Generalitat de Catalunya
Consorci per a la Formació Contínua de Catalunya

SOC Servei d'Ocupació de Catalunya

PROGRAMA FORMATIU

CEH - Certified Ethical Hacker

Generalitat de Catalunya

Unió Europea
Fons Social Europeu
L'FSE inverteix en el teu futur

IDENTIFICACIÓ DE L'ESPECIALITAT I PARÀMETRES DEL CONTEXT FORMATIU

Denominació de l'especialitat:	CEH - Certified Ethical Hacker
Família Professional:	Informàtica i comunicacions
Àrea Professional:	Desenvolupament
Codi:	(A emplenar pel SEPE)
Nivell de qualificació professional:	3

Objectiu general

Identificar les eines i metodologies usades per un Hacker Ètic per detectar bretxes de seguretat sobre sistemes informàtics i proposar-hi solucions.

Relació de mòduls de formació

Mòdul 1	Introducció al Hacking i reconeixement	20 hores
Mòdul 2	Hacking de Sistemes	20 hores
Mòdul 3	Evasió i hacking sobre aplicacions.	25 hores
Mòdul 4	Hacking a Xarxes Sense Fils	15 hores

Modalitats d'impartició

Presencial i teleformació

Durada de la formació

Durada total en qualsevol modalitat d'impartició 80 hores

Teleformació: Durada de les tutories presencials: 0 hores

Requisits d'accés de l'alumnat

Acreditacions/ titulacions	Complir com a mínim algun dels següents requisits: - Títol de Batxillerat o equivalent. - Títol de Tècnic Superior (FP Grau Superior) o equivalent. - Haver superat la prova d'accés a Cicles Formatius de Grau Superior. - Haver superat qualsevol prova oficial d'accés a la Universitat. - Certificat de professionalitat de nivell 3. - Títol de Grau o equivalent. - Títol de Postgrau (Màster) o equivalent.
Experiència professional	No es requereix.
Altres	Quan l'aspirant no disposi del nivell acadèmic mínim o de l'experiència professional, demostrarà coneixements i competències suficients per participar en el curs amb aprofitament mitjançant una prova d'accés.
Modalitat de teleformació	A més de l'indicat anteriorment, l'alumnat ha de tenir les destreses suficients per a ser usuaris de la plataforma virtual en la qual es recolza l'acció formativa.

Prescripcions de formadors i tutors

Acreditació requerida	Complir com a mínim algun dels següents requisits: - Llicenciat, Enginyer, Arquitecte o Títol de Grau corresponent o altres títols equivalents. - Diplomat, Enginyer Tècnic, Arquitecte Tècnic o el Títol de Grau corresponent o altres títols equivalents.
Experiència professional mínima requerida	Es requereix 1 any en l'àmbit d'Informàtica i comunicacions en cas de disposar de formació. Es requereix 3 anys en l'àmbit d'Informàtica i comunicacions en cas de no disposar de formació.
Competència docent	Complir com a mínim algun dels següents requisits: - Serà necessari tenir formació metodològica o experiència docent. - Certificat de Professionalitat de Docència de la Formació Professional per a l'Ocupació. - Màster Universitari de Formador de Formadors o altres acreditacions oficials equivalents.
Altres	Cal que el formador disposi d'acreditació oficial del fabricant.
Modalitat de teleformació	A més de complir amb les prescripcions establertes anteriorment, els tutors-formadors han d'acreditar una formació, d'almenys 30 hores, o experiència, d'almenys 60 hores, en aquesta modalitat i en la utilització de les tecnologies de la informació i comunicació.

Requisits mínims d'espais, instal·lacions i equipaments

Espais formatius	Superfície m² per a 15 alumnes	Incremento Superfície/ alumne(Màxim 30 alumnes)	Equipament
Aula informàtica	45m2	2,4 m2/alum	- Taula i cadira per al formador/a. - Taules i cadires per a l'alumnat. - Material d'aula - Pissarra. - PC instal·lat en xarxa, canó amb projecció i Internet per al formador. - PCs instal·lats en xarxa i Internet. - Programari específic vinculat amb l'especialitat formativa.

La superfície dels espais i instal·lacions estaran en funció de la seva tipologia i del nombre d'alumnes. Tindran com a mínim els metres quadrats que s'indiquen per a 15 alumnes i l'equipament suficient per a aquests.

En el cas que augmenti el nombre d'alumnes, fins a un màxim de 30, la superfície de les aules s'incrementarà proporcionalment (segons s'indica en la taula quant a m²/ alumne) i l'equipament estarà d'acord amb aquest augment.

No ha d'interpretar-se que els diversos espais formatius identificats hagin de diferenciar-se necessàriament mitjançant tancaments.

Les instal·lacions i equipaments hauran de complir amb la normativa industrial i higienicosanitària corresponent i respondran a mesures d'accessibilitat i seguretat de l'alumnat.

En el cas que la formació es dirigeixi a persones amb discapacitat es realitzaran les adaptacions i els ajustos raonables per a assegurar la seva participació en condicions d'igualtat.

Aula virtual

Si s'utilitza l'aula virtual han de complir-se les següents indicacions.

Característiques
La impartició de la formació mitjançant aula virtual s'ha d'estructurar i organitzar de manera que es garanteixi en tot moment que existeixi connectivitat sincronitzada entre les persones formadores i l'alumnat participant així com bidireccionalitat en les comunicacions. S'haurà de comptar amb un registre de connexions generat per l'aplicació de l'aula virtual en què s'identifiqui, per a cada acció formativa desenvolupada a través d'aquest mitjà, les persones participants a l'aula, així com les seves dates i temps de connexió.

Si l'especialitat s'imparteix en modalitat de teleformació, quan hi hagi tutories presencials, s'usaran els espais formatius i equipaments necessaris indicats anteriorment.

A més, en el cas de teleformació, s'ha de disposar del següent equipament.

Plataforma de teleformació:
La plataforma de teleformació que s'utilitzi per a impartir accions formatives haurà d'allotjar el material virtual d'aprenentatge corresponent, posseir capacitat suficient per a desenvolupar el procés d'aprenentatge i

gestionar i garantir la formació de l'alumnat, permetent la interactivitat i el treball cooperatiu, i reunir els següents requisits tècnics d'infraestructura, programari i serveis:

· **Infraestructura**

· Tenir un rendiment, entès com a nombre d'alumnes que suporti la plataforma, velocitat de resposta del servidor als usuaris, i temps de càrrega de les pàgines Web o de descàrrega d'arxius, que permeti:

a) Suportar un nombre d'alumnes equivalent al número total d'alumnat en les accions formatives de formació professional per a l'ocupació que estigui impartint el centre o entitat de formació, garantint un hostalatge mínim igual al total de l'alumnat d'aquestes accions, considerant que el nombre màxim d'alumnes per tutor és de 80 i un nombre d'usuaris concurrents del 40% d'aquest alumnat.

b) Disposar de la capacitat de transferència necessària perquè no es produeixi efecte retard en la comunicació audiovisual en temps real, havent de tenir el servidor en el qual s'allotja la plataforma una amplada de banda mínima de 300 Mbs, suficient en baixada i pujada.

· Estar en funcionament 24 hores al dia, els 7 dies de la setmana.

· **Software:**

· Compatibilitat amb l'estàndard SCORM i paquets de continguts IMS.

· Nivells d'accessibilitat i interactivitat dels continguts disponibles mitjançant tecnologies web que com a mínim compleixin les prioritats 1 i 2 de la Norma UNE 139803:2012 o posteriors actualitzacions, segons l'estipulat en el capítol III del Reial decret 1494/2007, de 12 de novembre.

· El servidor de la plataforma de teleformació ha de complir amb els requisits establerts en la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, per la qual cosa el responsable d'aquesta plataforma ha d'identificar la localització física del servidor i el compliment del que s'estableix sobre transferències internacionals de dades en els articles 40 a 43 de la citada Llei orgànica 3/2018, de 5 de desembre, així com, en el que resulti d'aplicació, en el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques respecte del tractament de dades personals i la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE.

· Compatibilitat tecnològica i possibilitats d'integració amb qualsevol sistema operatiu, base de dades, navegador d'Internet dels més usuals o servidor web, havent de ser possible utilitzar les funcions de la plataforma amb complements (connector) i visualitzadors compatibles. Si es requerís la instal·lació addicional d'algun suport per a funcionalitats avançades, la plataforma ha de facilitar l'accés al mateix sense cost.

· Disponibilitat del servei web de seguiment (operatiu i en funcionament) de les accions formatives impartides, conforme al model de dades i protocol de transmissió establerts en l'annex V de l'Ordre/TMS/369/2019, de 28 de març.

· **Serveis i suport**

· Sustentar el material virtual d'aprenentatge de l'especialitat formativa que a través d'ella s'imparteixi.

· Disponibilitat d'un servei d'atenció a usuaris que doni suport tècnic i mantingui la infraestructura tecnològica i que, de forma estructurada i centralitzada, atengui i resolgui les consultes i incidències tècniques de l'alumnat. Les maneres d'establir contacte amb aquest servei, que seran mitjançant telèfon i missatgeria electrònica, han d'estar disponibles per a l'alumnat des de l'inici fins a la finalització de l'acció formativa, mantenint un horari de funcionament de demà i de tarda i un temps de demora en la resposta no superior a 48 hores laborables.

· Personalització amb la imatge institucional de l'administració laboral corresponent, amb les pautes d'imatge corporativa que s'estableixin.

A fi de gestionar, administrar, organitzar, dissenyar, impartir i avaluar accions formatives a través d'Internet, la plataforma de teleformació integrarà les eines i recursos necessaris a tal fi, disposant, específicament, d'eines de:

· Comunicació, que permetin que cada alumne pugui interaccionar a través del navegador amb el tutor-formador, el sistema i amb els altres alumnes. Aquesta comunicació electrònica ha de dur-se a terme

mitjançant eines de comunicació síncrones (aula virtual, xat, pissarra electrònica) i asíncrones (correu electrònic, fòrum, calendari, tauler d'anuncis, avisos). Serà obligatori que cada acció formativa en modalitat de teleformació disposi, com a mínim, d'un servei de missatgeria, un fòrum i un xat.
· Col·laboració, que permetin tant el treball cooperatiu entre els membres d'un grup, com la gestió de grups. Mitjançant tals eines ha de ser possible realitzar operacions d'alta, modificació o esborrat de grups d'alumnes, així com creació de «escenaris virtuals» per al treball cooperatiu dels membres d'un grup (directoris o «carpetes» per a l'intercanvi d'arxius, eines per a la publicació dels continguts, i fòrums o xats privats per als membres de cada grup).
· Administració, que permetin la gestió d'usuaris (altes, modificacions, esborrat, gestió de la llista de classe, definició, assignació i gestió de permisos, perfils i rols, autenticació i assignació de nivells de seguretat) i la gestió d'accions formatives.
· Gestió de continguts, que possibilitin l'emmagatzematge i la gestió d'arxius (visualitzar arxius, organitzar-los en carpetes –directoris- i subcarpetes, copiar, pegar, eliminar, comprimir, descarregar o carregar arxius), la publicació organitzada i selectiva dels continguts d'aquests arxius, i la creació de continguts.
· Avaluació i control del progrés de l'alumnat, que permetin la creació, edició i realització de proves d'avaluació i autoavaluació i d'activitats i treballs avaluables, la seva autocorrecció o la seva correcció (amb retroalimentació), la seva qualificació, l'assignació de puntuacions i la ponderació d'aquestes, el registre personalitzat i la publicació de qualificacions, la visualització d'informació estadística sobre els resultats i el progrés de cada alumne i l'obtenció d'informes de seguiment.

Material virtual d'aprenentatge:
El material virtual d'aprenentatge per a l'alumnat mitjançant el qual s'imparteixi la formació es concretarà en el curs complet en format multimèdia (que mantingui una estructura i funcionalitat homogènia), havent d'ajustar-se a tots els elements de la programació (objectius i resultats d'aprenentatge) d'aquest programa formatiu que figura en el Catàleg d'Especialitats Formatives i el contingut de les quals compleixi aquests requisits:
· Com a mínim, ser l'establert en el citat programa formatiu del Catàleg d'Especialitats Formatives.
· Estar referit tant als objectius com als coneixements/ capacitats cognitives i pràctiques, i habilitats de gestió, personals i socials, de manera que en el seu conjunt permetin aconseguir els resultats d'aprenentatge previstos.
· Organitzar-se a través d'índexs, mapes, taules de contingut, esquemes, epígrafs o titulars de fàcil discriminació i seqüenciés pedagògicament de tal manera que permeten la seva comprensió i retenció.
· No ser merament informatius, promovent la seva aplicació pràctica a través d'activitats d'aprenentatge (autoavaluable o valorades pel tutor-formador) rellevants per a l'adquisició de competències, que serveixin per a verificar el progrés de l'aprenentatge de l'alumnat, fer un seguiment de les seves dificultats d'aprenentatge i prestar-li el suport adequat.
· No ser exclusivament textuals, incloent-hi variats recursos (necessaris i valuosos), tant estàtics com interactius (imatges, gràfics, àudio, vídeo, animacions, enllaços, simulacions, articles, fòrum, xat, etc.) de manera periòdica.
· Poder ser ampliats o complementats mitjançant diferents recursos addicionals als quals l'alumnat pugui accedir i consultar a voluntat.
· Donar lloc a resums o síntesis i a glossaris que identifiquin i defineixin els termes o vocables bàsics, rellevants o claus per a la comprensió dels aprenentatges.
· Avaluar la seva adquisició durant i a la finalització de l'acció formativa a través d'activitats d'avaluació (exercicis, preguntes, treballs, problemes, casos, proves, etc.), que permetin mesurar el rendiment o acompliment de l'alumnat

Vinculació amb capacitacions professionals

Aquesta formació prepara per a les proves d'acreditació del fabricant

Ocupacions i llocs de treball relacionats

-24391049 ENGINYERS DE SEGURETAT
-24691082 ENGINYERS TÈCNICS DE SEGURETAT

-2723 Analistes de xarxes informàtiques

Requisits oficials de les entitats o centres de formació

Estar inscrit al Registre d'entitats de formació (Serveis Públics d'Ocupació)

DESENVOLUPAMENT MODULAR

MÒDUL DE FORMACIÓ 1: Introducció al Hacking i reconeixement

OBJECTIU

Identificar la terminologia i conceptes bàsics que es faran servir al llarg de tot el curs, així com poder identificar actius a la xarxa, ports, serveis i vulnerabilitats presents en una xarxa objectiu.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 20 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS D'APRENENTATGE

Coneixements/ Capacitats cognitives i pràctiques

- Identificació de conceptes de hacking, seguretat i reconeixement.
  - Capacitat per entendre els diferents conceptes en termes de seguretat.
  - Mètodes per fer un correcte reconeixement dels objectius a internet.
  - Bones practiques per evitar publicació indeguda d'informació
- Identificació amb escanejats a la xarxa, ports, serveis, vulnerabilitats i contramesures
  - Escaneigs de reconeixement d'actius
  - Escaneigs de ports i serveis
  - Execució d'escaneigs d'identificació de sistemes operatius
  - Solucions que ajudin a prevenir escanejats de diferents tipus sobre els actius
  - Informació sensible exposada sobre serveis d'una organització
  - Vulnerabilitats com a possible vector d'atac a les organitzacions
  - Remeis a les vulnerabilitats

Habilitats de gestió, personals i socials

- Identificació de conceptes de seguretat.
- Reconeixement i identificació de les amenaces existents en un entorn digital.
- Comprendre els riscos que poden patir les companyies en un entorn digital.

MÒDUL DE FORMACIÓ 2: **Hacking de Sistemes**

OBJECTIU

Organitzar la informació recol·lectada en passos previs per donar pas al hacking en sistemes, per mitjà de diferents tècniques i eines.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 20 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS D'APRENENTATGE

Coneixements/ Capacitats cognitives i pràctiques

- Execució de tècniques de hacking per a la intrusió de sistemes
  - Tècniques d'atacs que es poden fer per accedir a un sistema
- Identificació de codi maliciós (malware) segons la seva funció
  - Tipus de programari maliciosos existents
  - Mitjans de propagació més usats per a distribució de codi maliciós (malware)
  - Eines d'anàlisi de xarxes per identificar bretxes de seguretat en protocols febles
- Identificació de tècniques d'enginyeria social
  - Atac DoS
  - Atac DDoS
- Identificació de contramesures de tècniques de hacking
  - Contramesures i controls per a malware
  - Controls per mitigar atacs que busquen afectar la disponibilitat de la informació

Habilitats de gestió, personals i socials

- Responsabilitzar-se dels processos de hacking que permetin accedir a sistemes febles o vulnerables.
- Coneixement dels riscos i les implicacions que un atac pot tenir.
- Capacitat d'identificació de controls i contramesures per a la prevenció d'atacs.

MÒDUL DE FORMACIÓ 3: **Evasió i hacking sobre aplicacions.**

OBJECTIU

Analitzar com un atacant pot fer atacs sobre sessions, aplicacions i bases de dades, així com saltar controls de seguretat i les contramesures existents per disminuir aquests atacs.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 25 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS D'APRENENTATGE

Coneixements/ Capacitats cognitives i pràctiques

- Identificació d'atacs enfocats al segrest de sessions
  - Atac d'home al medi actiu i passiu
  - Atacs de robatoris de sessions a les capes del model OSI
  - Implementació de protocols segurs
- Identificació dels diferents controls perimetrals
  - Classes de tallafocs
  - Tipus de Honeypots
  - IDS/IPS
  - Identificació de controls
  - Tècniques d'evasió de controls
- Identificació d'atacs a Servidors web
  - Mètodes i usos d'atacs a servidors web
  - Pas a pas de cada atac i el seu objectiu
  - Controls per mitigar exposició
  - Protocols segurs
  - Desplegament d'actualitzacions
- Identificació d'atacs a Aplicacions web
  - Tipus d'atacs existents sobre aplicacions web
  - Metodologia d'execució d'atacs sobre aplicacions web
  - Ús de codi segur
  - Codificació d'informació
- Comprensió de conceptes d'injecció SQL
  - Diferents query SQL
  - Tipus d'injecció SQL
  - Metodologies d'injecció SQL
  - Tècniques d'evasió
  - Ús d'aplicacions per identificar possibles errors

Habilitats de gestió, personals i socials

- Capacitat per reconèixer entorns insegurs on es poden arribar a materialitzar atacs a aplicacions.
- Participació en la solució d'errors de seguretat i/o identificació de controls que disminueixin la probabilitat d'atac a una empresa.
- Valoració d'entorns per determinar el nivell de risc que pot tenir un sistema.

MÒDUL DE FORMACIÓ 4: **Hacking a Xarxes Sense Fils**

OBJECTIU

Identificar els mètodes existents d'atacs i seguretat sobre tecnologies de més ús i que es troben en auge.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 15 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS D'APRENENTATGE

Coneixements/ Capacitats cognitives i pràctiques

- Comprensió de conceptes de Xarxes Sense fils
  - Tecnologies existents
  - Maquinari utilitzat en xarxes sense fil
  - Seguretat aplicada a xarxes sense fil
- Identificació d'amenaces a xarxes sense fils
  - Tipus d'atacs sobre xarxes sense fil
  - Metodologia d'atacs
- Identificació de contramesures i seguretat en xarxes sense fil
  - Eines d'auditoria
  - Controls i bones pràctiques
- Identificació de plataformes mòbils i vectors d'atac
  - Vectors OWASP Top 10 per a mòbils
  - Hacking a Android OS
  - Hacking iOS
  - Hacking Windows Phone US
- Comprensió de conceptes i seguretat BYOD i dispositius IoT
  - Arquitectura i seguretat BYOD
  - Tipus de dispositius IoT
  - Connexió de dispositius
  - Top 10 OWASP per a IoT
  - Contramesures
- Introducció a conceptes de computació al núvol
  - Tipus de serveis al núvol
  - Tipus de desplegaments al núvol
  - Beneficis del núvol
  - Atacs al núvol
  - Seguretat al núvol
- Identificació de conceptes de criptografia
  - Tipus de criptografia
  - Explicació d'algorismes simètrics i asimètrics
  - Hash, signatura i xifrat
  - Identificar els diferents atacs criptogràfics existents

Habilitats de gestió, personals i socials

- Capacitat d'avaluar diferents tecnologies emergents pel que fa al nivell de seguretat i confiança
  Capacitat propositiva en la implementació i/o millora de seguretat de protocols per mitjà de controls

criptogràfics

AVALUACIÓ DE L'APRENENTATGE EN L'ACCIÓ FORMATIVA

- L'avaluació tindrà un caràcter teoricopràctic i es realitzarà de forma sistemàtica i contínua, durant el desenvolupament de cada mòdul i al final del curs.
- Es pot incloure una avaluació inicial i de caràcter diagnòstic per detectar el nivell de partida de l'alumnat.
- L'avaluació es durà a terme mitjançant els mètodes i els instruments més adequats per comprovar els diferents resultats d'aprenentatge, i que en garanteixin la fiabilitat i la validesa.
- Cada instrument d'avaluació s'acompanyarà del sistema de correcció i puntuació corresponent en què s'expliciti, de manera clara i inequívoca, els criteris de mesura per avaluar els resultats assolits pels alumnes.
- La puntuació final assolida s'expressarà en termes d'apte/no apte.