

¿QUIERES APRENDER A TENER CIBER- SUPERPODERES?



Campus Tecnológico-Deportivo para
Jóvenes

Universidad de Oviedo



JOSÉ MANUEL REDONDO LÓPEZ PROYECTO "F-74 'ASTURIAS'" v1.0

Fuente: Microsoft Copilot



Organiza:



Colaboran:



Logo por: @creative_vanesa

¡BIENVENIDO!



José Manuel
Redondo López

- Bienvenido a este curso de **Ciberdefensa Personal a varios niveles**
- Gracias a él podrás conocer y poner en práctica una serie de técnicas que te **protegerán** antes un gran nº de ataques diferentes
 - Esto es cada vez más necesario debido al incremento actual de los mismos
- El curso identifica los más comunes y da **contramedidas** contra todos ellos
- La intención es mantener seguros tus equipos, los de tus amigos / familiares...o los que usas en el trabajo
- ¡Convertirte en un “**embajador de la ciberseguridad**” en tu entorno! 😊
- ¡Es un curso que forma parte de la iniciativa “**Cobra Kali**”!



La iniciativa
"Cobra Kali" por
José Manuel
Redondo López



Investigar Redes Sociales

Técnicas de investigación
para RRSS

F-31 "Descubierta"



Virtualización Básica

Creación y uso de máquinas
virtuales

R-11 "Príncipe de Asturias"

Rango 1
(Marinero)



Investigación de Webs

Detección de webs
problemáticas

S-64 "Narval"



Entendiendo la Mente del Crimen

Mentes criminales y
engaño

M-31 "Segura"



Ataques contra Personas

Ciberacoso

P-74 "Atalaya"

Rango 2
(Marinero de Primera)



Ciberseguridad General

Ciberseguridad general
para el día a día

F-74 "Asturias"



Crime-spotting

Ejemplos de fraudes
reales para
concienciación

"Nautilus"



Vigilancia de Redes

Entendiendo cómo funcionan
las redes modernas

F-83 "Numancia"

Rango 3
(Cabo)



Y si el cuerpo te pide marcha... 😊



La iniciativa
"Cobra Kali" por
José Manuel Redondo
López



Introducción a la Ciberdefensa Personal

Técnicas contra el cibercrimen y fraudes (Niveles A1, A2)
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



Investigación con Fuentes Abiertas (OSINT)

Técnicas de investigación con fuentes abiertas
OCW (parcialmente). "A-21 Poseidón"



Defensa contra el Cibercrimen

Técnicas contra el cibercrimen y fraudes
Divulgación pública, cursos. P-45 Audaz"

Rango 1
(Sargento)



Ciberdefensa Personal Avanzada

Técnicas contra el cibercrimen y fraudes (Niveles B1, B2)
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



Seguridad de Redes

Threat hunting
TBA. L-52 "Castilla"



Administración Segura de SO

Infrastructure as Code
MUINGEWB, OCW. L-62 "Princesa de Asturias"



Seguridad de Sistemas Informáticos

Introducción a la seguridad
Grado en Ing. del Software, OCW. S-81 "Isaac Peral"

Rango 2
(Suboficial Mayor)



Liderazgo en Ciberdefensa para Equipos

Técnicas contra el cibercrimen y fraudes (Nivel C1)
Proyecto UNIDIGITAL. "BPM P-51 'Asturias'"



Identificación y Análisis de Vulnerabilidades en Web

Seguridad ofensiva: Reconocimiento y Explotación
MUINGEWB, Microcredenciales. TK-210 "красный октябрь" (Octubre Rojo)



Desarrollo Seguro de Software

Platform Engineering Seguro
Guías INCIBE. F-113 "Menéndez de Avilés"

Rango 3
(Capitán de Fragata)



Innovación e Investigación en Ciberdefensa

Técnicas contra el cibercrimen y fraudes (Nivel C2)
Proyecto UNIDIGITAL. "BPM P-51 'Asturias'"



Post-Exploiting e Intrusión en Sistemas

Seguridad ofensiva: Post-Explotación
TBA. K-329 "Belgorod"



Protección de Servidores y Aplicaciones Web

Seguridad defensiva
MUINGEWB, Guías INCIBE, Microcredenciales. D-73 y C-33 "Blas de Lezo"






Rango 4
(Almirante)



¿POR QUÉ TIENE CINCO BLOQUES DISTINTOS?






José Manuel
Redondo López

- Este curso está inspirado en la aproximación a la seguridad defensiva del framework internacional **MITRE D3FEND 0.12-BETA-2** (Marzo de 2023)
 - <https://d3fend.mitre.org/>
- El curso está dividido en estos cinco bloques
 -  **Harden**: Técnicas y tácticas para **mejorar la seguridad** de distintos elementos
 -  **Detect**: Técnicas y tácticas para **detectar problemas de seguridad** en distintos elementos
 -  **Isolate**: Técnicas y tácticas para **aislar unos elementos de otros**
 - Para **reducir o mitigar** los efectos de ataques exitosos, o bien se prevengan en ciertos casos
 -  **Deceive**: Técnicas y tácticas para **usar y prevenir el engaño** como método de defensa
 -  **Evict**: Técnicas de **defensa proactiva** (bloqueo, expulsión...) ante ataques detectados
- Cada bloque está dividido en un conjunto de seis módulos
 - **Mismos seis módulos para cada bloque**
 - Cambiando la orientación de los contenidos según el objetivo del bloque en el que están

¿QUÉ MÓDULOS TIENE CADA BLOQUE?






José Manuel
Redondo López

-  **Aspectos Relativos a las Personas:** Los fallos humanos son la principal causa de problemas de seguridad en la actualidad
 - **Autenticación:** Protección de nuestras cuentas de usuario
 - **Computación “sensata”:** Desarrollo del sentido común
-  **Uso de Internet:** Simplemente usar Internet conlleva una gran cantidad de peligros que necesitan atención
 - **Usando el navegador de forma segura:** Navegar es una actividad de riesgo si no se hace correctamente
 - **Uso de redes sociales:** El mal uso de las mismas es un peligro, especialmente para la privacidad
-  **Uso de Sistemas de Mensajería**
 - **Email:** Tradicional puerta de entrada de malware y otros problemas de seguridad
 - **Aplicaciones de mensajería:** Otra puerta de entrada de malware y problemas, cada vez más presente

¿QUÉ MÓDULOS TIENE CADA BLOQUE?



José Manuel
Redondo López

-  **Dispositivos de Computación: Las máquinas también necesitan atención**
 - **Telefonía Móvil:** Nuestros “ordenadores de bolsillo” necesitan protección dada su extensión en la población y capacidad de cómputo
 - **Ordenadores:** Necesitamos proteger nuestra herramienta de trabajo diaria
-  **Redes y Dispositivos “Inteligentes”**
 - **Redes de comunicaciones:** En un mundo interconectado, proteger las máquinas debe ir acompañado de la protección de las comunicaciones entre ellas
 - **Dispositivos “Smart”:** Pequeños ordenadores en forma de dispositivos cotidianos interconectados entre ellos o con Internet, que también requieren atención
-  **Seguridad “En el Mundo Real”**
 - **Seguridad “Física”:** No solo hay que proteger a los equipos “por dentro”, sino también “por fuera”
 - Además de la **integridad física de las personas**
 - **Seguridad Financiera:** El objetivo de los ciberdelitos **siempre es económico**, directa o indirectamente
 - Esto requiere la mención de estrategias dirigidas a ello, que debemos prevenir

¿CÓMO SON LOS EJERCICIOS PRÁCTICOS?



José Manuel
Redondo López

- Los ejercicios de este curso cuentan con los siguientes elementos
 - **Código y enunciado** resumen de los objetivos
 - El código único es lo que se usa para **enlazar** teoría y práctica
 - **Infraestructura requerida** y (si es aplicable al curso) **puntuación** otorgada
 - **Descripción breve** del ejercicio
 - **Resultados esperados**: qué deberíamos obtener si realizamos el ejercicio correctamente
 - Incluye **posibles preguntas** que deben responderse para garantizar que se han entendido los conceptos
 - **Otra información complementaria**: Para hacerlo
 - Información de estudio y ayuda para complementar los conceptos de teoría asociados

Autenticación

Ejercicio AUTHA1_DETECT.FALSO_AVISO_LOGIN. Identifica falsos avisos que te piden que hagas login en una de tus cuentas pero en una página falsa

Infraestructura requerida	Un navegador cualquiera
Puntuación	

Descripción de la actividad

Consiste en aprender a detectar si alguna vez has recibido un falso aviso que te pide que metas tus datos te cuenta en una página que puede ser falsa

Resultados Esperados

Puedes contestar estas preguntas:

- ¿Alguna vez te ha llegado un aviso de este tipo?
- ¿Cuál ha sido el principal motivo por el que ha sospechado del mismo?
- ¿Has sido víctima de un timo de esta clase o conoces a alguien que lo fuera, y puedes determinar por qué acabó creyéndose el engaño?

Otra información necesaria para su realización

Este tipo de fraude donde recibimos avisos que normalmente requieren que hagamos clic en un enlace o bien que contestemos a un mensaje **son cada vez más frecuentes** y, por tanto, tenemos que ser conscientes de que lo más probable es que **nos va a llegar uno tarde o temprano**, y tendremos que reaccionar adecuadamente para no ser víctimas.

Lo importante es darse cuenta de que ningún mensaje legítimo de una compañía que realmente se preocupe por la seguridad **va a llevar jamás un enlace en el que debas hacer clic**. Los mensajes auténticos te van a pedir que entres en la banca online (o en el servicio correspondiente al mensaje) tú mismo, **navegando manualmente como lo haces de forma habitual**, pero **nunca van a tener un enlace para que hagas clic en él**. De tenerlo, el proveedor del servicio estaría cometiendo una temeridad puesto que el número de mensajes de este tipo con enlaces fraudulentos es altísimo, y por tanto un servicio legítimo nunca debería copiar el aspecto de uno de ellos. Me atrevo a decirte que si te encuentras con algo así algún día, te pienses si seguir con él, porque no es indicio de que se tomen la seguridad muy en serio. Esto es un aviso falso de este tipo, complementando los vistos en teoría:

¿CÓMO SON LOS EJERCICIOS PRÁCTICOS?



José Manuel
Redondo López

● Todos los ejercicios están vinculados con algún concepto de teoría por su código único

- Así puedes hacer el/los ejercicios que refuerzan ese concepto de teoría directamente
- ¡Teoría y prácticas siempre están enlazadas!
- No todas las transparencias de teoría requieren ejercicios para su comprensión

hecho login en un nuevo dispositivo es siempre falso

- Porque puede pasar y es legítimo
- **Pero sé muy prudente**
 - Si el mensaje de aviso trae un enlace/botón **NO LO USES**
 - Si el mensaje te pide que respondas algo **NO LO HAGAS**
 - Es para que te suscribas a un servicio que no quieres
- **Accede tú mismo a la cuenta** y comprueba la velocidad del mensaje



Autenticación

Ejercicio AUTHA1_DETECT.FALSO_AVISO_LOGIN. Identifica falsos avisos que te piden que hagas login en una de tus cuentas pero en una página falsa

Infraestructura requerida	Un navegador cualquiera
Puntuación	

Descripción de la actividad

Consiste en aprender a detectar si alguna vez has recibido un falso aviso que te pide que metas tus datos te cuenta en una página que puede ser falsa

Resultados Esperados

Puedes contestar estas preguntas:

- ¿Alguna vez te ha llegado un aviso de este tipo?
- ¿Cuál ha sido el principal motivo por el que ha sospechado del mismo?
- ¿Has sido víctima de un timo de esta clase o conoces a alguien que lo fuera, y puedes determinar por qué acabó creyéndose el engaño?

Otra información necesaria para su realización

Este tipo de fraude donde recibimos avisos que normalmente requieren que hagamos clic en un enlace o bien que contestemos a un mensaje **son cada vez más frecuentes** y, por tanto, tenemos que ser conscientes de que lo más probable es que **nos va a llegar uno tarde o temprano**, y tendremos que reaccionar adecuadamente para no ser víctimas.

Lo importante es darse cuenta de que ningún mensaje legítimo de una compañía que realmente se preocupe por la seguridad **va a llevar jamás un enlace en el que debas hacer clic**. Los mensajes auténticos te van a pedir que entres en la banca online (o en el servicio correspondiente al mensaje) **tú mismo, navegando manualmente como lo haces de forma habitual, pero nunca van a tener un enlace para que hagas clic en él**. De tenerlo, el proveedor del servicio estaría cometiendo una temeridad puesto que el número de mensajes de este tipo con enlaces fraudulentos es altísimo, y por tanto un servicio legítimo nunca debería copiar el aspecto de uno de ellos. Me atrevo a decirte que si te encuentras con algo así algún día, te pienses si seguir con él, porque no es indicio de que se tomen la seguridad muy en serio. Esto es un aviso falso de este tipo, complementando los vistos en teoría:

ELEMENTOS COMUNES DE TEORÍA



José Manuel
Redondo López

- Cada uno de los seis módulos de los 5 bloques de la teoría de este curso tiene algo para ayudarte a seguirlo

- Es una transparencia de “autoevaluación”
- Con un conjunto de preguntas que puedes hacerte para saber si has entendido correctamente los contenidos de dicho módulo
- Es la forma de no avanzar (si no quieres) hasta estar seguro de que has entendido cada parte
- Hace el curso muy modular y **facilita el aprendizaje** autónomo al ritmo de cada uno

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



José Manuel
Redondo López

?

● Autenticación

- ¿Sabes que cosas te puede pedir un mensaje alarmante que recibas que te hacen descartarlo inmediatamente?
- ¿Sabes qué hacer si ese mensaje te hace dudar?
- ¿Tienes claro que tipo de acciones pueden indicar que hay alguien dentro de tu cuenta usándola sin tu permiso?

● Computación “sensata”

- ¿Crees que el emisor de un correo o de un mensaje es fiable? ¿O se puede falsificar muy fácilmente?
- ¿Qué indicios crees que pueden indicar que un remitente de un mensaje es falso?
- ¿Qué no debes hacer con los enlaces de un mensaje?
- ¿Cuál es la forma más adecuada de actuar si un mensaje te hace dudar?

¿Y TODO EL RESTO DE MATERIAL?



José Manuel
Redondo López

- Durante este curso se hará mención a otros cursos complementarios que te regalo y que forman parte de la misma iniciativa
- Puedes encontrarlos todos aquí:
 - [https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-\(Capacitaci%C3%B3n-B%C3%A1sica\)](https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-(Capacitaci%C3%B3n-B%C3%A1sica))
- También tengo pensado en el futuro subir videos explicando cada curso en mi canal de YouTube
 - <https://www.youtube.com/@JoseRedondo-dj7xk>

¿QUIERES APRENDER A TENER CIBER- SUPERPODERES?

PRESENTACIÓN

