PRESTAKUNTZA-MODULUAREN IDENTIFIKAZIO-DATUAK

PRESTAKUNTZA-MODULUA	SEGURTASUN INFORMATIKOKO GORABEHEREN KUDEAKETA	Iraupena	90
Kodea	MF0488_3		
Lanbide-arloa	INFORMATIKA ETA KOMUNIKAZIOAK		
Lanbide-eremua	Sistemak eta telematika		
Profesionaltasun-ziurtagiria	Segurtasun informatikoa	Maila	3
Profesionaltasun-ziurtagiria osatzeko gainerako prestakuntza	Segurtasuna ekipo informatikoetan	Iraupena	90
	Segurtasun informatikoko auditoretza		90
	Datuen sarbiderako eta datu-tratamendurako sistema seguruak		60
	Sistema informatikoko zerbitzuen kudeaketa (zeharkakoa)		90
	Lanekoak ez diren lanbide-jardunbideak Segurtasun informatikoan		80

A atala: **GAITASUN-ERREFERENTEA**

Prestakuntza-modulu hau bat dator UC0488_3 SEGURTASUN-GORABEHERAK DETEKTATZEA ETA HORIEI ERANTZUTEA gaitasun-atalarekin

B atala: **AHALMENEN ETA EDUKIEN ZEHAZTAPENA**

Ahalmenak eta ebaluazio-irizpideak

A1: Crackerrak detektatzeko sistemak planifikatzea eta ezartzea segurtasun-arauen arabera.

EI1.1 Crackerren detekzioko eta prebentzioko teknikak deskribatzea eta hautaketa-irizpidetzat har daitezkeen parametro nagusiak azaltzea.

EI1.2 Crackerrak detektatzeko sistemen kopurua, mota eta kokapena zehaztea eta ezarpen-planean adierazitako trafikoaren monitorizazioa bermatzea.

EI1.3 Crackerrak detektatzeko sistemaren arauak hautatzea monitorizatu beharreko sistema informatikoaren arabera.

EI1.4 Sistemaren alarma-atalaseak zehaztea sistemaren erabilera-parametroak kontuan izanik.

EI1.5 Detektatze-arauak eratzea, baimenik gabe sartzeko tekniken ezaugarrietan oinarrituta.

EI1.6 Behar bezala zehaztutako kasu praktiko batean zerbitzariak kokatu dira sarbide lokalak eta urrunekoak egiteko aukerarekin; honako lan hauek egin behar dira:

- Alarmak biltzeko softwarea instalatzea eta konfiguratzea.
- Alarmak biltzeko hainbat maila konfiguratzea.

EI1.7 Kasu praktikoen bilduma batean, zerbitzarien ingurune kontrolatu bat dago Interneterako konexioa duen departamentuko sare bateko hainbat zonatan; honako lan hauek egin behar dira:

- Zein area babestu erabakitzea.
- Crackerrak detektatzeko sistema bat instalatzea.
- Detektatzeko arauak definitzea eta aplikatzea.
- Sistemaren funtzionamendua egiaztatzea eremu babestuei eraso eginez.
- Ondorioak zehazten dituen txostena egitea.

A2: Informazioa aztertzeko prozedurak aplikatzea, baita detektatutako gorabehera baten aurrean erasoari aurre egiteko prozedurak ere.

EI2.1 Crackerrak detektatzeko sistemetako informazioa aztertzea eta segurtasunerako garrantzitsuak diren gertaerak ondorioztatzea.

EI2.2 Baimenik gabeko sartzeen arrastoak aztertzea eta mehatxua gauzatu ahal izateko beharrezkoak diren baldintzatzaileak zehaztea.

EI2.3 Baimenik gabeko sartzeak detektatzeko sistemaren alertetako elementuak sailkatzea eta horien artean izan daitezkeen korrelazioak ezartzea, alertak denboraren eta segurtasun-mailaren arabera sailkatuta.

EI2.4 Kasu praktiko batean sistema informatikoan baimenik gabe sartzeko saialdiak egin dira; honako lan hauek egin behar dira:

- Baimenik gabeko sartzeak detektatzeko sistemen alertak biltzea.
- Baimenik gabeko sartzeak detektatzeko sistemek bildutako gertaerak erlazionatzea.
- Alerta adierazgarriak zehaztea.
- Txostena idaztea baimenik gabe gerta daitezkeen sartzeak adierazita, baita erakundearen sistema informatikoaren segurtasunerako ekar dezakeen arriskua ere.

EI2.5 Crackerrak detektatzeko erreminten eguneratze-prozesuak ezartzea funtzionalitatea bermatzearren, fabrikatzaileen zehaztapenei jarraiki.

A3: Kalteak zenbatekoak izan diren aztertzea eta gorabehera bat detektatzen denean berreskuratze-prozesuak zehaztea.

EI3.1 Segurtasun-gorabeheren aurrean jarduteko planaren faseak deskribatzea, baita fase bakoitzaren helburuak ere.

EI3.2 Ekipo informatikoen auzitegi-azterketaren faseak adieraztea eta fase bakoitzaren helburuak deskribatzea.
EI3.3 Sistemen auzitegi-azterketaren ebidentzia-motak sailkatzea eta honako datu hauek adieraztea: ezaugarriak eta bilketa eta azterketa egiteko metodoak.
EI3.4 Programa gaiztoak aztertzeko teknika guztiak deskribatzea eta erabilera-kasuak adieraztea.
EI3.5 Kasu praktiko batean, sistema informatiko batean baimenik gabeko sartze bat gertatu da; honako lan hauek egin behar dira:
- Ebidentzia hegazkorrak biltzea.
- Ebidentzia ez-hegazkorrak biltzea.
- Ebidentzien aurretiazko azterketak.
- Fitxategi-sistemaren jardueraren aldi baterako azterketa.
- Behin betiko txostena egitea eta honako datu hauek biltzea: topatutako ebidentziak, baimenik gabe sartzeko erabili ahal izan diren ahuleziak eta crackerrak egin duen jarduera, sisteman detektatutakoa.

EI3.6 Ekipo informatikoetako hondamendiak berreskuratzeko metodoak estandarizatzea baimenik gabeko sartzeak detektatzean.

Edukiak

1. Baimenik gabeko sartzeen detekzioko eta prebentzioko sistemak (IDS/IPS)
- Gorabeheren kudeaketaren, baimenik gabeko sarreren eta horien prebentzioaren kontzeptu orokorrak
- Sistemaren funtzionamenduko datuen identifikazioa eta ezaugarritzea
- Crackerrak detektatzeko sistemen arkitektura ohikoenak
- IDS/IPS mota guztien zerrenda, kokalekuaren eta funtzionalitatearen arabera
- IDS/IPSen kokalekua ezartzeko segurtasun-irizpideak

2. IDS/IPS sistemen ezarpena eta abiaraztea
- Erakundeak negozio-prozesuetan erabiltzen dituen zerbitzuen, protokoloen, eremuen eta ekipoen aurretiazko azterketa
- IDS/IPSetan baimenik gabe sartzeko saialdien etete-politiken definizioa
- IDS/IPS sistemak erregistratutako gertaeren azterketa, positibo faltsuak zehazteko eta IDS/IPS sistemaren etete-politiketan ezaugarritzeko
- Baimenik gabe sartzeko saiakeren gertaerak eta behar bezala funtzionatzen dutela gainbegiratzeko eta monitorizatzeko beharrezkoak diren IDS/IPS sistemaren auditoretza-erregistroen zerrenda
- IDS/IPS sisteman beharrezkoak diren eguneratze-maila, monitorizazio-maila eta probak ezartzea

3. Kode gaiztoaren kontrola
- Kode gaiztoa detektatzeko eta horri aurre egiteko sistemak
- Kode gaiztoa kontrolatzeko erreminta mota guztien zerrenda, instalazioaren topologiaren eta kontrolatu beharreko kutsatze-bideen arabera
- Kode gaiztoen aurrean babesteko erreminten konfiguraziorako segurtasun-irizpideak
- Kode gaiztoaren aurrean babesteko erremintak eguneratzeko tekniken eta eskakizunen zehaztapena
- Segurtasun-gertaerak eta behar bezala funtzionatzen dutela gainbegiratzeko eta monitorizatzeko beharrezkoak diren kode gaiztoaren aurrean babesteko erreminten auditoretza-erregistroen zerrenda
- Kode gaiztoaren aurrean babesteko erreminten proben eta monitorizazioaren ezarpena
- Programa gaiztoen azterketa desmihiztatzaileen eta exekuzio kontrolatuko inguruneen bitartez

4. Segurtasun-gorabeheren aurreko erantzuna
- Segurtasun-gorabeherekin loturiko informazioa biltzeko prozedura
- Segurtasuneko gertaeren eta informazioaren azterketarako eta korrelaziorako erabilitako erreminten eta tekniken azalpena
- Baimenik gabeko sartzea egiaztatzeko prozesua
- Cert motako gorabeherak kudeatzeko nazioko eta nazioarteko erakundeen izaera eta funtzioak

5. Baimenik gabe sartzeko saialdiak kudeatzeko eta jakinarazteko prozesua
- Erantzukizunen ezarpena baimenik gabe sartzeko saialdiak edo infekzioak kudeatzeko eta jakinarazteko prozesuan
- Baimenik gabe sartzeko saiakeren edo infekzioen ondoriozko gorabeheren kategorizazioa, inpaktu potentzialaren arabera
- Gorabeheraren kudeaketaren oinarri izango diren ebidentzia objektiboak zehazteko irizpideak
- Baimenik gabe sartzeko saialdien edo infekzioen ondoriozko gorabeherak detektatzeko eta erregistratzeko prozesuaren ezarpena
- Baimenik gabe sartzeko saialdiaren edo infekzioaren hasierako azterketa, sailkapena eta gida, izan dezakeen inpaktua kontuan izanik
- Aurreikus daitekeen inpaktuaren araberako esku-hartze mailaren ezarpena
- Baimenik gabe sartzeko saialdiaren edo infekzioen gorabeheren ikerketa eta diagnostikoa egiteko gida
- Baimenik gabe sartzeko saialdiaren edo infekzioaren ondoriozko gorabehera bat izan ostean sistemak berreskuratzeko eta berrezartzeko prozesuaren ezarpena
- Gorabeheren berri hirugarrenei emateko prozesua, hala badagokio
- Gorabehera ixteko prozesuaren ezarpena eta gorabeheraren historikoa dokumentatzeko beharrezkoak diren erregistroak

6. Auzitegi-azterketa informatikoa
- Auzitegi-azterketaren kontzeptu orokorrak eta helburuak

- Lockard-en Printzipioaren azalpena
- Ebidentzia elektronikoak biltzeko gida:
    - Ebidentzia hegazkorrak eta ez-hegazkorrak
    - Ebidentzien etiketatzea
    - Zaintza-katea
    - Ezkutuko direktorioak eta fitxategiak
    - Sistemaren ezkutuko informazioa
    - Ezabatutako fitxategien berreskuratzea
- Bildutako ebidentzia elektronikoak aztertzeko gida, ezkutuko direktorioen eta fitxategien azterketa, sistemaren ezkutuko informazioa eta ezabatutako fitxategien berreskuratzea ere barnean hartuta
- Auzitegi-azterketako erremintak hautatzeko gida

C atala: **ESKAKIZUNAK ETA BALDINTZAK**

Baldintza hauetakoren bat bete behar da:

– Batxilergoko titulua izatea.
– 3. mailako profesionaltasun-ziurtagiriren bat edukitzea.
– Lanbide-arlo eta -eremu bereko 2. mailako profesionaltasun-ziurtagiriren bat edukitzea.
– Goi-mailako heziketa-zikloetan sartzeko baldintza akademikoak betetzea edo goi-mailako zikloetara sartzeko dagozkion probak gainditu izana.
– 25 urte baino gehiagokoentzako eta/edo 45 urtetik gorakoentzako unibertsitatera sartzeko proba gainditu izana.
– Prestakuntzari behar adinako probetxua ateratzeko behar diren prestakuntza- edo lanbide-ezagupenak izatea, ezartzen den araudiaren arabera.

Prestatzaileen, instalazioen eta ekipamenduen arloko eskakizunei dagokienez, profesionaltasun-ziurtagiri honetarako ezarritako eskakizunak hartuko dira kontuan: Segurtasun informatikoa