Sergio Pérez Peló *(sergio.perez.pelo@urjc.es)*
Raúl Martín Santamaría *(raul.martin@urjc.es)*

Práctica 1 – Explotación en Linux y Windows

En esta primera práctica, se van a trabajar conceptos estudiados en el primer y segundo bloque de la asignatura. La idea principal de la práctica es ponerse en la piel de un atacante que está intentando explotar una vulnerabilidad conocida bien de Windows o bien de Linux.

Para realizar la práctica, será necesario emplear un software de virtualización, como puede ser VirtualBox. Podéis utilizar otras aplicaciones de virtualización, pero nosotros daremos asistencia y demostraremos el uso de VirtualBox dado que está disponible de forma gratuita y es de código abierto. Podéis obtener VirtualBox en el siguiente enlace: https://www.virtualbox.org/wiki/Downloads

Desarrollo de la práctica

La práctica se realizará en **grupos de tres personas**, permitiéndose en casos excepcionales que la práctica se realice de forma individual o por parejas, previa aprobación por parte de los profesores. La práctica constará de las siguientes fases:

1. Elección de vulnerabilidad o CVE: los miembros del grupo elegirán una vulnerabilidad o CVE existente, **menor a 3 años de antigüedad** (2021 en adelante).
2. Montar un entorno en el que esté presente la vulnerabilidad o CVE elegidos, utilizando bien un sistema de contenedores como Docker o bien una máquina virtual (recomendado).
3. Entender la explotación de la vulnerabilidad, comprendiendo, al menos, el siguiente contenido:

    a. Detección de la vulnerabilidad: si fueras un atacante, y el entorno montado en el punto 2 fuera el objetivo, ¿cómo detectarías si el sistema es vulnerable o está afectado por el CVE elegido?
    b. Explotación de la vulnerabilidad: una vez confirmada la posible existencia de la vulnerabilidad, ¿qué pasos son necesarios para explotarla?
    c. Validación de la explotación, ¿qué acciones te permite realizar la vulnerabilidad? ¿cuáles son sus consecuencias?

4. Presentación de los resultados obtenidos: presentación breve, de máximo 10 minutos, para un público técnico, en el que se resuma el trabajo realizado y

se demuestre la vulnerabilidad. **Es necesario explicar el funcionamiento de la vulnerabilidad o CVE elegidos.**

Importante: No es necesario desarrollar un exploit propio, se puede utilizar material o módulos existentes, pero **siempre referenciando la fuente de estos**. En general, siempre debéis referenciar todo el material utilizado.

Sistema de evaluación

La evaluación de la práctica se realizará de forma presencial en los días indicados en el calendario de la asignatura en el aula virtual. Cada grupo, deberá realizar una presentación de **máximo 10 minutos**, en la que los miembros del grupo deberán explicar el proceso completo: desde la elección del CVE, hasta la demostración del exploit en el entorno preparado.

Tras la presentación, habrá un turno de preguntas en las que los integrantes del grupo deberán defender el trabajo realizado. La nota de la práctica se calculará, principalmente, en función de tres aspectos:

1. Complejidad técnica del entorno desarrollado y la vulnerabilidad explotada.
2. Claridad y calidad de la presentación.
3. Demostración de conocimientos adquiridos a lo largo de la práctica (¿Por qué funcionan las cosas que has demostrado? ¿Qué sistemas existen por debajo que permiten que ocurra lo que ha sucedido?, etc.)

De forma adicional, es obligatorio entregar en el aula virtual un fichero ZIP con todos los materiales desarrollados a lo largo de la práctica (**NO incluyendo la máquina virtual**), y la presentación, vídeos o cualquier recurso auxiliar utilizado. **La no entrega de este material implicará la calificación de NO PRESENTADO en la práctica**. La entrega de este material **debe realizarse antes del 28/10/2024 a las 10:59** (justo antes del inicio de la clase).

Rúbrica de evaluación

La rúbrica que se seguirá para evaluar el contenido de las presentaciones es la siguiente:

Presentación de los miembros del grupo: 0,25 puntos

Contextualización: 0.75 puntos

Cómo se detecta la vulnerabilidad: 1 puntos

Pasos para su explotación: 1 punto

Explicación del exploit: 1 punto

Crear el entorno (propio, no copiado): 1 puntos

Demostración de la explotación en vídeo o en directo: 1 punto

Explicación del impacto de la vulnerabilidad: 1 puntos

PPT/PDF claro y entendible: 1 punto

Discurso claro y fluido: 1 punto

Responde correctamente a las preguntas: 1 punto

Penalizaciones

Si no hay bibliografía razonable: -2 puntos.

Si el CVE no afecta directamente al sistema operativo o a un software que venga instalado por defecto con el sistema operativo, **se aplicará una penalización de -5 puntos.**

Penalización por tiempo

Tiempo máx (min:seg)	**Penalización**
<10:30	0
10:30 – 12:00	-0.5
12:00 – 13:00	-1
13:00 – 14:00	-1.5
14:00 – 15:00	-2
>15:00:00	-5

Autores: Sergio Pérez Peló (sergio.perez.pelo@urjc.es), Raúl Martín Santamaría (raul.martin@urjc.es)

Práctica 2: CTF

El objetivo de esta segunda práctica es poner en práctica los conocimientos adquiridos en los temas previos de mediante la resolución de diferentes tipos de retos estilo CTF Jeopardy. Para ello, se utilizará la siguiente página: `https://th-gcib.numa.host/`
Ante cualquier duda durante la resolución de la práctica, escribir un email a sergio.perez.pelo@urjc.es y raul.martin@urjc.es. En caso de no poderse resolver la duda vía mail, se puede concertar una tutoría, siempre y cuando se concierte en un período de **hasta 48 horas antes** de la fecha de entrega de la práctica.

Normas y evaluación

- La realización de la práctica se realizará de forma **individual**.
- En la memoria deberán describirse los pasos que se han realizado para resolver el reto. Sugerimos incluir capturas de pantalla en todas aquellas partes que ayuden a la comprensión o aporten información interesante.
- Para cada ejercicio, la puntuación se otorgará de la siguiente forma: En caso de explicar de forma correcta cómo explotar el reto, se otorgará 50 % de la nota. Si, además, se consigue explotarla y obtener la flag se otorgará el 50 % restante de la nota.
- La fecha límite para entregar la práctica será el **10 de enero a las 23:55**.
- Esta práctica se corresponde con un 30 % de la nota final.

Sobre la memoria

Es obligatorio entregar una memoria donde se expliquen los siguientes puntos para cada uno de los retos a los que os habéis enfrentado:

- Descripción corta del reto y vulnerabilidad detectada.
- ¿Cómo has detectado la vulnerabilidad? De forma manual, utilizando herramientas...
- Explicación de la explotación de la vulnerabilidad.
- Flag del reto.

Entregables

Memoria de la práctica y todos los archivos auxiliares que el estudiante considere interesantes, como por ejemplo, el código implementado para resolver el reto.

¿Cuántos ejercicios tengo que resolver?

Será requisito realizar **al menos 3 ejercicios** para optar a la **nota mínima (5)** en la prueba.
Para cada reto, la mitad de la nota será asignada por resolver el reto y obtener la flag, y la otra mitad por la calidad de la explicación en la memoria. Por ejemplo, en caso de superar el mínimo de problemas resueltos y explicarlos de forma correcta en la memoria, obtendrás un 5 sobre 10. Del 5 al 10 la puntuación se basará en el rendimiento del resto de los compañeros, dependiendo de la puntuación final conseguida en la plataforma de retos, eliminando los *outliers*.

> Nota: Recuerda que cno es necesario obtener la flag para conseguir parte de los puntos en un determinado ejercicio.

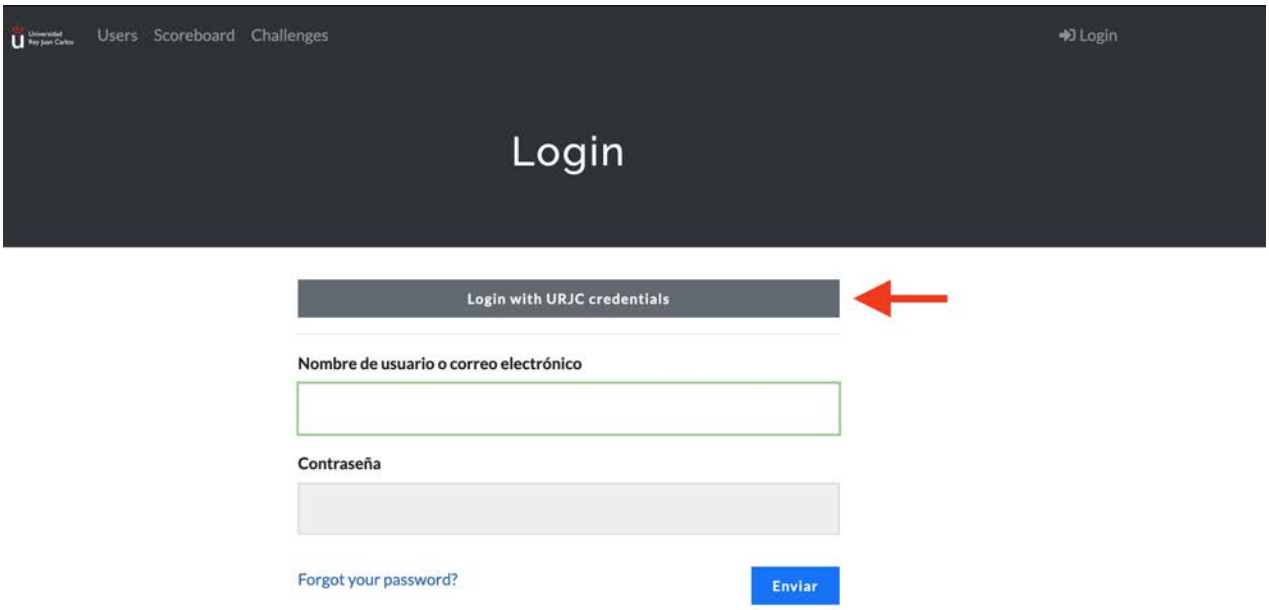
¿Qué es una flag?

Una flag es un fragmento de texto que se encuentra, entre otros sitios, en el código fuente de la aplicación, en la base de datos, en el sistema de ficheros del servidor, como variable de entorno... Es una forma de demostrar que el reto ha sido completado con éxito. Por ejemplo, el caso más común en una inyección SQL es que la flag se encuentre dentro de la base de datos, y pueda ser extraída utilizando la vulnerabilidad detectada. Ten en cuenta que no es suficiente con entregar la flag en la plataforma, revisa con atención el apartado de evaluación.

> Nota: Las flags pueden rotar cada cierto tiempo, así que es recomendable enviarlas siempre al encontrarlas y nunca dejarlo para más tarde.

1. Iniciar sesion

Para iniciar sesión en la plataforma, utilizad el siguiente botón (el botón de login superior derecho es solo para tareas de administración):



Al hacer click, os redirigirá al proveedor de identidad de la URJC, donde, si no teníais sesión iniciada, os solicitará que os autentiquéis.

> Nota: Cuidado con el phishing. En general, comprueba siempre el dominio antes de introducir las credenciales.

Una vez verificada vuestra identidad, os redirigirá de vuelta a la plataforma, donde podréis ver los diferentes retos y la clasificación en tiempo real.

2. Retos

En la pestaña superior “Challenges”, se encuentran disponibles los diferentes retos agrupados por categorías, dependiendo del tipo de reto. Haciendo click en cualquiera de los retos, se abrirá una popup con la información del reto, entre otros:

- Título del reto
- Descripción del reto: entre otros, descripción del funcionamiento del reto, enlace para interactuar con el reto, etc.
- Archivos para descargar: Los mismos archivos que está utilizando el servidor para ejecutar un servicio dado, a excepción de la flag que es diferente.
- Campo de texto para introducir la flag del reto.

> Nota: Aseguraos de tener el mínimo de retos resueltos establecido para completar la práctica con éxito y de tenerlos correctamente documentados en la memoria.

3. Sistema de puntuación

Debido a la imposibilidad de calcular la dificultad de cada reto, la puntuación de cada reto es dinámica: empieza en 500 puntos y se va reduciendo según aumenta el número de resoluciones del ejercicio. La puntuación de cada usuario en la plataforma se calcula como la suma de la puntuación de cada uno de los retos resueltos. Podéis ver la clasificación en tiempo real en el menú superior.

> Nota: Una de las consecuencias de este sistema de puntuación es que si, por ejemplo, resuelves un reto difícil, ayudar a otras personas a resolverlo hará que disminuya bastante tu puntuación.

4. Puntos extra

Se pueden obtener puntos adicionales sobre la nota final por reportar cualquier problema sobre:

- Cualquier error o unintended solution en cualquiera de los retos propuestos.
- Fallos en el sistema de autenticación delegada (`https://*.urjc.es` y `https://*.rediris.es` están fuera del scope, solo se podría revisar la parte que pertenezca a `https://th-gcib.numa.host` y `https://idp.numa.host`).

> Nota: antes que buscar una vulnerabilidad en el sistema de autenticación delegada, dedicad el tiempo a resolver un número mayor de retos. En caso de duda sobre un servicio que se quiera tratar de explotar, por favor, preguntadnos.