UNIVERSIDAD COMPLUTENSE MADRID

ntic master

TAREA EVALUABLE

Máster en Ciberseguridad

MÓDULO
Red Team y Purple Team

PROFESOR
D. Carlos Antonini Cepeda

Indice

1. Tarea Evaluable

1.1. Introducción

El Alumno deberá de descargar la ova con la máquina virtual y ejecutarla en VirtualBox, no se recomienda la reconversión de VirtualBox a VMware o similares, se recomienda el uso de VirtualBox para esta tarea evaluable, se establecerá el adaptador como bridge en las conexiones de red, el cual asignará una IP local dentro de la red en la que esté el Alumno.

1.2. Ejercicio 1.

Valor: 0,5 puntos

¿Cuál es el carácter que debes utilizar para producir el fallo de seguridad?

A. :
B. ;
C. ‘
D. “

1.3. Ejercicio 2.

Valor: 1 punto

¿Qué comando en PHP usarías para obtener una reverse shell en este ejercicio? (esta pregunta es abierta, sé rogaría que la contestación sea solo en 1 línea siendo clara y concisa con el comando introducido)

1.4. Ejercicio 3

Valor: 1 punto

Te reporta el Blue Team de que en tu empresa han conseguido comprometer esta funcionalidad en la página web y te preguntan como lo han podido hacer, te dicen que es posible que haya sido a través de un Server-Side Includes (SSI) Injection, ¿Puedes resolver como el atacante ha conseguido ejecutar comandos en el servidor? (esta pregunta es abierta, sé rogaría que la contestación sea solo en 1 línea siendo clara y concisa con el comando introducido)

1.5. Ejercicio 4

Valor: 1 punto

El equipo de respuesta ante incidentes de tu empresa (SOC-CSIRT) ha descubierto que han conseguido ejecutar un SQL Injection en esta funcionalidad de la web, podrías indicar

cuántos usuarios han conseguido extraer de la base de datos bWAPP.
(Deberás usar las opciones --dbs -D bWAPP --tables -T users --dump)

A. 1
B. 2
C. 3
D. 4

1.6. Ejercicio 5

Valor: 1 punto

La usuaria Alice ha reportado al Blue Team que le han cambiado la pass de acceso al FTP, esto no lo ha realizado ella, ¿Podrías averiguar la contraseña y mirar si ves algún fichero sospechoso y decirnos su contenido? (usar el diccionario /usr/share/wordlists/fasttrack.txt de Kali Linux este proceso puede tardar unos minutos.)

A. zkdZea
B. augYa1
C. Bcsde#
D. sdEfga

1.7. Ejercicio 6

Valor: 0,5 puntos

Hay un secreto en las cabeceras HTTP, ¿Puedes descifrarlo?

A. aQW55IGJ1Z3M%2F;
B. Any bugs?
C. QW55IGJ1Z3M/;
D. Any bugs6

1.8. Ejercicio 7

Valor: 1 punto

El equipo de desarrollo de tu empresa ha parcheado una serie de vulnerabilidades de Directory Traversal Attack te preguntan si puedes intentar vulnerar esta funcionalidad para que ellos confirmen que lo han realizado correctamente.

1.9. Ejercicio 8

Valor: 1 punto

Tenemos esta vulnerabilidad de Host Header Injection usando el email de pruebas bwapp-bee@mailinator.com tenemos que verificar si se ha corregido o no esta vulnerabilidad. (el código se recibirá usando nc para recibir el mensaje), por favor señala la respuesta correcta

A. 43e3431d0490d48ba493646f97ce6f2153951787
B. 38f389a8fe5cd20bfeb3509b7df06e7a384b0e40
C. 12066924ac88ee0b15712c1fade94bd33866ebfa
D. 742836d8b14a34b077922a180cd0e1b5c17d6188

1.10. Ejercicio 9

Valor: 1 puntos

Estás atacando esta web dentro de un equipo de Red Team, tienes la sensación de que esto puede ser un vector de entrada, ¿Qué harías para conseguir una reverse shell? (esta pregunta es abierta, sé rogaría que la contestación sea solo en 1 línea siendo clara y concisa con el comando introducido).

1.11. Ejercicio 10

Valor: 2 puntos

El Kernel de Linux de esta máquina es vulnerable a escala local de privilegios, usando la reverse shell del ejercicio 9. Get r00t! (adjuntar captura de pantalla con nombre ejercicio_10.png)

NOTA: en este ejercicio el servidor se puede quedar congelado, reiniciar la máquina en caso de que esto ocurra.

1.12. Cómo entregar la tarea

El alumno debe subir su trabajo en un archivo ZIP con el siguiente patrón en el nombre del archivo:

TAREA_DNI_NOMBRE_APELLIDO1_APELLIDO2.zip

Cualquier duda o incidencia con la entrega se puede consultar directamente con el profesor a través del foro y chat del Campus de la Universidad.