**Informe de la Máquina CTF - Pentesting Básico TryHackme**

**Resumen**

La presente es un informe detallado de las actividades realizadas durante la prueba de penetración en la máquina CTF Pentesting Básico. Se siguieron los procedimientos estándar de pruebas de penetración y se utilizaron herramientas como Nmap, Gobuster, smbclient, Hydra y John the Ripper para obtener acceso no autorizado a la máquina y recopilar información sensible. Cabe destacar que estas actividades fueron realizadas únicamente con fines educativos y no se infringió ninguna ley o política de seguridad.

1. **Escaneo de puertos:** Se realizó un escaneo de puertos utilizando la herramienta Nmap. Se identificaron los siguientes puertos abiertos:

* Puerto 22 (SSH): Se encontró acceso SSH en este puerto.
* Puerto 80 (HTTP): Se encontró una pagina web
* Puerto 139 y 445 (SMB)

***Comandos:***

* ***nmap -A <ip>***
* ***nmap -sS -sV <ip>***

1. **Enumeración de servicios y descubrimiento de directorios ocultos**: Se utilizó Gobuster para enumerar directorios y se descubrió un directorio oculto "/development". Dentro de este directorio se encontraron dos archivos: "dev.txt" y "j.txt".

***Comandos:***

***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/rockyou.txt***

1. **Contenido de archivos:** Se navego en el directorio oculto en la pagina web y se encontró:

* Archivo "dev.txt": Contenía las siguientes líneas:

2018-04-23: He estado experimentando con el framework Struts y es bastante interesante. Creo que sería genial alojarlo en este servidor también. Aún no he creado aplicaciones web reales, pero he probado el ejemplo que demuestra cómo funciona (¡y es la versión REST del ejemplo!). Actualmente estoy usando la versión 2.5.12, ya que las otras versiones me causaron problemas. -K

2018-04-22: Se ha configurado SMB. -K

2018-04-21: He configurado Apache. Agregaremos nuestro contenido más tarde. -J

* Archivo "j.txt": Contenía el siguiente mensaje: "Para J: He estado auditando los contenidos de /etc/shadow para asegurarnos de que no tengamos credenciales débiles y pude descifrar fácilmente tu hash. Conoces nuestra política de contraseñas, así que por favor, síguela. Cambia esa contraseña lo antes posible. -K"

1. **Acceso a recursos compartidos SMB:** Se utilizó smbclient para conectarse al recurso compartido "//10.10.136.162/anonymous". Se encontró el archivo "staff.txt", que contenía el siguiente mensaje: "Anuncio para el personal: POR FAVOR, no carguen elementos no relacionados con el trabajo en este recurso compartido. Sé que es divertido, pero así es como ocurren los errores. (¡Esto también va por ti, Jan!) -Kay"

***Comandos:***

***smbclient -L //10.10.5.162***

***smbclient //10.10.5.162/anonymous***

1. **Descifrado de credenciales y acceso SSH:** Se utilizó Hydra con la lista de contraseñas "rockyou.txt" para intentar descifrar las credenciales de inicio de sesión SSH del usuario "jan". Se obtuvieron las siguientes credenciales: Usuario: jan, Contraseña: armando. Con estas credenciales, se accedió con éxito al servidor SSH.

***Comandos:***

***hydra -l jan -P dicc.txt ssh://10.10.5.162***

***ssh jan@10.10.5.162***

1. **Descubrimiento de usuario adicional:** Se examinó el archivo /etc/passwd y se encontró un usuario adicional llamado "kay" con la siguiente información: kay:x:1000:1000:Kay,,,:/home

***Comandos:***

***cat /etc/passwd***

1. **Descifrado de la clave privada y acceso SSH adicional para escalamiento de privilegios:** Se utilizó la herramienta "ssh2john" para convertir el archivo "id\_rsa" en un formato compatible con John the Ripper, y se guardó el hash resultante en el archivo "hash.txt". Luego, se ejecutó John the Ripper con el archivo "hash.txt" y la lista de contraseñas "rockyou.txt" para descifrar la contraseña de la clave privada. La contraseña descifrada fue "beeswax". Con esta información, se accedió nuevamente al servidor SSH utilizando el comando "ssh -i id\_rsa ray@10.10.136.162". Es importante mencionar que el usuario "ray" tenía privilegios de sudo.

***Comandos:***

***ssh2john id\_rsa > hash.txt***

***john hash.txt --wordlist=dicc.txt***

***ssh -i id\_rsa ray@10.10.136.162***

Recuerda que estas actividades se realizaron únicamente con fines educativos y no se infringió ninguna ley o política de seguridad.