolgálók - szerverekről alapszinten

- szerver-kliens architektúra, szerverek jellegzetességei, hardvereltérések, szervertípusok
- a szerverekkel szemben támasztott követelmények és kihívások, ezek megoldásai
- adattárolás kialakítása, mdadm, lvm, lemeztitkosítás
- fájlrendszer kialakítása, kezelése
- szerver telepítés, annak módjai, telepítés menete, csomagkezelés
- alap hálózati infrastruktúra kialakítása, ip, útválasztás, névfeloldás beállítása
- szerverek általános konfigurációja - hálózat, lemezkezelés, időbeállítás, feladatütemezés, távelérés

- szerverüzemeltetés alapjai, indítás, leállítás, szolgáltatások indítása, monitoring, biztonsági mentés
- tűzfal, tűzfalszabályok
- fájlserver telepítése, ftp, samba
- webserver telepítése, apache
- fájlserver biztonsági hardeningje
- webserver biztonsági hardeningje

A kiszolgálókkal foglalkozó moduljainak célja, hogy azzal a tudással felvértezve, amit az internet és a hálózatok működéséről, biztonságáról, az azt alkotó gépekről megtudtunk, kiegészítsük a puzzle utolsó darabkájával, a szerverekkel. Minden szerver számítógép, de nem minden számítógép szerver. Biztos? Megismerjük a szervereket, összehasonlítjuk az eddigi ismereteinkkel és csinálunk magunknak egyet. Egy olyat, amin az általunk készített weboldal fut. Kint az interneten. Nagyjából biztonságban. :)

Mobil- és telekommunikációs technológiák – ha már úgyis nálunk van

- a mobiltelefon mint számítógép
- mobiltelefon operációs rendszerek
- mobiltechnológiák, hang- és adatátviteli megoldások
- publikusan elérhető mobiltelefonrendszerek felépítése
- okostelefonok a vállalati felhasználóknál
- pár szó az IoT-ről

A mobilkommunikáció és az IoT (Internet of Things – dolgok internete) két olyan terület, mely már ma körbefonja életünket, de ezen technológiák működéséről az átlagember vajmi keveset tud. Megnézzük, hogyan működnek az okostelefonok, milyen hálózati technológia van a működésük mögött, és hogyan használják ezeket a készülékeket a vállalkozások, valamint érintjük az IoT-t is, mint a várhatóan hamarosan a mindennapi élet részét képező technológiát.

A tanultak alkalmazása – egy kisvállalkozás infrastruktúrája

A képzés utolsó moduljában összefésüljük azt a sok elméletet és gyakorlatot, amit eddig elsajátítottunk, és a csoport közösen felépíti egy jogi személyiséget tekintve fiktív, de igényeit tekintve nagyon is valós kisvállalkozás teljes informatikai hátterét, a mobiltelefonoktól a szerverekig, valós és virtuális környezet vegyes felhasználásával.

A képzésen résztvevők annak elvégzésekor tehát valóban képessé válnak egy KKV vállalati alap-infrastruktúra megtervezésére és implementációjára, annak egy a fenyegető kiberbiztonsági környezetben való alapszintű védelmére valamint ennek napi szintű üzemeltetésére. Természetesen a képzési módszertan ugyanúgy dinamikusan illeszkedik a résztvevők igényeihez, akárcsak a tematika egyes elemei esetén várható kismértékű eltérés attól a technológiai változások lekövetése érdekében. A képzés célja, hogy minden résztvevő számára elérhető, de kihívást jelentő feladatot nyújtson, és az egyéni problémamegoldási képességeket és a csoportmunkára való képességet fejlessze.