National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS PLUS

Cyber Essentials Plus: Manyleb Prawf Enghreifftiol f3.1

Ebrill 2023

Cynnwys

Beth sy'n newydd

- Wedi ychwanegu pob gweinydd a gaiff ei letya'n fewnol at yr adran Profi Sampl
- Wedi diweddaru'r meini prawf ar gyfer is-brawf 2.1 i sgôr sylfaen CVSS o 7 neu uwch
- Wedi dileu profion 4 a 5 blaenorol a chynnwys Prawf 3 wedi'i ddiweddaru
- Wedi diweddaru'r profion Amddiffyn rhag Maleiswedd er mwyn cyd-fynd â newidiadau i'r gofynion technegol

Cynulleidfa

Mae'r ddogfen hon ar gyfer personél sy'n cynnal asesiadau Cyber Essentials Plus ar ran Cyrff Ardystio yn bennaf (yr 'Asesydd', neu 'chi').

Mae'n bosibl y bydd o ddiddordeb i'r sefydliad sy'n ceisio ardystiad Cyber Essentials Plus hefyd (yr 'Ymgeisydd') — efallai yr hoffai staff sy'n rhan o'r broses ddeall y meini prawf sy'n ffurfio'r asesiad.

Diben

Diben y fanyleb prawf hon yw hwyluso profion annibynnol er mwyn cadarnhau a yw'r Ymgeisydd yn cydymffurfio â gofynion technegol cynllun Cyber Essentials, a:

- sicrhau bod hyn wedi arwain at amddiffyniad digonol yn erbyn y bygythiadau yn y cwmpas
- rhoi manylion am y profion gofynnol, a'r meini prawf ar gyfer 'llwyddo' neu 'fethu' wrth asesu ar gyfer ardystiad

Rhaid i chi gytuno ar ffiniau'r cwmpas gyda'r Ymgeisydd *cyn* dechrau profi. Cyfeiriwch at y ddogfen **Gofynion ar gyfer Seilwaith TG** (cynllun Cyber Essentials).

Nod y fanyleb prawf enghreifftiol hon yw helpu Partner Cyflawni Cyber Essentials i ddatblygu ei fanylebau prawf ei hun er mwyn i'w Gyrff Ardystio gynnal asesiadau Cyber Essentials Plus.

Diben y ddogfen enghreifftiol yw annog dull gweithredu cyson, gan y dylai Ymgeiswyr allu disgwyl yr un canlyniad ardystio, ni waeth pa Gorff Ardystio a ddefnyddir ganddynt.

Drwy'r ddogfen enghreifftiol hon, byddwn yn ymdrin yn uniongyrchol â'r Asesydd, fel bod holl gamau'r tasgau mor glir â phosibl. Byddwn hefyd yn cynnwys rhai nodiadau cyd-destunol ar gyfer y Partner Cyflawni.

Cyn i chi ddechrau

Cyn i ddechrau profi, rhaid i chi sicrhau'r canlynol:

- eich bod wedi cael y caniatâd ysgrifenedig priodol gan yr Ymgeisydd
- eich bod wedi cytuno ar fanylion y system(au) i'w phrofi/profi, a phryd y caiff y profion eu cynnal, â'r Ymgeisydd
- bod gennych y templed cywir ar gyfer yr adroddiad y byddwch yn ei lunio ar gyfer yr Ymgeisydd – gosodir fformat yr adroddiad hwn gan y Partner Cyflawni

Rhagofynion cyffredinol ar gyfer profi

Bydd angen y rhagofynion canlynol arnoch ar gyfer profion 2 i 7:

- gallu anfon negeseuon e-bost mympwyol at gyfrif a weithredir gan yr Ymgeisydd – hynny yw, bydd angen system e-bost allanol arnoch nad yw'n hidlo ac nad yw ar restr gwrthod

- ffeiliau prawf, a gaiff eu lletya ar wefan allanol y mae'r Corff Ardystio yn berchen arni (gweler Atodiad B: Mathau o ffeiliau prawf) – mae'n bosibl y bydd angen i'r Ymgeisydd drefnu mynediad at y wefan, drwy ei hychwanegu at ei restr caniatáu o bosibl
- defnyddwyr â'r manylion priodol i gyflawni'r profion
- rhaglenni e-bost (a chyfeiriadau e-bost cysylltiedig) a phorwyr gwe gweithredol ar gyfer sampl o'r dyfeisiau defnyddiwr terfynol yn y cwmpas

Meini prawf llwyddiant

Canlyniadau profion

Mae'n rhaid i chi nodi canlyniad **pob** achos prawf ac is-brawf ag un o'r canlyniadau canlynol:

Llwyddo:

- Cyn i chi roi canlyniad Llwyddo i achos prawf, mae'n rhaid i chi sicrhau bod pob is-brawf o fewn yr achos prawf hwnnw wedi cael canlyniad Llwyddo hefyd — oni nodir eithriad arbennig yn y fanyleb prawf hon.
- Yn yr un modd, cyn i chi roi marc Llwyddo i'r asesiad cyffredinol (a fyddai'n arwain at ardystiad **Cyber Essentials Plus**), rhaid i chi sicrhau bod pob achos prawf wedi cael canlyniad Llwyddo.

Methu:

- Os bydd **unrhyw** is-brawf o fewn y fanyleb prawf hon yn cael canlyniad Methu, yna rhaid i chi hefyd roi canlyniad Methu i'r rhiant-achos prawf a'r asesiad cyffredinol.
- Er eglurder: Bydd unrhyw ganlyniad Methu unigol yn golygu y bydd yr asesiad cyfan yn Methu — oni bai y nodir eithriad arbennig yn y fanyleb prawf hon. Sut bynnag, dylech barhau i fod yn ddiwyd a chwblhau'r asesiad yn llawn, er mwyn rhoi arfarniad cyflawn i'r Ymgeisydd.

Nodiadau Cynghori

Cewch gynnwys Nodyn Cynghori gydag unrhyw ganlyniad. Defnyddiwch y rhain i roi gwybod i'r Ymgeisydd am unrhyw welliannau perthnasol y gallai eu gwneud yn hawdd er mwyn gwella seiberddiogelwch, ac i esbonio'r rhesymeg dros benderfyniadau ynghylch profion penodol.

Achos Prawf 1: Asesiad gwendidau o bell

Diben y prawf

Profi a all ymosodwr manteisgar ar y rhyngrwyd hacio i mewn i system yr Ymgeisydd gan ddefnyddio dulliau sgìl isel cyffredin.

Disgrifiad o'r prawf

Rhagofynion

Bydd angen y canlynol arnoch:

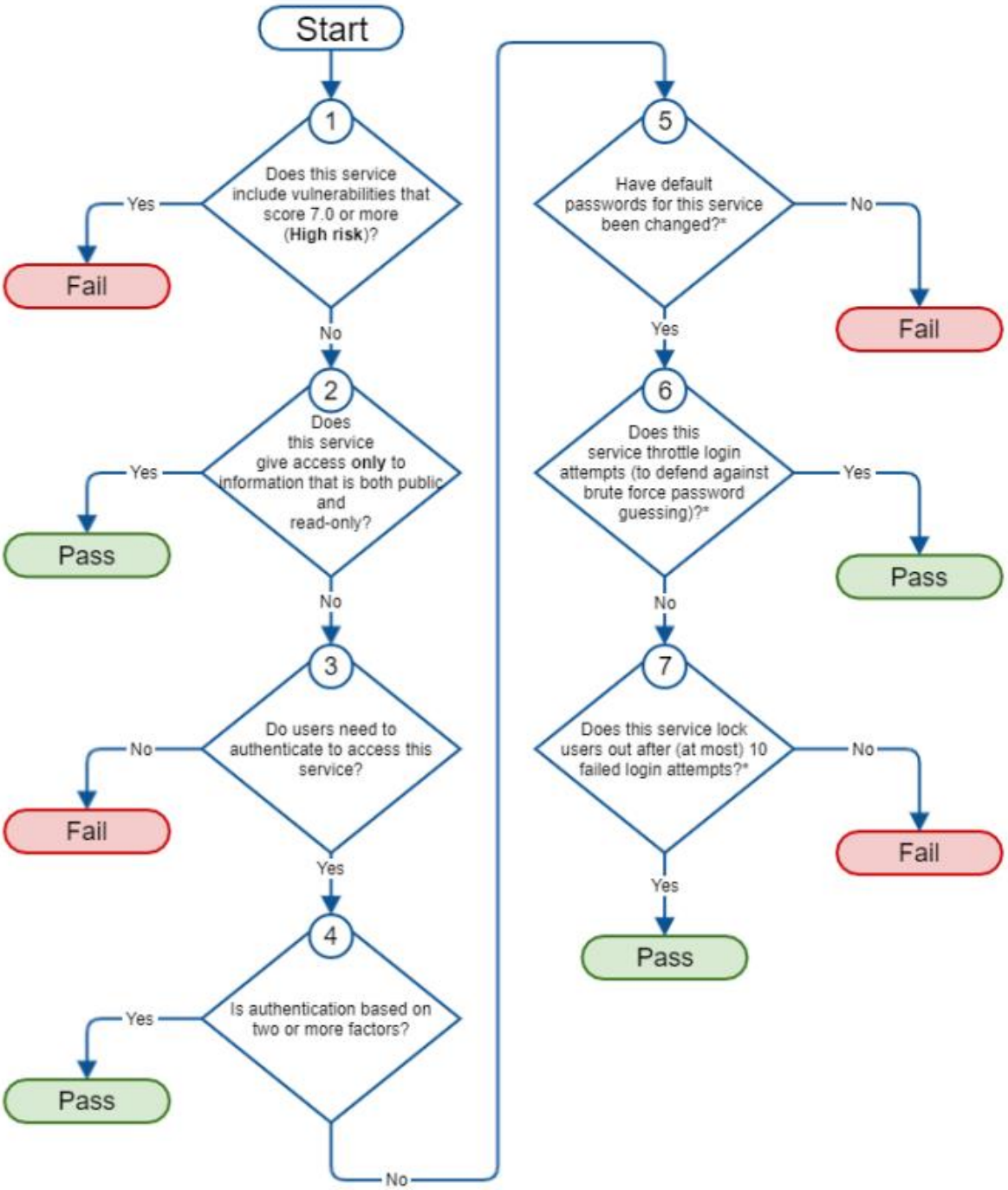
- adnodd sganio gwendidau a gymeradwywyd gan y Partner Cyflawni — gweler Atodiad A: Sganio am wendidau
- rydym wedi nodi'r cyfeiriadau IP i'w sganio

Lle caiff cyfeiriadau IP dynamig eu defnyddio ar gyfer cysylltiad â'r rhyngrwyd, gellir diffinio'r cwmpas o ran cofnodion DNS priodol.

Cymerwch ofal gyda chyfeiriadau o'r fath er mwyn sicrhau nad yw gwasanaethau fel NAT o safon yn anfon traffig asesu i'r cyrchfan anghywir drwy amryfusedd.

Is-brawf 1.1

1. Nodi'r holl gyfeiriadau IP a ddefnyddir gan yr Ymgeisydd ar hyn o bryd. Rhaid i hyn gynnwys Seilwaith fel Gwasanaeth (IaaS) pan gaiff ei ddefnyddio.
2. Sganio'r holl gyfeiriadau IP a nodir, ar y set argymelledig o byrth TCP ac UDP (gweler Atodiad A: Sganio am wendidau).
3. Ar gyfer pob gwasanaeth y dewch o hyd iddo y gellir cysylltu ag ef drwy'r we, defnyddiwch y diagram llif a'r nodiadau isod i bennu a ddylid cofnodi canlyniad Llwyddo neu Fethu ar gyfer y gwasanaeth.



Ffigur 1: Diagram llif yr is-brawf ar gyfer asesu gwasanaethau y gellir cysylltu â nhw drwy wal dân.

Dehongli canlyniadau'r achos prawf

Os byddwch yn rhoi canlyniad Llwyddo i bob gwasanaeth a brofir o dan Is-brawf 1.1, yna cofnodwch ganlyniad Llwyddo ar gyfer yr achos prawf hwnnw. Fel arall, cofnodwch ganlyniad Methu.

Profi Sampl

Mae'r profion sy'n weddill yn berthnasol i'r holl ddyfeisiau cyfrifiadurol o fewn ffiniau'r cwmpas. Mae hyn yn cynnwys:

- dyfeisiau defnyddwyr terfynol sy'n cysylltu â data neu wasanaethau sefydliadol
- pob gweinydd a gaiff ei letya'n fewnol
- pob math o wasanaeth cwmwl (IaaS, Paas, neu SaaS)

Ac eithrio'r rhwydweithiau lleiaf, ni fydd yn ymarferol profi pob dyfais sydd o fewn ffiniau'r cwmpas y cytunwyd arnynt. Yn hytrach, dylid profi sampl gynrychiadol - ond cymerwch gamau i sicrhau y gallwch fod yn hyderus bod eich sampl o ddyfeisiau (gan gynnwys gweinyddion a dyfeisiau defnyddwyr terfynol) yn gynrychiadol mewn gwirionedd.

- Mae llawer o sefydliadau yn defnyddio ffurfweddiad safonedig ar gyfer eu gweinyddion a'u dyfeisiau defnyddwyr terfynol. Mewn achosion o'r fath, gall nifer bach o samplau cynrychiadol gwmpasu cryn dipyn o gyfarpar y sefydliad.
- Argymhellwn eich bod yn ceisio bodloni eich hun fod eich profion, at ei gilydd, yn cynrychioli'r holl ddyfeisiau o fewn y cwmpas. Bydd nifer gwirioneddol y dyfeisiau cynrychiadol y bydd angen i chi eu profi er mwyn cyflawni'r lefel hon o hyder yn dibynnu ar swm yr amrywiad sy'n bodoli o ganlyniad i brosesau darparu penodol yr Ymgeisydd, a'u heffeithiolrwydd.

Rhaid profi pob gwasanaeth cwmwl gan ddefnyddio sampl gynrychiadol o gyfrifon defnyddwyr. Rhaid i hyn gynnwys o leiaf un defnyddiwr arferol ac un defnyddiwr gweinyddol ar gyfer pob gwasanaeth cwmwl a ddefnyddir. Gellir defnyddio'r un defnyddwyr ar gyfer sawl gwasanaeth cwmwl.

Achos Prawf 2: Gwirio patsio, drwy sgan gwendidau dilys o ddyfeisiau

Dylid cynnal y prawf hwn ar ddyfeisiau defnyddwyr terfynol a samplwyd, gweinyddion ac achosion IaaS.

Diben y prawf

Nodi patsys a diweddariadau diogelwch sydd ar goll sy'n peri gwendidau y gallai bygythiadau o fewn cwmpas y cynllun hwn gamfanteisio arnynt yn hawdd.

Disgrifiad o'r prawf

Rhagofynion

Yn ogystal â'r rhagofynion cyffredinol ar gyfer profi, bydd angen y canlynol arnoch:

- adnodd sganio gwendidau a gymeradwywyd gan y Partner Cyflawni — gweler Atodiad A: Sganio am wendidau

Is-brawf 2.1

Ar gyfer pob dyfais i'w phrofi, sganiwch gan ddefnyddio'r adnodd sganio gwendidau cymeradwy.

Gan ddefnyddio allbwn y sgan, nodwch wendidau sy'n bodloni unrhyw un o'r tri maen prawf canlynol:

- Disgrifir y gwerthwr fel ‘critigol’ neu ‘risg uchel’
- Mae wedi cael sgôr sylfaen CVSS v3 o 7 neu fwy
- Nid oes unrhyw fanylion am lefel y gwendidau y mae'r diweddariad a ddarperir gan y gwerthwr yn eu hatgyweirio

Os oes unrhyw wendidau sy'n bodloni'r meini prawf uchod, a lle mae'r pats a ddarparwyd gan y gwerthwr wedi bod ar gael am fwy nag 14 diwrnod cyn profi, cofnodwch ganlyniad Methu ar gyfer yr is-brawf. Fel arall, cofnodwch ganlyniad Llwyddo.

Y syniad yma yw asesu pob gwendid mewn cyd-destun a cheisio penderfynu a allai ymosodwr ar y rhyngrwyd gamfanteisio arno mewn gwirionedd a pheri niwed i'r Ymgeisydd.

Nid yw patsio rhithwir yn ddull lliniaru derbyniol ar gyfer gwendidau diogelwch hen systemau gweithredu nas cefnogir yn yr hirdymor ac felly ni chânt eu cydnabod fel dull cydymffurfio â gofynion Cyber Essentials.

Dehongli canlyniadau'r achos prawf

Os byddwch yn rhoi canlyniad Llwyddo i bob is-brawf, yna cofnodwch ganlyniad Llwyddo ar gyfer yr achos prawf hwn. Fel arall, cofnodwch ganlyniad Methu.

Achos Prawf 3: Gwirio amddiffyniad rhag maleiswedd

Dylid cynnal y prawf hwn ar ddyfeisiau defnyddwyr terfynol a samplwyd, gweinyddion sy'n darparu bwrdd gwaith defnyddiwr-ryngweithiol ac achosion IaaS.

Diben y prawf

Cadarnhau bod pob dyfais yn y cwmpas yn elwa ar lefel sylfaenol o amddiffyniad rhag maleiswedd o leiaf.

Disgrifiad o'r prawf

Rhagofynion

Nodi pa fath o amddiffyniad rhag maleiswedd a ddefnyddir gan bob dyfais yn y sampl (meddalwedd wrthfaleiswedd neu restr caniatáu cymwysiadau).

Gweler y rhagofynion cyffredinol ar gyfer profi, ac yn enwedig nodyn Atodiad B: Mathau o ffeiliau prawf.

Dewis is-brofion priodol

Dylid cynnal yr is-brofion canlynol fel y bo'n briodol ar gyfer y math o amddiffyniad rhag maleiswedd a ddefnyddir.

Is-brawf 3.1 (ar gyfer dyfeisiau sy'n defnyddio meddalwedd wrthfaleiswedd)

Ar gyfer pob dyfais yn y sampl, cadarnhau bod y feddalwedd wrthfaleiswedd wedi'i gosod, yn weithredol ac wedi'i diweddaru yn unol â chyfarwyddiadau'r gwerthwr.

Gan ddibynnu ar y feddalwedd a ddefnyddir, bydd yr asesydd yn penderfynu a ddylid profi'r gofyniad gan ddefnyddio ffeiliau prawf fel y disgrifir yn is-brofion 3.1.1, 3.1.2 a'r gwiriad â llaw yn is-brawf 3.13 neu drwy wiriadau â llaw fel y disgrifir yn is-brawf 3.1.4.

Is-brawf 3.1.1 (Gwirio effeithiolrwydd amddiffyniadau yn erbyn maleiswedd a anfonir drwy e-bost)

Dylid cynnal y prawf hwn ar unrhyw ddyfais a samplwyd neu wasanaeth lle gall defnyddiwr dderbyn e-bost.

Ar gyfer pob amgylchedd defnyddiwr yn y sampl:

1. Dylid sefydlu llinell sylfaen drwy anfon neges e-bost syml o'ch cyfrif prawf o bell, heb unrhyw atodiadau. Arsylwch ar y defnyddiwr er mwyn cadarnhau bod y neges e-bost hon yn cyrraedd y cyrchfan prawf yn llwyddiannus.
2. Penderfynwch pa fathau o ffeiliau y dylech brofi amdanynt a pharatowch eich negeseuon e-bost prawf. Bydd angen un neges e-bost arnoch ar gyfer pob math o ffeil i'w phrofi, gan y byddwch yn atodi un ffeil prawf i bob neges e-bost.
3. Ceisiwch anfon pob neges e-bost prawf o'ch cyfrif prawf o bell i'r cyrchfan prawf. Arsylwch ar y defnyddiwr yn ceisio agor pob ffeil prawf atodedig. Nodwch y canlyniad.

Os bydd unrhyw un o'r ffeiliau prawf maleiswedd yn cyrraedd yn llwyddiannus **ac nad** yw'r defnyddiwr wedi'i rwystro rhag eu hagor, cofnodwch ganlyniad Methu.

Os bydd unrhyw un o'r ffeiliau prawf gweithredadwy yn cyrraedd yn llwyddiannus **a** gellir eu gweithredu heb gam sy'n gofyn am ryngweithiad ychwanegol gan y defnyddiwr, cofnodwch ganlyniad Methu.

Fel arall, cofnodwch ganlyniad Llwyddo ar gyfer yr is-brawf hwn

Is-brawf 3.1.2 (Gwirio effeithiolrwydd amddiffyniadau yn erbyn maleiswedd a anfonir drwy borwr)

Dylid cynnal y prawf hwn ar unrhyw ddyfais a samplwyd neu wasanaeth lle gall defnyddiwr bori'r we.

Dylai'r ymgeisydd ffurfweddu hidlydd cynnwys y we er mwyn darparu swm o hidlo ar gyfer y wefan allanol gymeradwy sy'n cynrychioli'r broses hidlo a gyflawnir gyda'r rhan fwyaf o wefannau eraill a ganiateir (hynny yw, y rhai hynny nad ydynt wedi'u nodi'n benodol ar y rhestr gwrthod).

Mae'r rhesymeg ar gyfer y dull gweithredu hwn yn seiliedig ar y dybiaeth bod gwefan sydd ar y rhestr caniatáu yn rhywle y gellir lawrlwytho ffeiliau ohoni. Mae profion **Cyber Essentials Plus** yn efelychu hyn drwy ddefnyddio'r wefan allanol gymeradwy.

1. Penderfynwch ar y ffeiliau prawf priodol ar gyfer y System Weithredu rydych yn ei phrofi;
2. Arsylwch ar y defnyddiwr yn mynd ar y rhyngrwyd. Os caiff ei atal rhag mynd ar y rhyngrwyd, cofnodwch ganlyniad Llwyddo ar gyfer yr is-brawf hwn;
3. Arsylwch ar y defnyddiwr yn ceisio lawrlwytho ffeiliau prawf cymeradwy. Os caiff y defnyddiwr ei atal rhag lawrlwytho'r ffeiliau prawf cymeradwy, cofnodwch ganlyniad Llwyddo;
4. Os caiff y ffeiliau prawf eu rhwystro wrth eu hagor, cofnodwch ganlyniad Llwyddo;

Os bydd unrhyw un o'r ffeiliau prawf maleiswedd yn cael eu lawrlwytho'n llwyddiannus **ac nad** yw'r defnyddiwr wedi'i rwystro rhag eu hagor, cofnodwch ganlyniad Methu.

Os bydd unrhyw un o'r ffeiliau prawf gweithredadwy yn cael eu lawrlwytho'n llwyddiannus **a** gellir eu gweithredu heb gam sy'n gofyn am ryngweithiad ychwanegol gan y defnyddiwr, cofnodwch ganlyniad Methu.

Is-brawf 3.1.3 (Gwirio bod y feddalwedd wrthfaleiswedd wedi'i diweddaru)

Rhaid cynnal y gwiriad â llaw canlynol ar yr holl ddyfeisiau defnyddwyr terfynol a samplwyd, gweinyddion sy'n darparu bwrdd gwaith defnyddiwr-ryngweithiol ac achosion IaaS sy'n defnyddio meddalwedd wrthfaleiswedd.

- bod y feddalwedd wrthfaleiswedd wedi'i diweddaru yn unol â chyfarwyddiadau ffurfweddu'r gwerthwr

Os caiff y gwiriad ei gynnal a'i fod yn cadarnhau bod y feddalwedd wrthfaleiswedd wedi'i diweddaru yn unol â chofnod cyfarwyddiadau'r gwerthwr, cofnodwch ganlyniad Llwyddo ar gyfer yr is-brawf hwn, neu ganlyniad Methu os ddim.

Is-brawf 3.1.4 (Gwiriadau â llaw ar gyfer dyfeisiau sy'n defnyddio meddalwedd wrthfaleiswedd)

Rhaid cynnal y gwiriadau â llaw canlynol ar yr holl ddyfeisiau defnyddwyr terfynol a samplwyd, gweinyddion sy'n darparu bwrdd gwaith defnyddiwr-ryngweithiol ac achosion IaaS sy'n defnyddio meddalwedd wrthfaleiswedd ac na ddefnyddiwyd y ffeiliau prawf i brofi bod y feddalwedd wedi'i gosod a'i bod yn weithredol.

- bod y feddalwedd wrthfaleiswedd wedi'i gosod a'i bod yn weithredol drwy archwilio logiau.
- bod y feddalwedd wrthfaleiswedd wedi'i diweddaru yn unol â chyfarwyddiadau ffurfweddu'r gwerthwr

Os caiff y ddau wiriad eu cynnal a'u bod yn cadarnhau bod y feddalwedd wrthfaleiswedd wedi'i gosod, ei bod yn weithredol ac wedi'i diweddaru yn unol â chofnod cyfarwyddiadau'r gwerthwr, cofnodwch ganlyniad Llwyddo ar gyfer yr is-brawf hwn, neu ganlyniad Methu os ddim.

Is-brawf 3.2 (ar gyfer dyfeisiau sy'n defnyddio rhestr caniatáu ar gyfer cymwysiadau yn seiliedig ar dystysgrif)

Ar gyfer pob dyfais yn y sampl, gwiriwch y canlynol:

- mai'r rhestr o dystysgrifau gwraidd dibynadwy yw'r safon a bennwyd fel y darperir gan wneuthurwr y system weithredu, neu is-set ohoni
- mai dim ond gyda chytundeb penodol yr Ymgeisydd y caiff tystysgrifau gwraidd dibynadwy eu hychwanegu
- na fydd ffeil weithredadwy heb ei llofnodi, a ffeil weithredadwy wedi'i llofnodi â thystysgrif nad yw'n cadwyno i dystysgrif ddibynadwy, yn gweithio ar y ddyfais
- bod gosodiadau polisi'r system weithredu yn briodol i sicrhau bod prosesau llofnodi cod yn gymwys i fformat pob ffeil weithredadwy, fel sy'n berthnasol i'r ddyfais

Os bydd **pob** un o'r rhain yn wir, cofnodwch ganlyniad Llwyddo ar gyfer yr is-brawf hwn. Fel arall, cofnodwch ganlyniad Methu.

Dehongli canlyniadau'r achos prawf

Os byddwch yn cofnodi canlyniad Methu ar gyfer is-brawf 3.1 neu 3.2 lle mae dyfeisiau yn defnyddio'r dull cyfatebol o amddiffyn rhag maleiswedd, cofnodwch ganlyniad Methu ar gyfer yr achos prawf hwn. Fel arall, cofnodwch ganlyniad Llwyddo.

Achos prawf 4: Gwirio ffurfweddiad dulliau dilysu aml-ffactor

Dylid cynnal y prawf hwn ar bob gwasanaeth cwmwl.

Diben y Prawf

Profi bod gwasanaethau cwmwl a nodir yn y cwmpas wedi'u ffurfweddu ar gyfer dilysu aml-ffactor.

Disgrifiad o'r Prawf

Defnyddwyr dyfeisiau a samplwyd i geisio mewngofnodi i wasanaethau cwmwl y sefydliad gan ddefnyddio'r cyfrifon a ddarparwyd gan y sefydliad.

Pob gwasanaeth cwmwl i gael ei brofi ar gyfer Mynediad gan Ddefnyddiwr a Gweinyddwr. Pan fydd sawl gwasanaeth cwmwl yn rhannu gwasanaeth dilysu, dim ond unwaith ar gyfer pob gwasanaeth dilysu y bydd angen cynnal y prawf hwn.

Achos Prawf 4.1

1. Asesydd i arsylwi ar ddefnyddwyr yn cyrchu gwasanaethau cwmwl gan ddefnyddio'r cyfrifon a ddarparwyd gan eu sefydliad ar ddyfais annibynadwy neu o sesiwn gudd ar borwr.
2. Os na fydd prawf 1 yn bosibl, dylai'r asesydd rannu sesiwn gudd ar borwr o'i ddyfais ac yna arsylwi ar y defnyddiwr yn cyrchu'r gwasanaethau cwmwl.
3. Dylid ailadrodd y prawf ar gyfer pob gwasanaeth dilysu a ddefnyddir.

Os bydd y prawf yn arwain at y defnyddiwr neu'r gweinyddwr yn cael cais am fath o ddull dilysu aml-ffactor cyn y rhoddir mynediad, yna rhowch ganlyniad Llwyddo. Fel arall, cofnodwch ganlyniad Methu.

Dehongli canlyniadau'r achos prawf

Os byddwch yn rhoi canlyniad Llwyddo i bob is-brawf, yna cofnodwch ganlyniad Llwyddo ar gyfer yr achos prawf hwn. Fel arall, cofnodwch ganlyniad Methu.

Achos prawf 5: Gwirio ymwahaniad cyfrifon

Dylid cynnal y prawf hwn ar unrhyw ddyfeisiau defnyddwyr terfynol a samplwyd, gweinyddion sy'n darparu bwrdd gwaith defnyddiwr-ryngweithiol ac amgylcheddau lle gall prosesau gweinyddol gael eu rhedeg.

Diben y Prawf

Profi nad oes breintiau gweinyddwr wedi'u neilltuo i gyfrifon defnyddwyr

Disgrifiad o'r Prawf

Pan fydd wedi mewngofnodi â chyfrif defnyddiwr safonol, bydd yn ceisio rhedeg proses weinyddol ddiffiniedig.

Mae angen profi pob dyfais a samplwyd.

Achos prawf 5.1

1. Arsylwch ar ddefnyddiwr yn ceisio rhedeg proses weinyddol ar gyfer y systemau gweithredu penodol a samplwyd gyda'r cyfrif sydd wedi mewngofnodi ar y pryd.
2. Dylid ailadrodd y prawf ar bob dyfais a samplwyd yn yr archwiliad.

Os bydd y prawf yn arwain at y defnyddiwr yn cael cais am fanylion mewngofnodi pellach ac nad yw'r broses yn rhedeg gan ddefnyddio manylion cyfrif y defnyddiwr, rhowch ganlyniad Llwyddo. Fel arall, rhowch ganlyniad Methu.

Dehongli canlyniadau'r achos prawf

Os byddwch yn rhoi canlyniad Llwyddo i bob is-brawf ar gyfer pob dyfais a samplwyd, yna cofnodwch ganlyniad Llwyddo ar gyfer yr achos prawf hwn. Fel arall, cofnodwch ganlyniad Methu.

Cwblhau'r asesiad

Ar ôl cwblhau pob prawf, lluniwch eich adroddiad.

Efallai na fyddwch yn gallu cwblhau'r asesiad ar y diwrnod penodedig, a hynny oherwydd rhai anawsterau technegol penodol wrth brofi. Os felly, trafodwch â'r Partner Cyflawni — yn ôl ei ddisgresiwn, cewch ohirio profion a threfnu i'w cwblhau yn ddiweddarach.

Nodyn i'r Partner Cyflawni

Rydym yn argymell nad ydych yn caniatáu i brofion gael eu gohirio am fwy na mis.

Os byddwch yn rhoi canlyniad Llwyddo i **bob** achos prawf yna bydd yr Ymgeisydd yn pasio'r asesiad cyffredinol a chewch ddyfarnu tystysgrif **Cyber Essentials Plus** iddo.

Os byddwch yn rhoi canlyniad Methu i unrhyw achos prawf, ond bod y methiannau hyn o ganlyniad i nifer **bach** o fân faterion yn unig, yna trafodwch â'r Partner Cyflawni. Yn ôl disgresiwn y Partner Cyflawni, mae'n bosibl y gall yr Ymgeisydd basio'r asesiad cyffredinol o hyd yna cewch ddyfarnu tystysgrif **Cyber Essentials Plus**.

Nodyn i'r Partner Cyflawni

Disgwyliwn i'r eithriad hwn fod yn berthnasol i sefyllfaoedd lle:

1. Bydd dim ond gwyriad ymylol oddi wrth y safon, mewn llai na 5% o'r profion a gynhaliwyd.
2. Nad yw'r dystiolaeth yn dangos methiant ehangach ym mhrosesau seiberddiogelwch yr Ymgeisydd.

Fel arall, bydd yr Ymgeisydd yn methu'r asesiad cyffredinol ac ni fyddwch yn dyfarnu tystysgrif.

Atodiad A: Sganio am wendidau

Y gwasanaethau Rhyngrwyd mwyaf cyffredin sydd fwyaf tebygol o gael eu treiddio gan ymosodwyr ar y Rhyngrwyd sydd â lefel isel o sgiliau hefyd. Felly nod sganio am wendidau ar gyfer **Cyber Essentials Plus** yw dod o hyd i amddiffyniad yr holl wasanaethau o'r fath a ddefnyddir gan yr Ymgeisydd a'i adolygu.

- Defnyddiwch yr adnodd(au) sganio am wendidau a gymeradwywyd gan y Partner Cyflawni ar gyfer profion Cyber Essentials. I gael rhagor o wybodaeth am arferion da wrth ddefnyddio adnoddau o'r fath, gweler PCI Approved Scanning Vendors Program Guide.
- Sganiwch bob cyfeiriad IP sy'n gysylltiedig â'r Ymgeisydd. Yn hytrach na sganio pob porth sy'n gysylltiedig â phob cyfeiriad IP, gallwch sganio ystod fwy cyfyngedig a nodir gan y Partner Cyflawni.

Nodyn i'r Partner Cyflawni

Awgrymwn eich bod yn darparu rhestr o byrth TCP ac UDP y dylai'r Asesydd eu sganio. Fel man cychwyn da, gweler Well Known Port List: nmap services ar wefan nmap.org.

Atodiad B: Mathau o ffeiliau prawf

Mae'r Partner Cyflawni yn gyfrifol am ddarparu cyfres gynhwysfawr o ffeiliau prawf i'ch Corff Ardystio.

Mae eich Corff Ardystio yn gyfrifol am ddiffinio a lletya is-set i chi ei defnyddio i brofi, sy'n briodol i'r Ymgeisydd penodol. Holwch eich Corff Ardystio er mwyn sicrhau eich bod yn cael y ffeiliau cywir ar gyfer pob prawf.

Ar gyfer meini prawf canlyniadau profion, byddwn yn gwahaniaethu rhwng dau grŵp cyffredinol o ffeiliau prawf:

- ffeiliau prawf maleiswedd — dylai meddalwedd wrthfaleiswedd adnabod y rhain a rhwystro'r defnyddiwr rhag eu hagor
- ffeiliau prawf gweithredadwy — dylai'r defnyddiwr weld rhybudd a neges sy'n ei alluogi i benderfynu a ddylid parhau ai peidio

Nodyn i'r Partner Cyflawni

Mae'n rhaid i chi ddarparu set o ffeiliau prawf i'r Corff Ardystio sy'n cynrychioli pob math o ffeil y mae Ymgeiswyr yn debygol o ddod ar eu traws, ymlaen llaw.

Dylech hefyd annog y Corff Ardystio i deilwra'r is-set o ffeiliau prawf y bydd yr Asesydd yn eu defnyddio mewn gwirionedd, fel eu bod yn addas i bob Ymgeisydd. Dylai pob is-set adlewyrchu'r cymwysiadau a'r llwyfannau a ddefnyddir gan yr Ymgeisydd penodol.

Er enghraifft, os mai dim ond dyfeisiau OS X a ddefnyddir gan yr Ymgeisydd yna ni fyddai angen i'r is-set gwmpasu mathau o ffeiliau sy'n benodol i Windows. Neu, os bydd yr Ymgeisydd yn defnyddio amgylchedd cymysg yna dylai'r is-set gwmpasu set ehangach o fathau o ffeiliau.

Mae'n rhaid i'r set lawn o ffeiliau prawf cynrychioliadol a ddarperir gennych gynnwys y canlynol:

- fformatau cynnwys (megis .zip a .gz) y gall amgylchedd yr Ymgeisydd eu prosesu
- amrywiaeth o fathau o ffeiliau sy'n weithredadwy'n ddiofyn ar lwyfannau cyffredin — cod deuaidd brodorol ac ieithoedd sgriptio

- ffeiliau o fathau y gallai defnyddwyr eu derbyn yn rheolaidd — megis dogfennau a thaenlenni — ond sy'n cynnwys samplau anweithredol o faleiswedd

Hefyd, dylid nodi'r canlynol:

- dylai ffeiliau prawf gweithredadwy lansio ymddygiad amlwg (megis lansio porwr gwe i dudalen hysbys, neu greu deialog ar y sgrin) fel y gall yr Asesydd nodi'r weithred yn gyflym ac yn hawdd
- dylai samplau o faleiswedd fod yn ffeiliau anweithredol penodol y gwyddys bod y mwyafrif o systemau gwrthfeirysau cyffredin yn tynnu sylw atynt