Co-funded by the
Erasmus+ Programme
of the European Union

CYBER.VET.EU

IMPROVING CYBERSECURITY READINESS OF THE EUROPEAN VOCATIONAL EDUCATION AND TRAINING SECTOR

MATERIALES DE FORMACIÓN

CYBERSECURITY AWARENESS TRAINING MATERIAL FOR THE VET SECTOR

NGO NEST Berlin
AEII
tandem plus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

INTRODUCCIÓN A LOS MATERIALES DE FORMACIÓN

JORNADAS DE JUEGOS

INTRODUCCIÓN

Desde el otoño de 2021, relacionado con el Mes Europeo de la Ciberseguridad, hasta la primavera de 2022, los socios del proyecto CYBER.VET.EU organizaron varias GameJams en los países de los socios. Los jóvenes participaron dándoles la oportunidad de acercarse a los temas de ciberseguridad y proporcionándoles nuevas herramientas.

El objetivo principal de esta salida intelectual era resolver la necesidad de una mayor concienciación sobre la ciberseguridad. Se recurrió al proceso de "gamificación" para obtener una solución fácil de adoptar, rápida de implementar, escalable en el tiempo e inclusiva. El proceso de gamificación, definido como "la aplicación de la mecánica de los juegos a contextos no lúdicos con el objetivo de inducir el compromiso y elevar los niveles de motivación", es una forma demostrada de mantener a los usuarios comprometidos con las actividades de aprendizaje, con grandes resultados incluso en periodos cortos de tiempo gracias a la explotación del entretenimiento que motiva a los participantes a comprometerse más con el material y a practicar. Así pues, este producto actuará como una combinación de directrices, formación y práctica, con la característica de ser fácilmente actualizable cuando haya que añadir nuevo material.

RESULTADOS DE LAS ACTIVIDADES / JORNADAS DE JUEGO

- Mayor concienciación sobre la seguridad digital
- Aumento de la concienciación sobre seguridad digital entre las comunidades de los participantes (familia, amigos, colegas).
- Reducción de la tasa de éxito del malware en las instituciones
- Reducción de las fugas de datos
- Aumento del interés por el sector de la ciberseguridad como oportunidad laboral.

AEII / INERCIA DIGITAL [ES]

ACTIVIDADES

Las actividades más relevantes realizadas por los socios españoles AEII e Inercia Digital fueron:

- Hackathon
- Jornadas de juegos
- Jornadas informativas
- Conferencia internacional
- Evento de difusión

RESULTADOS

Las sesiones de GameJam en España proporcionaron algunos resultados útiles que pueden consultarse aquí:

https://scratch.mit.edu/projects/611211889/

https://scratch.mit.edu/projects/611201682/ https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

AEII / INERCIA DIGITAL [ES]

GAME JAM

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

AEII / INERCIA DIGITAL [ES]

Hackathon

Ciberseguridad en la educación

Los socios españoles AEII e Inercia Digital participaron online en un Hackathon del 20 al 22 de octubre de 2021, con 47 participantes, muchos de ellos expertos en informática. https://www.comprometidosporelfuturo.com/proyectos# apoyado por Boehringer Ingelheim en España.

PROBLEMA A RESOLVER

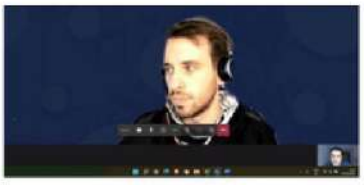
El ciberacoso es uno de los principales riesgos de Internet para los jóvenes. Es habitual encontrar posts con contenido ofensivo hacia algunas personas y que éstos sean utilizados con el fin de acosar y burlarse de las víctimas.

El ciberacoso suele provocar graves alteraciones en las víctimas, como trastorno de estrés postraumático, depresión, pensamientos y conductas suicidas o ansiedad.

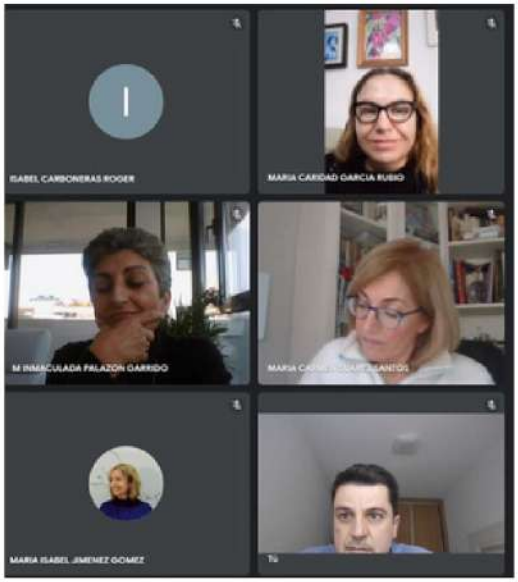
Este reto consiste en estudiar y analizar lo que los jóvenes saben sobre seguridad, así como concienciarles de los riesgos que corren en sus centros educativos y en su vida diaria.
Este reto busca, a través de la gamificación, la mayor concienciación de alumnos y profesores en el día a día en temas relacionados con la seguridad en el uso de las nuevas tecnologías.

RESULTADOS

- Juego y animación vinculados a la ciberseguridad en la educación
- Implicación de la administración pública, centros de FP, expertos en informática, profesores, alumnos y socio del proyecto
- Creación de vídeos cortos interactivos



AEII / INERCIA DIGITAL [ES]



En general, después de realizar numerosas encuestas, los conocimientos de ciberseguridad de los profesores y alumnos de los centros de FP siguen siendo bajos en España. Por ello, este proyecto y otros similares son muy relevantes en España.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

JORNADA DE JUEGOS

La ONG Nest Berlin, Extrafondente Open Source - EOS e IASIS realizaron conjuntamente una sesión GameJam en febrero de 2022. La GameJam comenzó el sábado 12 y duró 6 días en total. En ella, los equipos nacionales desarrollaron y trabajaron juntos en un borrador de juego (de un juego online o de mesa).
Se reunió un jurado independiente al que se le pidió que evaluara el proyecto de juego siguiendo unas directrices comunes y una plantilla de evaluación.
El equipo ganador recibió una tutoría de 6 meses, así como recursos técnicos para seguir desarrollando la idea de juego.

SOBRE EL JUEGO

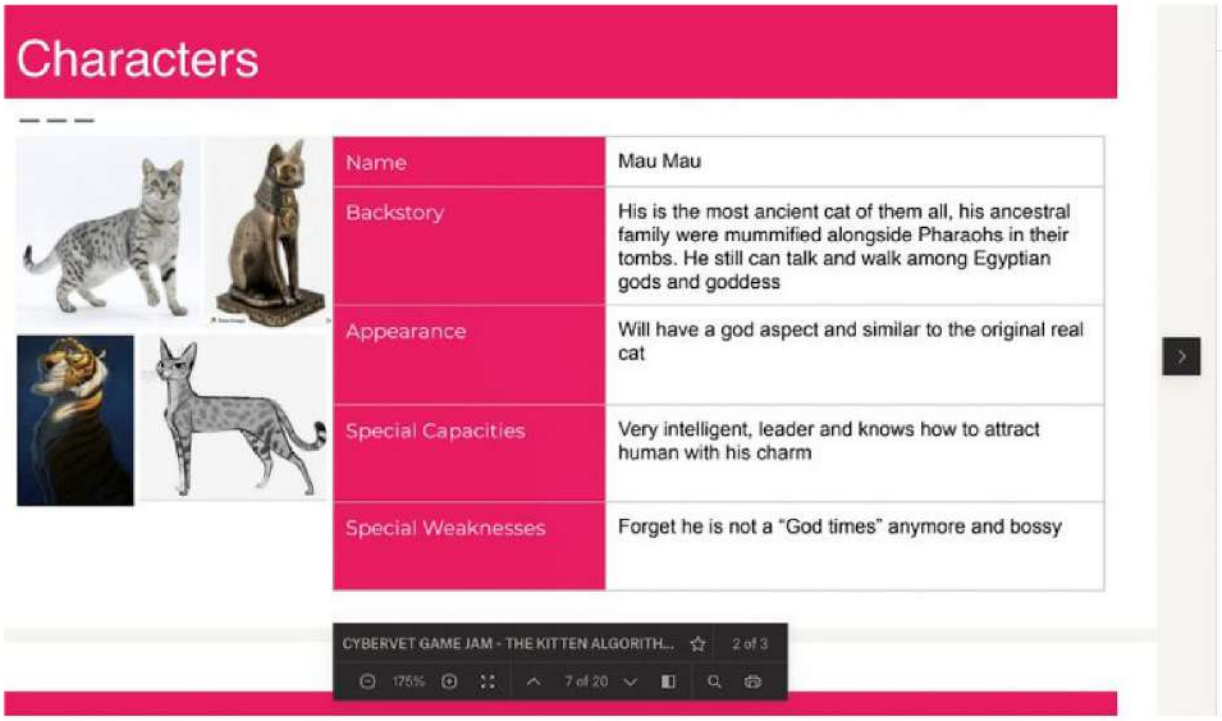
Es un juego de mesa estratégico de 2 a 6 jugadores por turnos, que se juega en unos 30 a 60 minutos. En este juego engañas a los humanos para convencerlos de que eres el mejor gato y consigues más prestigio al conseguir el mayor número de sirvientes de gatos humanos que puedas. Mantén los ojos abiertos, los otros gatos jefes tratarán activamente de sabotear tu camino para llegar a los humanos y llevarse la gloria para ellos. ¡No te fíes de sus bonitas caras!

Pierdes la partida si no tienes un número elevado de humanos como sirvientes o si se acaba la 10ª ronda y ninguno de los jugadores tiene al menos 4 humanos a su cargo.

La dificultad radica en que hay 6 Jefes que intentan engañar a los humanos para que sean sus sirvientes y así los jefes puedan controlarlos, pero todos tienen el mismo objetivo y algunos incluso podrían estar ayudando a los humanos a liberarse del control del gato.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

Mau Mau



LECSA (LV)

JORNADA DE JUEGOS

El socio LECSA de Letonia organizó un evento GameJam del 27 de septiembre al 1 de octubre de 2021. Debido a las restricciones epidemiológicas y a las diferentes ubicaciones de los participantes, se organizó como un evento de tipo híbrido (in situ en la Escuela Técnica de Saldus y a través de la plataforma Zoom). Durante el evento se formaron 6 equipos (4-5 personas por equipo) para trabajar en el desarrollo de prototipos de juegos. Para conseguir resultados tangibles, el concepto de la Game Jam preveía el desarrollo de dos tipos de juegos: de ordenador y de mesa.

ACTIVIDADES

- Los meses de agosto y septiembre de 2021 se dedicaron a la planificación y organización del evento (búsqueda de expertos en ciberseguridad y desarrollo de juegos, distribución de información a los posibles participantes, planificación de la agenda y definición de criterios para el juego, etc.)
- Evento multiplicador - Actualidad en los ciberataques (27.09.2021): Presentación del proyecto CYBER.EU.VET y conferencia sobre las tendencias en los ciberataques con el Sr. Armins Palms, experto en ciberseguridad de CERT.LV (Institución de Respuesta a Incidentes de Seguridad Informática de la República de Letonia)
  - Número de participantes: 26 personas
  - Lugar: Escuela Técnica de Saldus (ciudad de Saldus) y plataforma ZOOM
- Anuncio del Game Jame (27.09.2021): definición y debate sobre los retos actuales en materia de ciberseguridad (evaluación de necesidades); formación de equipos, reunión con los mentores y debate sobre el trabajo posterior (taller sobre el motor de juego Unity), lluvia de ideas sobre la idea y el concepto del juego.
- Actividades de la Game Jam en curso (28.09-30.09.2021): los equipos trabajaron en el desarrollo de prototipos, se consultó a los mentores, si era necesario.
- Presentación del progreso (30.09.2021): presentación de los conceptos del juego y del progreso del trabajo para recibir las sugerencias de los mentores.
- Gran final (01.10.2021): cuatro equipos presentaron sus resultados y los mentores hicieron una evaluación. Un equipo, que desarrolla un juego de ordenador, ha abandonado. Conclusión del evento y debate informal.
  - Número de participantes:
  - Lugar: Escuela Técnica de Saldus y plataforma ZOOM

LECSA (LV)

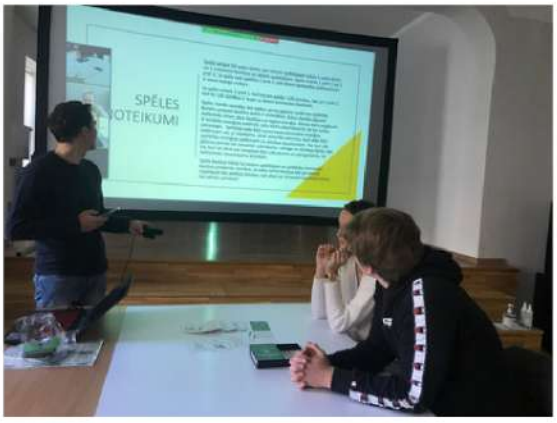
RESULTADOS

1.Prototipo de juego online - El Virus

2. Juego de mesa - Cartas sobre la seguridad

3. Juego de mesa - Ciberguerra

4. Juego de cartas competitivo - Mente cibernética



EJEMPLO - Mente cibernética - Un juego de cartas competitivo

Se trata de un juego de cartas educativo con elementos de concurso. La tarea principal del juego es enseñar
los fundamentos de la seguridad cotidiana en Internet y a qué se expone la gente al hacer tonterías en ella. Abarca temas como la seguridad en Internet y la protección de datos en el contexto del uso de las redes sociales. Como resultado del juego, las personas (los jugadores) deben ser capaces de reconocer los intentos de estafa en la vida real.

Desarrollado por el equipo Veiksminieki (del letón: gente de éxito), estudiantes de la escuela técnica Saldus durante la Game Jam de Letonia (octubre de 2021):
Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere y otros.
Nivel: básico (para principiantes). Destinatarios: alumnos, estudiantes, profesores y padres.
El juego contiene: 50 cartas, 2 almohadillas de salud (para contar la salud de los jugadores), 2 dados y tarjeta de reglas.

LECSA (LV)

JORNADA DE JUEGOS

SOBRE EL JUEGO

Los intentos de ciberataques en el mundo aumentan cada día, por lo que el gobierno mundial tuvo la idea de organizar un torneo para identificar a las personas de alrededor que están trayendo riesgos cibernéticos, y contraatacar contra ellos.

El juego educativo ayuda a conocer los principales tipos de ciberataques, los métodos de prevención y eliminación protegiéndose a sí mismo o a su equipo y contraatacando al adversario. El objetivo del juego es quitarle toda la vida al/los oponente/s.

CÓMO JUGAR - NORMAS

Número de jugadores: 2 o 4 personas (1 vs 1 o 2 vs 2).

Cada jugador o equipo (cuando es de 2 contra 2) tiene "100 vidas" (Salud=HP) al principio de la partida. El recuento de la salud se realiza mediante el uso de libretas negras u otras notas disponibles.

Asigna a una persona distinta que siga y calcule el consumo de energía y salud de los jugadores, si es posible. De lo contrario, los jugadores lo hacen por sí mismos.

Cada jugador recibe 5 cartas. Si la partida se juega 2 contra 2, ambos jugadores tienen "una mano común" en el equipo o 10 cartas juntas.

Hay tres tipos de cartas: Cartas de ataque (rojas), Cartas de escudo (amarillas) y Cartas de vida (verdes).

El juego se desarrolla en rondas. El jugador/equipo que saque el número más alto con los dados comienza la partida.

Cada carta cuesta energía. Al principio de cada ronda, el jugador tira 2 dados para definir una energía que se indica en la parte superior de la carta (en azul). Hay que jugar las cartas para no sobrepasar la cantidad de energía tirada.

El jugador/equipo que protagoniza la ronda puede atacar (con cartas de ataque), protegerse (cartas de escudo) o sumar vida (cartas de curación), mientras que los segundos sólo pueden usar cartas de ataque y de escudo para minimizar su vulnerabilidad de vida.

Ten en cuenta que el número máximo de vidas por jugador/equipo durante la partida puede ser de 100 HP (por ejemplo, si la suma de vidas y energía después de la ronda hace 110 HP en total, tu número de vidas sigue siendo - 100 HP).

El juego termina cuando un jugador/equipo se queda sin todas las vidas (0 vidas).

Si el juego se queda sin cartas, hay que barajar de nuevo las cartas del montón.

LECSA (LV)

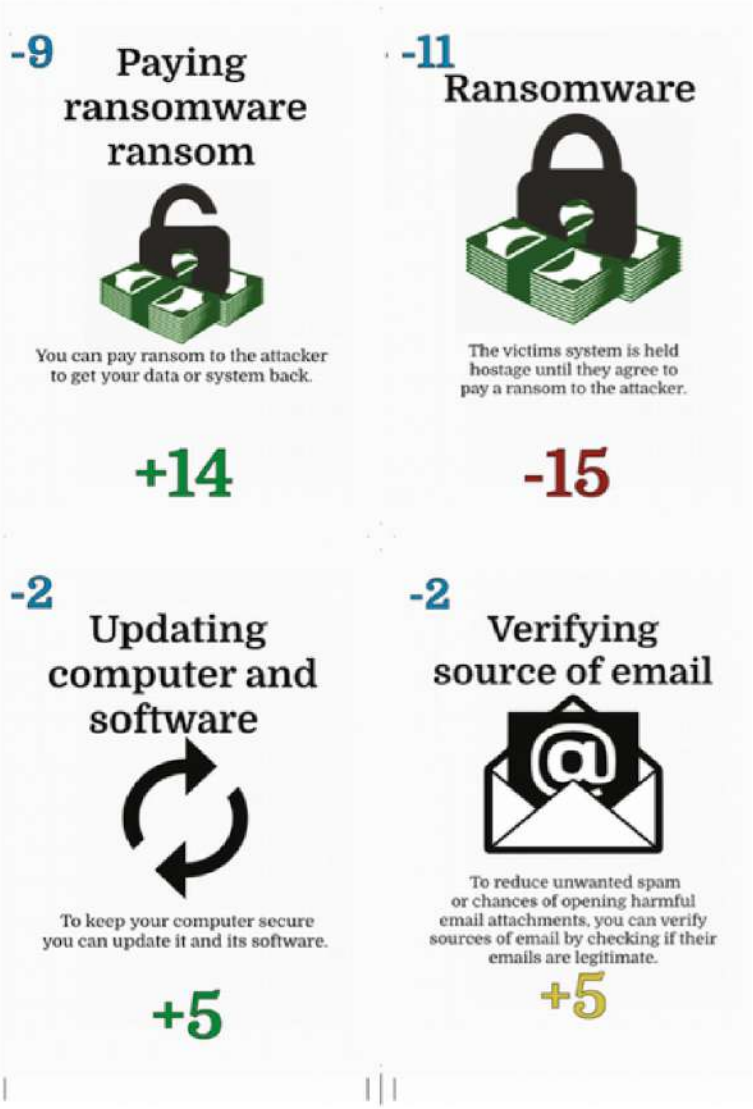
Ejemplo de cartas

En **azul** – energía

En **rojo** - cartas de ataque

En **amarillo** - cartas de escudo

En **verde** - cartas de vida



Ejemplo de cálculo de salud

EJEMPLO Guerra cibernética - juego de mesa

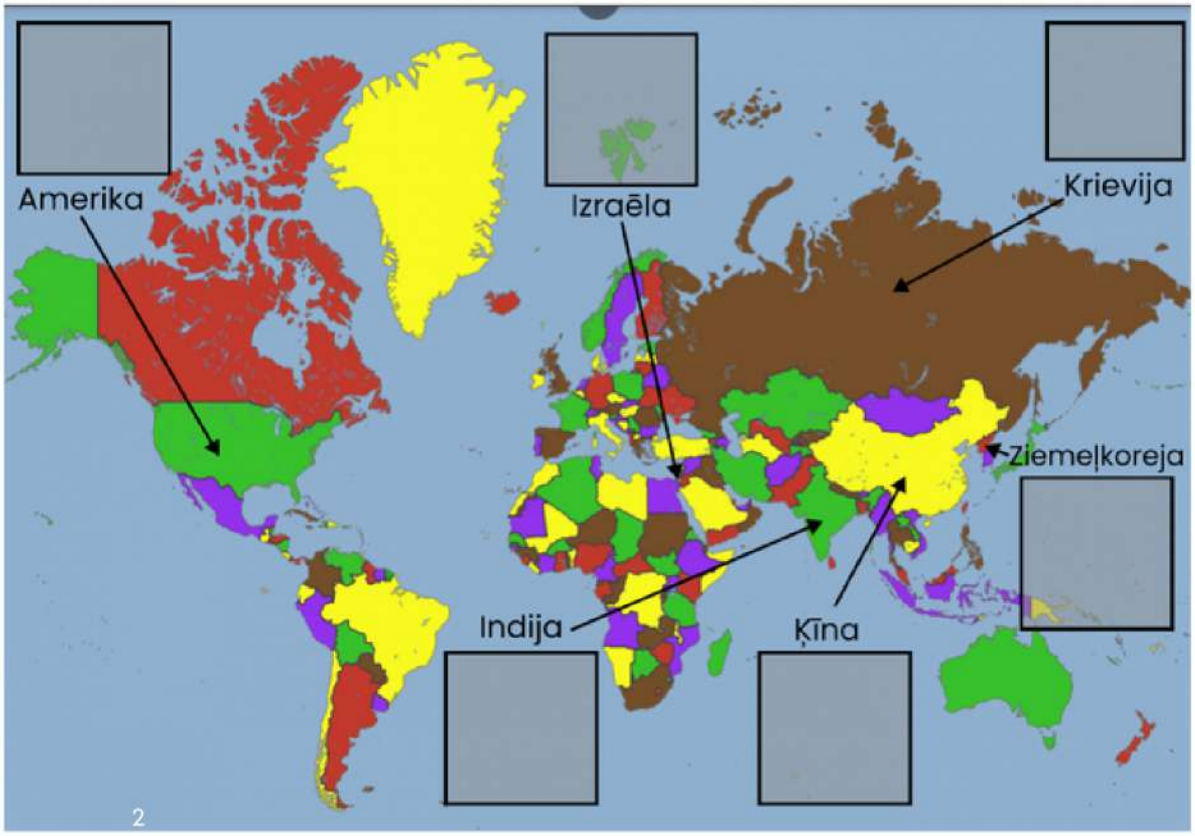
Desarrollado por el equipo Exodus (estudiantes de la Escuela Técnica de Saldus), líder del equipo Valdemārs Šperbergs.

2-6 jugadores < - > Adecuado para personas mayores de 15 años.
Un juego de mesa con un fuerte énfasis en la táctica y la aleatoriedad (azar).

Nivel: juego educativo para aquellos que tienen algunos conocimientos sobre ciberseguridad.
El juego contiene: El juego contiene: Mapa del mundo, 2 dados, servidores, tarjetas con función "ataque", "defensa" o "reacción", leyenda de vulnerabilidades.

SOBRE EL JUEGO

El objetivo del juego es proteger el país representado por el jugador y atacar a otros países para ganar la ciberguerra. En Cyberwar, cada jugador debe elegir un país para representar. Cada jugador tiene un servidor con 3 vulnerabilidades. El objetivo del jugador es hackear los servidores de otros países explotando dos de las tres vulnerabilidades o arreglar dos de las tres vulnerabilidades de su propio servidor.



LECSA (LV)

CÓMO JUGAR

Los jugadores eligen el país que van a representar y colocan un objeto del servidor en el lugar designado del mapa. Cada país tiene sus propias bonificaciones.

Cada jugador sortea (toma) 3 vulnerabilidades -una de cada nivel de dificultad-, y las coloca boca abajo en sus respectivas ubicaciones en sus campos de servidor. Las vulnerabilidades no son conocidas por los jugadores.

Las vulnerabilidades tienen 3 niveles de dificultad. El nivel de dificultad también determina el número necesario para explotar una vulnerabilidad (ver "Ataques"), así como determina cuántos movimientos se necesitarán para solucionar la vulnerabilidad (ver "Defensa").

El juego se desarrolla en rondas, en las que se pueden realizar las siguientes acciones (movimientos): **Exploración, Ataque y Defensa**. Los jugadores determinan la secuencia de jugadores tirando dos dados.

INICIO

- Cada jugador recibe 4 cartas al principio de cada ronda. Al final de la ronda, es posible - quedarse con 2 cartas o cambiarlas por otras existentes.
- La 1ª ronda es una ronda de exploración en la que no se permiten cartas de ataque o defensa. En las rondas siguientes, los jugadores pueden elegir entre Escanear o Atacar o intentar reparar sus vulnerabilidades (ver la defesa). El juego continúa ronda a ronda hasta que se alcanza una condición de victoria.

Exploración

- El atacante elige un país para explorar su vulnerabilidad (por ejemplo, "Estoy escaneando un ruso de 2º nivel de vulnerabilidad").
- El jugador realiza el chequeo - tira dos dados, aplicando las bonificaciones de su país representado, compara con el nivel de dificultad de la vulnerabilidad + las bonificaciones del país de la víctima.
- Si el atacante saca un número igual o mayor que el nivel de dificultad de la vulnerabilidad de la víctima, el atacante puede mirar la vulnerabilidad escaneada.

Las bonificaciones del país no se añaden cuando se explora.

-

Niveles de dificultad

1º - el jugador debe sacar al menos el número 4 (excluyendo las bonificaciones del país)

2º - el jugador debe sacar al menos el número 8 (excluyendo las bonificaciones del país)

3º - el jugado r debe sacar al menos el número 11 (excluyendo las bonificaciones del país).

ATAQUE

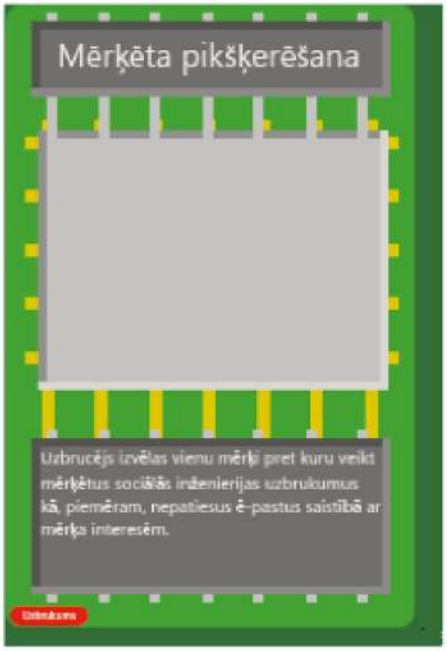
- El jugador nombra el objetivo del ataque (por ejemplo, "Ataco una vulnerabilidad rusa de nivel 2") y revela la carta de ataque a todos los jugadores, colocándola junto a la vulnerabilidad.
- El jugador tira los dados para ver si el ataque funciona comparando la tirada con la dificultad de la vulnerabilidad + los bonos (si el número tirado + los bonos coinciden o superan la dificultad, el ataque tiene éxito).
- Los ataques pueden ser forzados a retroceder utilizando la Carta de Reacción que está diseñada para ese ataque.
- Cada ataque tiene su propio tipo de reacción que se puede jugar y su propio tipo de vulnerabilidad para la que funciona.
- Si el ataque falla o es bloqueado por una Carta de Reacción - las cartas de Ataque y Reacción jugadas permanecen en la mesa hasta el final de la siguiente ronda e impiden el ataque de otros jugadores con el mismo ataque para la misma vulnerabilidad. Después del movimiento, ambas cartas vuelven al montón.

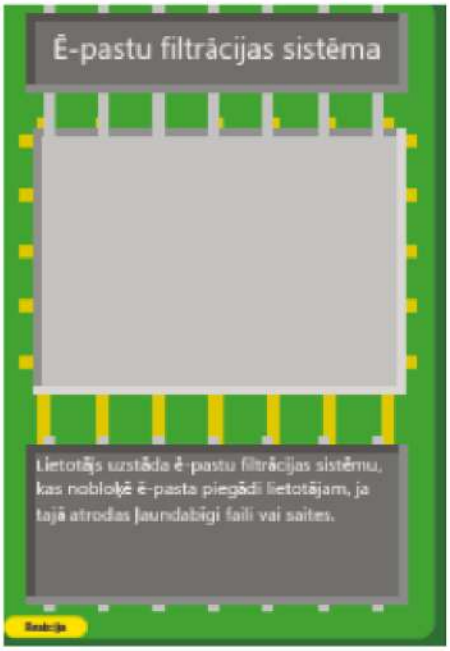
Niveles de dificultad

1º - el jugador debe sacar al menos el número 4 (excluyendo las bonificaciones del país)

2º - el jugador debe sacar al menos el número 8 (excluyendo las bonificaciones del país)

3º - el jugador debe sacar al menos el número 11 (excluyendo las bonificaciones del país).





LECSA (LV)

Defensa

- Defensa: elegir el método adecuado contra una vulnerabilidad concreta. Las Cartas de Reacción detienen (cancelan) el ataque entrante (y todos los demás ataques dirigidos a la misma vulnerabilidad) durante 1 turno.
- Para cancelar un ataque entrante, el jugador coloca una Carta de Reacción que coincida con el tipo de ataque (Ver tabla con las vulnerabilidades) sobre la carta de ataque tan pronto como se juegue el ataque.
- Para empezar a reparar una herida, el jugador coloca una Carta de Defensa al lado de la herida a reparar.
- Otros jugadores pueden atacar esta herida mientras está en Défense (antes de que termine el turno de Défense).
- Cuando el jugador intenta reparar una herida en su servidor con una Carta de Défense, ésta no puede atacar, pero puede intentar evitar los ataques con Cartas de Reacción. Para la reparación completa, se requiere un turno de |nivel de dificultad + 1|. La acción de exploración está permitida durante el periodo de reparación.
- Si el método de Defensa no es correcto, el jugador se salta 3 turnos y no puede usar Cartas de Defensa durante este periodo (las reacciones y las acciones de exploración están permitidas).

Bonificaciones de los países

Estados Unidos: +2 en exploración

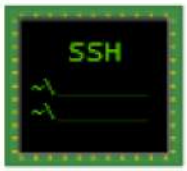
- Rusia: +2 en ataques
- China: +2 en defensa contra ataques
- Corea del Norte: +2 por defensa contra el escaneo
- India: +1 en todos los ataques, -1 contra ataques
- Israel: +3 en todos los ataques, -3 contra ataques

Vulnerabilidad por niveles

Vulnerability	Attacks	Défense	Reaction
1st vulnerability level			
SSH server with username	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel with User Name	Password guessing	Blocking external requests	Settings of Blocked Period
Untrained employee	Phishing campaigns	IT security trainings	Filtration system of e-mails; Implementation of e-mail SPAM list
Vulnerable SMB protocol	Exploitation of EternalBlue	Fixing vulnerability CVE-2017-0144	n/a
XSS vulnerability	Code injection; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist

SQL injection	Code injection; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Router panel with default username and password	Using default data	Complete replacement of authentication data	One session limit
2nd vulnerability level			
SSH server	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel	Username guessing	Blocking external requests	Settings of Blocked Period
XSS vulnerability with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
SQL injection with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Incompletely configured firewall	Packet fragmentation	Repair configuration	IDS implementation
WiFi network with WEP security	Packet Phishing	Using the WPA2 standard	RADIUS implementation
Busy CEO/boss	Phishing – catching the big fish	IT security trainings	Filtration system of e-mails; Implementation of e-mail SPAM list
3rd vulnerability level			
Service failure	DDoS	IP address blocking and load limiting	Load balancers
Vulnerable OpenSSL program	Heartbleed exploitation	Repair of CVE-2014-0160	n/a
Vulnerable Print Spooler program	PrintNightmare exploitation	Repair of CVE-2021-36958	n/a
Buffer overflow vulnerability	Buffer overflow	Introduction of buffer limits	Increasing the buffer
Weak hashing algorithm	Decryption of the hash value	Improving the hash algorithm	Usage of a strong and long password
Lazy IT expert	Targeted phishing	IT security trainings	Filtration system of e-mails; Implementation of e-mail SPAM list

LECSA (LV)



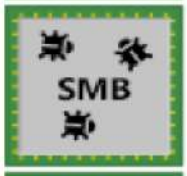
SSH serveris

SSH serveris ar lietotājvārdu

Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

Neapmācīts darbinieks

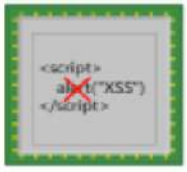


Ievainojams SMB protokols

XSS ievainojums

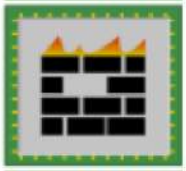
SQL injekcija

Rūtera panelis ar noklusējuma lietotājvārdu un paroli



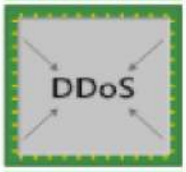
XSS ievainojums ar filtru

SQL injekcija ar filtru



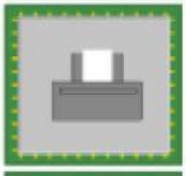
Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību

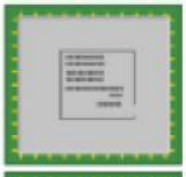


Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma



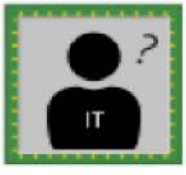
Ievainojama Print Spooler programma



Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

JORNADAS DE JUEGO

LECSA (LV)

CONSEJOS Y EXPERIENCIAS DE LA JORNADA DE JUEGOS EN LETONIA

- Durante los dos días del evento no es posible desarrollar un juego de ordenador real, sino el primer prototipo, que puede o no seguir desarrollándose dependiendo de la motivación de los participantes.
- Los premios u otros tipos de beneficios pueden ayudar a involucrar a más participantes y asegurar mejores resultados (más tangibles) al final (en nuestro caso - se proporcionó pizza y bebidas al final del evento, más apoyo de los mentores, (por ejemplo, la colocación de juegos en la plataforma)).
- Los mentores en materia de desarrollo de juegos y ciberseguridad desempeñan un papel importante en la Game Jam, ya que asesoran y ayudan a los participantes.
- Planificar con antelación: al tratarse de un evento bastante complejo, requiere una cuidadosa planificación.
- Los organizadores deben tener en cuenta que algunos equipos pueden quedar fuera de la competición (debido a la limitación de tiempo).

Consulta los posts de FB con los resultados del evento:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

¡El evento fue organizado por LECSA en cooperación con la Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ACTIVIDADES

- Reunión informativa de evaluación de necesidades con los estudiantes (formación en codificación en un centro local de educación de adultos)
- Jornada de juegos de 2 días (sesión informativa en línea el primer día; segundo día dedicado a la jornada de juegos)

Evento multiplicador - Mañana de concienciación sobre ciberseguridad

DESCRIPCIÓN & RESULTADOS

1) Reunión informativa de evaluación de necesidades con los estudiantes (formación en codificación en un centro local de educación de adultos) Fecha: Octubre 2021

DESCRIPCIÓN

Para difundir el proyecto e identificar los temas principales de la jornada de juegos, el equipo de Meath Partnership organizó una sesión informativa con los alumnos de una clase local de formación en codificación. El intercambio de información sobre ciberseguridad y el debate sobre las amenazas más recientes fueron seguidos por una sesión de lluvia de ideas en la que los estudiantes se dividieron en dos grupos para debatir cuestiones que permitieran identificar los temas más interesantes que se explorarían durante el Gamejam. También se compartió con los participantes más información sobre la jornada de juegos y el proyecto CYBER.EU.VET.

EJEMPLO DE EVALUACIÓN DE NECESIDADES


YBER.VET.EU

Co-funded by the Erasmus+ Programme of the European Union

Needs assessment meeting guidelines

1. What do you know about cybersecurity?
2. Why do I need to be worried about it?
3. What are the biggest cybersecurity concerns/threats right now?
4. Do you know how to recognise those threats?
5. What is a cyber attack?
6. Can you give us an example of a cyber attack?
7. Can you give us, at least, 3 possible solutions to it?

MEATH PARTNERSHIP (IE)

RESULTADOS

Como resultado de esta actividad, el equipo de Meath Partnership obtuvo una mejor comprensión de los conocimientos generales de los estudiantes en relación con la ciberseguridad y las ciberamenazas, además de recoger información que se incluyó posteriormente en el proceso de planificación y ejecución de la jornada de juegos.

LA EVALUACIÓN EN ACCIÓN

MEATH PARTNERSHIP (IE)

JORNADAS DE JUEGOS

2) Jornada de juegos de 2 días
(sesión informativa en línea el primer día; segundo día dedicado a la jornada de juegos)

DESCRIPCIÓN

El día 1 se dedicó a dar la bienvenida a los participantes y a presentar el proyecto CYBER.EU.VET y a inaugurar la Game Jam, así como a compartir información sobre los 2 temas identificados durante la reunión de evaluación de necesidades. Se ofreció a los participantes la posibilidad de trabajar individualmente o en equipo. También tuvieron la oportunidad de hacer cualquier pregunta o recibir más aclaraciones sobre los procedimientos
relacionados con el desarrollo de los juegos en el día 2.

El día 2 se dedicó al desarrollo de los juegos y los miembros de nuestro equipo y un experto en apoyo informático estuvieron disponibles a través de Zoom para apoyar a los participantes durante toda la duración de la Game Jam desde las 9 de la mañana hasta las 9 de la noche.
9 de la mañana hasta las 9 de la noche.
Se invitó a los participantes a subir sus juegos a la plataforma Itchio bajo un perfil creado para este evento: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

RESULTADOS

Después de que los participantes compartieran sus borradores de juegos con el equipo, uno de ellos decidió seguir adelante y subir el juego para su posterior evaluación. El resto de los participantes decidieron no presentar sus borradores, ya que estaban en una fase muy temprana.

Click or not click

Online interactive cybersecurity game

A short narrative driven game on raising awareness for cyber security threats. The game prompts players to make the right decision and avoid losing your security level.

Link: https://itch.io/jam/cybereuvet-cybersecurity-gamejam

Juego de ciberseguridad interactivo en línea:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

3) Evento multiplicador - Mañana de concienciación sobre ciberseguridad
Fecha: Noviembre 2021

DESCRIPCIÓN

El Evento Multiplicador se celebró en línea a través de Zoom con el fin de dar a conocer el proyecto y sus actividades. El evento fue ampliamente difundido entre una amplia variedad de partes interesadas o involucradas en la Ciberseguridad. El evento comenzó con una presentación y una visión general del proyecto y de la Game Jam, seguido de una presentación y un debate sobre la Ciberseguridad y el intercambio de información práctica sobre cómo mantenerse en línea (las amenazas cibernéticas actuales y cómo eliminar posibles ataques fueron posibles).

RESULTADOS

El Evento Multiplicador contribuyó a dar a conocer el proyecto y también creó la oportunidad de presentar los hitos logrados desde el inicio del proyecto a un público más amplio. También fue una gran oportunidad para compartir información práctica y consejos relacionados con la ciberseguridad con los participantes que asistieron al evento.

COFAC / UNIVERSIDADE LUSÓFONA (PT)

JORNADA DE JUEGOS

ACTIVIDADES

1) Postgrado en Ciber-Hacking Ético para futuros profesionales y profesores del mercado Oct 2021 - Feb 2022 (en colaboración con una consultora local llamada Cybersec)

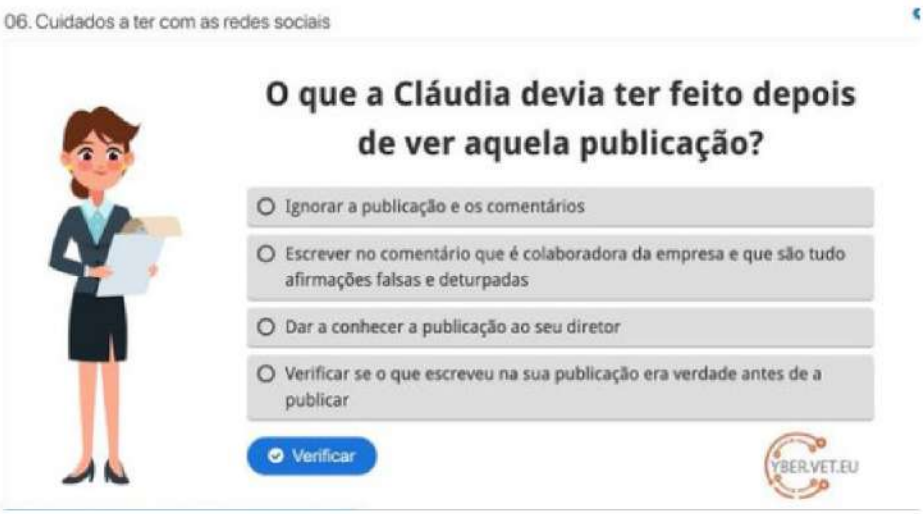
2) 2 sesiones de GameJam impartidas en enero de 2022 en centros de FP:
Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt
Escola Profissional Almirante Reis - https://www.epar.pt

3**)** Una ciberformación de tres días y medio para estudiantes de secundaria en marzo de 2022 en Universidad Lusofona como parte del evento Tecweb - https://tecweb.ulusofona.pt

RESULTADOS

Informe de difusión de pruebas donde se pueden ver las diferentes pruebas que se han realizado durante un año natural (abril 2021 a abril 2022). En este informe podemos ver capturas de pantalla de publicaciones en redes sociales, carteles de diferentes eventos, cuestionarios de concienciación sobre ciberseguridad (disponibles en idioma portugués en https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

Durante los Cyberjams, también se creó, a partir de las encuestas de concienciación sobre ciberseguridad, un conjunto de minijuegos amigables/interactivos sobre situaciones sencillas realizadas.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

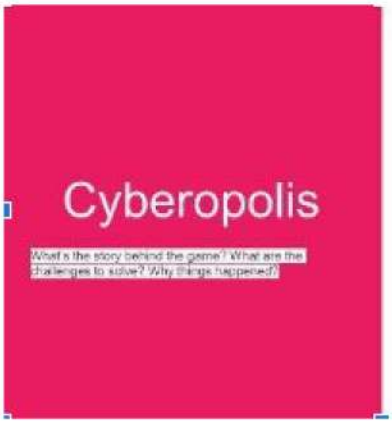
JORNADA DE JUEGOS

Herramienta de diseño de juegos (IASIS) - Ciberopolis

Este juego es un juego de mesa dirigido a personas interesadas en la ciberseguridad, con un máximo de 2 a 4 jugadores, y sus aspectos principales son la confidencialidad y la integridad de los datos... mientras que los temas que trata son el malware, el phishing, los ataques basados en la web, los ataques a aplicaciones web, el spam, el robo de identidad, el DDoS y el Man in the middle...

Consulta la imagen de ''Ciberopolis'' para entender mejor los pasos a seguir durante el juego y qué retos hay que resolver...

Capturas de pantalla del juego durante la sesión de GameJam donde podemos ver el éxito del juego y el gran interés mostrado por los participantes.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

VIDEO - Prevenir el ciberacoso

Este vídeo elaborado por el socio griego acerca a los visitantes a diferentes formas de prevenir y combatir el ciberacoso.

YBER.EU.VET

Funded by
the European Union

AVISO LEGAL

Diseño
NGO Nest Berlin e.V.
Berlin, 2022

Co-funded by the
Erasmus+ Programme
of the European Union