Trosolwg

Y weithgaredd o asesu system i weld a oes gwendidau diogelwch yw profi diogelwch gwybodaeth. Mae profi diogelwch rhwydwaith neu seilwaith yn cynnwys asesu dyfeisiau rhwydwaith, gweinyddwyr, a gwasanaethau seilwaith rhwydwaith eraill fel Gwasanaeth Enw Parth (DNS) i weld a oes gwendidau diogelwch. Yn gyffredinol, mae profi diogelwch rhaglenni yn cyfeirio at brofi rhaglenni meddalwedd arferol neu fasnachol i weld a oes gwendidau diogelwch. Mae profi diogelwch rhaglenni ar y we yn canolbwyntio'n benodol ar raglenni sydd ar gwe, ac mae profi diogelwch rhaglenni symudol yn canolbwyntio ar brofi rhaglenni symudol.

Defnyddir rhai mathau cyffredin o brofion diogelwch. Fel arfer, mae asesiad o wendidau yn cynnwys sganio am faterion diogelwch. Defnyddir cyfuniad o gyfarpar awtomataidd a thechnegau asesu â llaw i gadarnhau a oes gwendid, ond heb fanteisio ar y gwendid hwn mewn gwirionedd.

Mae profion treiddio yn nodi gwendidau ac yn manteisio arnynt. Y nod yw efelychu ymosodwr go iawn a all dorri i mewn i system a dwyn neu addasu data neu effeithio ar argaeledd systemau. Mae profion amser cynnal yn cynnwys asesu'r system ar gyfer materion diogelwch o safbwynt defnyddiwr terfynol. Mae adolygu cod yn golygu asesu rhaglen drwy adolygu ei god ffynhonnell. Mae peidio ag adolygu cod yn gadael system yn agored i fwy o risg o fygythiadau mewnol maleisus.

Mae'r safon hon yn nodi'r sgiliau sydd eu hangen i nodi a nodweddu bygythiadau, gwendidau ac ymosodiadau ar systemau gwybodaeth. Mae
hefyd yn cynnwys sut i gynnal profion diogelwch gwybodaeth.

Meini prawf perfformiad

Rhaid i chi allu:

1. nodi bygythiadau, gwendidau ac ymosodiadau sy'n gallu digwydd mewn systemau gwybodaeth yn unol â safonau sefydliadol
2. penderfynu ar y gwahanol brosesau a methodolegau ymosod y gellir eu defnyddio i gynnal ymosod ar ddiogelwch gwybodaeth
3. asesu bygythiadau i'r sefydliad ar hyn o bryd, dadansoddi tueddiadau ac amlygu materion diogelwch gwybodaeth sy'n berthnasol i'r sefydliad
4. profi i weld a oes gwendidau yn y parth cyhoeddus a'r posibilrwydd o gamfanteisio drwy gynnal ymarferion camfanteisio, lle bo'n briodol, ac adrodd ar broblemau posibl ac opsiynau lliniaru
5. gwerthuso a dosbarthu bygythiadau yn unol â fframweithiau cudd-wybodaeth am fygythiadau, safonau sefydliadol ac allanol
6. cofnodi unrhyw wendidau a bygythiadau a nodwyd yn ystod profion diogelwch ac adrodd arnynt yn briodol

Gwybodaeth a dealltwriaeth

Mae angen i chi wybod a deall:

1. y gwahaniaeth rhwng bygythiad, risg, ymosodiad a gwendid
2. bod bygythiadau yn camfanteisio ar wendidau i ddod yn ymosodiadau
3. ble i ddod o hyd i wybodaeth am fygythiadau, gwendidau ac ymosodiadau
4. beth yw'r bygythiadau, yr ymosodiadau a'r achosion nodweddiadol o gamfanteisio a'r cymhellion y tu ôl iddynt
5. sut mae ymosodiadau penodol yn gweithio gan gynnwys atal gwasanaeth, gwe-rwydo a gorlif byffer
6. yr ystod o dechnegau ar gyfer pennu dulliau ymosod gan gynnwys rhagchwilio, sganio, creu, profi, ymosod/cael mynediad, trosglwyddo heb awdurdod ac ymadael/cadwyn lladd ac ati.
7. sut mae defnyddwyr yn cael eu targedu mewn ymosodiad
8. pam na all profion diogelwch warantu diogelwch
9. beth mae profi gwendid a threiddgarwch yn ei olygu
10. yr ystod o fygythiadau a gwendidau y mae angen eu hystyried wrth ddylunio a datblygu profion treiddio
11. beth yw'r gofynion cyfreithiol ar gyfer profion treiddio
12. y technegau a dderbynnir ar gyfer profion treiddio, ystod y dulliau a chyfarpar sydd ar gael a sut i'w cymhwyso
13. pryd a sut i drefnu profion diogelwch gwybodaeth
14. pwysigrwydd cynnal profion diogelwch gwybodaeth yn rheolaidd ar wasanaethau sy'n bodoli o fewn y sefydliad
15. pwysigrwydd cofnodi canlyniadau profion treiddio a'u cyfleu yn gywir

Cyfrannu at weithgareddau profi diogelwch gwybodaeth

Datblygwyd gan	e-skills
Fersiwn rhif	1
Dyddiad cymeradwyo	01 Maw 2016
Dyddiad Adolygu Dangosol	01 Ebr 2019
Dilysrwydd	Ar hyn o bryd
Statws	Gwreiddiol
Sefydliad cychwynnol	The Tech Partnership
RCU gwreiddiol	TECIS60431
Galwedigaethau perthnasol	Swyddog Technoleg Gwybodaeth a Chyfathrebu, Technoleg Gwybodaeth a Chyfathrebu, Gweithwyr Proffesiynol Technoleg Gwybodaeth a Chyfathrebu
Cyfres/Set	Diogelwch Gwybodaeth
Geiriau Allweddol	Diogelwch gwybodaeth, seiberddiogelwch, profion diogelwch gwybodaeth, profion treiddio