ANEXO XIII
MODELO DE PROGRAMACIÓN DE MÓDULOS PROFESIONAIS

1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	2024/2025

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CE3IFC005000	Ciberseguridade en contornos das tecnoloxías da información	Ciclos formativos de grao superior	Réxime xeral-ordinario

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP5025	Hacking ético	2024/2025	5	120	144

(*) No caso de que o módulo profesional estea organizado en unidades formativas de menor duración

Profesorado responsable

Profesorado asignado ao módulo	MANUEL GONZÁLEZ REGAL,DIEGO GONZÁLEZ CANABAL (Subst.)
Outro profesorado	

Estado: Pendente de supervisión equipo directivo

2. Concreción do currículo en relación coa súa adecuación ás características do ámbito produtivo

A competencia xeral deste curso de especialización consiste en definir e implementar estratexias de seguridade nos sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando as medidas necesarias para mitigalas aplicando a normativa vixente e estándares do sector, seguindo os protocolos de calidade, de prevención de riscos laborais e respecto ambiental.
As ocupacións e postos de traballo máis relevantes son os seguintes:

* Experto en ciberseguridad.
* Auditor de ciberseguridad.
* Consultor de ciberseguridad.
* Hacker ético.

- A formación do módulo contribúe a alcanzar os seguintes obxectivos xerais:

* Combinar técnicas de hacking ético interno e externo para detectar vulnerabilidades que permitan eliminar e mitigar os riscos asociados.
* Revisar e actualizar procedementos de acordo con normas e estándares actualizados para o correcto cumprimento normativo en materia de ciberseguridad e de protección de datos persoais.
* Desenvolver manuais de información, utilizando ferramentas ofimáticas e de deseño asistido por computador para elaborar documentación técnica e administrativa.
* Analizar e utilizar os recursos e oportunidades de aprendizaxe relacionados coa evolución científica, tecnolóxica e organizativa do sector e as tecnoloxías da información e a comunicación, para manter o espírito de actualización e adaptarse a novas situacións laborais e persoais.
* Desenvolver a creatividade e o espírito de innovación para responder os retos que se presentan nos procesos e na organización do traballo e da vida persoal.
* Avaliar situacións de prevención de riscos laborais e de protección ambiental, propoñendo e aplicando medidas de prevención persoais e colectivas, de acordo coa normativa aplicable nos procesos de traballo, para garantir contornas seguras.
* Identificar e propoñer as accións profesionais necesarias para dar resposta á accesibilidade universal e ao «deseño para todas as persoas».
* Identificar e aplicar parámetros de calidade nos traballos e actividades realizados no proceso de aprendizaxe, para valorar a cultura da avaliación e da calidade e ser capaces de supervisar e mellorar procedementos de calidade.

- A formación do módulo contribúe a alcanzar as seguintes competencias profesionais, persoais e sociais:

* Detectar vulnerabilidades en sistemas, redes e aplicacións, avaliando os riscos asociados.
* Elaborar documentación técnica e administrativa cumprindo coa lexislación vixente, respondendo os requisitos establecidos.
* Adaptarse ás novas situacións laborais, mantendo actualizados os coñecementos científicos, técnicos e tecnolóxicos relativos á súa contorna profesional, xestionando a súa formación e os recursos existentes na aprendizaxe ao longo da vida.
* Resolver situacións, problemas ou continxencias con iniciativa e autonomía no ámbito da súa competencia, con creatividade, innovación e espírito de mellora no traballo persoal e no dos membros do equipo.
* Xerar contornas seguras no desenvolvemento do seu traballo e o do seu equipo, supervisando e aplicando os procedementos de prevención de riscos laborais e ambientais, de acordo co establecido pola normativa e os obxectivos da organización.

* Supervisar e aplicar procedementos de xestión de calidade, de accesibilidade universal e de «deseño para todas as persoas», nas actividades profesionais incluídas nos procesos de produción ou prestación de servizos.

3. Relación de unidades didácticas que a integran, que contribuirán ao desenvolvemento do módulo profesional, xunto coa secuencia e o tempo asignado para o desenvolvemento de cada unha

U.D.	Título	Descrición	Duración (sesións)	Peso (%)
1	Introducción á seguridade ofensiva	Introducción á seguridade ofensiva, ciberkill chain, MITRE ATT&Ck, tipos de auditorías, ...	4	3
2	Ferramentas básicas	Ferramentas básicas de pentesting (Kali Linux, cherrytree, markdown, bash, poweshell, wireshark, ...)	12	5
3	Fase de recopilación de información	Recopilación de información pasiva e activa (whois, dns, OSINT, ...)	15	13
4	Fase de enumeración de servizos	Enumeración de equipos e dos servizos máis habituais (ssh, smb, ftp, ...)	15	12
5	Fase de identificación de vulnerabilidades	Tipos e descubrimento de vulnerabilidades	6	5
6	Fase de explotación e mantemento de acceso	Explotación de sistemas e permanencia	15	13
7	Fase de postexplotación	Elevación de privilexios, movemento lateral e pivoting	15	13
8	Ataques a redes empresariais	Ataques á infraestructura de Active Directory	22.5	15
9	Fase de ocultación, limpeza e informe	Tácticas de ofuscación e antiforense, limpeza e elaboración de informes	5	2
10	Hacking web	Auditorías web (recoñecemento, detección, análise e explotación de vulnerabilidades)	20	15
11	Enxeñaría social. Phishing	Explotación do factor humano	6.5	2
12	Wireless Network Hacking	Auditoría en redes sen fíos	8	2

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introducción á seguridade ofensiva	4

4.1.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	NO

4.1.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.1 Definiuse a terminoloxía esencial do hacking ético
CA1.2 Identificáronse os conceptos éticos e legais fronte ao ciberdelito
CA1.3 Definíronse o alcance e as condicións dun test de intrusión
CA1.4 Identificáronse os elementos esenciais de seguridade: confidencialidade, autenticidade, integridade e dispoñibilidade
CA1.5 Identificáronse as fases dun ataque seguidas por un atacante
CA1.6 Analizáronse e definíronse os tipos vulnerabilidades
CA1.7 Analizáronse e definíronse os tipos de ataque
CA1.9 Determináronse as ferramentas de monitorización adecuadas dispoñibles no mercado en función do tipo de organización

4.1.e) Contidos

Contidos
Elementos esenciais do hacking ético.
Diferenzas entre hacking, hacking ético, tests de penetración e hacktivismo.
Recolección de permisos e autorizacións previos a un test de intrusión.
Fases do hacking.
Auditorías de caixa negra e de caixa branca.
Documentación de vulnerabilidades.
Clasificación de ferramentas de seguridade e hacking.
ClearNet, Deep Web, Dark Web, Darknets. Coñecemento, diferenzas e ferramentas de acceso: Tor. ZeroNet; FreeNet.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Ferramentas básicas	12

4.2.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	NO
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO

4.2.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
0CA1.10 Determináronse e empregáronse de forma correcta as ferramentas básicas para un pentester

Criterios de avaliación
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA3.3 Interceptouse tráfico de rede de terceiros para procurar información sensible

4.2.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking.
Ferramentas básicas para pentesters (distribución para pentest, bash, bash scripting, netcat, wireshark/tshark/tcpdump, powershell, ...)
Monitorizacion de tráfico.
Interceptación de comunicacións utilizando distintas técnicas.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Fase de recopilación de información	15

4.3.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO

4.3.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?

Criterios de avaliación
CA3.1 Compilouse información sobre a rede e sobre sistemas obxectivo mediante técnicas pasivas
CA3.2 Creouse un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo, mediante técnicas activas

4.3.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking. Fase de recoñecemento (footprinting).

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Fase de enumeración de servizos	15

4.4.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO

4.4.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA3.2 Creouse un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo, mediante técnicas activas

4.4.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking.
Fase de escaneo (fingerprinting).
Monitorizacion de tráfico.
Interceptación de comunicacións utilizando distintas técnicas.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Fase de identificación de vulnerabilidades	6

4.5.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	NO
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO

4.5.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.6 Analizáronse e definíronse os tipos vulnerabilidades
CA1.8 Determináronse e caracterizáronse as vulnerabilidades existentes
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA2.7 Realizáronse informes sobre as vulnerabilidades detectadas

Criterios de avaliación
CA3.2 Creouse un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo, mediante técnicas activas

4.5.e) Contidos

Contidos
Documentación de vulnerabilidades.
Clasificación de ferramentas de seguridade e hacking.
Ferramentas de procura e explotación de vulnerabilidades.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Fase de explotación e mantemento de acceso	15

4.6.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	NO
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO
RA4 - Consolida e utiliza sistemas comprometidos garantindo accesos futuros	NO

4.6.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.7 Analizáronse e definíronse os tipos de ataque
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA3.3 Interceptouse tráfico de rede de terceiros para procurar información sensible
CA3.4 Realizouse un ataque de intermediario lendo, inserindo e modificando a vontade o tráfico intercambiado por dous extremos remotos
CA3.5 Comprometéronse sistemas remotos explotando as súas vulnerabilidades
CA4.1 Administráronse sistemas remotos a través de ferramentas de liña de comandos
CA4.2 Comprometéronse contrasinais a través de ataques de dicionario, táboas rainbow e forza bruta contra as súas versións encriptadas
CA4.4 Instaláronse portas traseiras para garantir accesos futuros aos sistemas comprometidos

4.6.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking.
Monitorizacion de tráfico.
Interceptación de comunicacións utilizando distintas técnicas.
Manipulación e inxección de tráfico.
Administración de sistemas de maneira remota.
Ataques e auditorías de contrasinais.
Instalación de portas traseiras con troianos (RAT, Remote Access Trojan).

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Fase de postexplotación	15

4.7.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO
RA4 - Consolida e utiliza sistemas comprometidos garantindo accesos futuros	NO

4.7.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA3.3 Interceptouse tráfico de rede de terceiros para procurar información sensible
CA3.4 Realizouse un ataque de intermediario lendo, inserindo e modificando a vontade o tráfico intercambiado por dous extremos remotos
CA4.1 Administráronse sistemas remotos a través de ferramentas de liña de comandos
CA4.2 Comprometéronse contrasinais a través de ataques de dicionario, táboas rainbow e forza bruta contra as súas versións encriptadas
CA4.3 Accedeuse a sistemas adicionais a través de sistemas comprometidos
CA4.4 Instaláronse portas traseiras para garantir accesos futuros aos sistemas comprometidos

4.7.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking.

Contidos
Monitorizacion de tráfico.
Interceptación de comunicacións utilizando distintas técnicas.
Manipulación e inxección de tráfico.
Escalada de privilexios.
Administración de sistemas de maneira remota.
Ataques e auditorías de contrasinais.
Pivotaxe na rede.
Instalación de portas traseiras con troianos (RAT, Remote Access Trojan).

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Ataques a redes empresariais	22.5

4.8.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO
RA4 - Consolida e utiliza sistemas comprometidos garantindo accesos futuros	SI

4.8.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.5 Identificáronse as fases dun ataque seguidas por un atacante
CA1.6 Analizáronse e definíronse os tipos vulnerabilidades

Criterios de avaliación
CA1.7 Analizáronse e definíronse os tipos de ataque
CA1.8 Determináronse e caracterizáronse as vulnerabilidades existentes
CA3.2 Creouse un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo, mediante técnicas activas
CA3.3 Interceptouse tráfico de rede de terceiros para procurar información sensible
CA3.4 Realizouse un ataque de intermediario lendo, inserindo e modificando a vontade o tráfico intercambiado por dous extremos remotos
CA3.5 Comprometéronse sistemas remotos explotando as súas vulnerabilidades
CA4.1 Administráronse sistemas remotos a través de ferramentas de liña de comandos
CA4.2 Comprometéronse contrasinais a través de ataques de dicionario, táboas rainbow e forza bruta contra as súas versións encriptadas
CA4.3 Accedeuse a sistemas adicionais a través de sistemas comprometidos
CA4.4 Instaláronse portas traseiras para garantir accesos futuros aos sistemas comprometidos
CA4.5 Aplicáronse técnicas para ocultar a presenza do atacante e dificultar a labor de detección da intrusión

4.8.e) Contidos

Contidos
Auditorías de caixa negra e de caixa branca.
Documentación de vulnerabilidades.
Clasificación de ferramentas de seguridade e hacking.
Monitorizacion de tráfico.
Interceptación de comunicacións utilizando distintas técnicas.
Manipulación e inxección de tráfico.

Contidos
Ferramentas de procura e explotación de vulnerabilidades.
Escalada de privilexios.
Técnicas de ocultación e antiforenses
Administración de sistemas de maneira remota.
Ataques e auditorías de contrasinais.
Pivotaxe na rede.
Instalación de portas traseiras con troianos (RAT, Remote Access Trojan).

4.9.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
9	Fase de ocultación, limpeza e informe	5

4.9.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA4 - Consolida e utiliza sistemas comprometidos garantindo accesos futuros	NO

4.9.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA2.7 Realizáronse informes sobre as vulnerabilidades detectadas
CA4.5 Aplicáronse técnicas para ocultar a presenza do atacante e dificultar a labor de detección da intrusión

4.9.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking.
Realización de informes de auditoría e presentación de resultados.
Técnicas de ocultación e antiforenses

4.10.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
10	Hacking web	20

4.10.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	NO
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO
RA5 - Ataca e defende aplicacións web en contornos de proba, e consegue acceso a datos ou funcionalidades non autorizadas	SI

4.10.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.7 Analizáronse e definíronse os tipos de ataque
CA1.8 Determináronse e caracterizáronse as vulnerabilidades existentes
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA2.7 Realizáronse informes sobre as vulnerabilidades detectadas

Criterios de avaliación
CA3.4 Realizouse un ataque de intermediario lendo, inserindo e modificando a vontade o tráfico intercambiado por dous extremos remotos
CA5.1 Identificáronse os sistemas de autenticación web, destacando as súas debilidades e as súas fortalezas
CA5.2 Realizouse un inventario de equipamentos, protocolos, servizos e sistemas operativos que proporcionan o servizo dunha aplicación web
CA5.3 Analizouse o fluxo das interaccións realizadas entre o navegador e a aplicación web durante o seu uso normal
CA5.4 Examináronse manualmente aplicacións web na procura das vulnerabilidades máis habituais
CA5.5 Usáronse ferramentas de procuras e explotación de vulnerabilidades web
CA5.6 Realizouse a procura e a explotación de vulnerabilidades web mediante ferramentas software
CA5.7 Analizouse o protocolo http (cabeceiras, solicitudes, codificacións, ...) e tecnoloxías web máis importantes

4.10.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking.
O protocolo http (cabeceiras, solicitudes, codificacións, ...) e tecnoloxías web máis importantes
Negación de credenciais en aplicacións web.
Colleita de información.
Automatización de conexións a servidores web (exemplo: Selenium).
Análise de tráfico a través de proxies de intercepción.
Procura de vulnerabilidades habituais en aplicacións web.
Ferramentas para a explotación de vulnerabilidades web.

4.11.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
11	Enxeñaría social. Phishing	6.5

4.11.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO

4.11.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?

4.11.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking. Enxeñaría social. Phising.

4.12.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
12	Wireless Network Hacking	8

4.12.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	SI
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO

Resultado de aprendizaxe do currículo	Completo
RA4 - Consolida e utiliza sistemas comprometidos garantindo accesos futuros	NO

4.12.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.1 Configuráronse os modos de funcionamento das tarxetas de rede sen fíos
CA2.2 Describíronse as técnicas de encriptación das redes sen fíos e os seus puntos vulnerables
CA2.3 Detectáronse redes sen fíos e capturouse tráfico de rede como paso previo ao seu ataque
CA2.4 Accedeuse a redes sen fíos vulnerables
CA2.5 Caracterizáronse outros sistemas de comunicación sen fíos e as súas vulnerabilidades
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA2.7 Realizáronse informes sobre as vulnerabilidades detectadas
CA3.3 Interceptouse tráfico de rede de terceiros para procurar información sensible
CA4.2 Comprometéronse contrasinais a través de ataques de dicionario, táboas rainbow e forza bruta contra as súas versións encriptadas

4.12.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking. Comunicación sen fíos. Modo infraestrutura, ad-hoc e monitor.

Contidos
Análise e colleita de datos en redes sen fíos.
Técnicas de ataque e exploración de redes sen fíos.
Ataques a outros sistemas sen fíos.
Realización de informes de auditoría e presentación de resultados.
Monitorizacion de tráfico.
Interceptación de comunicacións utilizando distintas técnicas.
Manipulación e inxección de tráfico.
Ataques e auditorías de contrasinais.

5. Mínimos exixibles para alcanzar a avaliación positiva e os criterios de cualificación

CRITERIOS DE CUALIFICACIÓN:

Probas:

- Estas probas constarán de forma xeral de dúas partes:

* Escrita sobre contidos teóricos das unidades.

* Práctica simulando unha situación real de traballo, onde o alumno deberá demostrar o dominio dos contidos e procedementos adquiridos para levar a cabo a tarefa dunha forma axeitada e nun tempo adecuado.

- En cada parte figurará a puntuación asignada a cada pregunta.

- No enunciado informarase da puntuación mínima necesaria en cada parte para acadar o aprobado na proba.

- Como norma xeral a puntuación máxima dunha proba será 10, estando o aprobado nun 5 (traballando con ata 3 decimais) sempre que se chegue ó aprobado en cada parte. É dicir, hai que aprobar as dúas partes para que a proba se considere aprobada.

Traballos de investigación en grupo ou individuais:

- Consistirán na investigación e/ou exposición por parte dun ou dun grupo de alumnos ó resto dos seus compañeiros.

- O traballo versará sobre un tema concreto proposto polo profesor, ó que os alumnos poden suxerir ideas.

- Haberá traballos de reforzo que non sumarán para a nota de avaliación pero que sí son de entrega obrigatoria.

- Valorarase:

* A consecución dos obxectivos a acadar no traballo e a súa forma de implementación.
* Os contidos do traballo.
* A capacidade de investigación.
* A comprensión.
* A capacidade de explicación.
* Nivel de dificultade do traballo.

- En cada traballo o profesor indicará os obxectivos a acadar, a puntuación máxima e a puntuación necesaria para acadar a superación na proba.
- Todos os traballos son de entrega obrigatoria, salvo que o profesor indique o contrario. Non entregar o traballo en tempo e forma, implicará a consideración de suspenso (non superado).
- Como norma xeral a puntuación máxima dunha proba será 10 estando o aprobado nun 5, traballando con ata 3 decimais.

Avaliación:

- En cada avaliación haberá:
  * A lo menos unha proba.
  * Un ou máis traballos.

Avaliación positiva:

- Para ter unha avaliación positiva nunha avaliación é preciso superar todas e cada unha das probas e traballos de entrega obrigatoria. No caso de non superar todas as probas ou traballos, a avalación considerase como non superada.
- De superar todas as probas e traballos a avaliación considerase aprobada.
- De forma xeral, no caso de aprobar a avaliación o cálculo da nota seguirá o seguinte criterio:
  * as probas un 90% da nota da avaliación.
  * os traballos prácticos un 10% da nota da avaliación.
  * Esta porcentaxe será comunicada ó alumnado, e no caso de que a marcha da clase así o suxira poderá modificarse, comunicándollo ó alumnado con suficiente antelación.

Avaliación negativa:

- No caso de non superar algunha das probas nunha avaliación.
- No caso de que a media, tendo en conta a porcentaxe asignada ás probas e traballos, non chegue ó 5.
- Nesta situación non se calculan medias coas notas recibidas en partes superadas. A nota que aparecerá na avaliación será a menor das puntuacións obtidas nas probas.

Nota final:

- Para aqueles alumnos que superaron todas as avaliacións, a nota final será o promedio das notas das avaliacións.

Calquera modificación sobre a forma de avaliar recollida neste punto co gallo de mellor o proceso de ensinanza-aprendizaxe, será comunicada con antelación ó alumnado e explicada detalladamente.

MÍNIMOS ESIXIBLES

UD1 - Introducción á seguridade ofensiva

- Definir a terminoloxía esencial do hacking ético
- Identificar os conceptos éticos e legais fronte ao ciberdelito
- Definir o alcance e as condicións dun test de intrusión
- Identificar os elementos esenciais de seguridade: confidencialidade, autenticidade, integridade e dispoñibilidade
- Identificar as fases dun ataque seguidas por un atacante. Cyber Kill Chain e matriz MITTRE ATT&CK
- Analizar e definir os tipos vulnerabilidades
- Analizáronse e definíir os tipos de ataque
- Determinar as ferramentas de monitorización adecuadas dispoñibles no mercado en función do tipo de organización

UD2 - Ferramentas básicas

- Coñecer as diferentes distribución para pentesting
- Instalar, configurar e xestionar unha distribución de pentesting
- Ferramentas para tomar notas. Cherrytre. Linguaxe Markdown.
- Coñecer e empregar adecuadamente os comandos linux necesarios para pentesting
- Crear scripts que aceleren e/ou automaticen certas tarefas nas auditorías
- Coñecer e empregar adecuadamente ferramentas de monitorización de tráfico usando as opcións de captura e visualización axeitadas
- Analizar capturas de paquetes interpretando adecuadamente os resultados

UD3 - Fase de recopilación de información

- Compilar información sobre a rede e sobre sistemas obxectivo mediante consulta ás bases de datos whois
- Crear un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo
- Compilar información sobre a rede e sobre sistemas obxectivo mediante consulta ós DNS
- Crear un inventario de equipamentos e sistemas obxectivo
- Compilar información sobre a rede e sobre sistemas obxectivo mediante técnicas pasivas de OSINT
- Crear un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo

UD4 - Fase de enumeración de servizos

- Recopilar de información sobre o obxectivo mediante técnicas pasivas e activas (barrido e exploración portos)
- Enumerar de servizos (netbios/SMB, ftp, nfs, rlogin, email, base de datos, ldap, ...)

- Crear un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo
- Enumerar de servizos (netbios/SMB, ftp, nfs, rlogin, email, base de datos, ldap, ...)
- Crear un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo

UD5 - Fase de identificación de vulnerabilidades

- Analizar e definir os tipos vulnerabilidades
- CVE (Common Vunerabilities and Exposures)
- Determinar e caracterizar as vulnerabilidades existentes usando ferramentas de detección de vulnerabilidades (Nessus, OpenVAS, nmap NSE, ...)
- Realizar informes sobre as vulnerabilidades detectadas
- Crear un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo

UD6 - Fase de explotación e mantemento de acceso

- Analizar e definir os tipos de ataque
- Utilizar técnicas de red team
- Comprometer sistemas remotos explotando as súas vulnerabilidades
- Bind Shell e reverse shell
- Coñecer e empregar netcat e/ou semellantes para tarefas de pentest
- Comprometer contrasinais a través de ataques de dicionario, táboas rainbow e forza bruta contra as súas versións encriptadas
- Instalar portas traseiras para garantir accesos futuros aos sistemas comprometidos
- Administrar sistemas remotos a través de ferramentas de liña de comandos
- Cover channels

UD7 - Fase de postexplotación

- Empregar ténicas de elevación de privilexios no sistema atacado
- Empregar técnicas de exploración das redes internas
- Empregar técnicas de explotación a novos sistemas
- Empregar técnicas de pivoting para acceder a novos sistemas

UD8 - Ataques a redes empresariais

- Coñocer os compoñentes dun directorio activo e as súas funcionalidades
- Montar un directorio activo simulandomunha rede empresarial
- Analizar, definir os principais tipos de ataque nun AD para obter un acceso inicial
- Analizar e definir os tipos vulnerabilidades dun AD que permiten obter un acceso inicial
- Identificar as fases dos ataques iniciais nun AD que permiten obter un acceso inicial
- Realizar ataque de intermediario lendo, inserindo e modificando a vontade o tráfico intercambiado por dous extremos remotos

- Comprometer sistemas remotos explotando as súas vulnerabilidades
- Crear un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo, mediante técnicas activas
- Analizar e definir os tipos vulnerabilidades dun AD que permiten obter un acceso elevado
- Analizar, definir os principais tipos de ataque nun AD para obter un acceso elevado
- Identificar as fases dos ataques nun AD para obter un acceso elevado
- Comprometer sistemas remotos explotando as súas vulnerabilidades para obter un acceso elevado
- Administrar sistemas remotos a través de ferramentas de liña de comandos
- Acceder a sistemas adicionais a través de sistemas comprometidos
- Analizar e definir os tipos vulnerabilidades dun AD que permiten obter persistencia
- Analizar, definir os principais tipos de ataque nun AD para obter persistencia
- Comprometer sistemas remotos explotando as súas vulnerabilidades para obter persistencia
- Instalar portas traseiras para garantir accesos futuros aos sistemas comprometidos
- Aplicar técnicas para ocultar a presenza do atacante e dificultar a labor de detección da intrusión

UD9 - Fase de ocultación, limpeza e informe

- Aplicar técnicas para ocultar a presenza do atacante e dificultar a labor de detección da intrusión
- Utilizar técnicas de red team
- Realizar informe de auditoría e presentación de resultados.

UD10 - Hacking web

- Coñecer o protocolo http (cabeceiras, solicitudes, codificacións, ...) e tecnoloxías web máis importantes
- Realizar un inventario de equipamentos, protocolos, servizos e sistemas operativos que proporcionan o servizo dunha aplicación web
- Analizar o fluxo das interaccións realizadas entre o navegador e a aplicación web durante o seu uso normal
- Identificar os sistemas de autenticación web, destacando as súas debilidades e as súas fortalezas
- Usar ferramentas de procuras e explotación de vulnerabilidades web
- Examinar manualmente aplicacións web na procura das vulnerabilidades máis habituais
- Coñecer e explotar as vulnerabildades web máis habituais (XSS, SQL injection, LFI, Full Path Disclosure, Directory Transversal, ...)
- Usar ferramentas de explotación de vulnerabilidades web
- Realizar a procura e a explotación de vulnerabilidades web mediante ferramentas software

UD11 - Enxeñaría social. Phishing

- Coñecer e aplicar técnicas de enxeñaría social
- Deseñar unha campaña de phising e spear phishing
- Empregar técnicas de phishing para facer ataques client-side dirixidos

UD12 - Wireless Network Hacking
- Coñecer as comunicación sen fíos.
- Comprender e configurar distintos modos de rede: Modo infraestrutura, ad-hoc e monitor
- Coñecer e comprender as tramas IEEE 802.11
- Coñecer e comprender WEP e WPA
- Colleitar e analizar datos en redes sen fíos
- Coñecer e aplicar técnicas de ataque e exploración de redes sen fíos

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

No mes de xuño para o alumnado con partes pendentes (non superadas):
* haberá unha proba final personalizada por alumno, onde poderá recuperar aquelas partes da asignatura que teña suspensas.
* no caso de traballos non superados, o profesor asignará ó alumno unha serie de tarefas para entregar.
- De superar esta proba/traballos, considerarase que o alumno superou a asignatura.
- No caso de non superar esta proba/traballos, considerase que o alumno non superou a asignatura.
- Para aqueles alumnos que superaron o módulo, a nota final será o promedio das notas das avaliacións xunto coa nota da proba final.
- Para o alumnado que non superou o módulo, a nota final reflictirá a nota da proba final. Nesta situación non se calculan medias coas notas recibidas en partes superadas.

Despois da proba da segunda avaliación, o alumnado que non superou o módulo terá na aula virtual materiais de repaso/reforzo para preparar a proba final

6.b) Procedemento para definir a proba de avaliación extraordinaria para o alumnado con perda de dereito a avaliación continua

No curso de especialización non é de aplicación a perda de avaliación continua en base á Resolución do 6 de xullo de 2023, da Dirección Xeral de Formación Profesional, pola que se ditan instrucións para o desenvolvemento dos cursos de especialización de formación profesional no ano académico 2023/24 no ámbito da Comunidade Autónoma de Galicia.

Ademais, non ha lugar en educación a distancia e semipresencial

7. Procedemento sobre o seguimento da programación e a avaliación da propia práctica docente

Considerando que a programación é un documento que se elabora ó comezo do curso escolar, estará sempre aberta a calquera modificación baseándonos en diferentes factores que se inclúen no proceso de ensinanza-aprendizaxe. Avaliaranse os procesos de avaliación, técnicas e métodos, temporalización e momentos de aplicación, os recursos dos que dispoñemos e a metodoloxía.

Unidades didácticas:

Máis polo miudo, ó remate de cada unidade didáctica analizaremos:

Contidos:

- Na programación do vindeiro curso incluiranse novas actividades para aqueles contidos que supuxeron maior dificultade de aprendizaxe para o alumnado.
- Engadiranse tamén os contidos de ampliación tratados, se houbo algún. Terase en conta tamén o cambio daqueles contidos que se deciden impartir noutra unidade de traballo.
- Actualizanse os contidos para recoller ó avance da tecnoloxía.

Actividades:

- Eliminaranse da nova programación as actividades que non se realizaron por considerarse redundantes ou innecesarias, e incorporaranse todas as novas que o docente considerou necesarias para acadar os obxectivos da unidade, así como a modificación das xa existentes.

Recursos:

- Na programación vindeira incluiranse os recursos empregados que non se tiveran en conta ao facer a programación actual. Aqueles non usados indicarase que son opcionais.
- Se algún recurso necesario non se puido empregar por non existir no centro, solicitarase a súa compra nunha reunión de departamento. Na programación do curso seguinte comprobarase a dispoñibilidade dese recurso para incluílo ou non na mesma.

Metodoloxía:

- A metodoloxía empregada para o desenvolvemento de cada unidade de traballo baséase principalmente na exposición por parte do docente da parte teórica e de exemplos de actividades, e a realización do alumnado de tarefas e traballos sobre os contidos expostos.
- Se houbo algún cambio na metodoloxía que fixo que o alumnado acadase os obxectivos de xeito máis doado, incorporarase á nova programación.

Temporalización:

- O número de sesións asignadas axustaranse ao tempo real empregado na unidade de traballo.

Avaliacións

- Ó remate de cada trimestre, revisarase o proceso de avaliación, axustando o tipo e número de instrumentos de avaliación e en consecuencia as porcentaxes e o xeito de calcular as cualificacións parciais e final.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

- Ao comezo do curso, cubrirase un formulario onde se reflictan os seguintes aspectos recollidos desde o comezo do curso académico e ata a data de avaliación:

* Coñecementos teóricos.
* Destrezas e habilidades prácticas.
* Resultados nos controis.
* Traballos entregados.
* Relación co resto do grupo.
* Relación co profesor do módulo.
* Comportamento xeral na clase.
* Puntualidade e asistencia.

- Esta proba non será cualificable e só se terán en conta os resultados para adecuar o nivel de partida do proceso de ensino-aprendizaxe á realidade do grupo e/ou adoptar as medidas de reforzo que se consideren oportunas.

8.b) Medidas de reforzo educativo para o alumnado que non responda globalmente aos obxectivos programados

Medidas de reforzo:

- As medidas de reforzo teñen como obxectivo intentar axudar a superar algunha unidade de traballo a aqueles alumnos que non acadaron os obxectivos mínimos esixibles.
- Cada caso será analizado de forma particular, e as actividades teórico/prácticas serán indicadas o alumno para o seu desenrolo.

Medidas de ampliación:

- As medidas de ampliación teñen como obxectivo atender ás demandas de aqueles alumnos que superan amplamente ós obxectivos do módulo.
- As medidas de ampliación poden ser:
  * Investigación por parte do alumno de temas non tratados na aula.
  * Profundización en temas tratados.
  * Realización de traballos/tarefas adicionais.
- Todas estas tarefas estarán supervisadas e orientadas polo profesor, personalizando as tarefas según a situación especial de cada alumno..

9. Aspectos transversais

9.a) Programación da educación en valores

Os temas transversais que se atopan en todas as unidades de traballo son:

* Coñecemento e respecto pola normativa TIC legal vixente; en especial a Lei de Protección de Datos de Carácter Persoal (LOPD).
* Manexo da lingua inglesa para poder empregar manuais escritos nesta lingua, xa que ademais do castelán, é a lingua máis empregada en manuais técnicos informáticos.
* Aprendizaxe permanente ao longo da vida.
* Entendemento da importancia que ten o movemento de Software Libre no desenvolvemento da carreira profesional de cada alumno/a, no contorno produtivo de Galicia e as súas implicacións sociais.

Educación en valores

* A educación en valores na Formación Profesional está dirixida ao desenvolvemento da cultura profesional. A sociedade require algo máis que persoas adestradas para a función específica do mundo do traballo. Necesita profesionais con motivacións e capacidades para a actividade creadora e independente, tanto no desempeño laboral como investigador, ante os desafíos do coñecemento e información científico-técnica e da realización do seu ideal social e humano.
* A formación integral e especializada son dous piares da profesionalidade.
* A personalidade profesional maniféstase a través do conxunto de rasgos presentes no individuo, na actividade profesional, nos marcos de determinada comunidade e contexto.
* Por todo isto o profesorado fomentará:
  - O amor á actividade profesional.
  - O sentido de respecto socioprofesional.
  - O estilo de busca profesional creativo-innovador.
  - A comunicación interpersoal. Compañerismo.
  - Elevar a calidade profesional na solución de problemas.
  - Responsabilidade.
  - Honestidade.

9.b) Actividades complementarias e extraescolares

- Conferencias con expertos do sector.
- Participación en congresos e concursos de retos de ciberseguridade.