FELNŐTTKÉPZÉSI SZAKMAI PROGRAMKÖVETELMÉNY

1. a) A SZAKMAI PROGRAMKÖVETELMÉNY MEGNEVEZÉSE

Etikus hacker képzés

b) SZAKMAI VÉGZETTSÉG MEGNEVEZÉSE

Minősített etikus hacker

Szakmai programkövetelmény azonosító száma:	SzPk-00026-18-07 5 02 3 /2
Szakmai programkövetelmény érvényessége	2018-03-29

2. A SZAKMAI VÉGZETTSÉGGEL MEGSZEREZHETŐ KOMPETENCIÁKKAL

új, önálló tevékenység, munkaterületi feladat végezhető el

3. A SZAKMAI PROGRAMKÖVETELMÉNY MODULRENDSZERŰ

igen

programkövetelmény modul azonosító száma	modul megnevezése
SzPk-00026-18-07 5 02 3 /2 /M-01	Külső – Internet oldali – sérülékenység vizsgálat
SzPk-00026-18-07 5 02 3 /2 /M-02	Webes sérülékenység vizsgálat
SzPk-00026-18-07 5 02 3 /2 /M-03	Belső – LAN oldali – sérülékenység vizsgálat
SzPk-00026-18-07 5 02 3 /2 /M-04	Wifi sérülékenység vizsgálat
SzPk-00026-18-07 5 02 3 /2 /M-05	Az etikus hackelés speciális és kiegészítő területei

4. AZ OKJ-BAN SZEREPLŐ AZON SZAKMACSOPORT, AMELYBE A PROGRAMKÖVETELMÉNY BESOROLHATÓ

7 - Informatika

5. AZ EKKR-HEZ KAPCSOLÓDÓ MAGYAR KÉPESÍTÉSI KERETRENDSZER SZERINTI SZINTJÉNEK MEGHATÁROZÁSÁRA ÉS BESOROLÁSÁRA VONATKOZÓ MEGJELÖLÉSE

5 - szint

6. A SZAKMAI VÉGZETTSÉG JELLEGÉTŐL FÜGGŐEN A KÉPZÉS MEGKEZDÉSÉHEZ SZÜKSÉGES BEMENETI FELTÉTELEK

Iskolai előképzettség

érettségi végzettség

Szakmai előképzettség

szakmai előképzettséghez nem kötött

Egészségügyi alkalmassági követelmények

nem szükséges

Előírt gyakorlati idő

nem szükséges

Egyéb feltételek

nem szükséges

7. A SZAKMAI VÉGZETTSÉGGEL ELLÁTHATÓ LEGJELLEMZŐBB TEVÉKENYSÉG, VAGY MUNKATERÜLET RÖVID LEÍRÁSA

A résztvevők megismerik és elsajátítják az etikus hackelés módszertanát, képessé válnak külső (internet felőli), belső (LAN oldali), vezeték nélküli, mobilhálózati, valamint webes sérülékenységek feltárására. Megismerik a hálózati protokollokat és alkalmazásokat, emellett képesek lesznek Social engineering módszereket alkalmazni. A fentiek mellett elsajátítják, hogy az etikus hackelés munkákat milyen törvényi és jogi keretek között végezhetik.

8. SZAKMAI VÉGZETTSÉGGEL BETÖLTHETŐ MUNKAKÖR MEGNEVEZÉSE ÉS BESOROLÁSA

FEOR főcsoport megnevezése	FEOR száma	Foglalkozás megnevezése	A szakmai végzettséggel legjellemzőbben ellátható tevékenység, munkaterület
2. Felsőfokú képzettség önálló alkalmazását igénylő foglalkozások	2144	Számítógépes programozó	Etikus hacker

9. A SZAKMAI VÉGZETTSÉG MEGSZERZÉSÉHEZ SZÜKSÉGES KÉPZÉS KÉPZÉSI FORMÁTÓL FÜGGŐ MINIMÁLIS ÉS MAXIMÁLIS ÖSSZÓRASZÁMA, ÉS AZ ELMÉLETI ÉS GYAKORLATI IDŐ ARÁNYA

A képzés "Egyéni felkészítés" képzési formában megvalósítható?

Nem releváns

A képzés "Csoportos felkészítés" képzési formában megvalósítható?

Igen

Csoportos felkészítés	Minimum	Maximum
A képzés összóraszáma	216	264
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

A képzés "Távoktatás" képzési formában megvalósítható?

Igen

Távoktatás	Minimum	Maximum
A képzés összóraszáma	216	264
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

10. A SZAKMAI VÉGZETTSÉG MEGSZERZÉSÉT IGAZOLÓ DOKUMENTUM KIADÁSÁNAK FELTÉTELEI

1. a képzés felnőttképzési szerződésben megjelölt óraszámának hetven százalékán való részvétel, és
2. a szakmai záró beszámoló sikeres teljesítése

3.1. PROGRAMKÖVETELMÉNY MODUL RÉSZLETES BEMUTATÁSA

A programkövetelmény modul azonosító száma	SzPk-00026-18-07 5 02 3 /2 /M-01
A programkövetelmény modul megnevezése	Külső – Internet oldali – sérülékenység vizsgálat

3.1.1. A KÉPZÉS KÉPZÉSI FORMÁTÓL FÜGGŐ MINIMÁLIS ÉS MAXIMÁLIS ÓRASZÁMA, ÉS AZ ELMÉLETI ÉS GYAKORLATI IDŐ ARÁNYA

A modul "Egyéni felkészítés" képzési formában megvalósítható?

Nem releváns

A modul "Csoportos felkészítés" képzési formában megvalósítható?

Igen

Csoportos felkészítés	Minimum	Maximum
A képzés óraszáma	54	66
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

A modul "Távoktatás" képzési formában megvalósítható?

Igen

Távoktatás	Minimum	Maximum
A képzés óraszáma	54	66
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

3.1.2. SZAKMAI KÖVETELMÉNYEK LEÍRÁSA

A legjellemzőbb tevékenység vagy munkaterület ellátásához szükséges szakmai kompetenciákat leíró szakmai ismeretek, készségek és személyes kompetenciák, társas kompetenciák és módszerkompetenciák tanulási eredmények szerinti leírása

Tudás	Képesség	Attitűd	Felelősség, autonómia
Megismeri a külső sérülékenység vizsgálat módszereit és fázisait, a rendszerfelderítés technikáit és a penetrációs technikákat.	Képes a hálózati topológia feltérképezésére külső IP címről, a szolgáltatások behatárolására, azonosítására és a sérülékeny pontok azonosítására.	Módszereit az etikusság elvének megfelelően alakítja ki, ami azt jelenti, hogy a vizsgálat célja a rendszer védelmi szintjének emelése illetve hogy a vizsgált információs/informatikai rendszer rendelkezésre állása zavartalan marad.	Kialakított eszköztára használata során a felelőssége, hogy az alkalmazott módszerei az információs/informatikai rendszer rendelkezésre állását ne zavarják meg annak érdekében, hogy az üzletmenet folyamatos maradjon.

Megtanulja alkalmazni az automatikus és manuális sérülékenység vizsgálathoz tartozó tudását; a külső sérülékenységek elhárítását.	Képes lesz a külső sérülékenységek kiaknázására és elhárítására. Képessé válik automatikus és manuális sérülékenységvizsgálati feladatok menedzselésére és végrehajtására.	A feladat elvégzése során a megbízó igényeit és érdekeit maximálisan figyelemben tartva, legális keretek között, megbízási szerződés alapján végzi.	A feladat végrehajtása során felelőssége az információs/informatikai rendszer összes sérülékeny pontjának azonosítása, és mindegyikre tett megoldási vagy sérülékenység szint csökkentési javaslat megadása.
Megtanulja a feltárt sérülékenységek és azokra tett javaslatok megfelelő szóbeli és írásbeli kommunikációját.	Képessé válik a megbízót megfelelő módon és minőségben tájékoztatni a rendszer sérülékeny pontjairól és a megoldási javaslatairól.	A megbízót a feladat végrehajtása során megfelelő mélységben és minőségben tájékoztatja a feltárt sérülékenységekről és azok elhárítására tett javaslatairól.	Felelős a megbízó átfogó tájékoztatásáért, az átadott írásbeli dokumentumok és szóbeli információk minőségéért. Felelős azért, hogy az általa feltárt sérülékeny pontok rajta keresztül ne kerüljön illetéktelenekhez.

A tervezett képzés munkaerő-piaci relevanciája

Az etikus hackelés mára a világ egyik legnépszerűbb és legjobban megfizetett szakmája. Mára már a magánszemélyek és a cégek túlnyomó többsége él és dolgozik számítógéppel, számítógépes hálózattal, internettel, mobiltelefonnal, melyek nagy része szinte teljesen védtelen és felkészületlen az információ biztonsági sérülékenységeket kihasználó rosszindulatú hackerek támadásaival, vírusokkal, vagy a nem megfelelő fejlesztésből vagy üzemeltetésből adódó rendszerhibákkal szemben. Az etikus hackerek feladata megvédeni az információs és az informatikai rendszereket, feltárni a sebezhető pontjaikat, megfogalmazni a javító, illetve védelmi intézkedéseket és megoldásokat, sikeresen végigfuttatni a feladatot mindvégig együttműködve és kommunikálva a megbízóval. Mára a bankok, telekommunikációs cégek és a kormányzati, nemzetbiztonsági szféra egyaránt alkalmaz etikus hackereket, az ügyfeleik személyes adatainak védelme érdekében, vagyonuk biztonsága érdekében, illetve az ország kibertámadásokkal szembeni megfelelő védelmi és készültségi szintjének érdekében.

3.2. PROGRAMKÖVETELMÉNY MODUL RÉSZLETES BEMUTATÁSA

A programkövetelmény modul azonosító száma	SzPk-00026-18-07 5 02 3 /2 /M-02
A programkövetelmény modul megnevezése	Webes sérülékenység vizsgálat

3.2.1. A KÉPZÉS KÉPZÉSI FORMÁTÓL FÜGGŐ MINIMÁLIS ÉS MAXIMÁLIS ÓRASZÁMA, ÉS AZ ELMÉLETI ÉS GYAKORLATI IDŐ ARÁNYA

A modul "Egyéni felkészítés" képzési formában megvalósítható?

Nem releváns

A modul "Csoportos felkészítés" képzési formában megvalósítható?

Igen

Csoportos felkészítés	Minimum	Maximum
A képzés óraszáma	43	53
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

A modul "Távoktatás" képzési formában megvalósítható?

Igen

Távoktatás	Minimum	Maximum
A képzés óraszáma	43	53
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

3.2.2. SZAKMAI KÖVETELMÉNYEK LEÍRÁSA

A legjellemzőbb tevékenység vagy munkaterület ellátásához szükséges szakmai kompetenciákat leíró szakmai ismeretek, készségek és személyes kompetenciák, társas kompetenciák és módszerkompetenciák tanulási eredmények szerinti leírása

Tudás	Képesség	Attitűd	Felelősség, autonómia
Megismeri a webes sérülékenység feltárási módszereket és az informatikai rendszerek weben keresztüli kompromittálásának technikáit.	Képes egy informatikai rendszert annak webes felületén keresztül kompromittálni. Képes a webes alkalmazások sérülékenységeinek azonosítására.	Módszereit az etikusság elvének megfelelően alakítja ki, ami azt jelenti, hogy a vizsgálat célja a rendszer védelmi szintjének emelése, illetve, hogy a vizsgált információs/informatikai rendszer rendelkezésre állása zavartalan marad.	Kialakított eszköztára használata során a felelőssége, hogy az alkalmazott módszerei az információs/informatikai rendszer rendelkezésre állását ne zavarják meg annak érdekében, hogy az üzletmenet folyamatos maradjon.

Megtanulja alkalmazni a webes sérülékenységvizsgálattal kapcsolatos tudását; a feltárt sérülékenységek elhárítását.	Képessé válik a webes sérülékenységek kiaknázására és elhárítására. Képessé válik webes sérülékenységvizsgálati feladatok menedzselésére és végrehajtására.	A feladatok végrehajtása során a megbízó igényeit és érdekeit maximálisan figyelemben tartva, legális keretek között, megbízási szerződés alapján végzi.	A feladat végrehajtása során felelőssége az információs/informatikai rendszer összes sérülékeny pontjának azonosítása, és mindegyikre tett megoldási vagy sérülékenység szint csökkentési javaslat megadása.
Megtanulja a feltárt sérülékenységek és azokra tett javaslatok megfelelő szóbeli és írásbeli kommunikációját.	Képessé válik a megbízót megfelelő módon és minőségben tájékoztatni a rendszer sérülékeny pontjairól és a megoldási javaslatairól.	A megbízót a feladat végrehajtása során megfelelő mélységben és minőségben tájékoztatja a feltárt sérülékenységekről és azok elhárítására tett javaslatairól.	Felelős a megbízó átfogó tájékoztatásáért, az átadott írásbeli dokumentumok és szóbeli információk minőségéért. Felelős azért, hogy az általa feltárt sérülékeny pontok rajta keresztül ne kerüljön illetéktelenekhez.

A tervezett képzés munkaerő-piaci relevanciája

Az etikus hackelés mára a világ egyik legnépszerűbb és legjobban megfizetett szakmája. Mára már a magánszemélyek és a cégek túlnyomó többsége él és dolgozik számítógéppel, számítógépes hálózattal, internettel, mobiltelefonnal, melyek nagy része szinte teljesen védtelen és felkészületlen az információ biztonsági sérülékenységeket kihasználó rosszindulatú hackerek támadásaival, vírusokkal, vagy a nem megfelelő fejlesztésből vagy üzemeltetésből adódó rendszerhibákkal szemben. Az etikus hackerek feladata megvédeni az információs és az informatikai rendszereket, feltárni a sebezhető pontjaikat, megfogalmazni a javító, illetve védelmi intézkedéseket és megoldásokat, sikeresen végigfuttatni a feladatot mindvégig együttműködve és kommunikálva a megbízóval. Mára a bankok, telekommunikációs cégek és a kormányzati, nemzetbiztonsági szféra egyaránt alkalmaz etikus hackereket, az ügyfeleik személyes adatainak védelme érdekében, vagyonuk biztonsága érdekében, illetve az ország kibertámadásokkal szembeni megfelelő védelmi és készültségi szintjének érdekében.

3.3. PROGRAMKÖVETELMÉNY MODUL RÉSZLETES BEMUTATÁSA

A programkövetelmény modul azonosító száma	SzPk-00026-18-07 5 02 3 /2 /M-03
A programkövetelmény modul megnevezése	Belső – LAN oldali – sérülékenység vizsgálat

3.3.1. A KÉPZÉS KÉPZÉSI FORMÁTÓL FÜGGŐ MINIMÁLIS ÉS MAXIMÁLIS ÓRASZÁMA, ÉS AZ ELMÉLETI ÉS GYAKORLATI IDŐ ARÁNYA

A modul "Egyéni felkészítés" képzési formában megvalósítható?

Nem releváns

A modul "Csoportos felkészítés" képzési formában megvalósítható?

Igen

Csoportos felkészítés	Minimum	Maximum
A képzés óraszáma	65	79
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

A modul "Távoktatás" képzési formában megvalósítható?

Igen

Távoktatás	Minimum	Maximum
A képzés óraszáma	65	79
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

3.3.2. SZAKMAI KÖVETELMÉNYEK LEÍRÁSA

A legjellemzőbb tevékenység vagy munkaterület ellátásához szükséges szakmai kompetenciákat leíró szakmai ismeretek, készségek és személyes kompetenciák, társas kompetenciák és módszerkompetenciák tanulási eredmények szerinti leírása

Tudás	Képesség	Attitűd	Felelősség, autonómia
Megismeri a belső sérülékenység-vizsgálat fázisait, a belső hálózati topológia valamint a belső szolgáltatások jellemzőit és a belső sérülékenységvizsgálati technikákat.	Képes a belső hálózati topológia feltérképezésére, szolgáltatások behatárolására, sérülékeny pontok azonosítására.	Módszereit az etikusság elvének megfelelően alakítja ki, ami azt jelenti, hogy a vizsgálat célja a rendszer védelmi szintjének emelése, illetve, hogy a vizsgált információs/informatikai rendszer rendelkezésre állása zavartalan marad.	Kialakított eszköztára használata során a felelőssége, hogy az alkalmazott módszerei az információs/informatikai rendszer rendelkezésre állását ne zavarják meg annak érdekében, hogy az üzletmenet folyamatos maradjon.

Megtanulja önállóan végrehajtani az automatikus és a manuális szolgáltatás-ellenőrzést. Megtanulja az ellenőrzött szolgáltatások feltörését, jogosultságok szerzését és a nyomok elfedését.	Képessé válik a belső sérülékenységek kiaknázására és elhárítására. Képessé válik belső sérülékenységvizsgálati feladatok menedzselésére és végrehajtására.	A feladatok elvégzése során a megbízó igényeit és érdekeit maximálisan figyelemben tartva, legális keretek között, megbízási szerződés alapján végzi.	A feladat végrehajtása során felelőssége az információs/informatikai rendszer összes sérülékeny pontjának azonosítása, és mindegyikre tett megoldási vagy sérülékenység szint csökkentési javaslat megadása.
Megtanulja a feltárt sérülékenységek és azokra tett javaslatok megfelelő szóbeli és írásbeli kommunikációját.	Képessé válik a megbízót megfelelő módon és minőségben tájékoztatni a rendszer sérülékeny pontjairól és a megoldási javaslatairól.	A megbízót a feladat végrehajtása során megfelelő mélységben és minőségben tájékoztatja a feltárt sérülékenységekről és azok elhárítására tett javaslatairól.	Felelős a megbízó átfogó tájékoztatásáért, az átadott írásbeli dokumentumok és szóbeli információk minőségéért. Felelős azért, hogy az általa feltárt sérülékeny pontok rajta keresztül ne kerüljön illetéktelenekhez.

A tervezett képzés munkaerő-piaci relevanciája

Az etikus hackelés mára a világ egyik legnépszerűbb és legjobban megfizetett szakmája. Mára már a magánszemélyek és a cégek túlnyomó többsége él és dolgozik számítógéppel, számítógépes hálózattal, internettel, mobiltelefonnal, melyek nagy része szinte teljesen védtelen és felkészületlen az információ biztonsági sérülékenységeket kihasználó rosszindulatú hackerek támadásaival, vírusokkal, vagy a nem megfelelő fejlesztésből vagy üzemeltetésből adódó rendszerhibákkal szemben. Az etikus hackerek feladata megvédeni az információs és az informatikai rendszereket, feltárni a sebezhető pontjaikat, megfogalmazni a javító, illetve védelmi intézkedéseket és megoldásokat, sikeresen végigfuttatni a feladatot mindvégig együttműködve és kommunikálva a megbízóval. Mára a bankok, telekommunikációs cégek és a kormányzati, nemzetbiztonsági szféra egyaránt alkalmaz etikus hackereket, az ügyfeleik személyes adatainak védelme érdekében, vagyonuk biztonsága érdekében, illetve az ország kibertámadásokkal szembeni megfelelő védelmi és készültségi szintjének érdekében.

3.4. PROGRAMKÖVETELMÉNY MODUL RÉSZLETES BEMUTATÁSA

A programkövetelmény modul azonosító száma	SzPk-00026-18-07 5 02 3 /2 /M-04
A programkövetelmény modul megnevezése	Wifi sérülékenység vizsgálat

3.4.1. A KÉPZÉS KÉPZÉSI FORMÁTÓL FÜGGŐ MINIMÁLIS ÉS MAXIMÁLIS ÓRASZÁMA, ÉS AZ ELMÉLETI ÉS GYAKORLATI IDŐ ARÁNYA

A modul "Egyéni felkészítés" képzési formában megvalósítható?

Nem releváns

A modul "Csoportos felkészítés" képzési formában megvalósítható?

Igen

Csoportos felkészítés	Minimum	Maximum
A képzés óraszáma	27	33
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

A modul "Távoktatás" képzési formában megvalósítható?

Igen

Távoktatás	Minimum	Maximum
A képzés óraszáma	27	33
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

3.4.2. SZAKMAI KÖVETELMÉNYEK LEÍRÁSA

A legjellemzőbb tevékenység vagy munkaterület ellátásához szükséges szakmai kompetenciákat leíró szakmai ismeretek, készségek és személyes kompetenciák, társas kompetenciák és módszerkompetenciák tanulási eredmények szerinti leírása

Tudás	Képesség	Attitűd	Felelősség, autonómia
Megismeri a wifi hálózatok felépítését, működését, sérülékenységeit, az aktuális wifi titkosítási algoritmusokat.	Önállóan fel tudja tárni egy wifi hálózat gyengeségeit és sérülékenységeit.	Módszereit az etikusság elvének megfelelően alakítja ki, ami azt jelenti, hogy a vizsgálat célja a rendszer védelmi szintjének emelése, illetve, hogy a vizsgált információs/informatikai rendszer rendelkezésre állása zavartalan marad.	Kialakított eszköztára használata során a felelőssége, hogy az alkalmazott módszerei az információs/informatikai rendszer rendelkezésre állását ne zavarják meg annak érdekében, hogy az üzletmenet folyamatos maradjon.

Megtanulja alkalmazni a wifi hálózatok sérülékenységvizsgálatával kapcsolatos tudását; a feltárt sérülékenységek elhárítását.	Képes lesz a wifi hálózatok sérülékenységeinek kiaknázására és megoldást találni a feltárt sérülékenységek javítására vagy elhárítására. Képessé válik a wifi hálózathoz kapcsolódó sérülékenységvizsgálati feladatok menedzselésére és végrehajtására.	A feladatok végrehajtása során a megbízó igényeit és érdekeit maximálisan figyelemben tartva, legális keretek között, megbízási szerződés alapján végzi.	A feladat végrehajtása során felelőssége az információs/informatikai rendszer összes sérülékeny pontjának azonosítása, és mindegyikre tett megoldási vagy sérülékenység szint csökkentési javaslat megadása.
Megtanulja a feltárt sérülékenységek és azokra tett javaslatok megfelelő szóbeli és írásbeli kommunikációját.	Képessé válik a megbízót megfelelő módon és minőségben tájékoztatni a rendszer sérülékeny pontjairól és a megoldási javaslatairól.	A megbízót a feladat végrehajtása során megfelelő mélységben és minőségben tájékoztatja a feltárt sérülékenységekről és azok elhárítására tett javaslatairól.	Felelős a megbízó átfogó tájékoztatásáért, az átadott írásbeli dokumentumok és szóbeli információk minőségéért. Felelős azért, hogy az általa feltárt sérülékeny pontok rajta keresztül ne kerüljön illetéktelenekhez.

A tervezett képzés munkaerő-piaci relevanciája

Az etikus hackelés mára a világ egyik legnépszerűbb és legjobban megfizetett szakmája. Mára már a magánszemélyek és a cégek túlnyomó többsége él és dolgozik számítógéppel, számítógépes hálózattal, internettel, mobiltelefonnal, melyek nagy része szinte teljesen védtelen és felkészületlen az információ biztonsági sérülékenységeket kihasználó rosszindulatú hackerek támadásaival, vírusokkal, vagy a nem megfelelő fejlesztésből vagy üzemeltetésből adódó rendszerhibákkal szemben. Az etikus hackerek feladata megvédeni az információs és az informatikai rendszereket, feltárni a sebezhető pontjaikat, megfogalmazni a javító, illetve védelmi intézkedéseket és megoldásokat, sikeresen végigfuttatni a feladatot mindvégig együttműködve és kommunikálva a megbízóval. Mára a bankok, telekommunikációs cégek és a kormányzati, nemzetbiztonsági szféra egyaránt alkalmaz etikus hackereket, az ügyfeleik személyes adatainak védelme érdekében, vagyonuk biztonsága érdekében, illetve az ország kibertámadásokkal szembeni megfelelő védelmi és készültségi szintjének érdekében.

3.5. PROGRAMKÖVETELMÉNY MODUL RÉSZLETES BEMUTATÁSA

A programkövetelmény modul azonosító száma	SzPk-00026-18-07 5 02 3 /2 /M-05
A programkövetelmény modul megnevezése	Az etikus hackelés speciális és kiegészítő területei

3.5.1. A KÉPZÉS KÉPZÉSI FORMÁTÓL FÜGGŐ MINIMÁLIS ÉS MAXIMÁLIS ÓRASZÁMA, ÉS AZ ELMÉLETI ÉS GYAKORLATI IDŐ ARÁNYA

A modul "Egyéni felkészítés" képzési formában megvalósítható?

Nem releváns

A modul "Csoportos felkészítés" képzési formában megvalósítható?

Igen

Csoportos felkészítés	Minimum	Maximum
A képzés óraszáma	27	33
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

A modul "Távoktatás" képzési formában megvalósítható?

Igen

Távoktatás	Minimum	Maximum
A képzés óraszáma	27	33
Elméleti képzés idő aránya (%)	30	
Gyakorlati képzés idő aránya (%)	70	

3.5.2. SZAKMAI KÖVETELMÉNYEK LEÍRÁSA

A legjellemzőbb tevékenység vagy munkaterület ellátásához szükséges szakmai kompetenciákat leíró szakmai ismeretek, készségek és személyes kompetenciák, társas kompetenciák és módszerkompetenciák tanulási eredmények szerinti leírása

Tudás	Képesség	Attitűd	Felelősség, autonómia
Megismeri a GSM, GPRS, UMTS hálózatok interfészeit, sérülékeny pontjait, a mobilhálózatok dedikált eszközrendszerét, GPRS, UMTS hálózatok felépítését.	Képes felderíteni a mobil hálózati topológiát, valamint felismerni mobil hálózatok sérülékenységét.	Módszereit az etikusság elvének megfelelően alakítja ki, ami azt jelenti, hogy a vizsgálat célja a rendszer védelmi szintjének emelése, illetve, hogy a vizsgált információs/informatikai rendszer rendelkezésre állása zavartalan marad.	Kialakított eszköztára használata során a felelőssége, hogy az alkalmazott módszerei az információs/informatikai rendszer rendelkezésre állását ne zavarják meg annak érdekében, hogy az üzletmenet folyamatos maradjon.

Megtanulja alkalmazni a mobil kommunikációs hálózatok sérülékenységvizsgálatával kapcsolatos tudását; a feltárt sérülékenységek elhárítását.	Képessé válik a mobil kommunikációs hálózatok sérülékenységeinek kiaknázására és megoldást találni a feltárt sérülékenységek javítására. Képessé válik a mobil hálózathoz kapcsolódó sérülékenységvizsgálati feladatainak menedzselésére és végrehajtására.	A feladatok végrehajtása során a megbízó igényeit és érdekeit maximálisan figyelemben tartva, legális keretek között, megbízási szerződés alapján végzi.	A feladat végrehajtása során felelőssége az információs/informatikai rendszer összes sérülékeny pontjának azonosítása, és mindegyikre tett megoldási vagy sérülékenység szint csökkentési javaslat megadása.
Megismeri a Social Engineering (humán erőforrás hackelés) tevékenység fogalmát, jellemzőit és a Social Engineering a módszertan alkalmazását.	Képes a Social Engineering módszerével információs/informatikai rendszerek sérülékenységének feltárására és kiaknázására.	A feladatok végrehajtása során a megbízó igényeit és érdekeit maximálisan figyelemben tartva, legális keretek között, megbízási szerződés alapján végzi.	A feladatok végrehajtása során felelőssége az információs/informatikai rendszer összes sérülékeny pontjának azonosítása, és mindegyikre tett megoldási vagy sérülékenység szint csökkentési javaslat megadása.
Megtanulja a feltárt sérülékenységek és azokra tett javaslatok megfelelő szóbeli és írásbeli kommunikációját.	Képessé válik a megbízót megfelelő módon és minőségben tájékoztatni a rendszer sérülékeny pontjairól és a megoldási javaslatairól.	A megbízót a feladat végrehajtása során megfelelő mélységben és minőségben tájékoztatja a feltárt sérülékenységekről és azok elhárítására tett javaslatairól.	Felelős a megbízó átfogó tájékoztatásáért, az átadott írásbeli dokumentumok és szóbeli információk minőségéért. Felelős azért, hogy az általa feltárt sérülékeny pontok rajta keresztül ne kerüljön illetéktelenekhez.
Megismeri az etikus hacker szakmára vonatkozó jogi előírásokat, tisztában lesz a tevékenység végzéshez szükséges vonatkozó jogi, törvényi háttérrel. Megismeri a Btk. 300§ A/B/C bekezdéseit, értelmezi.	Képes ismereteit felelősségteljesen, a vonatkozó jogi keretek között alkalmazni.	A sérülékenységvizsgálati megbízást minden esetben legálisan végzi el, megbízásos keretek között,figyelembe véve az aktuális jogszabályi környezetet, a vonatkozó törvényeket és rendeleteket. Munkája minden esetben védelmi funkciót lát el.	Felelőssége, hogy naprakész legyen az aktuális vonatkozó jogszabályi háttérrel és vonatkozó rendelkezésekkel kapcsolatban.

A tervezett képzés munkaerő-piaci relevanciája

Az etikus hackelés mára a világ egyik legnépszerűbb és legjobban megfizetett szakmája. Mára már a magánszemélyek és a cégek túlnyomó többsége él és dolgozik számítógéppel, számítógépes hálózattal, internettel, mobiltelefonnal, melyek nagy része szinte teljesen védtelen és felkészületlen az információ biztonsági sérülékenységeket kihasználó rosszindulatú hackerek támadásaival, vírusokkal, vagy a nem megfelelő fejlesztésből vagy üzemeltetésből adódó rendszerhibákkal szemben. Az etikus hackerek feladata megvédeni az információs és az informatikai rendszereket, feltárni a sebezhető pontjaikat, megfogalmazni a javító, illetve védelmi intézkedéseket és megoldásokat, sikeresen végigfuttatni a feladatot mindvégig együttműködve és kommunikálva a megbízóval. Mára a bankok, telekommunikációs cégek és a kormányzati, nemzetbiztonsági szféra egyaránt alkalmaz etikus hackereket, az ügyfeleik személyes adatainak védelme érdekében, vagyonuk biztonsága érdekében, illetve az ország kibertámadásokkal szembeni megfelelő védelmi és készültségi szintjének érdekében.