UNIVERSIDAD TECNOLÓGICA NACIONAL - FACULTAD REGIONAL BUENOS AIRES
Ingeniería en Sistemas de Información
Seguridad Informática (082031)

Trabajo Práctico 1° Cuatrimestre 2022
Cátedra Seguridad Informática

Investigación de vulnerabilidades y contramedidas

Docente:

Ing. Matias Mevied

Ayudantes:

Ing. Gabriela Nicolao

Fernando Tavella

Índice

UNIVERSIDAD TECNOLÓGICA NACIONAL - FACULTAD REGIONAL BUENOS AIRES
Ingeniería en Sistemas de Información
Seguridad Informática (082031)

Introducción

El trabajo práctico consiste en la investigación sobre una vulnerabilidad, el desarrollo de un exploit y el armado de una contramedida. La vulnerabilidad seleccionada debe tener un CVE (Common Vulnerabilities and Exposures) asignado en el segundo semestre del 2022 y la vulnerabilidad debe pertenecer al reporte del top 10 de OWASP 2017 (Open Web Application Security Project). La aplicación donde se realice la investigación queda a elección del grupo y está sujeta a la aprobación de los docentes. La aprobación del trabajo práctico se compone de la aprobación parcial de cada entrega, la entrega final y la exposición del trabajo realizado.

Cada grupo tiene un margen de 1 día por cada entrega que puede ser administrado como cada grupo quiera, un total de 5 días de margen durante todo el trabajo. Si el grupo tiene más de esos días de demora en la entrega del trabajo se considera reprobado.

Todas las entregas parciales y la entrega final deben ser enviadas por mail a si_utn@googlegroups.com para su corrección.

Comunicación de las entregas

Las entregas parciales y la final deben ser subidas al aula virtual de Ciberseguridad. En cada entrega se debe adjuntar el avance del trabajo sumado a las entregas parciales anteriores en un mismo documento. El contenido del documento está indicado a continuación en cada entrega.

1° Entrega – Selección de la aplicación

Fecha límite de entrega vía mail: 23 de Abril 2022
Descripción: Se debe seleccionar una o más aplicaciones para poder realizar la investigación sobre una vulnerabilidad existente y de conocimiento público. En esta etapa se debe tener en cuenta que la aplicación seleccionada tenga diversas vulnerabilidades y que las vulnerabilidades tengan asignados CVE (Common Vulnerabilities and Exposures).
Se necesita en esta entrega informar a los docentes las aplicaciones seleccionadas y cuales vulnerabilidades seleccionaron como candidatas. Elegir e informar por lo menos 3 vulnerabilidades por aplicación.

2° Entrega – Selección de la vulnerabilidad

Fecha límite de entrega vía mail: 30 de Abril 2022

Descripción: Se debe redactar un documento que contenga como mínimo los siguientes apartados:

- Introducción: Indicar cuál es la vulnerabilidad elegida y su contramedida
- Infraestructura: Deben indicar la infraestructura que usa la aplicación y el detalle necesario para entender su funcionamiento. Es necesario que indiquen la infraestructura que tienen pensado utilizar para el trabajo práctico.
- Escenario de ataque: Graficar como un atacante podría explotar la vulnerabilidad seleccionada.

3° Entrega – Preparación del entorno de trabajo

Fecha límite de entrega vía mail: 21 de Mayo 2022
Descripción: En esta entrega se debe tener listo el entorno de trabajo donde se va a explotar la vulnerabilidad y aplicar su contramedida. Para demostrar el cumplimiento de esta entrega se solicitarán capturas de pantalla del entorno conformado y la explicación de cada una de las capturas.

4° Entrega – Investigación de la vulnerabilidad y su contramedida

Fecha límite de entrega vía mail: 4 de Junio 2022
Descripción: Se debe realizar una investigación exhaustiva de la vulnerabilidad elegida y hacer un informe técnico detallado de dicha vulnerabilidad. Por otra parte analizar alternativas de contramedidas para proteger o mitigar la explotación de la vulnerabilidad seleccionada.

5° Entrega – Desarrollo del Exploit y sus contramedidas

Fecha límite de entrega vía mail: 11 de Junio 2022
Descripción: Se debe desarrollar en el lenguaje que se desee el Exploit de la vulnerabilidad seleccionada y también se pueden utilizar herramientas ya existentes para la explotación. Además se deben desarrollar contramedidas para intentar evitar o mitigar la explotación de la vulnerabilidad.

Entrega Final

Fecha de entrega impresa: 18 de Junio 2022
Descripción: La entrega final debe contener:

- Todas las entregas parciales
- Reporte ejecutivo
- Conclusión

- Bibliografía

Exposición del trabajo práctico

En conjunto con la entrega final se debe entregar la presentación que van a realizar el día de la exposición. En caso que el grupo decida no armar una presentación de manera digital, los docentes deben estar informados y aprobar el cambio.