ESCENARIOS PROPUESTOS POR EL EQUIPO DE VENCERT-SUSCERTE PARA EL CIBERSIMULACRO VENEZUELA, 2024

En el contexto actual de la ciberseguridad, es esencial que las instituciones evalúen no sólo su capacidad para defenderse de posibles ciberataques, sino también su habilidad para identificar y mitigar amenazas como atacante. En este sentido, se ha diseñado un cibersimulacro desde el VenCert-Suscerte, en el que se plantean dos escenarios distintos. En el primer escenario, la institución asume el rol de atacante, poniendo a prueba su capacidad para identificar vulnerabilidades y ejecutar un ataque controlado. En el segundo escenario, se presentarán registros de *logs* para su análisis y la posterior toma de decisiones.

Se busca evaluar la capacidad ofensiva, así como la capacidad defensiva de las instituciones en materia de ciberseguridad, con el fin de fortalecer las medidas preventivas y su habilidad de respuesta ante posibles amenazas cibernéticas; es importante destacar que esta simulación no tiene como objetivo fomentar actividades maliciosas, sino promover el aprendizaje y la capacitación en el campo de la seguridad informática, ya que la identificación y corrección proactiva de vulnerabilidades es fundamental para proteger los sistemas contra posibles ataques cibernéticos y promover una cultura proactiva en ciberseguridad.

Este documento, detalla cada uno de los escenarios planteados, y dada la popularidad de WordPress como plataforma de gestión de contenido, enfocada a la creación de cualquier tipo de página web a nivel mundial, se considera crucial abordar los riesgos asociados con *plugins* o temas vulnerables que podrían comprometer la seguridad del sistema.

PREÁMBULO

Al dar inicio al cibersimulacro sólo se le facilitará la dirección IP del objetivo, sin darle ms información el participante, con sus habilidades deberá determinar qué servicio o servicios se encuentran en ejecución dentro del *host*, para ello deberá escanear los puertos que se encuentran activos en el equipo, para poder identificar que es un servicio web y poder determinar los servicios que se ejecutan en el sistema.

PRIMER ESCENARIO – EXPLOTACIÓN Y POST EXPLOTACIÓN

CONTEXTO

A los propietarios de la pequeña empresa de comida rápida de nombre "Pizza Pepperoni" les urge realizar un *pentesting* en su nuevo portal web, ya que han sido alertados sobre diversos focos de ataques cibernéticos hacia el *hosting* donde se aloja, que es un *hosting* accesible y de dudosa reputación cuyo dominio es: "hostbarato.com" y no se sabe con certeza si estos ataques han tenido éxito en otros portales alojados en el mismo *hosting*, de manera que en este caso la decisión mas oportuna para los propietarios es tomar medidas preventivas que permitan conocer el estado actual de su sistema en materia de riesgos y vulnerabilidades.

Asumirá el papel de un *hacker* ético y realizará el *pentesting,* se considera que conoce sobre la metodología *hacker,* en la cual deberá utilizar herramientas especificas para realizar reconocimiento activo, explotación y post-explotación sobre el portal web de "Pizza Pepperoni", así mismo deberá responder una serie de preguntas que han sido formuladas con antelación y que determinarán el nivel de seguridad del sistema.

DESARROLLO

<table>
<tr><th colspan="3">Explotación</th></tr>
<tr><th></th><th>Descripción</th><th>Herramientas</th></tr>
<tr><td rowspan="2">WordPress 4.2.36</td><td>Fuerza Bruta</td><td rowspan="2">• nmap
• whatweb
• dirb
• wpscan</td></tr>
<tr><td>El CMS cuenta con el panel wp-admin habilitado y cuenta con dos usuarios activos, uno tiene permisos limitados y el otro usuario es el administrador del sitio web.
Para identificar los usuarios activos deberá realizar fuerza bruta a los nombres de usuarios y cuando tenga identificado los usuarios deberá realizar nuevamente fuerza bruta pero esta vez al password de los usuarios, la contraseña del usuario con privilegios limitados se encuentra en el archivo rockyou.txt (/usr/share/wordlists)</td></tr>
</table>

WordPress 4.2.36	**Ejecución de Comando Remoto**	
	El CMS cuenta con un *plugins* llamado **Social Warfare** en la versión **3.5.2,** la cual es vulnerable a ejecución de comando remoto al utilizar *wpscan*, y al realizar el escaneo muestra las distintas vulnerabilidades que disponga el CMS entre los temas y los *plugins* dependiendo de la versión que disponga. Así mismo, refleja una referencia de cada vulnerabilidad que encontró, para este caso se puede utilizar la referencia que nos muestra *wpscan* y realizar dicha ejecución de comando remoto. **https://wpscan.com/vulnerability/7b412469-cc03-4899-b397-38580ced5618**	
Webmin 1.890	**Ejecución de Comando Remoto mediante Archivo de Webmin**	• Searchsploit • Metasploit
	El *host* cuenta con un servicio en el puerto 10000 el cual es *webmin*, de acuerdo a la versión *searchsploit* determino que cuenta con un *exploit* el cual nos permite realizar la explotación y nos da una sesión con privilegios *root*, para ello se utilizó *metasploit. Exploit* utilizado: **exploit/linux/http/webmin_backdoor**	

<table>
<tr><th colspan="3">Post-Explotación</th></tr>
<tr><th></th><th>Descripción</th><th>Herramientas</th></tr>
<tr><td rowspan="4">Debian 11</td><td>Persistencia</td><td rowspan="2">• Shell.perl
• wel-shell.php</td></tr>
<tr><td>Al realizar la explotación de ejecución de comando remoto presente en el plugin del CMS, Social Warfare, se lográ el acceso y posibilidad de subir archivos maliciosos tales como puertas traseras (Shell) al servidor web.</td></tr>
<tr><td>Escalada de privilegios</td><td rowspan="2">• Script en Python</td></tr>
<tr><td>Si se decide realizar la explotación de plugins de WordPress, para realizar la escala de privilegio, es necesarios que se verifiquen que archivos tengan los permisos SUID activos. Dentro de ellos hay un archivo llamado script2.py, y el código que dispone el script es el siguiente:

import os
os.system("chmod u+s /bin/bash")

Dicho código, indica que se le cambiaran los permisos la consola de bash al ser ejecutado.

Si el usuario decide realizar la explotación del webmin tendría acceso de root de forma directa.</td></tr>
</table>

CUESTIONARIO #1

1.- ¿Cual es la IP y la MAC del equipo vulnerable?
R.- 172.31.70.120-0e:66:a5:df:5c:00

2.- ¿Qué herramienta se utiliza para escanear los puertos, lo servicios y sus versiones?

R.- nmap

3.- ¿Cuales número de puertos se muestran con el estado "open" (abierto) en el equipo vulnerable?

R.- 10000, 22, 443, 80

4.- Señale el nombre de los servicios y las versiones del equipo vulnerable.

R.- Apache 2.4.57 -- OpenSSH 8.4p1 -- MiniServ 1.890

5.- ¿Qué manejador de contenido (CMS) usa el aplicativo web del equipo vulnerable?

R.- wordpress

6.- ¿Qué herramienta se puede utilizar para recolectar información "Banner Graving" del sistema web?

> DNSENUM
> HYDRA
> SQLMAP
> **WHATWEB**

7.- ¿Qué herramienta especifica se utiliza para escanear las vulnerabilidades del CMS?

> Joomscan
> CMSexplorer
> **Wpscan**
> Scandroid

8.- Escriba los nombres del plugin vulnerables del CMS

R.- social-warfare

9.- ¿Cuales son los usuarios registrados en el CMS?

R.- admin, pizza

10.- ¿Cual es la ruta del panel de administrador del CMS?

R.- wp-admin

11.- ¿Cual es la contraseña del usuario vulnerable a fuerza bruta del CMS?

R.- junior

12.- ¿ Qué tipo de vulnerabilidad afecta al CVE-2019-9978 ?

> Inyección SQL
> XSS
> **Ejecución de Código Remoto**
> Ruta Transversal

13.- ¿Cuál es el nombre de usuario (Linux) que obtiene al lograr explotar la vulnerabilidad CVE-2019-9978?

R.- www-data

14.- ¿Cual es el nombre "común" de los archivos que contienen las banderas?

R.- importante

15.- Escriba (separados mediante coma ejemplo: pedro,usuarios,pablo) el nombre de usuario y el nombre de grupo de los archivos que contienen las banderas

R.- chef:chef, www-data:www-data

16.- Escriba el nombre de la carpeta dentro de la cual se encuentra ubicada la llave de acceso al usuario "web"

R.- .ssh

17.- Siendo un usuario con privilegios limitados ¿Cuál es el número de SUID que te indica que puedes ejecutar los archivos con privilegio de superusuario?

R.- -4000

18.- En que formato se encuentran "codificadas" las banderas

>SHA1
>**BASE64**
>MD5
>C++
>CESAR
>SHA512
>AES
>RSA

19.- ¿Cuál es el nombre de la base de datos del CMS?

R.- worbd

20.- ¿Cuáles usuarios del CMS tienen una bandera?

R.- admin, pizza

21.- ¿Qué tipo de ataque explota la vulnerabilidad CVE-2019-15107?

> Denegación de Servicio (DoS)
> Hombre en el Medio (MiTM)
> **Ejecución de Código Remoto**
> Ruta Transversal

22.- Nombre el framework más utilizado por pentester para la ejecutar la fase de explotación

R.- metasploit

23.- ¿Cuál es el número de puerto del servicio afectado por la vulnerabilidad CVE-2019-15107?

R.- 10000

Banderas a encontrar	
Lugar de la bandera	**Respuesta**
Panel de WordPress - Usuario	v3nc3rt=pl5rd3rfs
Usuario www-data del sistema operativo	v3nc3rt=8i0y8a2d
Usuario Chef del sistema operativo	v3nc3rt=tg54rf63
Panel de WordPress - Usuario admin	v3nc3rt=cp0o9i8u7
Base de datos de WordPress	v3nc3rtn1=t6fidsdfs

DETALLES DEL PRIMER ESCENARIO

- El tiempo límite es de 2 Horas.
- El límite de intentos para cada respuesta es de 3.
- El puntaje de cada respuesta varia según los intentos que se utilicen de la siguiente manera:
  - 1er Intento = 20 Puntos.
  - 2do Intento = 15 Puntos.
  - 3er Intento = 10 Puntos.
- El puntaje de la respuesta 17 es de **25 Puntos** debido a su mayor dificultad.
- El patrón para la respuesta de las banderas comienza con lo siguiente: **v3nc3rt=**
- El puntaje de la captura de las banderas varia según los intentos que se utilicen de la siguiente manera:
  - 1er Intento = 50 Puntos.
  - 2do Intento = 15 Puntos.
  - 3er Intento = 10 Puntos.
- El puntaje máximo del primer escenario es de **715 Puntos.**

SEGUNDO ESCENARIO – ANÁLISIS DE *LOGS*

CONTEXTO

Pizza Pepperoni para ahorrar costos ha contratado un pasante con conocimientos de hacking ético de cierta universidad dedicada a la tecnología para realizar el pentesting de su portal web que ademas está alojado en un *hosting* de dudosa reputación sin embargo a pesar de las medidas preventivas que han tomado, han sido victimas de un ataque cibernético y en un primer análisis de las bitácoras se ha descubierto que los ciberdelincuentes han ejecutado un escaneo de puertos y de vulnerabilidades, para posteriormente realizar la explotación de las mismas, se conoce que el sistema está desarrollado en base a un CMS desactualizado y que ademas cuenta con una aplicación de configuración del sistema operativo que también es vulnerable.

Los atacantes lograron acceder al sistema y realizar una serie de acciones que usted deberá identificar y responder en un Cuestionario, para determinar las causas del incidente.

DESARROLLO

Análisis de *Logs*		
Debian 11	**Descripción**	**Herramientas**
	Para ingresar al servidor debe hacerse a través del puerto SSH, para ello se le dará las credenciales que se encuentra dentro del servidor web donde se respondieron las preguntas. Dentro del servidor se encontrará un archivo llamado **captura.pcap** el cual contendrá todo el trafico de los ataques que se realizaron. De la misma forma se puede acceder a la ruta de **/var/log/apache2** donde se encontraran todos los *logs*	**Wireshark**

	(**nota**: se puede utilizar el archivo captura.pcap o pueden usar los *log* del servidor).	

CUESTIONARIO #2

1.- Según el análisis del tráfico de red del archivo captura.pcap ¿ cuál es la IP del atacante ?
R.- 172.31.40.93
2.- ¿ Que protocolo de la capa de transporte es la vía usada para ejecutar los ataques ?
> **TCP**
> UDP
3.- Escriba correctamente el nombre del "user-agent" de la herramienta que usa el atacante para realizar el mapeo de los puertos
R.- "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
4.- Según el analisis de logs de apache ¿ Qué palabra correcta evidencia la ejecución de fuerza bruta sobre los usuarios del CMS ?
R.- author
5.- En relación a la pregunta anterior ¿ Qué número o nÚmeros asignados a esta "palabra" que arrojan como respuesta del servidor "200", indican que son usuarios validos del CMS.
R.- 1,2
6.- Escriba el nombre correcto del "user-agent" junto a la versión de la herramienta usada para realizar reconocimiento activo y poder obtener el "banner grabbing" del CMS.
R.- WhatWeb/0.5.5
7.- En relación a la pregunta anterior, escriba la fecha y hora exacta que fué registrada en el archivo de logs, la ejecución de esta herramienta de recolección del "banner grabbing".
R.- 25/Oct/2023:10:45:41
8.- Indique el nombre correcto de la herramienta utilizada para realizar fuerza bruta sobre los subdirectorios URL y que el atacante utilizó para descubrir la ruta del login
R.- dirbuster

9.- Según el análisis de logs ¿Cuál es el nombre y versión de la herramienta especializada que se usa para escanear vulnerabilidades en el CMS?

R.- WPScan v3.8.25

10.- En relación con la pregunta anterior ¿Cuál es la hora y fecha exacta en el cual se "inicio" el escaneo con esta herramienta especializada?

R.- 25/Oct/2023:11:19:56

11.- Según el análisis de logs ¿cuáles son los temas y plugins, que arrojan como respuesta del servidor "200" detectados por la herramienta especializada que se usa para escanear el CMS?

R.- social-warfare, twentythirteen

12.- Según el análisis de logs, escriba la fecha y hora exacta que evidencia el inicio de acceso no autorizado en el panel del login del CMS

R.- 25/Oct/2023:11:49:41

13.- Según el análisis de logs ¿Cuál es el nombre del archivo utilizado para realizar la ejecución de código remota en el CMS?

R.- 1.txt

14.- Según el análisis del tráfico del archivo "captura.pcap" ¿Cuál es el "comando exacto" que se ejecuta en el payload para iniciar una shell al explotar el CMS?

R.- <pre>system('perl shell.pl')</pre>

DETALLES DEL SEGUNDO ESCENARIO

- El tiempo límite es de 2 Horas.
- El límite de intentos para cada respuesta es de 3.
- El puntaje de cada respuesta varia según los intentos que se utilicen de la siguiente manera:
  - 1er Intento = 20 Puntos.
  - 2do Intento = 15 Puntos.
  - 3er Intento = 10 Puntos.
- El puntaje de la última respuesta es de **25 Puntos.**
- El puntaje máximo de la segunda fase es de **285 Puntos.**

EL PUNTAJE FINAL DE LOS 2 ESCENARIOS ES DE 1.000 PUNTOS