

'Wifi 2.' 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. Megszemélyesítéssel támadás kivitelezése RADIUS-os hitelesítés mellett

1.1 Indítson el a mérőgépen egy RADIUS szervert WPE patch-csel!

Elvégzett műveletek magyarázattal:

	1p
--	----

Sorolja fel milyen IP címmel rendelkező hitelesítőket fogad el a RADIUS szerver! A felsorolásban a megosztott titkot is jegyezze le!

	1p
--	----

Állapítsa meg, hogy milyen EAP hitelesítő módokkal lehet a RADIUS szervernél hitelesíteni!

	1p
--	----

Hol találhatóak a RADIUS-hoz tartozó tanúsítványok és privát kulcsok?

	1p
--	----

Az aktuális RADIUS szerver esetén meg kell-e adni kliens oldali adatokat? Miért?

	1p
--	----

1.2 Fordítson hostapd-t madwifi driver támogatással!

Elvégzett műveletek magyarázattal:

	3p
--	----

1.3 Konfigurálja be a hostapd-t úgy, hogy az a mérőgépen futó RADIUS szerverhez forduljon a hitelesítés elvégzéséért!

Elvégzett műveletek magyarázattal:

	5p
--	----

1.4 Az hostapd elindítása mellett hallgassa le a mérőgépet érintő RADIUS és EAPOL üzeneteket!

Elvégzett műveletek magyarázattal:

	5p
--	----

Vizsgálja meg és írja le, hogy milyen lépéseken keresztül kerül a TLS üzenet beágyazásra a RADIUS üzenetekbe!

	1p
--	----

Vizsgálja meg és írja le, hogy milyen lépéseken keresztül kerül a TLS üzenet beágyazásra a EAPOL üzenetekbe!

	1p
--	----

Milyen típuszámú RADIUS üzenetbe ágyazódik be az EAP és hányas számú üzenetbe a TLS az EAP-on belül?

	1p
--	----

Kérte-e a RADIUS szerver a klientsől, hogy küldjön tanúsítványt? Hogyan állapította meg?

	2p
--	----

1.5 Szerezze meg az automata kliens jelszavát!

Elvégzett műveletek magyarázattal:

	1p
--	----

Adja meg az automata kliens jelszavát!

	5p
--	----

1.6 Csatlakozzon az eredeti AP-hez!

Elvégzett műveletek magyarázattal:

	2p
--	----

Ellenőrizze, hogy hozzáfér-e a hálózathoz!

	1p
--	----

2. Captive portal elleni támadás DNS tunnelezéssel

2.1 Csatlakozzon a captive portallal védett AP-hoz, és próbáljon elérni külső szervert!

Elvégzett műveletek magyarázattal:

	3p
--	----

Mit tapasztalt?

	1p
--	----

2.2 Vizsgálja meg, hogy az AP védekezik-e a DNS tunnelezés ellen!

Elvégzett műveletek magyarázattal:

	3p
--	----

Mit tapasztalt és abból milyen következtetést tud levonni?

	2p
--	----

2.3 Ellenőrizze a crsys.hu zónabeállításait a mérésvezető segítségével!

Milyen beállításokkal rendelkezik a felelős DNS szerver az mérőcsoport zónáját illetően?

	1p
--	----

2.4 Állítsa be és indítsa el a DNS tunnel szerver oldalát!

Elvégzett műveletek magyarázattal:

	5p
--	----

2.5 A kliens oldal felparaméterezésével és SSH kapcsolat felépítésével tesztelje a DNS tunnelt a kliens!

Elvégzett műveletek magyarázattal:

	3p
--	----

Írja le a tapasztaltakat!

	1p
--	----

2.6 A kliens oldalon indítsa a DNS tunnelt úgy, hogy Socks proxy-ként lehessen használni az SSH kapcsolatot!

Elvégzett műveletek magyarázattal:

	3p
--	----

2.7 A webböngészőt állítsa be úgy, hogy minden forgalmat a DNS tunnelen keresztül bonyolítsa le! Hallgasson le egy ilyen forgalmat is!

Elvégzett műveletek magyarázattal:

	2p
--	----

Mit tapasztalt böngészés során!

	1p
--	----

Hogyan küldött üzenetet a DNS tunnelen keresztül a kliens a szervernek? Mutasson példát is!

	3p
--	----

Hogyan válaszolt a DNS tunnel szerver a kliensnek? Mutasson példát is!

	3p
--	----

2.8 Kiegészítő kérdések

Captive portal miként tud védekezni a DNS tunnel használatára ellen!?

	1p
--	----

DNS tunnel ellen védett captive portal milyen módszerrel támadható?

	1p
--	----