

'Wifi 1.' mérés

Mérési jegyzőkönyv

Név:	
Név:	
Dátum:	
Mérőhely:	
Jegy:	

Minden feladat esetén érthetően és rekonstruálhatóan le kell írni, hogy milyen parancsok voltak szükségesek, azok milyen céllal futottak, valamint milyen műveleteket kellett elvégezni a helyes működéshez konfigurációs fájlokon, interfészeken stb. Egy korábban kifejtett munkafolyamatot nem kell újra és újra részletesen leírni, elég arra utalni, illetve az eredetihez képest történt változtatásokat jelezni.

Az egyes feladatoknál feltett kérdésekre tömören ugyanakkor érthetően kell válaszolni!

1. Csatlakozás rejtett SSID-jű AP-hoz

Milyen módban (*sta, ap, monitor, stb.*) van a vezeték nélküli kártya? Írja le, hogyan állapította meg?

	2p
--	----

1.1 Fedje fel a rejtett SSID-t!

Elvégzett műveletek magyarázattal:

	4p
--	----

Sorolja fel az összes rejtett SSID-jű AP-t az SSID és a BSSID megnevezésével!

	1p
--	----

Milyen feltételnek kell teljesülnie az SSID visszafejtéséhez (eltekintve attól az esettől, hogy brute force módon mindent kipróbálunk)?

	2p
--	----

A mérésvezetővel való egyeztetés után egy kiválasztott AP beacon üzenetét hallgassa le, hasonlítsa össze egy olyannal, ahol az SSID nem rejtett!

	2p
--	----

Milyen hitelesítést igényel az AP?

	1p
--	----

1.2 Csatlakozzon a rejtett SSID-jű AP-hoz! Ha nem nyílt az AP, a további lépésekhez kérjen jelszót a mérésvezetőtől.

Elvégzett műveletek magyarázattal:

	1p
--	----

Mit tapasztalt?

	1p
--	----

1.3 Derítse ki, hogy ki csatlakozik a MAC szűréssel ellátott AP-hoz!

Elvégzett műveletek magyarázattal:

	5p
--	----

1.4 Csatlakozzon a rejtett SSID-jű AP-hoz a megfelelő MAC címet hamisítva!

Elvégzett műveletek magyarázattal:

	3p
--	----

Milyen további biztonsági megoldással lehet védetté tenni a hálózatot?

	1p
--	----

1.5 Szerezze meg a mérés helyhez tartozó Feladat Hitelesítő Kódot!

Elvégzett műveletek magyarázattal:

	4p
--	----

Adja meg a Feladat Hitelesítő Kódot!

	1p
--	----

2. WEP elleni támadás

2.1 Derítse ki a megtámadandó AP adatait! Előtte egyeztessen a mérésvezetővel, hogy rendelkezésre álljon szabad (mások által nem támadott), WEP-pel védett AP!

Elvégzett műveletek magyarázattal:

	1p
--	----

Jegyezze le az AP adatait!

	1p
--	----

SSID:

BSSID:

Csatorna:

2.2 Indítson el egy lehallgatást kizárólag az adott AP-ra szűrve!

Elvégzett műveletek magyarázattal:

	2p
--	----

2.3 Végezzen el álhitelesítést az AP-nál!

Elvégzett műveletek magyarázattal:

	2p
--	----

Mit tapasztalt a lehallgató-terminálon?

	1p
--	----

A művelet miért nem tekinthető valódi hitelesítésnek? Mire nem képes a támadó a jelen helyzetben?

	1p
--	----

2.4 Szerezzen meg egy IV-hez tartozó 1500 bájt hosszú kulcsfolyamot!

Elvégzett műveletek magyarázattal:

	2p
--	----

A program futása során választott (és lementett) pcap fájl miért volt megfelelő?

	1p
--	----

Milyen IV-hez tartozó kulcsfolyamot szerzett meg?

	1p
--	----

Hogyan állapította meg az IV-t, melyik művelet után?

	2p
--	----

Az XOR fájlban hol található az IV?

	1p
--	----

Honnan lehet felismerni, hogy egy kulcsfolyam két különböző csomag esetén megegyezik?

	1p
--	----

2.5 Készítsen egy visszainjektálható szabályos csomagot!

Elvégzett műveletek magyarázattal:

	2p
--	----

Milyen típusú csomagot fog visszainjektálni?

	1p
--	----

Hogyan állapította meg a visszainjektálandó csomag típusát, milyen művelet után ?

	2p
--	----

Milyen más típusú csomagot lehetne még visszainjektálni?

	1p
--	----

Milyen értékei vannak az egyes LLC/SNAP fejléc mezőinek a visszainjektálható csomagban?

	1p
--	----

2.6 Kényszerítse az AP-t különböző IV csomagok küldésére!

Elvégzett műveletek magyarázattal:

	2p
--	----

Mennyi csomag elküldése után állította le a küldést? Miért pont ott?

	1p
--	----

2.7 A WEP kulcs kiszámítása

Elvégzett műveletek magyarázattal:

	2p
--	----

Mi a WEP kulcs és milyen bizonyossággal jelenthető ki, hogy a jó kulcsot találta meg?

	1p
--	----

Mennyi idő alatt futott le a WEP kulcs törése? Mennyi kulcsot tesztelt az algoritmus, és hány különböző IV-jű csomagot sikerült lementeni?

	1p
--	----

Futásidő:

Tesztelt kulcsok száma:

Különböző IV-jű csomagok száma:

Hány szavazatot kaptak a jó kulcs egyes bájtjai és mennyit a második legvalószínűbb bájtok?

	1p
--	----

2.8 Csatlakozzon az WEP-pel védett AP-hez, és kérje le a Feladat Hitelesítő Kódot!

Elvégzett műveletek magyarázattal:

	6p
--	----

Adja meg a Feladat Hitelesítő Kódot?

	1p
--	----

3. WPA biztonsági hitelesítés

3.1 Fejtse vissza a WPA jelszót brute force támadással! Ha az alapszótár használatával nem jár sikerrel, egészítse ki a szavakat egy számmal!

Mi szükséges a sikeres támadáshoz?

	1p
--	----

Elvégzett műveletek magyarázattal (alapszótáras támadás):

	4p
--	----

Szótár kiegészítése (forráskód, parancs, stb.):

	3p
--	----

Elvégzett műveletek magyarázattal (kiegészített szótáras támadás):

	1p
--	----

Becsülje meg, hogy egy 100.000 szót tartalmazó szótár esetén mennyi ideig tartana a támadás!

	3p
--	----

A lehallgatott négyutas kézfogás vizsgálatával állapítsa meg, hogy milyen rejtjelező és integritásvédő algoritmusban állapodnak meg a felek!

	2p
--	----

3.2 Fejtse vissza az idegen eszköz kommunikációját!

Miért nem triviális feladat más eszköz kommunikációjának lehallgatása ismert jelszó mellett?

	1p
--	----

Elvégzett műveletek magyarázattal:

	3p
--	----

Állapítsa meg a Feladat Hitelesítő Kód megszerzéséhez szükséges weblap címet!

	2p
--	----

3.3 Csatlakozzon az WPA-val védett AP-hez, és kérje le a Feladat Hitelesítő Kódot!

Elvégzett műveletek magyarázattal:

	3p
--	----

Adja meg a Feladat Hitelesítő Kódot?

	1p
--	----

Σ:

	90p
--	-----